L’Internet de les Coses: arquitectures, protocols i aplicacions

Estudiant: Mario Pareja Nieto

MUET UOC-URL

Setembre 2014 – Gener 2015

Consultor: Pere Tuset Peiró

11 de Gener de 2015

Resum

Les demandes d'informació de la societat actual són cada cop més elevades, creixen inexorablement dia a dia. La principal premisa que ens trobem és que, a través del tractament i anàlisi d'aquesta informació es podrà obtenir un major coneixement del medi que ens envolta. Al seu torn, la intenció final és que aquest major grau coneixement repercutirà, d'una manera o altra, en majors beneficis per als individus i per la societat en general; en definitiva, una major qualitat de vida.

Més informació comporta més comunicació mitjançant mitjans telemàtics, per tal de que els usuaris puguin comunicar-se entre ells o bé amb les màquines, segons l'esquema tradicional de comunicació home-home o home-màquina. Per la seva banda i, sense cap mena de dubte, avui dia la principal xarxa global de comunicacions és Internet, tant en l'àmbit personal com a professional. Per tant, tenim que la majòria de les comunicacions usuari-usuari o usuari-màquina que es realitzen avui dia ho fan a través d'aquesta xarxa global.

L'Internet de les Coses (IoT o *Internet of Things*, en anglès) és un concepte encara prou recent, que representa un pas més enllà en les comunicacions a la Xarxa, segons el qual aquestes darreres passen a ser directament màquina a màquina (M2M o *Machine-To-Machine*, en anglès) i sense cap tipus d'interacció per part de cap usuari. En la pràctica, això significa, en realitat, millions de dispositius de tota mena –equipats amb tot tipus de sensors, moltes vegades minúsculs de baix consum, de la mida d'una "mota" de pols- i que formen xarxes de sensors sense fils (WSN o *Wireless Sensor Networks*, en anglès) que es connecten a Internet, fent servir tecnologies com Bluetooth LE, ZigBee, Wi-Fi, etc.i posteriorment amb altres dispositius (per exemple, actuadors, servidors web o de bases de dades) per tal d'intercanviar informació. Això ha estat possible gràcies a la progressiva disminució dels costos de les comunicacions, així com dels costos de fabricació de l'electrònica necessària per "sensoritzar" (els nodes normalment s'implementen fent servir circuits integrats del tipus 'Sistema en un Xip' (SoC o *System on a Chip*, en anglès) i, en paral·lel, gràcies al progressiu augment de potència d'aquests darrers.

Alguns dels reptes més importants amb els qualss'enfronta aquesta nova forma de comunicació són:

- Estandardització de les comunicacions a les xarxes sense fils personals (WPAN o *Wireless Area Personal Networks*, en anglès). Per tal d'evitar la confusió originada per l'aparació de diverses tecnologies similars, molts cops propietàries, es va crear 802.15.4, que és un estàndarde l'IEEE (*Institute of Electrical and Electronics Engineers*) que defineix el nivell físic (PHY) i el control d'accés al medi (MAC) a WPANs amb baixes taxes de transmissió (fins 250 Kbps) i baix consum. Altres alternatives possibles passen, per exemple, per l'ús de l'estàndard Bluetooth Low Energy (BLE).

- Manca d'adreces IPv4 per als milers de millions de dispositius que es poden arribar a connectar a la Xarxa, fet que fa imprescindible que l'Internet de les Coses estigui basada en IPv6, ja que d'aquesta manera es pot suportar un total de 2^{128} adreces públiques. D'aquesta manera, s'ha de parlar de protocols com ara 6LowPAN (*IPv6 over Low power Wireless Personal Area Networks*), una implementació de IPv6 –capa d'adaptació- específica per a xarxes de sensors sense fils de baix consum i amb pèrdues.

- Assegurar un grau de seguretat el suficientment alt a l'hora de connectar els dispositius a Internet, donat que moltes vegades les dades que viatjaran seran sensibles (per exemple paràmetres de salut d'un pacient, si una casa es troba buida o no, etc). Per a aquest fi, seran necessaris protocols de securetat i de control d'accés al medi com ara 802.11i (WPA2) i 802.1AE (MACsec), així com mètodes d'encriptació (AES) que han sigut desenvolupat per tal d'assegurar dades en entorns sense fils i en moviment.

- Assegurar fiabilitat en les comunicacions. Donat que el medi que es fa servir és l'aire i, per tant, estem parlant de xarxes amb pèrdules (*lossy networks*, en anglès) s'ha de trobar nous mecanismes que permetin disminuir la probabilitat d'error en l'enviament de paquets el màxim possible o, dit d'una altra manera, que permetin augmentar l'eficiència de dades enviades en entorns "hostils" on pot haver-hi interferències (*jamming*, en anglès) ocasionades per obstacles, vehicles, maquinària industrial, etc. Alguns clars exemplesde protocols orientats a aquest fi són CoAP (*Constrained Application Protocol*) i MQTT (*Message Queuing Telemetry Transport*).

- Assegurar el correct encaminament dels paquets en entorns com el descrit anteriorment. En aquest tipus de xarxes de tant curt abast, entre d'altres, l'encaminament (*routing*, en anglès) ha de ser dinàmic i proactiu i ha de permetremúltiples salts entre diferents nodes *(multi-hop*, en anglès) per tal de salvar majors distàncies i així poder arribar a la destinació – normalment una pasarel·la cap a Internet. Un clar exemple el tenim amb RPL (*Routing Protocol for Low-Power and Lossy Networks*), que és el protocol estàndard d'IPv6 per a aquest fi.

El ventall d'aplicacions que podem trober en una Internet de les Coses és pràcticament il·limitat: des de els *wearables* (peces de robes amb de sensors que poden mesurar la temperatura corporal, humitat, calòries consumides, sensació de fred, etc.) fins al monitoratge de la salut de persones depenents, passant per la domòtica (o el que és el mateix, automatització de la casa, amb rentadores, frigorífics o sistemes de calefacció amb sensors que controlen la bugada, la quantitat de menjar que tenim o la temperatura de la casa), aplicacions vehiculars (sensors als cotxes que mesuren el tipus de conducció de l'usuari i que poden fer-se servir per dissenyar nous plans de pagament per part de les companyies d'assegurances), monitoratge i control del trànsit a la ciutat (una dels típics exemples per definir el concepte de Ciutat Intel·ligents o *Smart Cities*, en anglès), monitoratge de conreus i granjes, etc.

Paraules clau: IEEE 802.15.4e, TSCH, 6LoWPAN, RPL, CoAP, CC2538, OpenMote, OpenWSN.

Abstract

Information needs in today's society are increasing from day to day, relentlessly. The main premise here is that, through dataprocessing and analysis, knowledge is extracted. In turn, the final aim of extracting knowledge from our environment is to rebound, some way or another, in benefits for both individuals in particular and society in general. In other words: more info means more knowledge and more knowledge can lead, eventually, to a higher quality of life.

More info implies more telematics, so that the end users can communicate remotely to each other (user-to-user schema) or to a machine (user-to-machine schema). These are the traditional ways individuals can communicate at present. On the other hand and, with no doubt, Internet is, on these days, the main global network everyone -both for personal and professional reasons- uses on a daily basis. Then, we have that almost all of the user-to-user or user-to-machine communications are already being carried out through the Internet.

The Internet of Things (hereinafter IoT) is a new concept perhaps a little ambiguous or "ethereal" yet, which represents one step further to traditional Internet communications. On the IoT, communications are carried out directly between machines (M2M or Machine-to-Machine) with no interaction or control at all by any user. In practice, this means, in the real world, billions of devices of any kind -equipped with several types of sensors, most of the times tiny and low-powered ones, called "motes"- meshed together in what is generically called a Wireless Sensor Network (WSN), by means of wireless technologies (Bluetooth LE, ZigBee, Wi-Fi, ...) and connected to the Internet and then, on the other end, to other devices (for example actuators, web servers or database servers) in order to store or exchange information. This has been possible thanks to the progressive reduction on communications' costs, as well as progressively decreasing costs on electronics' manufacturing (wireless nodes are normally deployed by using 'Systems on a Chip' –SoC- based ICs).

Some of the most important challenges this new paradigm of communication must face are the following:

- Wireless personal area networks' (WPAN) standardization. In order to prevent the confusion originated by multiple emerging and similar technologies, most of the times propietary ones, the standard 802.15.4 was created by the IEEE (Institute of Electrical and Electronics Engineering), which defines physical and access media layers for WPANs with low data rates (up to 250 Kbps) and low power consumption. Possible alternatives to this standard are, for example, the new Bluetooth Low Energy (BLE) standard.

- IPv4 address exhaustion or, in other words, not enough addresses to handle billions of devices that could be connected to the Network in the next years. This big issue makes imperative the use of IPv6 for this new IoT paradigm, which can support up to 2^{128} public addresses. Additionally, it is necessary to introduce 6LoWPAN protocol, which is nothing but an IPv6 implementation specifically created for low-powered wireless sensor networks (WSN).

- To be able to fulfill a high security level when connecting devices to the Internet, enough to ensure confidentiality of sensible data (pacients' health information, whether somebody's at home or not, etc.). To this extent, security and media access control protocols will be needed like 802.11i (WPA2) and 802.1AE (MACsec) will be needed, as well as encryption methods (AES) which have been developed to protect data on wireless and "in motion" environments.

- To ensure communications' reliability. Since the medium is the air and, therefore, we are talking about lossy networks, new mechanisms permitting to minimize the error probability during packet transmission must be found or, in other works, which permit to increase data transmission efficiency on "hostile" environments, where interferences (jamming) can be present due to obstacles, vehicles, industrial machinery, ... The clearest examples of these kind of protocols are CoAP (Constrained Application Protocol) and MQTT (Message Queuing Telemetry Transport).

- To ensure correct packet routing on environments like the ones described before. On networks like those which such a short range and, among others characteristics, routing should be dynamic and should allow traversing different nodes (multi-hop) before getting to the destination -typically a gateway to the Internet, this is, in order to achieve higher distances. An example of hit is RPL (Routing Protocol for Low-Power and Lossy Networks), pronounced "ripple", which is the standard IPv6 protocol to achieve this.

The scope of application of the IoT in today's world is almost unlimited: from *wearables* (tiny electronic sensors incorporated on clothing and which can measure body temperature, humidity, calories' consumption, ...) to health monitoring for elder or disabled people, domotics (home automation, with washers, fridges or heating systems having sensors that can control the laundry, food level/quantity or room's temperature), vehicular applications (cars equipped with sensors measuring user's driving style or number of kilometres driven and that can be used by insurance companies to design more personalized new insurance plans), traffic monitoring and control on cities (one of the typical examples on which the Smart Cities concept is based), crop and farm monitoring, ...

Keywords: IEEE 802.15.4e, TSCH, 6LoWPAN, RPL, CoAP, CC2538, OpenMote, OpenWSN.

Taula de continguts

Índex d'il·lustracions

Índex de taules

1. Introducció

1.1. Definició

L'anomenada "Internet de les Coses" (*Internet of Things* o simplement IoT, en anglès) és un concepte relativament nou que, en la seva definició més bàsica, representa un nou paradigma de comunicació, pel qual, qualsevol "cosa" (dispositiu, servidor, ordinador, electrodomèstic, persona, etc.) es pot connectar amb qualsevol altra "cosa", fent servir xarxes sense fils i Internet, per tal d'intercanviar informació.

En la seva accepció més clàssica, l'IoT es "modela"mitjançant dispositius electrònics que es comuniquen directament entre ells (comunicació "màquina a màquina") via sense fils i sense cap interacció per part dels usuaris. Aquest concepte representa un gir de 180 graus respecte al paradigma tradicional de comunicació "usuari a usuari" (per exemple, dues persones que parlen entre elles a un xat o a les xarxes socials) o bé "usuari a màquina" (per exemple, una persona que es connecta a un servidor web).

Entrant una mica més en detall, veiem que l'IoT és una nova forma de comunicació, formada per una xarxa de nodes minúsculs sense fils, nodes que contenen sensors (W*ireless Sensor Network* o simplement WSN, en anglès) que es comuniquen, bé entre ells mateixos i/o bé amb altres dispositius remots (per exemple, servidors) o, en general, amb qualsevol "cosa", que es troba allunyada físicament i a la qual s'hi arriba a través de la xarxa "pública" Internet. Aquests servidors remots als quals els nodes es connecten –normalment per enviar les dades mesurades pels sensors- podrien estar allotjats, per exemple, al núvol (*Cloud*, en anglès), és a dir, fent servir un proveïdor de serveis de núvol públic, a una ubicació física indeterminada però que proporciona redundància i alta disponibilitat al servei [37].

En aquest tipus de xarxes, com ja s'ha dit, els nodes solen incorporar un o diversos sensors (temperatura, pressió, humitat, llum, proximitat, etc.) i s'intenta que siguin el més petits possibles, tant per raons de transport –logística- com sobretot de consum de bateries. És per aquesta raó que a cada node d'una WSN normalment se li anomena informalment "mota" (*mote*, en anglès).

Podem trobar escenaris on les motes es connecten directament a Internet, a través de una pasarel·la (*gateway*, en anglès), formant el que s'anomena una topologia de xarxa en estrella (*star*), o bé les motes poden reenviar-se els paquets de dades entre elles, amb la finalitat de poder salvar majors distàncies (en altres paraules, les motes intermèdies actuarien d'encaminadors –*routers* o *forwarders*, en anglès) per a, finalment, arribar al *gateway* que enviarà els paquets cap a Internet, formant el que s'anomena una topologia de xarxa en malla (*mesh*, en anglès). Altres topologies possibles podrien ser punt a punt (*Peer to Peer* o P2P, en anglès) on únicament es tenen parells de nodes que es comuniquen directament entre ells o bé arbre (*tree*) que segueix una estructura jeràrquica on uns nodes són els "pares" i sota el mateixos neixen nodes fills, fent que la comunicació pugui ser "cap amunt" o "cap avall" en funció de si es vol comunicar un pare amb un fill o a la inversa.

A la següent figura [74] es pot veure un diagrama amb les quatre tipologies de xarxa comentades anteriorment (punt a punt, arbre, estrella i xarxa) on els punts representarien, en el nostre cas, cadascuna de les motes que formen una xarxa sense fils. Normalment, els nodes "mestres" serien els que es connecten a la xarxa remota (amb una pasarel·la a Internet, tal i com es comentava abans):

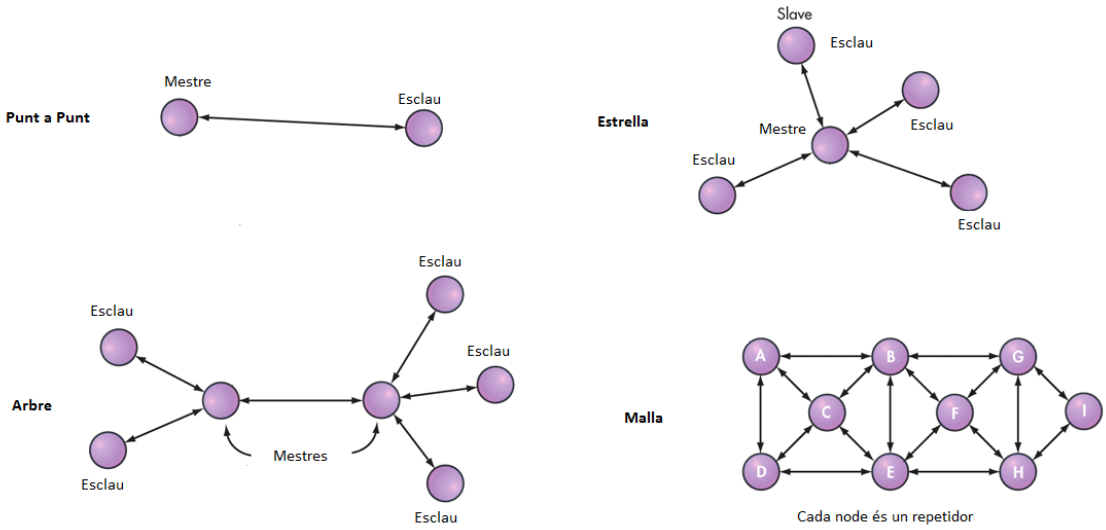


Figura 1. Topologies de xarxa més comuns.

De manera paral·lela al concepte d'IoT, també existeix el de M2M o *Machine to Machine*. A la práctica i informalment, ambdós conceptes es confonen i es barrejen encara que, a nivell formal/teòric, no signifiquen ben bé el mateix:

Per un cantó, M2M significa simplement una comunicació màquina a màquina i més, concretament, a les tecnologies de comunicacions que fan possible aquest tipus d'enllaç (típicament punt a punt). No obstant però, no especifica si la comunicació ha de ser mitjançant cables o sense fils, ni quins protocols s'han de fer servir, ni quina xarxa s'utilitzarà com a transport (una xarxa privada, Internet, etc). Podem afirmar, llavors, que M2M és un concepte genèric pero alhora limitat, que únicament defineix una comunicació directa entre dispositius. Un exemple d'M2M podria ser la comunicació entre dos vehicles que circulen per la carretera i que s'intercanvien informació sobre la velocitat de cadascun d'ells, si cap d'ells ha trepitat el fre, etc. (d'aquesta manera, un dels dos vehicles podria canviar automàticament de carril en cas de frenada brusca del vehicle del davant o bé podria també frenar o disminuir la seva velocitat, etc). Un altre exemple pot ser el d'un sensor de temperatura a una habitació de casa, que es comunica amb un termostat i aquest darrer, al seu torn, encen o apaga la caldera en funció de la temperatura.

En canvi, IoT va més enllà de M2M, ja que per a poder parlar de l'Internet de les Coses, es presupossa que s'acompleixen una sèrie de requisits, al menys a nivell formal:

- Quan es parla d'IoT, parlem de xarxes sense fils de nodes –motes- amb sensors, de baix consum (típicament inferior a 1 mW), amb amplada de banda limitat (màxim 250 Kbps) i en entorns amb pèrdues (l'aire). A aquest tipus de xarxes se'ls hi anomena *Low Power and Lossy Networks* o simplement LLNs, en anglès [14]. Les xarxes han de ser obligatòriament de baix consum perquè s'ha d'intentar que les motes estiguin funcionant el màxim de temps possible –la vida útil de la bateria ha de ser el més gran possible, ja que normalment les motes estaran desateses. Per altre cantó, quan es parla de xarxes sense fils, estem parlant sempre d'un medi amb perduès-, ja que la potència rebuda pel receptor disminueix amb la distància, segons les equacions de Friis (veure Annex I per a més informació).

- Com que poden haver desplegades fins i tot milions de motes dins d'una misma xarxa de sensorització, amb IoT es fa obligatòria la utilització d'IPv6 (*Internet Protocol*, versió 6), que permet un total de 2^{128} adreces –a la pràctica, gairebé infinites/il·limitades-, podent d'aquesta manera assignar a cada mota una adreça IP pública diferent i sense haver de recórrer a mecanismes tradicionals com ara NAT (traducció d'adreces de xarxa o *Network Address Translation*, en anglès) que són necessaris a IPv4 per tal de poder assignar una mateixa IP pública a un conjunt de nodes d'una xarxa privada. A la pràctica, qualsevol mota del món es podria comunicar amb qualsevol altra, fent servir la seva adreça IPv6 unequívoca.

- De la mateixa manera, es presuposa la utilització d'estàndards oberts i oficials, com ara l'IEEE 802.15.4, estàndard de l'Institut d'Enginyers Elèctrics i Electrònics (*Institute of Electrical and Electronics Engineers* o simplemente IEEE, en anglès) en el qual es basen tecnologies/especificacions com ara ZigBee, WirelessHart o ISA SP-100. Tanmateix, també s'assumeix l'ús d'altres protocols de capa superior, com ara 6LoWPAN (*IPv6 over Low power Wireless Personal Area Networks*), RPL (*Routing Protocol for Low-Power and Lossy Networks*) i CoAP (*Constrained Application Protocol*).

- Com s'ha dit al començament del capítol, l'IoT no tracta de connectar únicament una màquina amb una altra (com passa amb M2M) sinó que pot connectar "coses" en general, com ara màquines, sensors, dispositius, productes de consum (rellotjes, llaunes de conserva, etc.) amb altres "coses" o bé amb sistemes (aplicacions de negoci empresarials, sistemes d'anàlisi, sistemes de control, magatzems d'informació - *datawarehouses*) o fins i tot amb persones (treballadors, consumidors, pacients, col·laboradors, etc.). Un exemple d'ioT seria un rellotge inteligent (*smartwatch*, en anglès) que avisa a una persona, a través del telèfon mòbil, si les sees pulsacions són molt elevades o si no s'ha arribat a un mínim establert de crema de calories diàries, etc. En aquest cas, estaríem parlant d'una aplicació M2P (*Machine to People*) [80].

Per tant, podem concloure que:

- IoT "inclou" M2M –o dit, d'una altra manera, M2M és un subconjunt d'IoT- en el sentit de que M2M es refereix a la comunicació remota entre dos dispositius, mentre que IoT engloba un significat més ampli, en el que dispositius es poden connectar també a persones i amb "coses"; en altres paraules, de la interconnexió de remota d'objectes quotidians, fent servir Internet.

- Per altra banda, M2M fa referència, a la pràctica, a una comunicació que fa servir protocols propietaris i tancats, així com a connexions, cablejades o sense fils, típicamentde tipus cel·lular en el darrer cas, fent servir xarxes GSM (*Global System for Mobile Communications*), GPRS (*General Packet Radio Service*) o LTE (*Long Term Evolution*), mentre que IoT fa referència aestàndards oberts, és a dir, a l'ús d'IPv6, IEEE 802.15.4 i a Internet i el *Cloud Computing* com a base del seu funcionament.

- Amb M2M es posa èmfasi en el maquinari (*hardware* o HW, en anglès), normalment propietari (específic de cada fabricant, personalitzat), mentre que IoT posa l'èmfasi en el programari (*software* o SW, en anglès), fent servir estàndards, protocols, aplicacionsi plataformes de desenvolupament obertes, com podrem veure més endavant en els següents capítols.

- Per últim, amb M2M, es fa difícil la interoperativitat i integració entre diferents xarxes i sistemes, precisament pels factors que hem comentat abans (HW i SW tancats, protocols propietaris, xarxes heterogènies, etc.) mentre que amb IoT la integració és molt més fàcil, degut a la utilització d'estàndards i plataformes obertes i comunes, facilitant l'escalabilitat del sistema resultant.

Per a més informació sobre les diferències entre IoT i M2M, veure l'Annex II.

1.2. Antecedents i orígens

En primer lloc, és indubtable que l'IoT prové –"hereta" les seves característiques- de les tradicionals xarxes sense fils i, concretament, de les WSN o xarxes de sensors sense fils. Els origen d'aquestes xarxes s'ha de buscar en el programa DSN (*Distributed Sensor Networks*) de la DARPA (*Defense Advanced Research Projects Agency*), allà al 1980. Per aquella data, ARPANET (*Advanced Reseach Projects Agency Network*) ja estava operativa des de feia uns anys, amb un total d'aproximadament 200 nodes (*hosts*) repartits en universitats i instituts d'investigació. La finalitat del programa DSN era la de tenir molts nodes sensors de baix cost separats espacialment –geogràficament- que col·laboressin amb els altres nodes però que poguessin operar de manera autònoma, amb la informació essent encaminada a aquell node que fos el millor en cada moment.En aquell moment, la xarxa estava formada per microordinadors, que incloien sensors acústics, mòduls de comunicació i processament, així com programari distribuït.

Amb el temps, els nodes sensors han anat disminuint de mida progressivament, des de un mida similar al d'una capsa de cigarrets a, fins i tot, una partícula de pols (també anomenada "mota"). De la mateixa manera, el preu dels mateixos també ha anat decreixent, situació que va propiciar l'aparició de moltes aplicacions en l'àmbit civil, com para monitoratge de l'entorn, xarxes de sensors vehiculars (V2V o *Vehicle to Vehicle*), xarxes de sensors per a monitoratge del cos, etc. En aquest sentit, DARPA va actuar de nou com a pionera, llençant una iniciativa/programa d'investigació anomenat SensIT, que proporcionava a les xarxes de sensors de l'època amb noves capacitats com ara la creació de xarxes personalitzada (*ad hoc networking*), consultes i execució de tasques dinàmicament, reprogramació, multitasca, etc. Al mateix temps, l'IEEE va adonar-se del baix cost i altes capacitats que les xarxes de sensors podien oferir. Per aquesta raó, aquesta organització va definir l'estàndard IEEE 802.15.4, a través del seu grup de treball "IEEE 802.15 WPAN Task Group", dirigit a les xarxes sense fils d'àrea personal (abast de pocs metres) i baixa taxa de transferència. Un exemple d'estàndard –especificació de conjunt de protocols d'alt nivell- IEEE 802.15.4 és ZigBee, creat per la ZigBee Alliance, que aconsegueix una taxa de transferència màxima de 250 Kbps (en funció de la banda freqüencial que es faci servir) i que és la base de nombroses WSN actuals.

A la següent figura podem veure l'esquema bàsic –topologia- d'una xarxa de nodes sensors sense fils [69]:

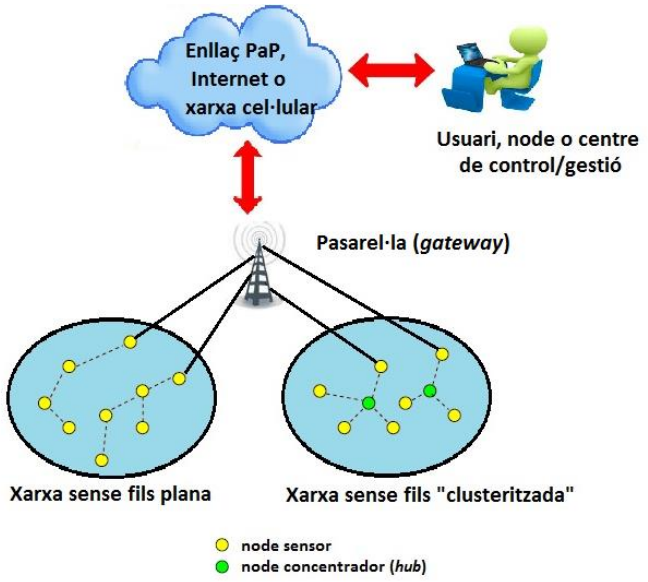


Figura 2. Esquema bàsic d'una WSN amb connexió a una xarxa remota

Per altra banda, el concepte general d'una xarxa de dispositius intel·ligents (*smart devices*, en anglès) ha estat discutit al menys des de 1991. El 1994, en la publicació IEEE Spectrum, Reza Raji va descriure aquest concepte com a "el moviment de petits paquets de dades a través d'un gran conjunt de nodes, amb la finalitat d'automatitzar-ho tot, des d'electrodomèstics fins a factories senceres". Tot i així, no va ser fins el 1999 que aquest concepte va guanyar *momentum* (importància). Aquell any, Bill Joy, el cofundador de SUN Microsystems, va visionar la comunicació D2D (*Device to Device*) com a part del seu marc de treball de "Les Sis Webs", presentat al Fòrum Econòmic de Davos del mateix any.

Per últim tenim que, també el 1999, el britànic Kevin Ashton, cofundador i Director Executiu de l'Auto-ID Center al MIT (Institut Tecnològic de Massachusetts)i creador d'un sistema estàndard per a RFID (*Radio Frequency Identification*) va fer la següent dissertació a l'edició de juliol de la publicació RFID Journal, en l'article "*That 'Internet of Things' Thing*" [68]:

"*...Els ordinadors actuals –i, per tant, Internet- són pràcticament dependents dels éssers humans per a demanar informació. Una majoria dels gairebé 50 Petabyte (1 Petabyte són 1,024 Terabyte) de dades disponibles a Internet van ser inicialment creats per humans -a força de teclejar, pressionar un botó, prendre una imatge digital o escanejar un codi de barres. Els diagrames convencionals d' Internet (...) deixen fora els encaminadors més importants de tots, les persones. El problema és que les persones tenen temps, atenció i precisió limitades -el que vol dir que no són molt bons a l'hora d'aconseguir informació sobre coses al món real. I això és un gran obstacle. Som cossos físics, de la mateixa manera que el medi que ens envolta... No podem menjar bits, ni cremar-los per resguardar-nos del fred, ni ficar-los en tancs de gas. Les idees i la informació són importants, però les coses quotidianes tenen molt més valor. Encara que, la tecnologia de la informació actual és tan dependent de les dades escrits per persones, que els nostres ordinadors saben més sobre idees que sobre coses. Si haguéssin ordinadors que sabessin tot el que haguessin de saber sobre les "coses", mitjançant l'ús de dades que ells mateixos poguessin recollir sense la nostra ajuda, nosaltres podríem monitoritzar, comptar i localitzar tot al nostre voltant, d'aquesta manera es reduirien increïblement despeses, pèrdues i costos. Sabríem quan reemplaçar, reparar o recuperar el que fos, així com conèixer si el seu funcionament estigués sent correcte. L'Internet de les Coses té el potencial per canviar el món tal i com va fer la revolució digital fa unes dècades. Potser fins i tot més..."*

De fet, en aquell moment, l'identificació per radiofreqüència es va considerar com un "prerrequisit" per a l'Internet de les Coses: si tots els objectes i gent, en la seva vida diària, estiguessin equipats amb identificadors, llavors els ordinadors podrien gestionar-los i inventariar-los. Per altra banda, a més a més de l'RFID, també es poden utilitzar altres tècniques/tecnologies per etiquetar les coses, com ara NFC, codis de barres, codis QR (*Quick Response*) i marques d'aigua digitals.

Per tant, podem concloure que, mentre que IoT es basa, a nivell de xarxa, en les xarxes de sensors sense fils o WSN (concretament aquelles de baix cost, baix consum i en entorns amb pèrdues), el paradigma de comunicació s'originà fa 15 anys i es basà, inicialment, el l'ús de l'identificació per radiofreqüència.

1.3. Principals estàndards i protocols

Tal i com ja s'ha comentat en apartats anteriors, per un cantó tenim que l'IoT es basa en les WSN i, per altres, en l'ús de tecnologies com ara RFID o NFC. En concret, aquesta darrera es pot entendre com una evolució de la primera, ambdues basades en l'estàndard ISO 14443 [120] però traballant la darrera amb un abast espacial inferior –per temes de seguretat- i poguent treballar en dos modes de funcionament: actiu (els dos dispositius presents en la comunicació –emissor i receptor- generen el seu propi cam electromagnètic) i passiu

(únicament un dispositiu genera camp electromagnètic i l'altre se n'aprofita de la modulació de càrrega per a la transferència de dades).

Per altre cantó, també s'ha parlat que IoT inclou/es basa en el paradigma M2M (comunicació "màquina a màquina"), amb la diferència de que, a la pràtica, M2M és un concepte més limitat, que acostuma a fer servir protocols, maquinari i programari –i, en definitiva, arquitectures- propietàries- mentre que IoT no es pot entendre sinó és amb l'ús de plataformes i protocols oberts com ara IPv6 o 6LoWPAN. Tot i així, degut al continu desenvolupament i implantació de solucions M2M, s'han creat diversos cossos (*bodies*) tècnics d'estandardització, l'objectiu dels quals és proporcionar una arquitectura de sistema unificada, d'extrem a extrem (*end-to-end*) que sigui la clau habilitadora que substituirà les aplicacions verticals propietàries existents [64]. Alguns d'aquests cossos són:

- *ETSI (European Telecommunications Standards Institute) M2M Technical Comitte*
- *3GPP (3rd Generation Partnership Project) TSG Service and Systems Aspects*
- *TIA (Telecommunications Industry Association) TR-50 Engineering Committee*
- *CCSA (China Communciations Standard Association) TC10*
- *GIFSI (Global ICT Standardization Forum for India)*
- *ITU (International Telecommunication Union)*
- *OMA (Open Mobile Alliance)*
- *M2M Standardization Task Force*
- *GSC (Global Standards Collaboration) M2M Standardization Task Force*

En el següent diagrama, podem veure que el GSC actua com a coordinador de les diferents organizacions anteriors, involucrades totes elles en l'estandardització de les comunicacions M2M. El GSC assegura a més la col·laboració entre els cossos, reunint els principals estàndards oficials d'USA, Canada, l'UE, China, Japó, Coreo, Australia i la ITU, de manera que es pugui accelerar la creació d'estàndards globals.

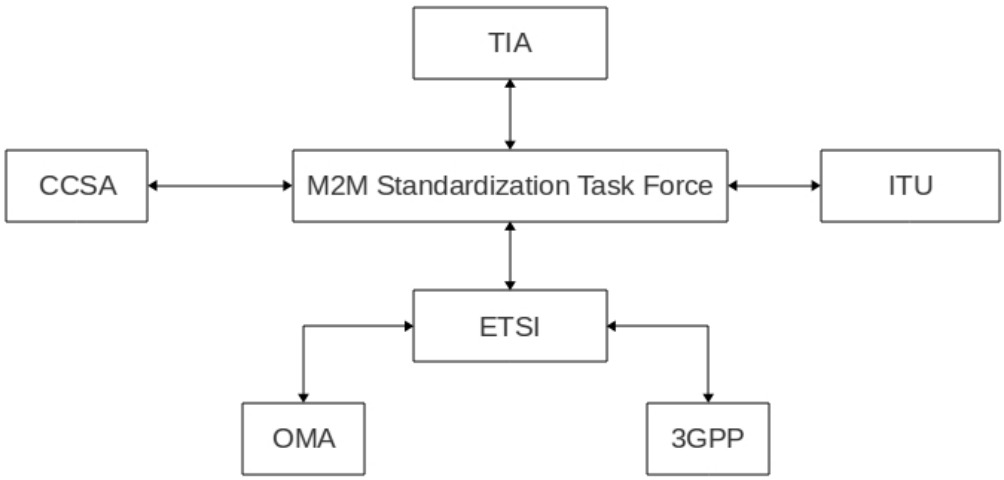


Figura 3. Enllaços de col·laboració entre els diferents cossos d'estandardització M2M [64].

Per a més informació sobre els principals estàndars i protocols IoT/M2M, veure l'Annex III.

1.4. Àmbits d'aplicació

En general, totes les grans empreses d'IT i consultoria especialitzada coincideixen en pronosticar un augment imparable de l'IoT, traduït en nombre de dispositius intel·ligent connectats a la Xarxa (Intenet). Aquest dispositius poden incorporar qualsevol de les tecnologies sense fils que hem vist –per sobre- fins ara: RFID, NFC, Wi-Fi, 802.154e, etc. Tot i així, les estimacions varien molt entre companyies. Així, tenim per exemple que l'empresa de consultoria Gartner pronostica que per al 2020 hi haurà un total de 26 mil milions de dispositius connectats a l'Internet de les Coses [40], mentre que, per la seva banda, l'altra gran consultora mundial, IDC (*International Data Corporation*), pronostica que, per al mateix any, el nombre de dispositius connectats serà de 212 mil millions (unes vuit vegades més) [41]. L'empresa Silicon Labs diu que la xifra serà de 40 mil milions, també per al 2020 [47]. Cisco, per la seva banda, pronostica que el nombre de dispositius connectats serà d'uns 50 mil milions, també per al mateix any [48]. La companyia Clarice Technologies comparteix amb Cisco la mateixa cifra [82], que equivaldria a uns vuit dispositius connectats per persona, en fer el repartiment entre el nombre mundial d'habitants [75].

En qualsevol cas i, tot i la diferència entre estimacions (fet que deixa entrevure que qualsevol pronòstic a cinc o sis anys vista no deixa de ser una pura especulació) estaríem parlant d'una quantitat immensa de nodes, que únicament podrien gestionar-se de manera individualitzada –identificar-se unequívocament- si es fa servir el protocol IPv6 per a l'assignació d'adreces IP, tal i com ja s'ha comentat en apartats anteriors (a menys que no volguem crear "illes" aïllades de dispositius amb adreces IPv4 ja que, en aquest cas, estaríem parlant en tot cas de múltiples *Intranet of Things* connectades entre sí, en comptes d'una veritable *Internet of Things* mundial).

Per la seva banda, parlant un altre cop de Gartner, podem veure, a través del seu mundialment famós gràfic *Hype Cycle for Emerging Technologies* (Cicle d'Expectació per a Tecnologies Emergents) on, a data juliol de 2014, l'IoT es troba a la cúspide de la gràfica, en plena fase "Pic d'Expectacions Inflades" (*Peak of Inflated Expectations*). A aquesta fase s'hi arriba després d'una primera fase inicial (*Innovation Trigger* o Disparador de l'Innovació), quan ja fa uns quants anys que la tecnologia ha sorgit al mercat, s'ha començat a desenvolupar i tothom en parla d'ella, esperant una gran quantitat d'àmbits d'aplicació i, per tant, d'escenaris on es pot implementar. Normalment, aquesta expectació és exagerada i, al cap d'un temps (dos o tres anys màxim), la tecnologia es comença a "desinflar" i la seva expectació o "moment d'importància" baixa fins a nivells més realistes, en una tercera fase que es denomina "Vall de la Desil·lusió" (*Through of Disillusionment*). Per exemple, en aquesta tercera fase podem trobar ara la tecnologia M2M que, com ja hem vist, és la "base" de l'IoT. Al camp d'uns anys més, la tecnologia arriba a una cuarta fase, denominada *Slope of Enlighment* (Pendent de la Il·luminació) en el qual la tecnologia "repunta" un altre cop, en el sentit de que torna a guanyar *momentum*, un cop que ja és prou madura i tothom sap el que es pot esperar d'ella. Per últim, a la darrera fase, anomenada *Plateau of Productivity* (Altiplà de Productivitat), s'hi arriba quan la tecnologia ja és completament coneguda i madura i se'n sap del cert quins àmbits i aplicacions són les més adequades; en aquesta fase, s'aconsegueix el màxim de

productivitat de la tecnologia, amb multitud d'empreses desenvolupant productes i serveis sobre la mateixa.

A la figura de sota podem veure el *Hype Cycle* de Gartner, amb data juliol 2014, tal i com s'ha comentat abans:

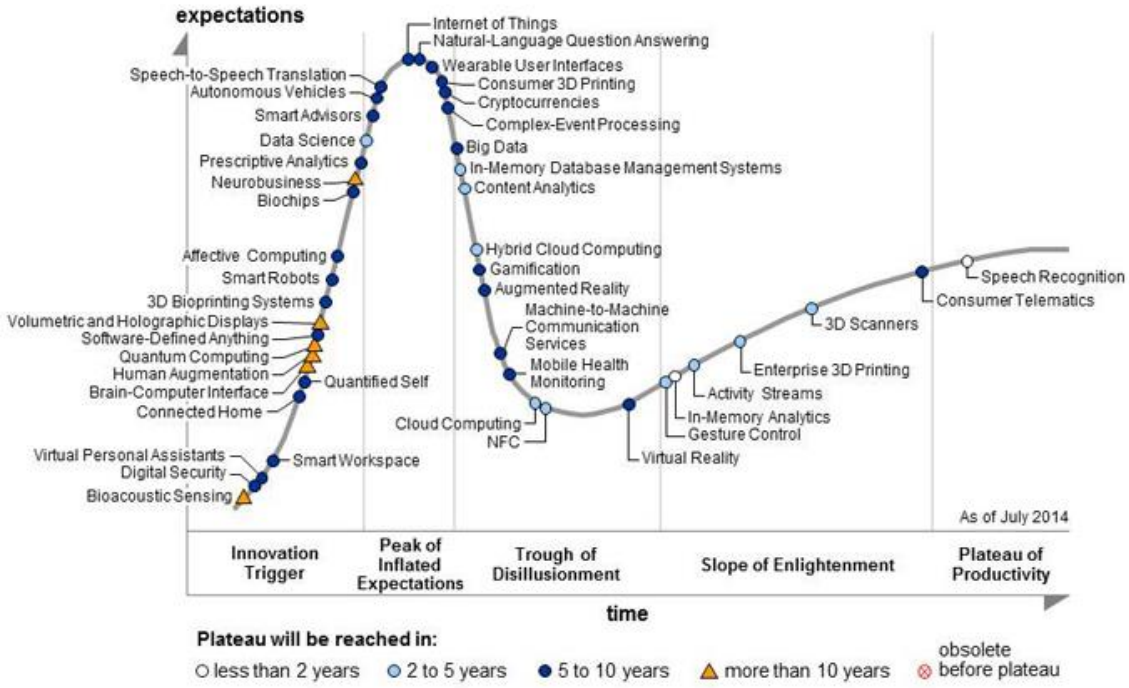


Figura 4. Cicle d'Expectació per a tecnologies emergents de Gartner, juliol 2014

Després d'assimilar aquesta informació, podem pensar que els àmbits d'aplicació són i seran múltiples i probablement no ens equivocarem, tot i que alguns escenaris concrets potser no passaran de la "fase d'expectacions inflades", normalment perquè els usuaris –la societat- no demandarà aquest tipus de solucions concretes; en altres paraules, no s'arribarà a veure certes aplicacions bàsicamente per falta de demanda, per molt que la tecnologia hi existeixi i sigui madura. Aquest fet no és exclusiu de l'IoT sinó que ocorreix en general amb qualsevol tecnologia emergent. Tenim exemples propers de tecnologies que han passat per les mateixes fases, com ara SOA (*Services-Oriented Architecture* o Arquitectura Orientada a Serveis) o Virtualització. Per exemple, amb SOA, fa uns anys es va viure una "febre" per part de les companyies (però, sobretot, per part dels fabricants de maquinari i empreses de consultoria IT) perquè els seus clients migressin totes les seves plataformes SW a productes SOA o bé perquè es realitzissen les modificacions i actualitzacions al programari empresarial existent per fer de fer-lo *SOA Enabled*. Passat el temps, s'ha vist que moltes empreses continuen amb el mateix tipus de programari que ja tenien fins el moment, tot i que algunes han adquirir nou SW o modificat algunes de les seves aplicaciones per fer-les interoperatives amb altres aplicacions de dins o de fora de l'empresa. Amb les tecnologies de virtualització ha passat una mica el mateix, ja que avui dia, tot i que moltes empreses empren aquesta tecnologia per als seus entorns de desenvolupament i proves, per a entorns de producció continuen preferint la instal·lació d'entorns físics (quan es requereix més potència) o bé s'està provant noves

solucions com ara la provisió de serveis al núvol, com per exemple IaaS (*Infrastructure as a Service*).

Dit això, podem afirmar que els àmbits d'aplicació de l'IoT -com gairebé passa amb qualsevol altra tecnologia emergent i, en especial, aquelles relatives o relacionades amb les telecomunicacions- és el següent:

- Militar (MIoT – *Military Internet of Things*),
- Ciència i Tecnologia (salut, medi ambient),
- Industrial,
- Agricultura i Ramaderia,
- Serveis públics,
- Gran consum.

Per a més informació sobre els àmbits d'aplicació d'IoT, veure l'Annex IV.

1.5. Anàlisi DAFO

Per a l'explicació de què és un anàlisi/matriu DAFO, veure l'Annex V.

Si apliquem aquesta metodologia/procediment al paradigma IoT, sabent tot el que hem vist en aquest capítol introductori, una probable matriu DAFO podria ser la següent:

	Fortaleses	**Debilitats**
Anàlisi Intern	. Existeixen estàndards ben definits d'associacions com l'IEEE, IETF, etc. que contribueixen/cooperen per al desenvolupament global de l'IoT. . El camp de les WSN no és nou (tecnologia madura i provada) . Tecnologies escalables i flexibles, que permeten integració de dispositius	. S'han creat moltes plataformes (maquinari i programari) propietàries, enfocades a M2M, difícilment interoperables entre elles, que poden suposar un entrebanc. Falta d'un únic estàndard global. . Necessitat de nodes autònoms a nivell energètic. La vida útil dels nodes/motes depèn en gran mesura del grau d'utilització de l'antena (ràdio). Encara s'ha de millorar, a nivell tècnic, en aquest aspecte. . La tecnologia encara no és prou senzilla d'implementar (la instal·lació de noves infraestructures pot ser complexa). .Manca d'aceptació per part dels consumidors per culpa del desconeixement de la tecnologia i del seu potencial, o bé recel de voler utilitzar-la.

	Oportunitats	Amenaces
Anàlisi Extern	. Molts àmbits d'aplicació. Milers de possibles serveis/solucions a molts camps (agricultura, ramaderia, Smart Cities, Industrial, ...). Demanda creixent. . Noves oportunitats de negoci . El cost de fabricació ha abaixat moltíssim en els darrers anys (economies d'escala), abaratint les solucions . La potència de processament ha augmentat molt en els darrers anys, fent possible solucions més complexes . Major eficiència energètica/optimització de processos industrials, etc.	. Possibles problemes legals relacionats amb l'ús de les freqüències, limitació en les potències màximes d'emissió, , ... (marc regulatori) . Manca de suport/promoció a nivell polític . Possibles riscos de privacitat, si no es prenen mesures adequades (encriptació) . La indústria IT ha de voler comfiar en els estàndards oberts proposats per a l'IoT (es necessita suport dels fabricants i desenvolupadors)

Taula 1. Matriu DAFO per a l'Internet de les Coses

Explicacions detallades sobre el contingunt de la matriu anterior es poden trobar a l'Annex VI.

2. Estat de l'art

Dins del camp tecnològic i industrial, s'entèn com "estat de l'art" –o "estat de la tècnica"- tots aquells desenvolupaments de darrera tecnologia realitzats per a un producte o servei, bé que es troben encara en fase de desenvolupament o bé que ja han estat provats i acollits/acceptats per diferents institucions i fabricants.

En aquest capítol, per tant, el que es pretèn es exposar els diferents estàndards de comunicació existents avui dia per a creació de xarxes sense fils i, més concretament, s'intentarà argumentar quins d'ells estan enfocats a xarxes sense fils de sensors (WSNs) i, sobretot, en aquelles de baix cost, baix consum i en entorns amb pèrdules (LLNs). En altres paraules, s'intentarà dilucidar aquells estàndards enfocats al paradigma IoT (comunicació d'objectes amb altres objectes remots, fent servir Internet com a xarxa de transport).

Veurem que, depenent de l'estàndard, alguns estan més enfocats a xarxes de llarg abast, altres a xarxa de curt abast i altres a xarxes de molt curt abast o personals. En cadascun d'ells, les taxes de transmissió aconseguides són diferents però també els requeriments d'energia (potència d'emissió/transmissió), freqüències utilitzades (llicenciades/sense llicenciar), etc.

2.1. Estàndards de comunicació en xarxes sense fils

2.1.1. IEEE 802.11 - Wi-Fi

L'estàndard 802.11, creat i mantingut per l'IEEE, defineix els dos nivells inferiors de la capa OSI (capa física –PHY- i capa d'enllaç de dades -MAC) per al seu ús en xarxes WLAN (*Wireless Local Area Network*); per tant, es tracta d'un estàndard orientat a xarxes locals sense fils encara que, a la pràctica, es poden aconseguir abasts –rangs de cobertura- que fan que aquest estàndard també pugui ser adequat, de vegades, per a xarxes d'àrea metropolina (WMAN – *Wireless Metropolitian Area Network*). L'associació internacional sense ànim de lucre Wi-Fi Alliance és l'encarregada de certificar l'interoperabilitat dels prodcutes basats en 802.11.

Aquestestàndard va ser creat l'any 1997 (versió base, 802.11-1997) i pot treballar en quatre rangs/bandes freqüencials: 2.4, 3.6, 5 i 60 GHz. L'estàndard, que consisteix en una sèrie de tècniques de modulació *half-duplex* -fent servir l'aire com a medi- proporciona la base per al que es denomina comunament com a Wi-Fi (*Wireless Fidelity*). La primera vesió àmpliament acceptada va ser 802.11b (taxa màxima 11 Mbps), seguida de 802.11a (taxa màxima 54 Mbps), 802.11g (taxa màxima 54 Mbps), 802.11n (taxa màxima 150 Mbps) i 802.11ac (taxa màxima 867 Mbps). Altres versions es consideren correccions i extensions d'especificacions prèvies. Per la seva banda, hi ha altres versions encara en procés, com ara 802.11ah (que fa servir la banda sense llicenciar per sota d'1 GHz, enfocada a xarxes de sensors, mesurament intel·ligent, etc) i que no estarà enllestida fins el 2016 o bé 802.11ax (*High Efficiency WLAN*) que té una data de publicació cap a maig del 2018.

Les diferències bàsiques entre especificacions són:

- la freqüència que es fa servir (2.4, 3.7. 5 o 60 GHz –aquesta darrera encara sota desenvolupament),

- l'amplada de banda (20, 22, 40, 80 o 160 MHz),

- la posibilitat de ver servir tècniques MIMO (*Multiple Input – Multiple Ouput*; és a dir, vàries antenes d'emissió/recepció simultàniament). A l'Annex VII es pot trobar un gràfic amb els diferents tipus de tecnologia MIMO actuals.

- el tipus de modulació: DSSS (*Direct-Sequence Spread Spectrum*), FHSS (*Frequency-Hopping Spread Spectrum*), OFDM (*Orthogonal Frequency-Division Multiplexing*), MIMO-OFDM (igual que OFDM però fent servir MIMO al mateix temps),

- El rang de cobertura, tant en interiors –*indoor*- con en exteriors –*outdoors*i que pot arribar fins als 70 m aproximadamente en el primer cas i fins als 250 m en el segon cas, segons la potència que es faci servir. Fins i tot es podrien arribar a distàncies de 5 Km, fent servir OFDM.

Per a més informació tècnica sobre l'estàndard IEEE 802.11 veure l'Annex VIII.

2.1.2. IEEE 802.11ah – Low-Power Wi-Fi

Aquest estàndard de l'IEEE es tracta d'una esmena de l'anterior versió 802.11-2007. Avui dia es troba encara en versió esborrany (*draft* 2.10 a data setembre 2014) i s'espera que estigui finalitzat el proper 2016, encara que alguns fabricants ja tindran xips enllestits el proper 2015. Bàsicament, l'estàndard estableix les capes PHY i MAC pera utilitzar freqüències per sota d'1 GHz (*sub 1 GHz* – S1G), que són bandes ISM (*Industrial, Scientific and Medical*, bandes que no necessiten llicència per operar), en comptes de fer servir les bandes 2.4 o 5 GHz com utilitza l'802.11 tradicional. A més, aquest estàndard està enfocat a la reducció del consum d'energia, suportant per tant el concepte d'IoT, que permet crear grans xarxes de sensors que cooperen per compartir el senyal.

A grans trets, IEEE 802.11ah estaria indicat per omplir la bretxa entre les actuals xarxes de sensors i les actuals xarxes WLAN. En el primer grup, tenim el protocol 802.15.4 –i les especificacions 802.15.4g/e/k-, especialment indicat per a WSNs però de curt abast i amb pocs requeriments de transferència de dades (baix *throughput*, fins a 250 Kbps). En el segon grup, per la seva banda, tenim les xarxes 802.11 i el seu gran problema de consum d'energia. Per tant, cal un nou tipus de xarxes que puguin, al mateix temps, transferir quantitats més grans de dades (de l'ordre de Mbps), tenir un llarg abast i uns requeriments baixos d'energia.

Per a més informació sobre Low-Power Wi-Fi, veure l'Annex IX.

2.1.3. IEEE 802.16 – WiMAX

IEEE 802.16 és un conjunt d'estàndars de banda ampla que defineixen les especificacions PHY i MAC per a xarxes metropolitanes (MANs) sense fils, bé fixes (versió 802.16d, any 2004) o mòbils (802.16e, any 2005). En essència, recull l'estàndard *de facto* WiMAX (*Worldwide Interoperability for Microwave Access*) tot i que oficialment, dins l'àmbit de l'IEEE, els estàndars es coneixen com a WirelessMAN. La darrera versió disponible de l'estàndard és la 802.16-2012. Tanmateix, existeixen dues altres versions (802.16.1b i 802.11p) que incorporen millores per permetre aplicacions M2M; en concret, s'especifiquen les modificacions a nivell de PHY i MAC que permeten un baix consum de potència dels dispositius, suport de gran nombre de dispositius per part de les estacions base, suport eficient per a petites transmissions en ràfega i autenticació de dispositius millorada.

L'organització WiMAX Forum promou i certifica la interoperabilitat dels productes basats en IEEE 802.16. La versió sudcoreana de WiMAX es coneix com a WiBro.

El conjunt de freqüències que fa servir WiMAX és, per un cantó des de 2 fins a 11 GHz per a la comunicació en la darrera milla (dels usuaris/dispositius client fins a les estaciones base) i, per altra banda, des de 10 fins a 66 GHz per a la comunicació entre les estacions base (anomenada *backhaul*, en anglès). Aquesta darrera ha de ser una comunicació amb línia de visió directa entre les *base stations* (LoS – *Line of Sight*), mentre que entre clients i BS no cal LoS per establir comunicació. A la pràctica, es fa servir 3.5 i 5.8 GHz per a WiMAX fixe i 2.3, 2.5 i 3.5 GHz per a WiMAX mòbil.

Per a més informació sobre l'estàndard IEEE 802.16, veure l'Annex X.

2.1.4. IEEE 802.20 – MWBA

L'estàndard IEEE 802.20, també conegut com a Accés Mòbil Sense Fils de Banda Ampla (*Mobile Broadband Wireless Access* – MBWA) recull les especificacions PHY i MAC per a xarxes d'accés d'alta velocitat, mòbils i sense fils –típicament xarxes d'accés a Internet, per al transport de serveis basats en IP [36]. L'estàndard fou publicat el 2008 i actualment ja no es desenvolupa de manera activa. Algunes de les seves característiques principals són:

- Opera a bandes licenciades (per sota de 3.5 GHz),
- Utilitza una arquitectura de paquets (optimizat per a transport IP),
- Baixa latència,
- Possibilitat de fer servir MIMO,
- *Roaming* (associació del dispositiuclient a un altre operador) i *handoff* (associació del dispositiu client a una altra estació base dins de la mateixa cel·la o a una altra cel·la) a més d'1 Mbps.

- Pot suportar fins a 100 trucades de veu per MHz (manega eficientment baixes taxes de transferència),

- Optimitzat per funcionar amb dispositius mòbils a velocitats de fins i tot 250 Km/h,

- Possibilitat de configurar múltiples rutes (camins únics a la xarxa),

- Dos modes d'operació:

    - *Wideband*
        - Modulació OFDMA (*Orthogonal Frequency-Division Multiple Access*),
        - Multiplexació FDD (per freqüència) /TDD (per temps),
        - Amplades de banda de canal de 2.5, 5, 10 i 20 MHz,
        - Taxes de transferència –pic- de 288 Mbps, fent servir 4x4 MIMO i 20 MHz d'amplada de banda,
        - Latència de l'*intra-cell handoff* de 8.9 ms.

    - 625k-MC
        - Modulació SDMA (*Space-Division Multiple Access*); múltiples canals espacial on el mateix canal convencional,
        - Multiplexació TDD,
        - Espaiat de 625 KHz entre portadores,
        - Operació multi-portadora (*Multi-Carrier* o MC),
        - Taxes de transferència –pic- de 1.493 Mbps (baixada) 571.2 Kbps (pujada),
        - Fa servir modulació i codificació adaptatives (AMC),
        - Permet QoS (prioritat per sessió), segons el model DiffServ [95] per permetre VoIP i *streaming.*

Per a més informació sobre MWBA, veure l'Annex XI.

2.1.5. IEEE 802.22 – WRANs

L'IEEE 802.22 és un estàndard per a xarxes sense fils d'àmbit regional (*Wireless Regional Area Network* o WRAN), que utiliza els espais blancs en el espectre de freqüències dels canals de televisió (els "espais blancs" són freqüències que, tot i estar assignades a serveis de difusió, no s'utilitzen a nivell local). El desenvolupament d'aquest estàndard fa servir tècniques de ràdio cognitiva (*Cognitive Radio* - CR) per permetre l'ús compartit de l'espectre geogràfic no utilitzat. La idea és utilitzar aquest espectre de freqüència, assegurant que no hi ha inteferències perjudicials a l'peració incumbent (TV analògic o digital) per oferir accés de banda ampla a zones a les que difíclment es podria proporcionar aquest servei, com ara zones de baixa densitat de població, rurals, etc.

L'estàndard P802.22.1 és la definició de l'estàndard en sí mateix mentre que el P802.22.2 són les pràctiques recomenades per a la instalació i desplegament de sistemes IEEE 802.22.

Els esborranys inicials de l'estàndard defineixen que la xarxa hauria d'operar en mode punt a multipunt (P2MP) i estaria formada per estacions base (BS) i equips al lloc del client (CPE). Els CPEs estarien "connectats" a una BS a través d'un enllaç sense fils. Les BSs controlarien el medi d'accés per a tots els CPEs connectats a la primera. Una característica clau de les BSs es que serian capaces de realitzar un sensat cognitiu (que significa que els CPEs estarien sensant l'espectre i enviarien informes periòdics a la BS informat sobre el que estan sensant. Llavors, la BS, amb la informació recollida, evaluaria si és necessari fer canvis en el canal utilitzat o, pel contrari, hauria de mantenir-se emetent i rebent en el mateix).

Per a més informació sobre l'estàndard IEEE 802.22, veure l'Annex XII.

2.1.6. IEEE 802.11af–Super WiFi

L'estàndard IEEE 802.11af (aprovat el passat febrer de 2014), també conegut com White-Fi o Super Wi-Wi, de manera molt semblant al ja vist 802.22, defineix l'accés "oportunista" a xarxes mòbils fent servir els espais blancs -assignats però temporalment no utilitzats- de les bandes de televisió VHF/UHF. La diferència amb aquest darrer consisteix en que 802.11af està orientat a WLANs (xarxes locals sense fils) amb un radi màxim de fins a 5 Km, mentre que 802.22 està orientat a WRAN (xarxes regionals sense fils) amb radis de fins a 100 Km. Fa servir tècniques de ràdio cognitiva (ràdio intelligent que pot ser programada i configurada dinàmicament, amb transceptor dissenyat per utilitzar els millors canals sense fins en el seu veïnatge) i, al igual que 802.22 fa servir OFDM, amplades de canal de 6-8 MHz i *channel bonding* (fins a quatre canals).

Altres característiques de l'estàndard són:

- Permet l'ús de MIMO,

- Taxa de dade de 26.7 Mbps per a canals de 6-7 MHz (426.7 Mbps amb quatre canals ajuntats i quatre fluxes espacials) i 35.6 Mbps per a 8 MHz (568.9 Mbps amb quatre canals ajuntats i quatre fluxes espacials),

- Els punts d'accés i les estacions determinen la seva posició fent servir un sistema de posicionament per satèl·lit, com ara GPS (*Global Positioning System*) i fan servir Intrnet per consultar una base de dades de geolocalització (GDB), proporcionar per una agència regulatòria regional, per descobrir què freqüències –canals- estan disponibles per a una hora i posició determinades.

Tot i que el radi de cobertura d'aquest estàndard el podria fer més adient per a xarxes de sensors, tampoc no és adequat perquè no incorpora funcions d'estalvi d'energia, ni permet tècniques d'encaminament de dades entre nodes –formant una malla- per salvar major distàncies. De fet, com que l'estàndard basa el seu funcionament en la consulta de dades fent servir GPS i Internet, això ja penalitzaria la vida de les possibles bateries del dispositiu, quedant clar que aquesta especificació està orientada a dispositius fixes que tenen alimentació elèctrica assegurada. A més, el fet de que els dispositius hagin de tenir un receptor GPS també encareix el preu del producte final, justament el contrari del que s'espera d'una WSN de baix cost.

2.1.7. IEEE 802.15 – WPANs

IEEE 802.15 és un Grup de Treball (*Working Group* - WG) del'IEEE que especifica estàndars per a xarxes sense fils d'àrea personal (WPAN), és a dir, aquelles que tenen un abast de pocs metres de cobertura. Es divideix en un total de set grups de tasques (*Tasks Groups* – TG):

- TG 1 (WAN – Bluetooth): aquest grup es basa en la tecnologia Bluetooth i defineix les especificacions per les capes PHY i MAC per a connectivitat sense files tant per dispositius fixes, mòbils i en moviment dintre d'un àmbit d'operació personal. Van publicar dos estàndars, els anys 2002 i 2005.

- TG 2 (Coexistència): aquest grup és dirigeix a la coexistència de les WPAN amb altres dispositius sense fils que operen en freqüències sense llicenciar com per exemple les WLAN. Van publicar l'estàndard IEEE 802.15.2-2003 i després el grup va quedar en "hibernació".

- TG3 (WPANs d'alta velocitat): aquest grup defineix un estàndard MAC i PHY per a WPANs d'alta velocitat (de 11 fins a 55 Mbps).

    - IEEE 802.15.3a va ser un intent de proporcionar una millora a nivell de capa física -d'ultra banda ampla (UWB)- per a aplicacions d'imatge i multimèdia. No es va arribar a un acord entre les tecnologies a fer servir (*Multi-Band* OFDM) o *Direct Sequence* UWB, proposades per dues aliances industrials diferents i, per tant, es va retirar el 2006.

    - IEEE 802.15.3b-2005 és una revisió que millora la implementació i la interoperabilitat de la capa MAC, al mateix temps que assegura compatibilitat cap a enrrere.

    - IEEE 802.15.3c-2009 va desenvolupar una alternativa de tipus "milímetre d'ona" (mmWave) per a la capa PHY. Aquesta xarxa wwMwave opera en banda lliure, incloent la banda 57-64 GHz; també permet coexistència amb altres sistemes de microones de la família 802.15. Per últim, permet taxes d'al voltant de 2 Gbps –es preveu properes taxes de 3 Gbps- per a aplicacions com ara Intrenet, *streaming* de vídeo, (HDTV, vídeo sota demanda, etc.).

- TG4 (WPANs de baixa velocitat): aquest grup, IEEE 802.15.4-2003, també anomenat *Low Rate* WPAN, s'encarrega de les xarxes que necessiten baixa taxa de transferència, llarga vida de les bateries -de l'ordre d'anys- i molt baixa complexitat. L'estàndard defineix les capes PHY i MAC del model OSI. Molts protocols de xarxa –tant estandaritzats com propietaris- funcionen sobre xarxes basades en 802.15.4, incloent IEEE 802.15.5 (estàndard per a WPANs de tipus *mesh*), ZigBee, 6LoWPAN, WirelessHART i ISA 100.11a.

- 4a (Capa PHY): IEEE 802.15.4a és una esmena a l'estàndard original que especifica capes físiques adicionals. El principal objectiu és el de proporcionar capacitats de cobertura i localització amb major precisió (un metre de precisió o més), major taxa de transferència agregada, afegir escalabiliat a les taxes de dades, major rang de cobertura, menor consum de potència i menor cost. Les línies base consisteixen en dues capes PHY opcionals de tipus UWB *Pulse Radio* –operant a la banda sense llicència UWB- i *Chrip Spread Spectrum* -operant en la banda de 2.4 GHz, també sense necessitat de llicència.

- 4b (revisió i millores): l'objectiu d'aquest grup fou el de crear un projecte per millores específiques, així com clarifications a l'estàndard 802.15.4-2003, com per exemple resolució d'ambigüetats, reducció de complexitat innecesària, increment de la flexibilitat en l'ús de claus de seguretat, etc. L'estàndard es va publicar com a IEEE 802.15.4-2006.

- 4c (esmena PHY per a Xina): com el seu propi indica, aquest estàndard defineix esmenes per a la capa PHY que té en comptes els canvis regulatoris a la Xina, com per exemple l'obertura dels rangs 314-316 MHz, 430-434 MHz i 779-787 MHz per a WPANs.

- 4d (esmena PHY i MAC pel Japó): similar al grup 4c però, en aquesta ocasió, les esmenes a la capa PHY i MAC (de l'estàndard 802.15.4-2006) tenen en compte suport per a la banda 950-956 MHz, així com coexistència amb sistemes d'etiquetes passives.

- 4e (esmena MAC per a aplicacions industrials): aquest TG defineix els canvis/esmenes a l'estàndard 802.15.4.-2006 per a la capa MAC per millorar i afegir funcionalitats per a un millor suport d'aplicacions industrials i permetre compatibilitat amb les modificacions proposades dintre de les WPAN xineses. S'afegeixen millores específiques per afegir salts de freqüència en ranures de temps (*Time-Slotted Channel Hopping* o TSCH), compatibles amb l'estàndard ISA100.11a.

- 4f (esmena PHY i MAC per a RFID Actiu): aquest TG defineix una nova capa PHY i millores a la capa MAC de l'estàndard 802.14.5-2006 per permetre sistemes RFID bidireccionals i aplicacions de determinació de la localització.

- 4g: (esmena PHY per a xarxes d'*Smart Metering*): aquest TG (també anomenat *Smart Utility Networks* – SUN) té com a objectiu crear esmenes al 802.15.4 original per porocionar un estàndard que faciliti aplicacions de control de processos molt grans, com ara xarxes *smart* grid repartides geogràficament, amb una infraestructura mínima i que puguin tenir milions de dispositius fixes. El 2012 es va alliberar l'estàndard ràdio.

- TG 5 (xarxes en malla): l'IEEE 802.15.6 proporciona el marca de treball arquitectònic per permetre als dispositius WLAN interoperables, estables i escalables per a xarxes sense fils en topologia *mesh* (mall). L'estàndard es composa de dues parts: WPANs de malla de baixa taxa i WPANs de malla d'alta taxa. Les de baxa taxa de transferència es basen en la capa MAC IEEE 802.15.4-2006 mentre que les d'alta velocitat fan servir la MAC de l'IEEE 802.15.3/3b. Ambdues tenen característiques comuns com ara: inicialització de xarxa, adreçament, multisalt *unicast*, etc.

- TG 6 (xarxes d'àrea corporal): el 2001, el TG IEEE 802.15.6 va aprovar un esborrany d'un estàndard per a tecnologies de xarxes d'area corporal (*Body Area Network* – BAN). Aquest estàndard es focalitza en xarxes de baix consum i poca cobertura, optimizades per a dispositius que operin sobre, dintre o al voltant del cos humà (o qualsevol animal) i que pot servir a una varietat d'aplicacions com ara mèdiques, electrònica de consum, entreteniment, etc.

- TG 7 (comunicacions amb llum visible): l'III 802.15.7 ha presentat diversos esborranys que defineixen les capes PHY i MAC d'un estàndard per a comunicacions amb llum visible (*Visible Light Communications* – VLC). En concret, el grup està dirigit a la creació d'estàndars fent servir comunicacions en l'espai obert (medi no guiat).

Segons el que s'ha pogut veure, l'estàndard 802.15.4 –i les seves posterios esmenes/revisions- és el més adient per a xarxes de sensors sense fils (WSN) de baix cost i de baix consum. En concret, 802.15.4e introdueix millores i funcionalitats específicament dirigides a aplicacions industrials [8]. Tot i així, altres estàndars, com el 802.15.1 -en el qual es basa Bluetooth- o 802.15.6 -xàrxes d'àrea corporal- també permeten crear xarxes de sensors i, per tant, també es poden incluoure dintre del paradigma IoT.

2.1.7.1. IEEE 802.15.1 - Bluetooth

Bluetooth és estàndard tecnològic per a xarxes sense fils en distàncies curtes, que fa servir ones de ràdio d'UHF -ona curta- de la banda ISM de 2.4-2.4835 GHz (incloent bandes de guarda), tant per a dispositius fixes com a mòbils, permetent crear xarxes d'area personal. Va ser inventant per la company Ericsson el 1994 i es va concebre inicialment com un substitut per a l'interfície cablejada RS-232. Actualment, Bluetooth és gestionat pel *Bluetooth Special Interest Group* (SIG), amb més de 20.000 companies membres en les àrees de telecomunicacions, computació, xarxes i electrònica de consum. Bluetooth fou estandaritzat com a IEEE 802.15.1, com s'ha pogut veure en l'apartat anterior, encara que l'estàndard ja no es manté.

Bluetooth fa servir FHSS, igual que Wi-Fi. Les dades a transmetre es divideixen en paquets i cada paquet es transmet en un dels 79 possibles canals Bluetooth designats, tenint cada canal una amplada de banda d'1 MHz. El primer canal comença als 2402 MHz i continua fins als 2480 MHz en pasos d'1 MHz, a un ritme de 1600 salts per segon, fent servir salt de freqüència adaptatiu (*Adaptative Frequency Hopping* – AFH).

Com a modulació, originàriament es feia servir tan sols GFSK (*Gaussian Frequency-Shift Keying*) però més tard, amb noves versions de la tecnologia, es va permetre l'ús de π/4-DQPSK i 8DPSK entre dispositius compatibles. Amb la primera modulació –els dispositius funcionant amb aquesta es diu que operen en *Basic Rate* o BR- es pot aconseguir una taxa instantània d'1 Mbps, mentre que amb la segona i tercera –els dispositius que les fan servir es diu que operen en *Enhanced Data Rate* o EDR- es pot aconseguir 2 i 3 Mbps, respectivament. Quan una ràdio Bluetooth accepta els dos modes, es classifica com a ràdio BR/EDR.

Per a més informació sobre Bluetooth, veure l'Annex XIII.

2.1.7.2. *Bluetooh Low Energy*

Bluetooth Low Energy –o simplement BLE- és un subconjunt de Bluetooth 4.0, que consta d'una pila (*stack*) de protocol completament nova i que està destinada a aplicacions de molt baix consum i dispositius de mida petita –que funcionen amb piles de botó- i de baix cost de fabricació. Inicialment es va anomenar Wibree, més tard Bluetooth ULP (*Ultra Low Power*) i després BLE. Avui dia, s'utilitzen el termes *Bluetooth Smart Ready* per als *hosts* –per exemple, un PC- i *Bluetooth Smart* per als sensors [62].

Es permeten dos tipus d'implementació a nivell de xip: *dual-mode* i *single-mode* [97]. En el mode únic o *single*, únicament s'implementa la pila de protocol de baix consum, mentre que en el mode dual, la funcionalitat *Bluetooth Smart* s'integra dins d'un controllador *Classic Bluetooth*. En altres paraules, *Bluetooth Smart* no és compatible cap endarrere amb *Bluetooth Classic* encara que es poden implementar amdues especificacions dins el mateix xip. Tot i així, totes dues especificacions fan servir el mateix rang de 2.4 GHz per la qual cosa els dispositius en mode dual poden compartir la mateixa antena (tot i que BLE fa servir un esquema de modulació més simple). En canvi, amb BLE els canals no són d'1 MHz d'amplada de banda sinó de 2 MHz, per la qual cosa pot haver-hi un màxim de 40 canals (en comptes de 79 canals com era el cas del Bluetooth clàssic). La potència màxima de transmissió és de 10 mW (a mig camí entre els dispositius Classe 1 i Classe 2 del Bluetooth clàssic) i la taxa màxima és d'1 Mbps [96].

Per a més informació sobre Bluetooth Smart, veure l'Annex XIV.

2.1.7.3. 802.15.4

2.1.7.3.1. ZigBee

ZigBee és una especificació –concebuda l'any 1998, estandaritzada el 2003 i revisada el 2006- per a un conjunt de protocols d'alt nivell (capa 3 OSI i superiors), basada en l'estàndard IEEE 802.15.4, per a la creació de WPANs de molts dispositius, fent servirnodes de mida petita, baix cost i baix consum de ràdio. A aquest tipus de xarxes se'ls hi anomena *Low-Rate WPAN* o LR-WPAN.

Un baix consum limita, al seu torn, la màxima distància possible (entre 10-100 metres, dependent de l'existència de LoS). Tot i així, es podem salvar majors distàncies fent servir una topologia de malla, per la qual els dispositius es poden interconnectar/comunicar entre sí i es creen rutes entre origen i destinació, on els nodes intermitjos funcionen com a encaminadors, reenviat les dades a altres dispositius encaminadors, fins arribar a la destinació final (per exemple, fins a una pasarel·la que pot connectarcap a una altra xarxa com ara Internet).

Tal i com s'ha dit, ZigBee es basa en l'estàndard IEEE 802.15.4. Aquest estàndard defineix únicamentla capa física (PHY) i subcapa d'enllaç (MAC) per a la creació de xarxes sense fils d'àrea personal o WPAN que no necessitin qualitat de servei o amb requeriments molt simples en aquest sentit. En canvi, ZigBee és una implementació d'aquest estàndard -la més coneguda i implementada avui dia probablement- i es centra en afegir funcionalitats a nivell de xarxa, transport i aplicació a l'estàndard anterior. A la taula de sota es pot veure la relació entre els nivells genèrics OSI i les correspondències a nivell 802.15.4 i ZigBee.

Model OSI	802.15.4 + ZigBee
Capa d'aplicació	Objectes d'Aplicació ZigBee (ZAO) Objectes Dispositiu ZigBee (ZDO) Serveis de Seguretat ZiGbee
Capa de transport	
Capa de xarxa	Encaminament ZigBee (AODV)
Control lògic de l'enllaç	802.1 LLC (*Logical Link Control*)
Control d'accés al medi	802.15.4 MAC
Capa física	802.15.4 PHY (Interfície aire - 868 MHz / 915 MHz / 2.4 GHz)

Taula 2. Relació entre els nivells OSI i IEEE 802.15.4/ZigBee

Per tant, el primer punt que s'ha de deixar ben clar és que 802.15.4 i ZigBee no són exactament el mateix: el primer és un estàndard que defineix la capa física (nivell 1) i subcapa d'accés al medi (nivell 2) per a la creació de xarxes d'àrea personal i comunicació punt a punt entre dispositius, mentre que el segon és una implementació d'aquest estàndard, que afegeix serveis extra com són encaminament mitjançant una topologia d'arbre, seguretat –encriptació- i serveis d'aplicació.

ZigBee –i, de fet, qualsevol implementació de l'estàndard 802.15.4- s'utilitza principalment en aplicacions que requereixen una llarga vida de les bateries (donat que els dispositius no estaran connectats a la xarxa elèctrica i estaran desatesos). A més, ZigBee és adequat per a entornsque necessitin seguretat (les dades s'encripten amb claus simètriques de 128 bit) i que tinguin una baixa taxa de transferència (fins a 250 Kbps). En altres paraules, està enfocat a la transmissió intermitent de dades des d'un sensor o dispositiu d'entrada.

Les aplicacions possibles poden incloure des de sistemes de gestió del trànsit, *home automation* (automatització de llars), control de condicions ambientals, agricultura, etc.

En definitiva, l' objectiu final de l'estàndard 802.15.4 és crear WPANs més simples i barates que amb altres tecnologies/estàndars sense fils, com ara Wi-Fi o Bluetooth.

Per a més informació sobre ZigBee, veure l'Annex XV.

2.1.7.3.2. IEC 62591 - WirelessHART

WirelessHart és una tecnologia per a xarxes sense fils que també es basa –al igual que ZigBee- en l'estàndard IEEE 802.15.4, per la qual cosa fa servir la mateixa capa PHY i MAC. Per tant, opera també en la banda ISM de 2.4 GHz –però únicament fa servir aquesta i no altres. Fa servir, a nivell ràdio, una combinació de tècniques FHSS i DSSS, paquet per paquet, per poder anar canviant de freqüència –i, per tant, de canal- en funció de les condicions d'aquest darrer (per exemple, en presència de soroll o si el canal ja està ocupat) i així evitar interferències, fent que la transmissió sigui més robusta i confiable. D'igual manera, també es pot fer servir CCA (*Clear Channel Assessment*) de manera opcional, abans de començar a transmetre, així com *blacklisting* de canals en funció de la quantitat d'energia. Com a modulació, fa servir O-QPSK, igual que ZigBee.

És important fer notar que, dels 16 canals que defineix 802.15.4 a la banda de 2.4 GHz, WirelessHART fa servir únicament 15 (el darrer canal no s'utilitza degut a regulacions nacionals, ja que no és legal fer-lo servir en alguns països). Cada canal té una amplada de banda de 3 MHz i estan separats entre ells per una amplada de 5 MHz.

A nivell de PHY PDU (*Protocol Data Unit*), és idèntica a la de 802.15.4, donat que WirelessHART es basa en aquest darrer estàndard.

En definitiva, amb WirelessHART es poden crear xarxes sense fils mallades, multisalt, auto-organitzades (*self-organizing*) i amb auto-recuperació (*self-healing*) [11].

WirelessHART és compatible amb la seva tecnologia predecessora HART (*Highway Addressable Remote Transducer*).Per la seva part, HART és una implementació temprana (mitjans de la dècada de 1980) de Fieldbus, un protocol digital per a automatització industrial. El seu avantatge més notable és que HART pot comunicar-se fent servir antic cablejat anàlog d'instrumentació 4-20 mA, compartint el mateix parell de cables utilitzats en aquests antic sistemes.

Per a més informació sobre WirelessHART, veure l'Annex XVI.

2.1.7.3.3. IEC 62734 - ISA-100.11a

ISA-100.11a (d'ara en endavant, ISA-100) és una tecnologia de xarxa sense fils desenvolupada per la Societat International d'Automatització (*International Society of Automation* – ISA). La descripció oficial de la mateixa és "Sistemes sense fils per automatització industrial: control de processos i aplicacions relacionades". La seva finalitat és la d'habilitar una infraestructura sense fils simple i integrada per a plantes industrials, així com l'entrega d'una familia d'estàndards que defineixin sistemes sense fils per automatització industrial i aplicacions de control. Una de les premises d'ISA-100 és la coexistència en entorns on hi hagui altres xarxes sense fils que poden estar o no basades en el mateix estàndard. ISA-100 es considera un estàndard completament redundant i auto-recuperable i soporta fiabilitat extrem a extrem.

L'arquitectura d'ISA-100 permet suportar des de xarxes úniques, petites i aïllades, fins a diverses xarxes que incloguin molts milers de dispositius i cobrint plantes de diversos km^2.

L'any 2011, ISA fou aprovat per l'IEC (*International Electrotechnical Commission*) amb la denominació IEC 62734. Per la seva banda, existeix un comité ISA-100 des del 2005, format per uns 400 professionals i 250 empreses. El comité estableix els estàndars i defineix procediments per a la implementació de sistemes sense fils en entorns d'automattzació i control; tanmateix, també vetlla per l'evolució i avanç dels estàndards ISA-100.

Per a més informació sobre ISA-100.11a, veure l'Annex XVII.

2.1.8. EN13757-4 - Wireless M-Bus

L'estàndard Wireless M-Bus (també abreviat simplement wM-Bus) conté especificacions de capes PHY i MAC (nivells 1 i 2 de l'OSI) per crear enllaçosde comunicacions RF que permetin la lectura remota de mesuradors de fonts d'energia, com ara aigua, gas, calor i electricitat. Es tracta d'un estàndard europeu (EN13757-4:2005 i posteriorment, EN13757-4:2012) on s'està acceptant àmpliament per a aplicacions de mesurament intel·ligent (*Smart Metering*) o AMI (*Advanced Metering Infrastructure*).

Originalment, únicament permetia operar en la banda sense llicenciar de 868-870 MHz, que dóna un bon compromís entre rang de cobertura i mida d'antena, encara que recentment s'han introduït dues noves bandes -169 i 433 MHz- a les especificacions, introduïnt per tant solucions de banda estreta i amb rang de cobertura superior a 868 MHz. El focus primari d'aquest estàndard son els dispositius de curt abast o SRD (*Short Range Devices*) [15].

L'estàndard es basa en el seu homònim M-Bus (*Meter-Bus*) per a xarxes cablejades, definit en la norma europea EN 13752-2. Aquest darrer únicament defineix també les capes PHY i MAC. Per la seva banda, un altre estàndard defineix el nivell d'aplicació (capa 7), l'EN 1357-3.

Per a més informació sobre wM-Bus, veure l'Annex XVIII.

2.1.9. DASH7

DASH7 és un estàndard de codi obert basat en RFID (identificació per radiofreqüència) per a la creació de xarxes de sensors sense fils, orientat a dispositius de curt abast (SRD). Existeix com estàndard ISO, concretament definit a l'ISO/IEC 18000-7 (ratificat l'any 2004 i posteriorment modificat l'any 2008). Algunes característiques d'aquesta especificació són:

- Opera en la banda ISM de 433 MHz (disponible en gairebé tot el món, excepte India i Japó, on aquesta banda està restringida). Això el fa immune a interferències d'altres tecnologies que operen en la banda de 2.4 GHz (per exemple 802.11/Wi-Fi).

- Els dispositius tenen bateries que duren molt de temps (10 anys o més) degut al baix consum de potència.

- El rang de cobertura pot arribar fins a 1 o 2 Km (depenent de la potència de sortida i la taxa de dades). Fins i tot s'han arribat a cobertures de 10 Km en la Unió Europea, on las regulacions no són tan fortes com en EEUU.

- Permet localització en interiors amb un metre de precisió/granularitat.

- Baixa latència quan es connecta a objectes mòbils (2 segons màxim).

- Pila de protocols de mida molt petita (i a més, *open source*).

- Suporta encriptació AES (*Advanced Encryption Standard*) de 128 bit de clau compartida.

- Taxa de dades de fins a 200 Kbps.

- Creat inicialment per usos militarsperò reorientat per oferir també aplicacions comercials.

La tecnologia DASH7 està promoguda per la *DASH7 Alliance*, un consorci industrial sense ànim de lucre que impulsa estàndars de xarxes de sensors sense fils. Per la seva banda, aquest estàndard, en ser de codi obert, rivalitza amb altres alternatives propietàries, com ara ZigBee o Z-Wave.

Per a més informació sobre DASH7, veure l'Annex XIX.

2.1.10. ITU T G.9959 - Z-Wave

Z-Wave és un protocol de comunicacions sense fils dissenyat per a automatització de llars, específicament per a control remot d'aplicacions en entorns residencials i comercials (en aquest darrer cas, en entorns de baixa càrrega). Va ser dissenyat per una empresa danesa anomeada Zen-Sys, que posteriorment va ser adquirida per la companyia Sigma Designs l'any 2008. Z-Wave fa servir, igual que altres alternatives sense fils, tecnologia RF de baix consum, amb antenes que es poden trobar encastrades en qualsevol mena de dispositiu electrònic com ara d'il·luminació, de control d'accesos, sistemes d'entreteniment o electrodomèstics. Les capes PHY i MAC de la tecnologia venen definides per l'estàndard ITU-T G.9959 [114].

Per la seva part, existeix la *Z-Wave Alliance*, de manera similar als estàndars que s'han vist anteriorment. Està formada per uns 250 fabricants independents, que s'han d'acord per

desenvolupar i fabrica productes de control de llars sense fils, seguint l'estàndard Z-Wave. Alguns d'aquests fabricants son ADT, Linear, Evolve o la pròpiaSigma Designs. A data de 2014, existeixen més de 1.000 productes cerfificats per l'aliança, que cobren tant el mercat tant en els àmbits residencials i comercials. Alguns d'aquests productes inclouen ventilació, calefacció i aire condicionat (HVAC –*Heating, Ventilating and Air Conditioning*), control de seguretat, *Home Theaters*, controls per piscines i spas, accés a garatges, alarmes contra incendis, etc

Z-Wave fa servir tecnologia sense fils de baix consum -potència de sortida de l'antena d'1 mW i cicle de treball de 0.1%-i està optimitzat per a baixa latència i alta fiabilitat, amb taxes de dades màximes de fins 100 Kbps, encara que les típiques són de 9.6 –amb xips antics- o 40 Kbps, al contrari que altres estàndards con Wi-Fi, que proporcionen taxes molt més elevades però a costa d'un major consum d'energia. El rang de cobertura màxim acostuma a ser d'uns 30 metres en camp obert (LoS).

Z-Wave, al igual que altres estàndars vists fins ara, opera en la banda ISM sub-1 GHz de 900 MHz i, per tant, de lliure accés. Un dels avantatges de fer servir aquesta banda és que s'eliminen possibles interferències amb altres tecnologies com Wi-Fi o Bluetooth, que fan servir les bandes –molt més saturades- de 2.4 o 5 GHz. En aquest sentit, la banda de 900 MHz es fa servir també per alguns telèfons sense fils.

Per a més informació sobre Z-Wave, veure l'Annex XX.

2.1.11. ANT

ANT és una tecnologia per a xarxes de sensors sense fils, basada en accés obert i *multicast*. Va ser desenvolupada per ANT Wireless, una divisió de la companyia Dynastrem Innovations que, al seu torn, va esdevenir una subsidiaria de la companyia Garmin, coneguda muldialment per la fabricacio de dispositius amb GPS integrat.

ANT opera en la banda ISM de 2.4 GHz i es basa en ràdios fabricades per les empreses Nordic Semiconductors i Texas Instruments, encara que també en combinació amb d'altres xips de connectivitat fabricats per Broadcom, MediaTek o Qualcomm. Es pot considerar que qualsevol transceptor ANT és com una mena de "caixa negra" que ja ve amb el programari –protocol- precarregat i que s'ha de controlar amb una aplicació externa fent servir per exemple una interfície sèrie o USB. Alguns transceptors més nous també venen en forma de SoC (sistema en un xip) i, per tant, una processador extern no és necessari [115].

La principal característica d'ANT és la seva baixa sobrecàrrega computacional i la seva eficiència mitja-baixa, que resulten en un baix consum de les ràdios, permetent dispositius que poden funcionar amb piles de botó des de varis mesos fins a anys.

Per a més informació sobre ANT, veure l'Annex XXI.

2.1.12. ETSI-EN-300 - DECT/DECT ULE

DECT són les sigles de *Digital Enhanced Cordless Telecommunications* (Telecomunicacions Digitals Millorades Sense Fils). Es tracta d'un estàndard creat l'any 1987, utilitzat principalment per a sistemes de telefonica sense fils i que funciona a la banda de 1900 MHz.

DECT es va originar a Europa, on és l'estàndard predominant -de fet, es troba especificat a l'ETSI EN-300, definit l'any 1993- i reemplaça a tecnologies antigues com ara CT1 i CT2 (*Cordless Telephone Generation 1* i *Generation 2*, respectivament) i que operaven a la banda de 900 Mhz. A més d'Europa, també s'utilitza a Austràlia i a la major part d'Àsia i Sudamèrica. Als Estats Units també es fa servir però la versió DECT 6.0, que fa servir un rang de freqüències lligerament diferent, degut a temes regulatoris [116].

DECT es fa servir principalment als telèfons sense fils de les llars i petites oficines però també es troba als sistemes de centralita (PBX – *Public Branch Exchange*) de mitjans i grans empreses. Per altra banda, a més de per a sistemes de telefonica, també es pot fer servir per altres aplicacions com ara monitors de nadons, caixers automàtics, enllumenat públic, obridors de portes, control remots industrials i transmissió de dades (encara que en aquest darrer àmbit ha estat eclipsat per l'ús de Wi-Fi). A països com l'Índia i Sudàfrica, DECT també es fa servir com un reemplaç sense fils de tecnologies cablejades d'última milla (coure) ja que, fent servir antenes molt direccionals i sacrificant capacitat, el radi de cobertura es pot extendre fins als 10 Km [119].

Per a més informació sobre DECT i DECT ULE, veure l'Annex XXII.

2.1.13. ISO/IEC 14443 - RFID

La identificació per radiofreqüència o RFID (*Radio-Frequency Identification*) és una tecnologia sense fils que es basa en l'ús de camps electromagnètics per transferir dades, amb el propòsit d'identificar i fer seguiment automàtic dels objectes que incorporin etiquetes (*tags*, en anglès) RFID. Aquestes etiquetes normalment venen en forma d'enganxina i es poden col·locar a gairebé qualsevol objecte com ara peces de roba, CDs, DVDs, paquets de qualsevol tipus, menjar, electrodomèstics, etc.

Les etiquetes RFID contenen informació emmagatzemada electrònicament. En funció de la forma de carregar l'etiqueta i de transmetre la informació, aquestes es poden dividir en passives, semi-passives i actives [120]:

- Les etiquetes passives no tenen transceptor ni bateria incorporades. Únicament es carreguen –i funcionen- quan el camp electromagnètic (EM) generat per un lector és el suficient com per fer-les "despertar". Quan una etiqueta passiva s'activa –en rebre el senyal de ràdio codificat enviat pel lector- el que fa és reflectir el senyal rebut, un cop modulat, retornant-lo al lector, amb les dades que l'etiqueta porta emmagatzemades (identificació i altra informació relacionada: número de sèrie, número de lot, data de producció, etc). A aquesta tècnica se li diu *backscatter*. La operació finalitza quan el lector rep i decodifica la resposta de l'etiqueta. Aquestes etiquetes són les més utilitzades actualment degut al seu baix cost. El seu rang de cobertura és bastant petit.

Com a curiositat, aquest tipus d'etiquetes han de ser "il·luminades" amb un nivell de potència aproximadament tres vegades més gran del que es necessita per a transmetre. En aquest sentit, sorgeix problemes relatius a possibles interferències o exposició humana a la a radiació.

- Altres tipus d'etiqueta, tot i que també fan servir la tècnica del *backscatter* per despertar-se i enviar la seva informació, incorporen una font de potència local –una bateria, normalment- per poderampliar el rang de cobertura i arribar fins a centenars de metres del lector (anomenat també interrogador). A aquest tipus de targetes se'ls hi anomena BAP (*Baterry Assisted Passive*) o semi-passives. Una modificació de les BAP són aquelles que funcionen amb un panell solar i un ultracondensador en comptes d'amb una bateria. La bateria incorporada, a més de per ampliar la cobertura, es pot fer servir per donar energia a altres elements com ara microcontroladors o sensors o bé per millorar la velocitat de lectura (per exemple per a identificació ràpida automàtica de vehicles).

- Per últim, les etiquetes actives són aquelles que tenen un transceptor de senyal i una bateria per fer-les funcionar. A diferència de les anteriors, poden estar actives tota l'estona tot i que no hi hagi un lector en les proximitats (ja que no es basen en el *backscatter*). Aquest tipus de bateries és el que té un rang de cobertura més gran però també un cost major. És el tipus que es fa servir normalment per a sistemes de localització en temps real (*Real Time Location Systems* – RTLS).

De manera diferent a un codi de barres, una etiqueta RFID no necessita trobar-se necessàriament en el camp de visió del lector (no necessita LoS). Un altre avantatge d'RFID respecte els codis de barres és que un lector pot llegir fins a centenars d'etiquetes RFID a la vegada, mentre que únicament es pot llegir un codi de barres al mateix temps. Les etiquetes RFID són uns dels mètodes per a AIDC (*Automatic Identification and Data Capture*), junts amb l'OCR (reconeixement òptic de caràcters), els codis de barres tot just nombrats, el reconeixement de veu, etc. [123]

Per a més informació sobre RFID, veure l'Annex XXIII.

2.1.14. ISO/IEC 18092 – NFC

NFC són les sigles de *Near Field Communication* (Comunicació de Camp Proper). Es tracta d'una tecnologia de comunicació sense fils de molt curt abast, creada l'any 2002, on l'antena és molt més petita que la longitud d'ona de la portadora (situació que, entre d'altres, prevé que es desenvolupin ones estacionàries en l'antena) i destinada a ser la "successora" d'RFID, pel que fa a comunicació fent servir etiquetes passives de baix cost.

En el camp proper, se sap que una antena pot produir un camp elèctric o un camp magnètic, però no un camp electromagnètic. Per tant, NFC fa servir, per a la comunicació, un camp modulat elèctricament o magnèticament, però no per ràdio (ones electromagnètiques). Per exemple, una petita antena cercle (*loop antenna*) produeix un camp magnètic, que pot ser recollit per altra antena cercle que estigui el suficientment propera.

Les arrels d'NFC s'han de buscar en RFID. Recordem que aquesta darrera tecnologia permet a un lector enviar ones de ràdio a una etiqueta electrònica passiva que "desperta" i envia la informació que té emmagatzemada, fent-se servir principalment per a identificació, autenticació o seguiment d'objectes. Per tant, NFC es construeix com a tecnologia a partir de RFID però permetent ara una comunicació bidireccional entre dos extrems, on RFID únicament permetia una comunicació en una via o unidireccional (per exemple, en targetes intel·ligents sense contacte per a accés a edificis).

Els dispositius NFC poden treballar en tres modes diferents [122]:

- Mode de lectura/escritura: el dispositiu NFC (per exemple un *smartphone*) pot llegir la informació d'altres objectes com ara etiquetes, engaxines, pòsters, braçalets [121], etc. que tinguin incorporat un xip NFC. Aquest mode compleix amb l'ISO 14443 i amb FeliCa. És el mode que més s'assembla a l'RFID tradicional.

- Mode P2P: en aquest mode, dos dispositius NFC comparteixen dades. Per exemple, es poden intercanviar targetes de visita o fotografies, música, etc. o bé compartir els paràmetres de configuració d'una connexió Wi-Fi o Bluetooth. Aquest mode es troba estandaritzat per l'ISO/IEC 18092.

- Mode d'emulació de targeta (*card emulation*): el dispositiu NFC es presenta a un lector extern com si fos una simple targeta intel·ligent. Això permet per exemple pagaments sense contacte de dispositius com ara telèfons mòbils, sense haver de canviar una infraestructura de pagament NFC ja existent.

NFC es basa en el mateix estàndard que RFID a 13.56 MHz, l'ISO/IEC 14443, així com en l'estàndard FeliCa (abreviació de *Felicity Card*, un tipus de targeta moneder RFID desenvolupat per Sony al Japó). Això significa que NFC també opera en aquesta mateixa banda de freqüència. La interfície ràdio es troba especificada al'estàndard ISO/IEC 18000-3, amb taxes de dades que van des de 106 Kbps fins a 424 Kbps, passant per 212 Kbps (també existeix una velocitat superior, 848 Kbps, però que no compleix amb l'estàndard ISO/IEC 18092). Pel que fa a la seguretat de xarxa en NFC, ve definida per l'ISO/IEC 13157 (canal segur i serveis de secret compartit per a NFC).

Per a més informació sobre NFC, veure l'Annex XXIV.

2.1.15. Taula resum

Un cop explicades les tecnologies/estàndars més importants existents en l'actualitat per a la creació de xarxes sense fils, es plasma en la següenta taula un resum de les característiques més importants de cadascuna d'elles, amb la finalitat de fer més fàcil la seva comparació directa:

Tecnologia	Estàndard	*Throughput*	Cobertura	Freqüència	Potència TX
Wi-Fi	IEEE 802.11n	185 Mbps	250 m	2.4 GHz, 5 GHz	100 mW
Low-Power Wifi	IEEE 802.11ah	250 Kbps	1 Km	900 MHz	12 mW
WiMAX	IEEE 802.16d	27 Mbps (*up*) 7 Mbps (*down*)	70-75 Km	3.5 GHz, 5.8 GHz	200 mW (node) 20 W (BS)
MWBA	IEEE 802.20	0.7 – 1.5 Mbps	5 Km	< 3.5 GHz	100 mW
WRAN	IEEE 802.22	19 Mbps	100 Km	54-790 MHz	100 mW
Super Wi-Fi	IEEE 802.11af	27 Mbps	5 Km	VHF – UHF	100 mW
Bluetooth	IEEE 802.15.1	2-3 Mbps (EDR)	100 m	2.4 GHz	1 mW, 2.5 mW, 100 mW
BLE	IEEE 802.15.1	260 Kbps	50 m	2.4 GHz	1 mW, 2.5 mW, 10 mW
ZigBee	IEEE 802.15.4	250 Kbps	100 m 1.5 Km (Pro)	2.4 GHz	1-10 mW
ISA-100.11a	IEC 62734	250 Kbps	100 m	2.4 GHz	10 mW
WirelessHart	IEC 62591	250 Kbps	100 m	169 MHz, 433 MHz, 868 MHz	10 mW
WM-Bus	EN 13757-4	100 Kbps	1.5-2 Km	433 MHz	10 mW
DASH7	ISO/IEC 18000-7	200 Kbps	10 Km	868 MHz	< 1 mW
Z-Wave	ITU-T G.9959	40 Kbps	30 m	2.4 GHz	1 mW (USA) 25 mW (Europa)
ANT	-	1 Mbps	50-100 m	2.4 GHz	1 mW
DECT ULE	ETSI EN 300-175	1.15 Mbps	70 m (*indoor*) 600 m (*outdoor*)	1.8-1.9 GHz	4 mW (USA) 10 mW (Europa)
RFID	ISO/IEC 14443	640 Kbps (FM0)	100 m	125-134 KHz 13.56 MHz 860-960 MHz 2.45 GHz	1 W (lector)
NFC	ISO/IEC 18092	424 Kbps	20 cm	13.56 MHz	10 mW

Taula 3. Resum de característistiques de diverses tecnologies de xarxes sense fils

Deixant de banda altres aspectes no enumerats a la taula, com ara les codificacions/modulacions emprades per cada estàndard (que, al final, per al que serveixen és per a aconseguir una major taxa de dades i/o una major distància), el que es pot veure en la taula és, a grans trets, el següent:

- A major freqüència de treball, major taxa de dades (*throughput*) i menor distància,
- A menor freqüènciade treball, menor taxes de dades (*throughput*) i major distància.

Per altra banda, també s'aprecia que es poden dividir les tecnologies segons la seva potència de transmissió típica/màxima:

- Molta potència (≥100 mW): Wi-Fi, WiMAX, 802.20, 802.22, Super Wi-Fi, Bluetooth Classe 1),

- Poca potència (≈ 10 mW): Low-Power Wifi, BLE (o Bluetooth Classe 2), ISA-100.11a, ZigBee, WirelessHart, WM-Bus, DECT ULE, NFC,

- Molt poca potència (≈ 1 mW): BLE (o Bluetooth Clase 3), ZigBee, DASH7, Z-Wave, ANT, RFID.

Per tant, si l'objectiu és crear xarxes sense fils de baix consum, s'hauran d'escollir aquelles tecnologies amb nodes emetent amb menys potència ja que, d'aquesta manera, la vida útil de les bateries dels dispositius es maximitzarà. Això ens porta a haver d'escollir qualsevol tecnologia basada en IEEE 802.15.4 (habitualment ZigBee/PRO, ja que les seves ràdios emeten típicament amb 1 mW de potència), BLE, DASH7, Z-Wave, ANT o RFID. Això suposa que les taxes de transmissió quedaran força limitades (des dels 40 Kbps típics de Z-Wave fins a 1 Mbps d'ANT, passant pels 200 Kbps de DASH7, 250 Kbps de ZigBee o 260 Kbps de BLE). És per això que les tecnologies de xarxes sense fils de baix consum són també sempre de baixa taxa de dades i per això s'anomenen LR-WPANs (*Low-Rate Wireless Personal Area Network*), donat que la distància típica entre nodes -sense fer salts- acostuma a ser d'uns 75-100 metres, tot i que es poden arribar a distàncies de fins a 1 Km en entorns exteriors amb línia de visió o, lògicament, fent servir la tècnica de salts entre nodes per tal de reenviar les dades més enllà i així cobrir distàncies més llarges.

D'entre la llista curta (*shortlist*) de tecnologies anteriors, potser DASH7 sembla una de les més interessants, sinó la que més, ja que permet distàncies de fins a 10 Km en exteriors, penetra molt bé els murs, la pluja i altres obstacles, té una taxa de 200 Kbps –suficient per a monitoratge i sensorització, no treballa en la banda saturada de 2.4 GHz, fa servir únicament 1 mW de potència máxima i permet una gran precisió en la localització dels nodes. Això explicaria per què es la tecnologia que es fa servir per a ús militar/defensa USA i l'UE.

No obstant això, potser el major inconvenient de DASH7 és que es tracta d'una tecnologia encara potser massa jove, amb projectes de codi obert no madurs del tot, amb una comunitat de desenvolupament limitada (deixant de banda el projecte OpenTag) i que no disposa de tanta documentació com IEEE 802.15.4. Aquest darrer estàndard, implementat juntament amb 6LowPAN (adaptació d'IPv6 per a LR-WPANs), RPL (protocol d'encaminament) i CoAP (i altres protocols de nivell 7) és una aposta guanyadora, ja que es poden crear xarxes sense fils de manera ràpida i amb molt baix cost (per exemple fent servir un SoC com ara el TI CC2538, que té un preu unitari d'uns 8 EUR o 4 EUR si es compra per volum) i, a més, es pot accedir a tots els protocols propis d'IP (TCP, UDP, DHCP, HTTP, ICMP, etc.), disposant de plataformes de programari gratuïtes, com ara els sistemes operatius Contiki, TinyOS, etc. A més, el *duty cycle* que es pot aconseguir amb xarxes basades en IEEE 802.15.4e és típicament de 0.1% o menys.

Per aquesta raó, es decideix que, de cara al proper capítol, s'estudiarà l'estàndard 802.15.4e.

3. Estàndard IEEE 802.15.4

Com ja s'ha comentat en el capítol anterior, l'IEEE 802.15.4 és un estàndard per a la creació de xarxes sense fils que necessitin d'una baixa taxa de dades (també anomenades LR-WPANs); concretament, l'estàndard defineix les capes física (PHY) i de control d'accés al medi (MAC) del model OSI. Aquest estàndard el manté el grup de treball (*Working Grup* o WG) IEEE 802.15 i va ser definit per primer cop l'any 2003. Avui dia, l'IEEE 802.15.4 és la base de diverses especificacions de xarxes sense fils, entre elles ZigBee, ISA-100.11a, RF4CE (*Radio Frequency for Consumer Electronics*), MiWi i WirelessHart, ja explicades també en el capítol anterior, i que "extenen" l'estàndard original mitjançant el desenvolupament de capes superiors, no definides al propi IEEE 802.15.4. A més i, tal i com es veurà més endavant en aquest mateix capítol, IEEE 802.15.4 també es pot fer servir amb 6LowPAN, que és un protocol que permet integrar/traduir IPv6 en xarxes 802.15.4. A més, es poden fer servir altres protocols com ara RPL (encaminament de paquets IPv6) i CoAP (protocol d'aplicació amb suport de transaccions).

L'objectiu d'IEEE 802.15.4 és el d'oferir les capes baixes de xarxa per a la creació de WPANs focalitzades en un baix cost, baix consum i baixa velocitat, amb dispositius propers entre ells, on no es necessiti cap altra infraestructura (per exemple, estacions base) o aquesta sigui la mínima possible, fent que el consum de potència i el cost sigui tot el baix que es pugui. Això fa que els camps d'aplicació siguin molt variats: xarxes vehiculares, xarxes industrials, jocs interactius, mesurament remot, etc.

El mode de treball bàsic de l'estàndard permet un rang de cobertura entre nodes de 10 metres i una taxa de transferència de 250 Kbps. Les bandes de freqüència que es poden fer servir són tres: 868 Mhz, 915 MHz i 2.45 GHz. Com a mode d'accés al medi, es preveuen mecanismes CSMA/CA per evitar col·lisions, així com reserva de ranures de temps garantizades.

Els propers apartats d'aquest capítol estan dirigits a mostrar les particularitats tècniques de l'estàndard tant a nivell PHY com MAC, així com els mecanismes i protocols d'encaminament típics (capa de xarxa) i per últim els protocols de capa d'aplicació (bassats en missatges o en serveis) que s'utilitzen habitualment per a la comunicació en LLNs. Eventualment, es realitza un recorregut per les plataformes de maquinari (mòduls de sensorització) i programari (sistemes operatius) més utilitzades avui dia per a la implementació d'aquest tipus de xarxes.

3.1. Capes física i d'enllaç

3.1.1. IEEE 802.15.4-2011

3.1.1.1. Capa PHY i subcapa MAC

La capa física (PHY) és la capa inicial/més baixa en el model de referència OSI. Aquesta capa proporciona el servei de transmissió de dades, així com la interfície a l'entitat de gestió de capa física, que ofereix accés a cada funció de gestió de la capa; també manté una base de dades amb informació de xarxes d'àrea personal relacionades.

Per tant, es pot dir que la capa PHY gestiona el transceptor RF físic ('ràdio') i realitza les funcions de selecció de canal, així com gestió del senyal i l'energia.

Per la seva banda, la capa de control d'accés al medi (MAC) habilita la transmissió de trames MAC fent ús del canal físic. A més del servei de dades, també ofereix una gestió de la interfície i gestiona l'accés al canal físic i a les balises de xarxa (*beacons*, en anglès). Controla, a més, la validació de trames, garantitza les ranures temporals i manega l'associació de nodes. Per últim, també ofereis serveis de seguretat.

De l'estàndard IEEE 802.15.4 existeixen tres "grans" versions: l'original de l'any 2003, una revisió posterior del 2006 i encara una altra del 2011. Cadascuna té les seves particularitats:

- IEEE 802.15.4-2003: es tracta de la versió inicial, que proporciona dues capes PHY diferents, una per a les bandes de freqüències baixes de 868 i 915 MHz i una altra per a la banda de 2.4 GHz. Totes dues capes fan servir l'esquema de modulació DSSS (explicat en el capítol anterior). En les bandes baixes les taxes de dades poden ser de 20 o 40 Kbps mentre que en la banda de 2.45 GHz el *throughput* és de 250 Kbps.

- IEEE 802.15.4-2006: aquesta *release* actualitza la PHY per a les bandes de 868 i 915 MHz, proporcionant una millora en la taxa de dades que es pot aconseguir en aquestes (100 i 250 Kbps). També es defineixen nous esquemes de modulació (tres per a les bandes baixes i un per a la banda de 2.4 GHz), definint en total quatre PHY, en funció de la modulació que es faci servir. Tres d'aquestes modulacions es basen en DSSS i l'altra en ASK. En el cas de les modulacions DSSS, es pot fer servir bé BPSK o O-QPSK en les bandes baixes i únicament O-QPSK en la banda de 2.4 GHz. Per altra banda, es suporta el canvi dinàmic entre les PHYs 868/915 MHz.

  Més tard, el 2007 es va publicar l'IEEE 802.15.4a, que augmenta les PHYs de quatre a sis, amb la inclusió de DS-UWB (*Direct Sequence - Ultra Wide Band*) i CSS (*Chrip Spread Spectrum*): la primera (UWB), fent servir els rangs de menys de 1 GHz, 3-5 GHz i 6-10 GHz, mentre que la segona (CSS), fent servir el rang 2.4 GHz.

  Posteriorment, l'any 2009 es publiquen les revisions 802.15.4c i 802.15.4d que agumenten encar més les PHYs: 780 MHz (utilitzant O-QPSK o MPSK) per a la Xina i 950 MHz (utilitzant GFSK o BPSK) per al Japó. A més, s'actualitzen les PHYs ja existents.

- IEEE 802.15.4-2011: aquesta tercera gran versió inclou bàsicament l'IEEE 802.15.4-2006 més les revisions 4a, 4c i 4d. També es fa la diferenciació entre MAC i Seguretat en tres parts: protocol MAC, serveis MAC i Seguretat.

Pel que fa als canals disponibles en cada banda de freqüència, tenim:

- Banda 868-868.6 MHz (centrada als 868.3 MHz): únicament hi ha un canal disponible (Canal 0), amb una taxa de dades de 20 Kbps. Aquesta banda es fa servir a Europa.

- Banda 902-928 MHz: aquí hi ha 10 canals disponibles (Canal 1, .., Canal 10), amb una taxa de dades de 40 Kbps. Els canals no es solapen entre sí i tenen una separació de 2 MHz. Aquesta banda es fa servir a USA.

- Banda 2.4-2.483 GHz: en aquesta banda hi ha 16 canals disponibles (Canal 11, .., Canal 26), amb una taxa de dades de 250 Kbps. Els canals no es solapen entre sí i tenen una separació de 5 MHz. Aquesta banda és global (es fa servir a tot el món).

Per a més informació sobre les capes PHY/MAC de 802.15.4, veure l'Annex XXV.

3.1.1.2. Model de xarxa

L'estàndard IEEE 802.15.4 defineix dos tipus de nodes/dispositius, cadascú d'ells poden adoptar rols diferents:

- FFD (*Full-Function Device* o Dispositiu de Funció Completa): aquest dispositiu por funcionar tant com a coordinador de la PAN (*Personal Area Network*), com a coordinador genèric/encaminador o com a un simple node comú (en el darrer cas s'anomena informalment "mota" o "dispositiu final"). En concret, aquest tipus de dispositiu implementa un mode general de comunicació que permet parlar amb qualsevol altre node; a més, també pot reenviar missatges provinents d'altres nodes, actuant llavors amb un rol de coordinador (encaminador); fins i tot, pot fer també de coordinador de la PAN, quan es troba a càrrec de tota una xarxa (vindria a ser el dispositiu "mestre" de la mateixa).

- RFD (*Reduced-Function Devices* o Dispositiu de Funció Reduïda): són dispositius extremedament simples amb requeriments de recursos i comunicació molt limitats. Per aquesta raó, únicament poden comunicar amb dispositius que tinguin rol FFD però mai actuar com a coordinadors (no poden tenir aquest rol).

Pel que fa a les topologies permeses, únicament n'hi ha dues: punt a punt (P2P) i estrella. En qualsevol dels dos casos es necessitarà sempre un coordinador PAN. Cada dispositiu s'identifica amb un codi únic "llarg" –extès- de 64 bits o bé un codi "curt" de 16 bits (aquest darrer únicament en entorns restringits, és a dir, quan la comunicació és entre dispositius dins d'un mateix domini PAN).

- En el cas de les xarxes P2P, aquestes poden formar patrons de connexió arbitraris i la seva extensió està limitada únicament per la distància entre cada parell de nodes. Aquesta topologia és la base de les xarxes *ad hoc*, capaces de auto-organitzarse i auto-gestionar-se. Donat que l'estàndard no defineix la capa de xarxa, la funció d'encaminament (*routing*) no està suportada de manera directa encara que mitjançant capes adicionals es pot suportar comunicacions multisalt. Per altra banda, l'estàndard també menciona l'estructura d'arbre d'agrupació (*cluster tree*) on un RFD pot associar-se únicament amb un FFD al mateix temps, per formar una xarxa on els RFDs poden ser únicament fulles d'un arbre i la major part dels nodes són FFDs. A més, aquesta darrera estructura pot extendre's com una xarxa de malla genèrica, on els nodes són

xarxes d'arbres d'agrupació, amb un coordinador local per cada agrupació o *cluster*, a més d'un coordinador global.

- Pel seu cantó, també és possible la topologia d'estrella, on el coordinador de la xarxa ha de ser necessàriament el node central. Una xarxa d'aquest tipus es pot originar quan un FFD decideix crear la seva pròpia PAN i declarar-se ell mateix com a coordinador, després d'escollir un identificador de PAN únic. Un cop fet d'això, altres dispositius poden associar-se a la xarxa, que seria completament independent de la resta de xarxes d'estrella.

A la figura de sota es mostra un exemple de xarxa amb topologia d'estrella i amb topologia punt a punt, on s'aprecien els rols de coordinador de la PAN, FFD i RFD:

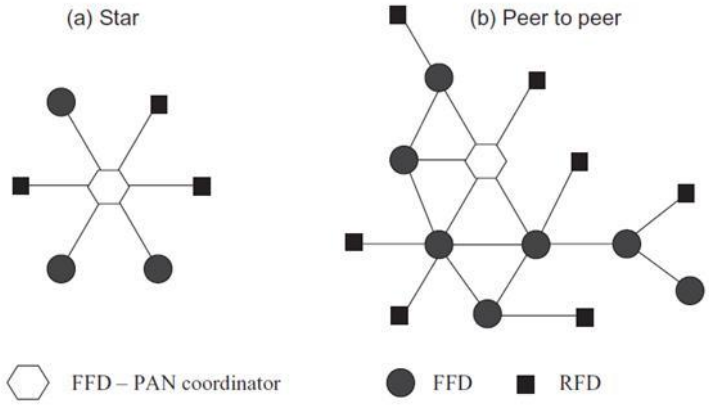


Figura 5. Topologies de xarxa amb IEEE 802.15.4 [12].

3.1.1.3. Arquitectura de transport de dades

Amb IEEE 802.15.4, les trames són la unitat bàsica de transport de dades. Hi ha quatre tipus de trames possibles, que proporcionen bon equilibri entre simplicitat i robustesa:

- Dades: són les trames que porten les dades d'usuari.

- Reconeixement (*acknowledgment*): trames per a reconeixement d'una transmissió de dades correcta (únicament s'envien si es demanen prèviament).

- Balisa (*beacon*): trames retransmeses per un coordinador per tal d'organitzar la xarxa.

- Trames de comandes MAC: es fan servir per a tasques d'associació, desassociació, petició de dades o balises, notificació de conflictes, etc.

Per altra banda, com a mètode de control d'accés al canal tenim CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*). Aquesta tècnica permet l'accés múltiple a la xarxa mitjançant el sensat de portadora. Bàsicament, el funcionament és el següent: el node que vol emetre, primer escolta el canal per veure si està lliure i únicament si ho està, comença a transmetre, després d'haver deixat passar un temps aleatori adicional (aques temps es defineix fent servir un algorisme anomenat *random exponential backoff* o retrocés aleatori exponencial). Posteriorment, el node receptor ha d'enviar un paquet d'ACK (reconeixement) que ha de rebre l'emissor, confirmant així que el paquet va arribar intacte; si l'ACK no es rep, es pot decidir si intentar la retransmissió del paquet de nou o simplement abortar (encara que, en determinades circumstàncies –per exemple quan s'intenta maximitzar la bateria dels dispositius- es pot decidir ometre els missatges de confirmació i s'assumeix que aquestos es reben sempre correctament; en aquests casos, el que s'acostumen a implementar són xequejos periòdics dels missatges pendents, amb una freqüència configurable segons l'aplicació.

En definitiva, fent servir CSMA/CA, s'intenten evitar col·lisions entre dos o més nodes que podrien transmetre alhora; per exemple, aquesta situació es dóna quan un node és visible per a un punt d'accés però no per a la resta de nodes; a aquesta situació se li anomena "problema del node ocult" i es la que donaria en cas de fer servir CSMA/CD (*CSMA with Collision Detection*) propi de les xarxes Ethernet. Amb CSMA/CA, quan un node inicia la transferència, transmet el paquet de dades complet.

Per a més informació sobre el transport de dades amb 802.15.4, veure l'Annex XXVI.

3.1.1.4. Seguretat

Pel que fa a la seguretat amb IEEE 802.15.4, aquesta és gestionada a la subcapa MAC, per sota del control d'aplicacions. De fet, l'aplicació especifica els requeriments de seguretat necessaris, mitjançant l'establiment dels paràmstres de control adequats dins de la pila ràdio. Si una aplicació no especifica cap paràmetre, llavors no s'habilita cap seguretat per defecte; per tant, les aplicacions han d'especificar, explícitament, que volen habilitar la seguretat i de quin tipus volen que sigui.

Dels quatre tipus de trames 802.15.4, les de reconeixement no soporten seguretat. Per la resta de tipus, es suporta opcionalment també protecció d'integritat i protecció de confidencialitat per al camp de *payload* [61].

802.15.4 especifica una sèrie de *Security Suites* (jocs de seguretat) que defineixen el tipus de protecció que es proporciona a les dades transmeses. Cada *suite* ofereix un conjunt de propietats de seguretat i garanties diferents, així com differents formats de paquets. En total, es defineixen vuit jocs de seguretat, que a grans trets es defineixen en tres grups: sense seguretat, únicament encriptació (AES-CTR), únicament autenticació (AES-CBC-MAC), encriptació i autenticació (AES-CCM). Recordem que l'ús d'aquestes *suites* ha de ser especificat per les capes superiors (aplicacions):

Suite de seguretat	Tècnica	Descripció
Null	-	Sense seguretat (per defecte).
AES-CTR	Encriptació (*Advanced Encryption Algorithm – Counter Mode*).	Encriptació CTR. Aporta confidencialitat i *freshness*.
AES-CBC-MAC-128 AES-CBC-MAC-64 AES-CBC-MAC-32	Autenticació (*Advanced Encryption Algorithm - Cipher Block Chaining Message Authentication Code*)	Autenticació 128 bit MAC, 64 bit MAC o 32 bit MAC Aporta integritat.
AES-CCM-128 AES-CCM-64 AES-CCM-32	Encriptació + Autenticació	Encriptació + 32/64/128 bits MAC Aporta integritat, confidencialitat i *freshness*.

Taula 4. Opcions de seguretat amb IEEE 802.15.4 [49].

Per tant, tenim que la securetat la proporciona la subcapa MAC però són les aplicacions les que decideixen quin joc de seguretat utilitzar: sense seguretat, encriptació, autenticació o ambdues darreres. En el mode insegur, únicament es fan servir llistes de control d'accés (ACLs) que permeten decidir si s'accepta una trama o no, en funció del seu origen (aquesta tècnica és intrínsecament insegura ja que l'adreça d'origen es pot falsificar fàcilment). Per la seva banda, les *suites* que inclouen encriptació també aporten una característica anomenada *freshness* (frescor) que bàsicament es basa en realitzar revisions entre recepcions successives per assegurar que trames presumiblement antigues o dades que no es consideren ja vàlides puguin "passar" a les capes superiors.

3.1.2. IEEE 802.15.4e-2012

L'IEEE 802.15.4e-2012 és una esmena –revisió- de la subcapa MAC de l'IEEE 802.15.4. En principi, havia de tractar-se d'una esmena a la revisió IEEE 802.15.4-2006, amb la intenció d'oferir un millor suport per a mercats industrials i de permetre compatibilitat amb les modificacions proposades per a les WPANs xineses. Finalment, però, es tracta d'una revisió de l'IEEE 802.15.4-2011 i també inclous canvis per abordar les necessitats de les aplicacions proposades pels grups de treball TG4f (nova capa PHY i millores a la subcapa MAC per suportar sistemes RFID actius bidireccionals i aplicacions de determinació de la posició; inclou les bandes UWB, 2.4 GHz i 433 MHz) i TG4g (esmena PHY per proporcionar un estàndard que faciliti aplicacions de control de processos a molt gran escala –*smart neighbour networks*- com per exemple xarxes *smart grid* per a la industria energètica; inclou la banda 902-928 MHz). Alguns d'aquests canvis ja van ser aprovats durant l'any 2011 tot i que la revisió va ser publicada l'any 2012.

Específicament, la revisió 4e inclou, entre d'altres, la possibilitat de salt de canal (*channel hopping*), així com ranures de temps variable (*variable time slot*), que són compatibles amb l'estàndard i aplicacions ISA-100.11a. L'opció de salt de canal potencia el suport pels mercats industrials, ja que millora la robustesa contra interferències externes i dismueix l'esvaniment multicamí persistent (*multi-path fading*, en anglès) [13].

3.1.2.1. Subcapa MAC

El format de trama (subcapa MAC) amb l'IEEE 802.15.4 és una mica diferent al del 802.15.4 original. A la figura de sota es pot veure l'estructura de trama en aquesta nova versió:

<table>
<tr><td>Octets:
1/2</td><td>0/1</td><td>0/2</td><td>0/1/2/8</td><td>0/2</td><td>0/1/2/8</td><td>0/1/5/6/10/14</td><td colspan="2">variable</td><td>variable</td><td>2</td></tr>
<tr><td rowspan="2">Frame Control</td><td rowspan="2">Sequence Number</td><td>Destination PAN Identifier</td><td>Destination Address</td><td>Source PAN Identifier</td><td>Source Address</td><td rowspan="2">Auxiliary Security Header</td><td colspan="2">Information Elements</td><td rowspan="2">Frame Payload</td><td rowspan="2">FCS</td></tr>
<tr><td colspan="4">Addressing fields</td><td>Header IEs</td><td>Payload IEs</td></tr>
<tr><td colspan="7">MHR</td><td colspan="2">MAC Payload</td><td>MFR</td></tr>
</table>

Figura 6. Format de trama MAC amb IEEE 802.15.4

Per a més informació sobre la Subcapa AMC d'IEEE 802.15.4e, veure l'Annex XXVII.

3.1.2.2. Funcionalitats

Pel que fa a les funcionalitats incloses ala versió IEEE 802.15.4e, aquestes són:

- Mode d'extensió multi-canal determinista i síncron (*Deterministic & Synchronous Multichannel Extension* - DSME): aquest mode proporciona suport per a aplicacions industrials i comercials que necessiten latència determinista i fiabilitat d'enllaç més alta, alta disponibilitat, escalabilitat i robustesa.

  Les xarxes amb DSME funcionen amb balises, on tots els dispositius sincronitzen una "multi-supertrama" a través de trames balisa. Aquesta multi-supertrama resulta de l'agrupació de vàries supertrames i estén l'operació des d'un sol canal durant el període lliure de contenció (CFP) a una operació multi-canal, bé mitjançant la commutació o el salt entre canals. En aquest mode, un parell de nodes es desperten a les seves ranures GTS (*Guaranteed Time Slots*) reservades i llavors intercanvien trames de dades i trames ACK.

- Mode de salt de canal per ranures temporals (*Time-Slotted Channel Hopping* - TCSH): mode especialment adient per a aplicacions d'automatització de processos i, en particular, per al monitoratge de processos. El mode d'operació és el següent: tot els dispositius dintre d'una mateixa xarxa tenen *slotframes* sincronitzats, on les ranures temporals estan contingudes dintre d'un cicle d'*slotframe* i les ranures es repeteixen cada període d'*slotframe*. Llavors, la comunicació node a node dintre d'una ranura inclou un paquet TX/RX i un ACK TX/RX. Aquest mode està explicat amb més detall a apartats següents.

- Mode de xarxa determinista de baixa latència (*Low Latency Deterministic Network* – LLDN): aquest mode suporta automatització de fàbriques i de processos (per exemple robots per a la fabricació d'automòbils, maquinària per donar la volta a peces, grues, etc). S'utilitzen balises i ranures de temps assignades per proporcionar determinisme. És un mode dissenyat per a xarxes i trames petites. Es produeix una reducció substancial de la sobrecàrrega MAC que permeten supertrames molt petites i, per tant, latències molt baixes. Inclou una funció *Group ACK* que redueix les necessitats d'ample de banda.

- Formats de trama adicionals: aquests formats són necessaris per a LLNs. S'afegeix una trama multipropòsit que, entre d'altres, serveix per a dispositius únicament transmissors (descrits pel TG4f), habilita un mode de baixa energia (LE), redueix la sobrecàrrega MAC fins a únicament 4 bytes i proporciona configurabilitat i extensibilitat.

- Baixa energia (LE): es tracta d'una tecnologia que permet als dispositius operar amb cicles de treball de menys d'un 1% i s'aconsegueix fent servir les tècniques CSL i RIT (explicades als apartats següents). Amb LE s'aconsegueixen xarxes de sensors IP on es crea la il·lusió de que estan sempre actives però aconseguint al mateix temps una baixa latència, capacitat de multidifusió i ACKs síncrons.

- Elements d'informació (IE): els *Information Elements* són mètodes d'encapsulació de la informació, que també es fan servir al TG4f i TG4g. A grans trets, es tracta de contenidors d'informació simples, flexibles i extensibles, que permeten afegir informació al format de trama existent sense haver de definir-ne un de nou; aquesta informació pot estar relacionada amb la sincronització, estata de la xarxa, etc.

  El format general d'un IE conté un camp identificador (ID), un camp de longitud i un camp de contingut. Els IEs s'encapsulen dins de les trames IEEE 802.15.4e, amb la seva capçalera a l'MHR (*MAC Header*) i el sey *payload* al *MAC Payload*. La capçalera té un camp per indicar la longitud del camp de contingut, un identificador únic i un camp *Type* que permet identificar el tipus d'IE. El contingut d'un IE és molt variable, donat que cada mode de funcionament o funcionalitat (DSME, TSCH, LLDN, CSL, RIT, etc.) té definits els seus propis IEs específics.

  A la figura de sota es pot apreciar el format de capçalera d'un IE:

Bit: 0-6	7–14	15	Octets: 0 … 127
Length	Element ID	Type = 0	IE Content

Figura 7. Format de capçalera d'un IE

Els espais d'identificadors (IDs) dels IEs poden ser gestionats o no gestionats, la qual cosa afegeix flexibilitat al sistema.

- Balises millorades (EB) i peticions de balisa millorades (EBR): les balises millorades (*Enhanced Beacon*) són extensions basades en l'IEEE 802.11 que proporcionen una major flexibilitat en contingut que les balises de l'estàndard 802.15.4. En concret, les BEs permeten transportar informació adicional a les balises (IEs). Per diferenciar una balisa normal d'una EB es fa servir el camp *Version* de la trama (si el valor d'aquest camp és '0b10' llavors es tracta d'una EB).

  Per altra banda, els EBR (*Enhanced Beacon Request*) es diferencien dels BR (*Beacon Requests*) normals també pel camp *Version*. Els EBR es fan servir per sol·licitar EBs i permeten especificar certs filtres en la resposta, de tal manera que únicament s'enviï en l'EB la informació demanada per l'EBR; d'aquesta manera, es redueix la mida de la trama enviada.

  A la figura de sota es pot veure el format de trama d'un EB:

<table>
<tr><td>Octets: 1/2</td><td>0/1</td><td>variable</td><td>0/1/5/6/10/14</td><td colspan="2">variable</td><td>variable</td><td>2</td></tr>
<tr><td rowspan="2">Frame Control</td><td rowspan="2">Sequence Number</td><td rowspan="2">Addressing fields</td><td rowspan="2">Auxiliary Security Header</td><td colspan="2">Information Elements</td><td rowspan="2">Beacon Payload</td><td rowspan="2">FCS</td></tr>
<tr><td>Header IEs</td><td>Payload IEs</td></tr>
<tr><td colspan="4">MHR</td><td colspan="2">MAC payload</td><td>MFR</td></tr>
</table>

Figura 8. Format de trama d'un BE

Com es pot apreciar, l'MHR conté un camp específic per als IEs (*Header IEs*) i, al seu voltant, el *MAC Payload* també té un camp específic per als mateixos (*Payload IEs*).

- Altres millores: bàsicament es poden resumir en les següents:

  - Associació ràpida: mode que permet a un dispositiu enviar una resposta d'associació en una comunicació directa, eliminant el retad en l'ordre de resposta d'associació que hi ha en una comunicació indirecta normal.

  - Mètriques de xarxa: s'afegeixen atributs relatius a la transmissió (*macRetryCount*,*macMultipleRetryCount*,*macTXFailCount*,*macTXSuccessCount*) i recepció (*macFCSErrorCount*, *macSecurityFailure*, *macDuplicateFrameCount*, *macRXSuccessCount*) de trames de dades.

  - ACKs millorats: els ACKs poden ser assegurats (*securized*), poden incloure *payloads* i configurar un retard que permeti als dispositius el temps suficients per a desencriptar les dades, etc.

- Diversitat de canal: proporciona suport per a salt de canal a través d'una seqüència de salt PIB (*PAN Information Base*) i una seqüència de salt per defecte.

Amb totes aquestes millores s'ha aconseguit que, avui dia, algunes de les solucions de xarxa basades en IEEE 802.15.4e permetin nodes que únicament consumeixen uns 10µA de current mitjà, amb una taxa d'entrega de paquets extrem a extrem per sobre del 99,999% [13].

És important destacar que, tot i que 802.15.4e defineix els mecanismes que permeten a un node comunicar-se amb altres nodes fent servir les funcionalitats abans enumerades (per exemple TSCH), no defineix, en canvi, cap funcionalitat pròpia de les capes superiors, fora del que és la capa PHY i subcapa MAC. Per tant, no es defineixen, entre d'altres: polítiques per construir i mantenir una programació de la comunicacio; com aparellar aquesta programació amb els camins multi-salt mantinguts pel protocol d'encaminament (per exemple RPL); com adaptar els recursos assignats entre nodes veïns a fluxes de tràfic; com fer complir un tractament diferenciat per a dades generades per la capa d'aplicació (polítiques de qualitat de servei - QoS); missatges de senyalització necessaris per al protocol 6LoWPAN o PRL per poder descobrir veïns; com reaccionar a canvis de topologia; autoconfiguració d'adreces IP; etc.

En els següents apartats es descriuen les tècniques de TSCH, CSL i RIT, que permeten a les motes 802.15.4e obtenir una major fiablitat/taxa d'entrega de paquets (TSCH) i un menor consum d'energia (CLS, RIT), respectivament.

3.1.2.3. TSCH (*Time-Slotted Channel Hopping*)

La tècnica de TSCH (salt de canal per ranura temporal) permet als dispositius IEEE 802.15.4 suportar un ampli ventall d'aplicacions industrials, tal i com ja s'ha comentat abans (els requeriments d'encaminament per a aquest tipus d'aplicacions, fent servir LLNs, es troba definit a l'RFC 5673). A grans trets, aquesta tècnica d'accés al medi es basa en tenir els nodes sincronitzats entre ells a nivell temporal, situació que permet un consum ultra-baix d'energia; per altra banda, el salt de canal –canvi de freqüència d'operació- permet augmentar la fiabilitat. Per tant, es pot entendre que 802.15.4e supossa un redisseny del protocol MAC original 802.15.4, més que no pas una millora. Per altra banda, TSCH no canvia res de la capa PHY original. Aquesta tècnica de salt de canal també es fa servir en altres estàndars com ara Bluetooth LE i WirelessHART [25].

El mode TSCH prové del TSMP (*Time Synchronized Mesh Protocol* – Protocol de Malla de Temps Sincronitzat), on l'espai temporal es divideix en una sèrie infinita –nombre infinit- de ranures discretes, on cada node de la xarxa manté un registre sincronitzat de les ranures que ja han transcorregut. En concret, amb TSCH, els nodes es sincronitzen per *slotframes* periòdics, on cada *slotframe* està compost per un nombre determinat de ranures temporals (*timeslots*); cada *slotframe* correspon a un cicle *k*. Fent servir el valor de *k* com a únic *input* –valor d'entrada- d'una equació coneguda per tots els nodes, es pot calcular el canal d'operació a cada ranura temporal –és a dir, per a un moment donat.

D'aquesta manera, la comunicació es porta a terme de manera "aleatòria", fent servir canals "aleatoris", reduïnt així la influència de possibles interferències externes, així com l'esvaniment multicamí, donat que el risc d'aquestes amenaces es reparteix entre tots els canals. Això fa que aquesta tècnica sigui especialment útil en WSNs i, en especial, en LLNs, on els nodes estan sotmesos a interferències externes d'altres xarxes (per exemple Wi-Fi) o components com ara motors, forns microones, etc.

A les dues figures de sota [21] es mostra, per un cantó, la representació gràfica d'un *slotframe* (que es podria traduir com "trama de ranures") composat, en aquest cas, per quatre ranures; per altra banda, es mostra la representació d'una ranura temporal (*time slot*):

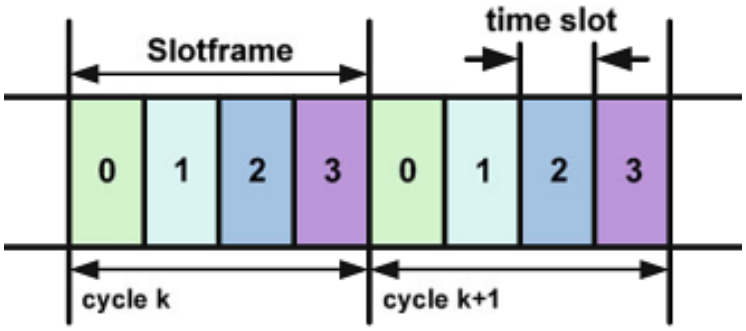


Figura 9. *Slotframe* format per quatre *timeslots*

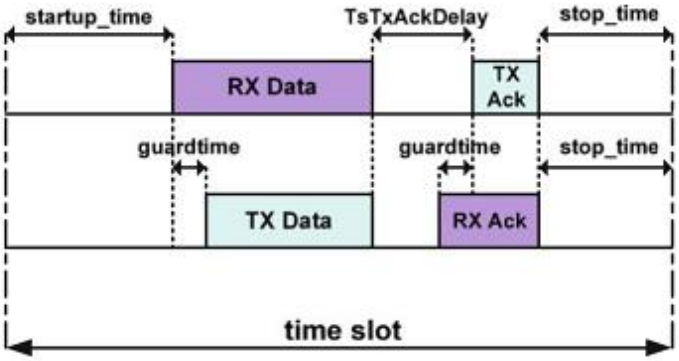


Figura 10. Divisió d'una ranural temporal

Cada ranura temporal o *timeslot*dins d'un *slotframe* té una durada –típicament- de 10 ms i permet a un node emissor enviar una trama de mida màxima (127 byte) i rebre l'ACK corresponent per part del receptor. Si el reconeixement no es rep en un temps predeterminat (període de *timeout*), llavors la retranmissió de la trama queda diferida fins a a la següent ranura assignada a la mateixa parella de nodes emissor-receptor. A la figura de dalt, es pot veure un *slotframe* compost per quatre ranures temporals, on cada *slotframe* porta associat un cicle *k* (*k*, *k*+1, *k*+2, .., *k*+*n*). Els nodes es troben sincronitzats gràcies a que tots ells coneixen el valor del cicle *k* en cada moment.

Per altra banda, a la segona figura es veu com una ranura temporal es divideix en els següents temps:

- En la part del receptor: hi ha un temps inicial de configuració o *startup time*; un temps de recepció de les dades de l'emissor (RX de dades); un temps d'espera o retard fins que s'envia l'ACK a l'emissor; un temps d'enviament de l'ACK; per últim, un temps de parada o *stop time*.

- En la part de l'emissor: hi ha un temps de guarda o *guard time*; un temps de transmissió de dades al receptor; un temps de guarda abans de rebre l'ACK del receptor; temps de recepció de l'ACK; per últim, temps de parada.

Fent servir TSCH, es pot "saltar" entre els 16 canals disponibles (banda de 2.4 GHz), on cada canal queda identificat per la variable *channelOffset*, que és un enter que pot anar del 0 al 15. Una limitació de la tècnica és, per tant, que els 16 canals es fan servir indiscriminadament, quan normalment cada canal acostuma a presentar un nivell d'interferències diferents. Per aquesta raó, una possible millora de la tècnica de TSCH seria, per exemple, ficar certs canals en una llista negra (*blacklist*) amb la finalitat de no ser utilitzats; normalment això es farà quan el canal presenti baixa qualitat (baix valor d'SNR o *ratio* de senyal/soroll). A aquesta millora se li anomena A-TSCH o TSCH adaptatiu. D'aquesta manera, es saltarà únicament entre un subconjunt de canals considerats confiables, en comptes de fer servir tots els 16 canals. Alguns experiments [25] han demostrat que, fent servir A-TSCH, es pot aconseguir un percentatge de millora en el nombre de paquets enviats satisfactòriament de fins el 8.1%.

Com es pot veure, TSCH es focalitza únicament en la capa MAC. De tota manera, aquesta tècnica es pot utilitzar sense problemes amb protocols de capa superior, com per exemple 6LoWPAN (definit a l'RFC6282), RPL (RFC6550) o CoAP (RFC7252).

3.1.2.4. CSL (*Coordinated Sampled Listening*)

L'escolta mostrejada coordinada o CSL es tracta d'una de les tècniques de baixa energia (LE) que, a grans trets, permet als dispositius receptors mostrejar periòdicament el canal per veure si existeixen transmissions entrants, aconseguint d'aquesta manera disminuir el cicle de treball. Dit d'una altra manera: els potencials receptors efectuen, a intervals periódics, sondes d'escolta molt curtes, per veure si algú està transmetent; a més, el període de transmissió queda estés per cobrir l'interval de la sonda.

Aquest mecanisme es fa servir durant el període CAP (*Contention Access Period*), quan es treballa amb balises, i està indicat per a aplicacions que necessiten relativament poca latència (menys d'un segon). CSL va ser dissenyat com a coordinador per tal de transmetre trames de dades pendents a dispositius que es troben "adormit".

Amb CSL, el BI (*Beacon Interval*) és superior a un BI normal; en concret, les trames balisa no s'envien cada BI sinó únicament cada *macLowEnergySuperFrameSyncInterval* (essent el valor d'aquesta variable superior al BI) o bé quan explícitament es demana transmetre una balisa. D'aquesta manera, el *duty cycle* és fins i tot menor que amb l'estàndard 802.15.4 original, on es transmet una balisa per cada BI.

Entrant en detall, el funcionament de CSL es basa en un tipus de trames especial anomedades "trames per despertar" (*wake-up frames*). Aquest tipus de trama són multipropòsit, tenen una mida de 12 bytes, no porten *payload* i contenen un camp anomenat *RZ Time* (Temps de *Rendezvous* - Temps de Cita). A la figura de sota es pot veure el contingut d'una d'aquestes trames:

Octets: 1	1	2	2	4	2
Frame Control	Sequence Number	Dest. PAN ID	Dest. Address	RZ Time Header IE	IE List Terminator

Figura 11. Composició d'una trame multipropòsit *Wake-up*

El camp *RZ Time* inclou la quantitat de temps esperada –en unitats de 10 símbols- entre el final de la transmissió de la trama *wake-up* i el començament de la transmissió del *payload*. Aquest valor de temps és fixat per la capa immediatament superior (NHL - *Next Higher Layer*) quan se li demana transmetre a la subcapa MAC.

A la figura de sota es veu l'esquema temporal d'operació de CSL, tant al costat emissor (*sender*) com receptor (*receiver*):

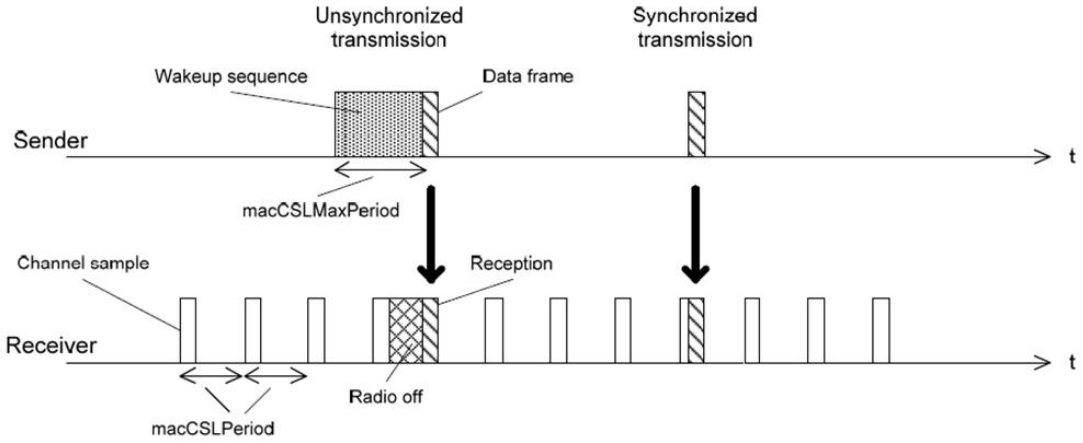


Figura 12. Principi d'operació de la tècnica CSL.

Com es pot veure, tot comença quan, tenint un emissor i un receptor desincronitzats, l'emissor transmet una *seqüència wake-up*. Aquesta seqüència pot constar de vàries trames *wake-up* seguides (en anglès, *back-to-back frames*). La durada de la seqüència ve determinada pel valor de la variable *macCLSMaxperiod*i, al igual que l'*RZ Time*, també es defineix en unitats de 10 símbols; quan *macCLSMaxperiod* val 0, llavors es deixa d'enviar la seqüència (per exemple, quan l'NHL així ho demana perquè emissor i receptor estan sincronitzats). Un cop termina la seqüència, l'emissor comença a enviar la trama de dades d'usuari. Per altre cantó, la darrera trama *wake-up* de la seqüència tindrà el valor de *RZ Time* a zero.

Per la seva banda, al costat del receptor, tenim que aquest va samplejant (escoltant) el canal periòdicament, amb un interval entre escoltes definit per la variable *macCSLPeriod* (quan val 0, significa que el receptor està escoltant tota l'estona; és a dir, que CLS està desactivat). Llavors, durant una d'aquestes sondes per escoltar el canal, es rep una de les trames de *wake-up* de la sequència enviada per l'emissor. Això fa que s'activi la ràdio del receptor en el temps determinat per *RZ Time* i llavors, ara ja sincronitzats, l'emissor envia el *payload* i el receptor el rep al mateix temps.

Els avantatges de fer servir CSL són diversos:

- Dóna la il·lusió de que els nodes estan sempre actius (amb la ràdio encesa),
- És un mètode adient per a comunicació asíncrona i dirigida a events,
- És valid per IP,
- És adient per a nodes en mobilitat i per a descobriment de nodes,
- És *stateless* (no es requereix sincronització prèvia, ni horària ni d'estat),
- Presenta un bon compromís entre latència i energia consumida, quan la comunicació és infreqüent,
- Es poden aplicar altres tècniques de l'LE (baixa energia) per sobre de CSL.

3.1.2.5. RIT (*Receiver Initiated Transmission*)

La tècnica de RIT (Transmissió Iniciada pel Receptor) és una alternativa LE a CSL, quan no es fa servir el mode amb balises (*Beacon Order* = 15). Això significa que CSL i RIT no es poden fer servir al mateix temps. A grans trets, el que fa és permetre a un dispositiu demanar dades als seus dispositius veïns (tant emissor com receptor han de suportar el mode RIT). Únicament es pot utilitzar en FFDs (dispositius de funció completa).

Entrant en detall, el funcionament de RIT és el següent: el receptor emet, periòdicament, trames de petició de dades (*RIT Data Rquest o DataReq*) i llavors escolta, per un petit període de temps, possibles transmissions entrants. El període que el receptor escolta després de la petició de dades ve definit per la variable *macRITDataWaitDuration* mentre que la petició dades s'envia cada *macRITPeriod*. Per la seva banda, l'emissor espera fins que rep una trama DataReq i llavors transmet immediatament el *payload*.

A la figura següent es pot veure un diagrama temporal del funcionament d'aquesta tècnica:

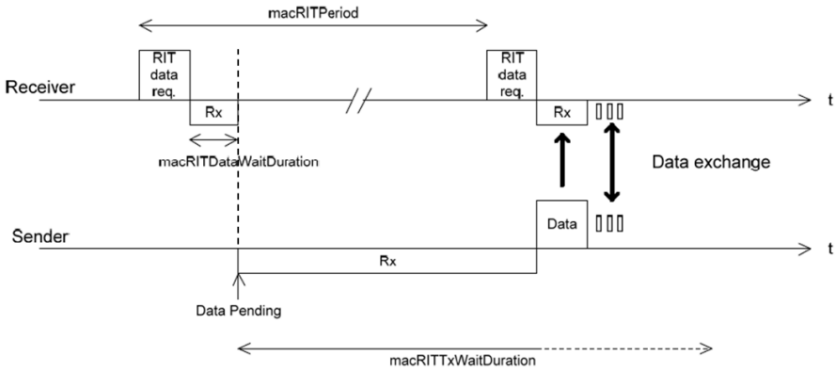


Figura 13. Principi d'operació de la tècnica RIT.

Com et pot apreciar, al costat del receptor, tenim que aquest fa una difusió d'una trama *RIT DataReq*i llavors escolta durant un interval *macRITDataWaitDuration*. Durant aquest temps, la ràdio de l'emissor està apagada i, per tant, no pot escoltar la petició del receptor, per la qual cosa no envia cap dada. Llavors, el receptor continua enviant trames *DataReq* periòdicament fins que, en una d'elles, la ràdio de l'emissor es troba encesa, per la qual cosa rep la trama i comença a enviar les dades immediatament.

Per la seva banda, amb RIT també es pot configurar una programació de les escoltes, mitjançant la incorporació, a la trama *DataReq*, de dos valors que indiquen el nombre de vegades que el receptor ha d'escoltar un cop s'ha enviat la trama, així com l'interval de temps que ha de psassar entre cada cop que s'escolta. Aquests valors s'anomenen, respectivament, *Number of Repeat* (N) i *Repeat Listen Interval (T*) i es poden afegir al *payload* opcional de la capa MAC. A la figura de sota queda exemplificada aquesta opció:

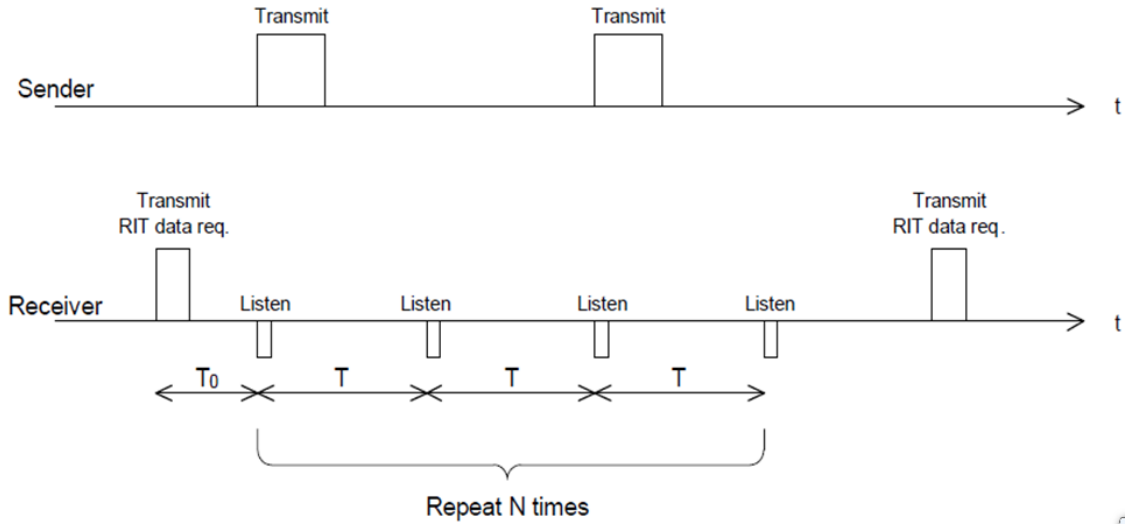


Figura 14. RIT quan *DataReq* incorpora programació d'escoltes.

Podem concloure que, tot i que la capa de protocol MAC original (IEEE 802.15.4) ja proporcionava una eficiència de potència bastant bona, els mecanismes CSL i RIT de la versió 802.15.4e milloren aquesta eficiència, per aquelles aplicacions que necessiten uns cicles de treball encara més baixos, tant en LLNs funcionant amb balises com sense elles.

En resum, podem dir que 802.15.4e transforma l'IEE 805.15.4 original en un estàndard més fàcil de "llegir" i més extensible, amb millores substancials com ara DSME, TSCH, CSL i RIT que permeten xarxes gestionades, amb un comportament determinístic, que poden acomodar un nombre de dispositius més gran i gestionar millor comportaments de xarxa. Per últim, les tècniques adicionals per a *Low Energy* permeten augmentar la vida de les bateries i millorar els temps de resposta.

3.1.2.6. Possibles millores

A l'Annex XXVIII s'exposen un parell de propostes de millora adicionals per tal d'augmentar la vida útil dels nodes, mitjançant la reducció del consum d'energia del mateixos. Aquestes proposes es poden enmarcar dins de les capes PHY/MAC de 802.15.4 i 802.15.4e.

3.2. Capa de xarxa

3.2.1. 6LoWPAN

6LoWPAN és l'acrònim d'IPv6 per a Xarxes Sense Fils d'Àrea Personal i de Baix Consum (*IPv6 over Low Power Wireless Personal Area Networks*). Es tracta del nom d'un grup de treball de l'IETF (*Internet Engineering Task Force*). El concepte de 6LoWPAN es va originar de l'idea de que el protocol Internet hauria de poder aplicar-se fins i tot als dispositius més petits i aquells que requereixen poc consum d'energia i que tenen capacitats de processament limitades, per tal de que puguin ser ser partíceps de l'Internet de les Coses.

A la pràctica, 6LoWPAN es tracta d'una capa d'adaptació/integració que defineix uns mecanismes d'encapsulació i compressió de capçaleres per pemetre que paquets IPv6 puguin ser enviats i rebuts en xarxes basades en l'IEEE 802.15.4, donat que IP és el protocol més utilitzat avui dia per a xarxes d'àrea local, xarxes metropolitanes i xarxes d'àrea extensa, com ara Internet. En definitiva, el que fa és realitzar un "mapeig" de datagrames entre el protocol IPv6 i les xarxes IEEE 802.15.4 [6].

A més de la compressió, 6LoWPAN també s'encarrega de la fragmentació dels datagrames IPv6 en múltiples trames de capa d'enllaç, per poder acomodar l'MTU (unitat màxima de transmissió) pròpia 802.15.4, com veurem més endavant. Una altra funcionalitat és d'efectuar reenviament de datagrames IPv6 a nivell 2 OSI; per poder fer això, la capa d'adaptació pot portar adreces de nivell d'enllaç als extrems d'un "salt IP" (cada salt de ràdio es considera un salt IP o *IP hop*) [59].

L'especificació original de 6LoWPAN es trobava inicialment a l'RFC4944, que va ser actualitzat més tard per l'RFC6282 (especificacions de com comprimir els datagrames) i l'RFC6775 (optimització del procés de descobriment de veïns). Per la seva banda, tenim RFCs informatius com ara l'RFC4919 (visió de conjunt del que és 6LoWPAN, problemes que afronta i els seus objectius), l'RFC6568 (disseny i espais d'aplicació per a 6LoWPANs) i l'RFC6606 (plantejament del problema i requeriments d'encaminament amb 6LoWPAN).

Per a més informació sobre 6LoWPAN, veure l'Annex XXIX.

3.2.2. Encaminament

Quan es tracta de WSNs (per exemple, MANETs – *Mobile Ad Hoc Networks*) es pot parlar de tres grans "famílies" de protocols d'encaminament [7]:

- Protocols reactius (demanen rutes "sota demanda", únicament quan es necessiten),
- Protocols proactius (també anomenats *table-driven*, amb actualitzacions periódiques de taules de rutes),
- Híbrids (mescla de protocols reactius i proactius).

En qualsevol dels casos, l'objectiu final és aconseguir xarxes que siguin auto-organitzades i que tinguin capacitat de regenerar-se (*self-healing network*, en anglès) en cas de fallades, a més de poder transmetre el paquets a través de múltiples salts.

Dins dels protocols reactius tenim, entre d'altres: AODV, DSR, ABR, DYMO, LOAD, RPL. Pel que fa als protocols proactius tenim, entre d'altres: ORSR, WRP, DSDV, CGSR, ACOR, MultihopLQI, CTP. Per últim, pel que fa als protocols híbrids, tenim com a principals: ZRP i TORA.

A la figura següent es mostra un diagrama amb les famílies esmentades i els protocols més representatius de cadascuna d'elles:

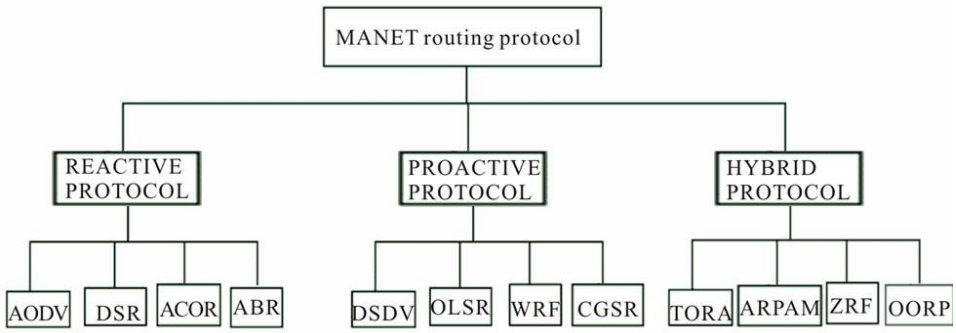


Figura 15. Principals protocols d'encaminament en xarxes sense fils

3.2.2.1. Encaminament reactiu

L'encaminament reactiu o sota-demanda té com a premisa "descobreix únicament quan es necessiti". Aques tipus de protocols tendeixen a reduir la sobrecàrrega de tràfic deguda a missatges de control però a costa de tenir una major latència per a descobrir noves rutes. En aquests protocols, no es distribueix la informació d'encaminament a tota la xarxa sinó que únicament la té el node que la necessita. Aquest tipus d'encaminament, on la informació es consulta de manera selectiva, comporta taules d'encaminament més petites però en canvi necessita un esforç administratiu més gran, degut a que les rutes que encara no s'han utilitzat han de ser determinades en primer lloc. Per tant, aquests protocols poden ser una solució eficient per a aplicacions que no són de missió crítica (no crítiques a nivell de temps).

L'encaminament reactiu escala molt bé amb la mida de la xarxa, fins i tot quan s'utilitzen milers de nodes.

A l'Annex XXX, es descriuen els principals protocols d'encaminament reactiu: AODV, DSR, ABR, DYMO, ACOR i LOAD.

3.2.2.2. Encaminament proactiu

A diferència dels protocols reactius, els proactius es basen en una o vàries taules amb rutes entre parells de nodes, que s'han de mantenir/actualitzar periòdicament, de manera proactiva (no cal que el node origen necessiti/demani la ruta perquè aquesta es trobi a la taula d'encaminament). Això fa que, entre d'altres, la taula pugui contenir rutes innecesàries, que poden no fer falta mai. Per altra banda, es necessita un major ample de banda per transmetre les actualitzacions de rutes.

A l'Annex XXXI, es descriuen els principals protocols d'encaminament proactiu: OSRL, CGSR, WRP, MultihopLQI, HybridLQI, CTP i RPL.

3.2.2.3. Encaminament híbrid

Aquest mètode d'encaminament proporciona un bon balanceig entre els avantatges d'un apropament reactiu i un proactiu, incorporant característiques de tot dos tipus. Acostumen a ser protocols bastant escalables, que proporcionen una latència mitja global més gran que els protocols proactius però més petita que els reactius [26].

A l'Annex XXXII, es descriuen els principals protocols d'encaminament híbrids: ZRP i TORA.

3.2.2.4. Resum

Als Annexos es descriuen tota una sèrie de protocols d'encaminament, que es poden classificar en tres grans famílies o grups: reactius, proactius i híbrids. Per la seva banda, segons el tipus d'encaminament, els protocols poden ser de: Vector Distància, Vector Distància amb Encaminament a l'Origen, Funcions de Cost, Estat d'Enllaç o Enllaç Invertit. En la taula següent es mostra un resum de tots ells, el grup al que pertanyen i el tipus d'encaminament:

Protocol	Família	Tipus
AODV	Reactiu	Vector Distància
DSR	Reactiu	Vector Distància - Encaminament a l'Origen
ABR	Reactiu	Vector Distància - Encaminament a l'Origen
DYMO (AODVv2)	Reactiu	Vector Distància
ACOR	Reactiu	Funcions de cost
LOAD/LOADng	Reactiu	Vector Distància
OSLR	Proactiu	Estat d'Enllaç
DSDV	Proactiu	Vector Distància
CGSR	Proactiu	Vector Distància
WRP	Proactiu	Vector Distància
MultihopLQI	Proactiu	Vector Distància
HybridLQI	Proactiu	Vector Distància
CTP	Proactiu	Vector Distància
RPL	Proactiu	Vector Distància
ZRP	Híbrid	Estat d'Enllaç
TORA	Híbrid	Enllaç Invertit

Taula 5. Protocols d'encaminament per a MANETs i WSNs

Com es pot veure, la gran majoria dels protocols (tant reactius com proactius) pertanyen al tipus Vector Distància, ja sigui amb Encaminament fixat a l'origen o basat en la destinació.

Les característiques principals i els avantatges i inconvenients de cada grup són els següents:

- Protocols reactius
    - Les rutes es creen únicament quan es necesiten, sota demanda. No existeixen rutes predefinides. No hi ha taules de rutes o aquestes són molt petites.
    - La xarxa es manté en silenci si no hi ha dades per transmetre (no hi ha *overhead* degut a paquets d'actualització de rutes).
    - Són altament escalables.
    - Alta latència (*setup delay*) abans de començar a transmetre dades cap a una destinació per la qual no hi ha ruta prèvia, donat que es necessita un temps intern per establir la ruta.
    - Són adequats per a xarxes sense patrons definits de tràfic (quan no hi ha molta més comunicació cap a un node destinació en concret que cap a la resta de nodes, situació típica d'una topologia *peer-to-peer* o quan no ha servidors).
- Protocols proactius
    - Es basen en una o vàries taules amb rutes entre parells de nodes, que s'han de mantenir/actualitzar periòdicament.

- A la taula es troben rutes innecesàries que poden no fer falta mai.

- Baixa latència per començar a transmetre (degut a que es disposa de totes les rutes d'avantmà).

- Baixa escalabilitat (xarxes amb milers de nodes implica molt *overhead* degut a la transferència de les actualitzacions de les rutes, sobretot en entorns en moviment).

- Necessita de més ample de banda per transmetre les actualitzacions de rutes. Això implica més consum per part dels nodes (major utilització de la CPU i de la ràdio). També necessita nodes amb més memòria per a poder manegar grans taules d'encaminament.

- Protocols híbrids

    - La xarxa es divideix en petites zones, amb nodes "pasarel-la" pertanyent a més d'una zona simultàniament.

    - L'encaminament entre nodes d'una mateixa zona és de tipus proactiu (la ruta s'emmagatzema en una taula).

    - L'encaminament entre nodes de diferents zones és de tipus reactiu (es demana la ruta sols quan es necessita).

    - Aquest mètode proporciona un bon balanceig entre un apropament reactiu i proactiu.

    - Són bastant escalables.

    - Proporcionen una latència mitja global més gran que els protocols proactius però més petita que els reactius.

Segon tot l'anterior, sembla clar que, en general, per a LLNs (xarxes sense fils de baix consum i amb nodes amb recursos limitats) és molt més adient fer servir protocols reactius, ja que no guarden cap informació d'encaminanent a cap base de dades o taula, pe la qual cosa els nodes no necessiten de grans requeriments de RAM o CPU per computar les llistes de rutes. A més, com que no s'ha d'intercanviar informació relativa a actualitzacions de rutes, els nodes poden estar en mode *sleep* durant més temps i, per tant, estalviant energia i disminuint l'ample de banda (deixant més capacitat a la xarxa per transmetre dades). Els protocols proactius serien més adients, en general, per a xarxes cablejades de més velocitat, on no hi ha problema en que els nodes s'intercanviin informació perquè aquests disposen de RAM i processador suficients per processar la informació i, a més, l'ample de banda és de decenes o centenars de Mbps, a banda de que es tracta de dispositius normalment endollats al corrent i per tant sense problemes de vida de bateria.

Tot i així, hi ha exemples de protocols proactius, com ara RPL, que poden funcionar molt bé en LLNs, sobretot si es fa servir el mode *non-storing*, que no emmagatzema cap ruta a cap taula i per tant no necessita de nodes amb gran quantitat de memòria o capacitat de procés (tot i que llavors els missatges que s'envien augmenten de mida i això implica augmentar el cicle de treball dels nodes)

En definitiva, sembla ser que els esforços actuals s'enfoquen a dissenyar protocols que uneixin el millor dels dos mons: la baixa latència dels protocols proactius i el baixos requeriments de memòria i processador i menor *duty cycle* dels protocols reactius. Del conjunt de protocols exposats en els apartats anteriors, dos són els que més complexien aquests requeriments: LOAD (LOADng) i RPL, el primer d'ells reactiu i el segon proactiu però tots dos preparats per a treballar amb 6LoWPAN i, per tant, amb nodes/xarxes IPv6.

Pel que fa a les tendències actuals i futures en els protocols d'encaminament tenim:

- Intentar reduir l'*overhead* i el *duty cycle* fent servir tècniques novedoses, com ara la utilització dels missatges propis de la subcapa MAC, per tal de no haver d'enviar missatges balisa (HELO).

- Possibilitat d'encaminament a nivell d'enllaç o a nivell de xarxa, segons convingui.

- Creació de grafs dirigits (DODAGs) amb utilització de pesos/rangs que serveixin per a un encaminament més eficient i també per evitar bucles (i conseqüents congestions).

- Creació de "zones" –conjunts- de nodes locals per evitar *overhead* a nivell global i millorar l'encaminament local.

- Utilització de mètriques/indicadors de la qualitat dels enllaços, per decidir com encaminar, amb possibilitat de distinguir entre enllaços ascendents o descendents.

3.3. Capa d'Aplicació

3.3.1. REST

REST són les sigles de Transferència d'Estat Representacional (*Representational State Transfer*). Es tracta d'una arquitectura de programari per a sistemes multimèdia com ara la WWW, orientada a comunicacions d'un únic sentit (*one-way*) entre un client i un servidor. El terme es va originar l'any 2000 per un dels autors del protocol HTTP i avui dia a passat a ser ampliament utilitzat per les comunitats de desenvolupadors. Si bé originàriament el terme es referia a un conjunt de principis d'arquitectura, en l'actualitat es fa servir en un sentit més ampli, per descriure qualsevol interfície web simple que fa servir XML i HTTP, sense les abstraccions adicionals dels protocols basats en patrons d'intercanvi de missatges, com ara SOAP (*Service Oriented Application Protocol*). Els sistemes que segueixen els principis REST s'acostumen a anomenar *RESTful* [9].

Segons REST, la Web tal i com la coneixem ha estat escalable com a resultat d'una sèrie de dissenys fonalmentals clau:

- Un protocol client/servidor sense estat: cada missatge HTTP conté tota la informació necessària per comprendre la petició. Com a resultat, ni el client ni el servidor necessiten enrecordar-se de cap estat de les comunicacions entre missatges. Això no treu que avui dia moltes aplicacions basades en web facin servir *cookies* o altres mecanismes per a mantenir o guardar l'estat de la sessió, encara que aquesta tècnica ni altres com per exemple la reescritura d'URLs no estan permeses amb REST).

- Un conjunt d'operacions ben definides que s'apliquen a tots els "recursos" d'informació: HTTP defineix un petit conjunt d'operacions, anomenades "mètodes", entre els quals destaquen POST, GET, PUT i DELETE. Aquestes operacions es podrien comparar, salvant les distàncies, amb les d'alta, baixa, modificació i consulta (CRUD, en anglés) pròpies de les bases de dades.

- Una sintaxi universital per identificar els recursos: en un sistema REST, cada recurs és adreçable únicament mitjançant del seu URI (*Uniform Resource Identifier*).

- L'ús d'hipermitjans tant per a la información de l'aplicació com per a les transicions d'estat de la mateixa: la representació d'aquest estat en un sistema REST és típicament HTML o XML. Com a conseqüència d'això, és possible navegar d'un recurs REST a molts altres, simplement seguint els enllaços disponibles, sense requerir l'ús de registres o una infraestructura adicional.

Per a més informació sobre REST, veure l'Annex XXXIII.

3.3.2. MQTT

MQTT és un protocol de connectivitat bidireccional (*two-way*) per a xarxes sense fils i, en general, orientat a paradigmes M2M i IoT. La primera versió va ser creada el 1999 i les sigles significaven originàriament *Message Queue Telemetry Transport* (Transport de Telemetria de Cola de Missatges). Bàsicament, es tracta d'un protocol de missatgeria lleuger, que es fa servir per sobre de TCP/IP i que segueix un model publicació-subscripció, on hi ha un node que publica missatges i altres nodes interessats que es "suscriuen" al primer node per tal de poder rebre aquests missages. Les especificacions del protocols són públiques i es poden fer servir sense haver de pagar *royalties* (llicència gratuïta).

Actualment, el protocol ja va per la versió 3.1.1. Els competidors directes d'aquest protocol són CoAP i XMPP, que s'expliquen en els propers apartats. L'exemple més famós d'aplicació que fa servir MQTT és Facebook Messenger (l'aplicació de missatgeria instantània de Facebook, disponible tant en versió ordinador com per a *smartphones*). Des de l'any 2013 MQTT és un estàndard certificat per OASIS (*Organization for the Advancement of Structured Information Standards*).

MQTT està especialment orientat a comunicació entre dispositius remots amb recursos limitats i en xarxes amb molta latència o amb enllaços poc confiables, és a dir, nodes que disposen de poc ample de banda i poca memòria i xarxes sense fils en entorns complicats, com per exemple indústries, quan no hi ha LoS entre els nodes, etc. Per tant, és un protocol idoni er a LLNs. A més, MQTT busca minimitzar la quantitat d'informació que s'envia a la xarxa. El fet de ser lleuger i necessitar pocs recursos en anglès s'anomena *small footprint* o emprempta petita.

El funcionament del protocol, com qualsevol altre basat en publicació-subscripció, es basa en la presència d'un *message broker*, un programa intermediari que "tradueix" el llenguatge d'un sistema a un altre llenguatge i que a més és responsable de distribuir els missatges des del publicador fins als subscriptors interessats en el tema (*topic*) del missatge.

El *broker* més utilitzat avui dia per MQTT és potser Mosquitto, encara que també hi ha d'altres com CloudMQTT, HiveMQ, RabbitMQ (via *plugin*), etc.

Pel que fa als ports que fa servir MQTT, aquests estan reservats per l'IANA (*Internet Assigned Numbers Authority*) i són el 1883/tcp i el 8883/tcp en cas de fer servir MQTT sobre SSL (*Secure Sockets Layer*).

Per a més informació sobre MQTT, veure l'Annex XXXIV.

3.3.3. AMQP

AMQP són les sigles de Protocol d'Enqueuament de Missatges Avançat (*Advanced Message Queuing Protocol*). Es tracta d'un protocol obert de capa d'aplicació originat l'any 2003/2004 i orientat a missatges, que fa les funcions de *middleware* (programa intermediari). Les seves principals característiques són, com ja s'ha dit, la seva orientació a missatges, enqueuament, encaminament (incloent del tipus 'punt a punt' i 'publicació-subscripció'), confiabilitat i seguretat. Per tant, al igual que altres protocols basats en *publisher-subscriber*, es basa en un *broker* o "corredor" que fa d'intermediari entre clients o *peers*. Aquesta arquitectura es mostra clarament a la figura de la pàgina següent:

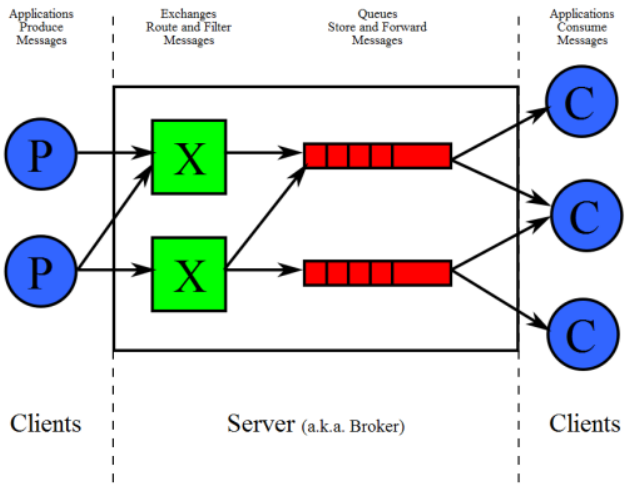


Figura 16. Esquema bàsic d'un protocol publicador-subscriptor basat en *broker*

AMQP determina el comportament del proveïdor de missatges i del client, de tal manera que les diferents implementacions dels fabricants són verdaderament interoperatives (poden funcionar sota diferents plataforma de programari i maquinari), de la mateixa manera que altres protocols com ara SMTP, HTTP, FTP, etc. també ho són. De fet, AMQP es considera com un complement del protocol HTTP: mentre que el primer està orientat a petició/resposta, el segon està orientat a publicació/subscripció i transaccions (un dels objectius és intentar incloure suport natiu per a AMQP en els navegadors webs, amb una transició fent servir clients Javascript). El rendiment d'aquest protocol és molt alt, ja que pot arribar a proccesar fins a 150.000 missatges per segon a través d'un únic *broker*.

Altres intents anteriors d'estandarizar aquest programari intermig o *middleware* (com per exemple JMS – *Java Message Service*) ho eren a nivell d'API (Interfície de Programació d'Aplicacions) i, per tant, no es podia assegurar l'interoperabilitat entre sistemes. De fet, AMQP és un protocol a nivell de "cable" (*wire-level*); això significa que el protocol és una descripció –en format XML (*eXtensible Markup Language*)- del format de les dades que s'envien a la xarxa, com un fluxe d'octets. D'aquesta manera, qualsevol eina que pugui crear i interpretar els missatges conforme a aquest format de dades pot interoperar amb qualsevol altre eina que també implementi el llenguatge.

A més de proporcionar una comunicació orientada a missatges i amb control de fluxe, AMQP també garantiza l'entrega de la comunicació amb les mateixes opcions o qualitats de servei que ja oferia MQTT:

- *At-most-once* (el missatge s'entrega com a molt una vegada o potser mai),
- *At-least-once* (el missatge s'entrega com a mínim una vegada però potser més),
- *Exactly-once* (el missatge s'entrega exactament una vegada; ni més ni menys).

També es suporta autenticació i encriptació basada en SALS (*Simple Authentication and Security Layer*) y TLS (*Transport Layer Security*). Per a aquesta finalitat, el protocol assumeix una capa de transport confiable, com ara TCP.

Encara que originat anys enrera (quan va ser dissenyat per a ser utilitzat per al banc JPMorganChase), la versió 1.0 d'AMQP no va ser publicada fins l'any 2011. Per la seva banda, el protocol va esdevinir un estàndard OASIS (*Organization for the Advancement of Structured Information Standards*) l'any 2012 i, des del passat Abril de 2014, també consta com estàndard ISO, concretament l'ISO/IEC 19464.

Pel que fa al port que fa servir AMQP, aquest està reservat per l'IANA i és el 5672 (TCP i, en un futur, també SCTP – *Stream Control Transmission Protocol*).

Per a més informació sobre AMPQ, veure l'Annex XXXV.

3.3.4. XMPP

XMPP són les sigles de Protocol de Presència i Missatgeria Extensible (*eXtensible Messaging and Presence Protocol*). Es tracta d'un protocol de comunicacions de la capa d'aplicació, orientat a missatges, destinat a fer d'intermediari. Originàriament el seu nom era Jabber i va ser desenvolupant l'any 1999 per a l'aplicació de missatgeria instantània que portava el mateix nom. Avui dia s'utilitza en sistemes publicació-subscripció, senyalització VoIP, transferència de fitxers, jocs, serveis de xarxes socials i aplicacions IoT com ara *smart grid*.

Al contrari que altres protocols de missatgeria instantània, XMPP es defixeix com un estàndard obert, basat en XML, i fa servir un apropament de sistemes oberts, per la qual cosa qualsevol persona pot implementar un servei XMPP i interoperar amb altres implementacions que corrin sota altre maquinari o programari. Actualment, existeixen quatre especificacions de l'IETF referents a XMPP: RFC3920, RFC3921, RFC3922 i RFC3923, que van ser aprovades com estàndard l'any 2004.

Avui dia, les especificacions anteriors han estat substituïdes per les més recents RFC6120 (definició de comunicació client-servidor fent servir fluxes XML) i RFC6121 (defineix el seu ús per a *Instant Messaging* i Presència) i addicionalment l'RFC 6122 (especifica el format d'adreça XMPP).

Per altra banda, la XMPP *Standards Foundations* (XSF) desenvolupa activament extensions per a XMPP, com ara extensions per a xat multiusuari, publicació-subscripció (fent-lo similar a protocols com MQTT i AMQP), dades de formulari, descobriment de serveis, PEP (*Personal Eventing Protocol*), transferència de fixers, capacitats d'entitat, XHTML-ID, etc. Altres extensions són encara part d'una implementació experimental, com ara: EXI (*Efficient XML Interchange*), dades de sensors, provisió, concentradors, etc.

Els punts forts del protocol XMPP són els següents:

- Descentralització: l'arquitectura de xarxa d'XMPP és similar a la del correu electrònic, en el sentit de que qualsevol persona pot executar el seu propi servidor i no existeix cap servidor "mestre" central.

- Especificació oberta: XMPP es basa en estàndards de l'IETF especificats a RFCs, com s'ha comentat abans. No es requereix pagar cap llicència per poder implementar suport de les especificacions. L'intercanvi de missatges fa servir XML estàndard.

- Maduresa: l'especificació original XMPP té més de 15 anys per la qual cosa existeixen múltiples implementacions de l'estàndard, tant a nivell client, servidor, components i llibreries de codi.

- Seguretat: XMPP té suport per a autenticació/encriptació amb SASL i TLS, respectivament (al igual que AMQP, vist abans), indicada per a entorns no segurs o confiables.

- Flexibilitat: es poden afegir funcionalitats personalitzades per sobre d'XMPP, amb les extensions més comuns estant gestionades per l'XSF (*XMPP Standards Foundation*). Els àmbits d'aplicació, com hem vist abans, van des de la missatgeria instantània fins al *Cloud Computing* passant per VoIP o geolocalització. A més, està indicant quan els missatges són llargs i potencialment complicats.

- Gran escalabilitat: es poden aconseguir xarxes de fins i tot 100.000 nodes o més.

En canvi, els principals punts dèbils o mancances d'XMPP són:

- No soporta QoS: l'assegurança en l'entrega de missatge s'ha de programar per sobre de la capa XMPP; no ve definida en el propi protocol.

- Comunicació basada en texte: donat que es basa en XML, XMPP té un alt *overhead* quan es compara amb protocols purament binaris. Aquest problema està sent abordat per l'extensió EXI (*Efficient XML Interface*) on XML es serialitza de manera binària, espcialment en un mode anomenat *schema-informed*.

- Transferència de dades binàries "en banda" limitada: les dades binàries s'han de codificar amb codificació base64 abans de poder transmetre's *in-band*. Per tant, quan s'han de transmetre grans quantitats de dades binàries (per exemple en transferència de fitxers) és millor transmetre en "fora de banda" (*out-of-band*) fent servir missatge "en banda" per a la coordinació. Un exemple el tenim amb l'extensions Jingle d'XMPP.

Pel que fa a la comunicació, el protocol XMPP original/natiu fa servir TCP; concretament, es basa en l'enviament de fluxes XML entre dos extrems oberts, a través de connexions TCP de llarga durada, fent servir els ports reservats 5222/tcp i 5269/tcp, així com el 5269/tcp quan es fa servir TLS. Una alternativa a aquest mode és fer servir HTTP/S com a transport (port 80/tcp o 443/tcp) utilitzant clients web, que és de molta utilitat quan hi ha usuaris al darrera de dispositius tipus tallafocs, que poden rebutjar connexions provinents d'altres protocols/ports diferents al de la navegació web. Per la seva banda, un fluxe XML consisteix de tres possibles etiquetes o *tags*: `<presence/>`, `<message/>` i `<iq/>` (*info/query*).

Per a més informació sobre XMPP, veure l'Annex XXXVI.

3.3.5. CoAP

CoAP són les sigles de Protocol d'Aplicació Constret (*Constrained Application Protocol*). Es tracta d'un protocol de comunicació de la capa d'aplicació dissenyat pel Grup de Treball CoRE (*Constrained Resource Environment*) de l'IETF, estant avui dia completament estandaritzat i amb especificacions documentades a l'RFC 7252 (a més d'altres extensions que es troben actualment en procés d'estandarització) [33].

A grans trets, CoAP és un protocol similar a HTTP, en el sentit de que es basa en transferència de documents. La diferència més gran, però, és que CoAP s'ha dissenyat tenint en compte les necessitats de nodes amb restriccions de consum/potència, processament i memòria, com acostuma a passar amb les motes d'una LLN (és a dir, xarxes amb altes taxes d'error de paquets, *throughput* d'uns 10 Kbps, etc). CoAP també està enfocat a altres components com ara commutadors, vàlvules i altres dispositius electrònics de baix consum, que necessiten ser supervisats i controlats remòtament a través de la xarxa Internet.

CoAP está dissenyat per poder "traduir" fàcilment a HTTP, permetent per tant una forta integració amb la Web. Al mateix temps, també incorpora altres requeriments com ara suport de *multicast*, *overhead* molt baix i alta simplicitat, conceptes molt importants per a dispositius M2M/IoT (*smart energy*, *home automation*, etc.) que tendeixen a estar fortament encastrats i diposen de molta menys memòria, capacitat de processament i alimentació de potència que els dispositius tradicionals com ara ordinadors o telèfons mòbils intel·ligents.

Els trets característics de CoAP són els següents:

- Segueix un model semblant al de client/servidor: els clients fan peticions als servidors (fent servir mètodes GET, PUSH, POST i DELETE, de manera similar a HTTP). Llavors, aquests darrers envien les seves respostes de tornada cap als clients. La diferència és que, en entorns M2M, un mateix dispositiu fa al mateix temps de client i de servidor.

- Està dissenyat per interoperar amb HTTP i, per tant, amb l'arquitectura REST (disseny RESTful). El mapeig entre CoAP i HTTP es troba ben definit, permetent als *proxies* proporcionar accés a recursos CoAP via HTTP, de manera uniforme.

- Suport d'URIs (identificadors de recursos) i *Content-Type*.

- Suport integrat per a descobriment de recursos i serveis, proporcionat per part de serveis CoAP coneguts.

- Baixa sobrecàrrega de capçalera i complexitat de *parseig*. CoAP fa ús extensiu de camps de bits (*bitfields*) i mapejos (*mappings*) per estalviar espai. Per altra banda, els paquets es generen de manera simple i poden ser analitzats sense haver de consumir RAM extra. A més, els paquets CoAP són molt més petits que els fluxes HTTP (en primer lloc, perquè la capçalera CoAP es molt petita i en segon lloc, degut a la MTU pròpia de les xarxes 802.15.4)

- Procés de subscripció a recursos molt simple, resultant en notificacions tipus *push*.

- Cau de continguts basada en la propietat *max-age*.

- CoAP fa servir UDP en comptes de TCP. D'aquesta manera, els clients i servidors es comuniquen entre ells fent servir datagrames sense connexió. D'aquesta manera, els reintents i la reordenació de paquets s'implementen a la capa d'aplicació. Fent servir UDP es permet xarxes implementar IP fins i tot en petits microcrontroladors limitats (8 bits)

- Suport per a *multicast* i *broacast* en l'enviament de dades.

- Intercanvi de missatges asíncron entre extrems (*endpoints*).

L'objectiu de CoAP no és simplement "comprimir" HTTP sinó més aviat especificar un subconjunt de REST, comú amb HTTP, però optimitzat per a aplicacions M2M. Tot i que CoAP es pot fer servir com un *restyling* d'HTTP en un protocol més compacte, introdueix altres característiques adicionals per a M2M, tal i com s'han enumerat abans: descobriment, multicast, missatges asíncrons, etc.

Per a més informació sobre CoAP, veure l'Annex XXXVII.

3.3.6. Resum

En els apartats anteriors hem analitzats els següents protocols de capa d'aplicació: REST, MQTT (MQTT-SN), AMQP, XMPP i CoAP. Per la seva banda, ens hem hagut de deixar altres opcions més o menys conegudes, com ara DDS (*Data Distribution Service*), que en aquest cas, encara que també segueix un esquema publicador/subscriptor i ofereix característiques com QoS, *multicast*, confiabilitat mitjançant TCP, redundància, etc. està enfocat més aviat en distribuir dades directament entre dispositius (per exemple, passar informació directament d'un sensor a un actuador i, per tant, més enfocat a M2M).

A la taula de sota es mostra un resum dels protocols d'aplicació exposats i les seves característiques principals:

Protocol	Orientació	Estàndar	Transport	QoS
HTTP REST API	Serveis	Obert	TCP	NO
MQTT/MQTT-NS	Missatges	Obert	TCP	SÍ (*Fire & Forget*, *Acknowledged Delivery*, *Assured Delivery*)
AMQP	Missatges	Obert	TCP	SÍ (*At-most-once*, *At-least-once*, *Exactly-once*)
XMPP	Missatges	Obert	TCP	NO
CoAP	Serveis	Obert	UDP	SÍ (*Confirmable*, *NonConfirmable*)

Taula 6. Protocols d'aplicació per a WSNs/LLNs

Les conclusions que es poden treure són les següents:

- CoAP és bastant similar a MQTT-SN en quant a objectius i àmbits d'aplicació.

- CoAP és una arquitectura orientada a serveis, no a missatges (com la resta dels protocols exposats i altres com DDS).

- CoAP és el protocol més adient si es vol construir una xarxa/plataforma/sistema que hagi d'interactuar amb sistemes remots en Internet (i, per tant, basats en IPv4/IPv6).

- Dos dels protocols més "prometedors" per a dispositius petits són MQTT/MQTT-NS i CoAP (encara que XMPP amb l'extensió EXI també pot ser addient però no soporta QoS).

- Tots els protocols són estàndars oberts (OASIS o IETF) i implementables gratuïtament.

- Tots ells són molt millor opció que HTTP/ REST API per a dispositius/entorns limitats.

- Mentre que MQTT dóna flexibilitat pel que fa a patrons de comunicació i actua purament com una "canonada" per a dades binàries, CoAP s'ha dissenyat per ser interoperable amb la Web.

- MQTT és un protocol *many-to-many* (molts a molts) per passar missatges entre múltiples clients fent servir un *broker* central. El protocol desacobla el "productor" i el "consumidor", deixant que els clients publiquin i permetent que el *broker* decideixi on encaminar i copiar els misssatges. En canvi, CoAP és primàriament un protocol *one-to-one* per transmetre informació d'estat entre un client i un servidor.

- MQTT proporciona suport per a etiquetatge de missatges amb tipus i altres metadades per tal d'ajudar als clients entendre els missatges. Tot i que els missatges MQTT es poden fer servir per a qualsevol propòsit, tots els clients han de conèixer els formats de missatge per poder permetre la comunicació. En canvi, CoAP proporciona suport integrat per a negociació de contingut i descobriment, permetent que els dispositius es sondegin entre ells per trobar formes d'intercanviar dades.

- Diversos experiments han demostrat que MQTT és millor opció que REST API quan es fan servir dispositius mòbils (donat que HTTP amb mòbils és pesat, fràgil i fa massa ús de les bateries). En concret, aquests experiments han demostrat que MQTT és fins 93 vegades més ràpid, fa servir 12 vegades menys de bateries per enviar, gairebé 200 vegades menys bateries per rebre, necessita la meitat de consum per mantenir una connexió oberta i introdueix vuit vegades menys *overhead* que REST.

- Tots els protocols exposats tenen els seus "pros" i les seves "contres" i escollir l'ideal dependrà en tot cas de cada sistema/aplicació concreta. L'escenari ideal seria poder realitzar experiments, construir prototipus i implementar dispositius de prova.

- En general, per a LLNs amb milers de nodes que han de ser directament encaminables (sense NAT) i que han de connectar-se a xarxes remotes a través d'Internet o bé directament al núbol, s'ha d'escollir una solució que permeti comunicació asíncrona, funcioni amb IPv6, afegeixi molt poc *overhead*, disposi de de característiques de *multicast*, QoS, seguretat i tingui disponible una gran varietat d'implementacions. En aquest sentit, CoAP sembla ser la millor opció disponible ara per ara.

3.4. Tecnologies

Quan es vol dissenyar i posteriorment implementar una xarxa sense fils fent servir IEEE 802.15.4, hem d'escollir entre un ampli ventall d'opcions de maquinari (HW) i programari (SW) disponibles en el mercat. En el següent apartat es fa un recull d'algunes de les opcions més conegudes de cada camp.

3.4.1. Maquinari

Pel que respecta al maquinari, sabem que les xarxes de sensors sense fils IEEE 802.15.4 estan formades per nodes de mida petita –anomenades motes- que s'encaminen missatges entre elles, fins arribar a una pasarel·la que connecta amb una xarxa exterior (per exemple Internet o altra xarxa de sensors). Aquest maquinari en cada node acostuma a ser una plataforma de desenvolupament o "mòdul" que consta d'un SoC (*System on a Chip*) que, al seu voltant, consta d'un processador (CPU) o, més habitualment, un microcontrolador (µC – MCU), memòria RAM i un transceptor ràdio i antena interna [51]. El SoC també acostuma a incorporar altres components com ara ports Ethernet/USB/sèrie/I2C (necessaris per poder programar la mota), connector per a una antena RF externa, connectors d'expansió, bateries, etc. A més, el mòdul també sol incorporar un o diversos sensors (temperatura, humitat, vent, llum, etc.) que recullen i transformen les variables a monitorar.

En la figura de sota es pot veure un diagrama de blocs genèric amb els components estàndard d'una mota amb mòdul ràdio IEEE 802.15.4 (per exemple ZigBee): microcontrolador (o microprocessador), memòria (SRAM, Flash, EEPROM), ràdio RF, antena interna, sensors (si escau), bateria i ports/interfícies de comunicació (UART, I^2C, USB, Serial, etc.):

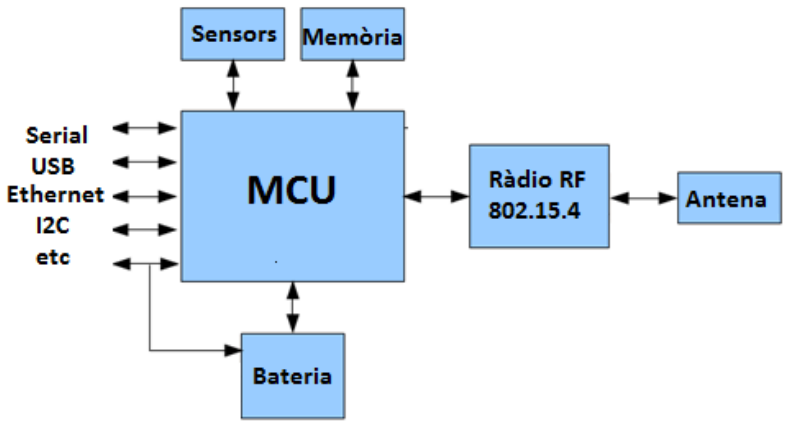


Figura 17. Diagrama de blocs dels components maquinari d'una mota 802.15.4

Per la seva banda, la següent figura mostra un exemple real de mòdul sensor sense fils programable [124], concretament el model RM090 de l'empresa RMONI, destinat al monitoratge de humitat i temperatura i que consta d'un microcontrolador MSP430F5437 de la companyia Texas Instruments (TI), una ràdio IEEE 802.15.4/ZigBee model CC2520 també de TI, una EEPROM de 2 KB, una memòria Flash de 128 KB, un connector per a antena externa, un connector d'expansió i un connector USB per a la programació del node:

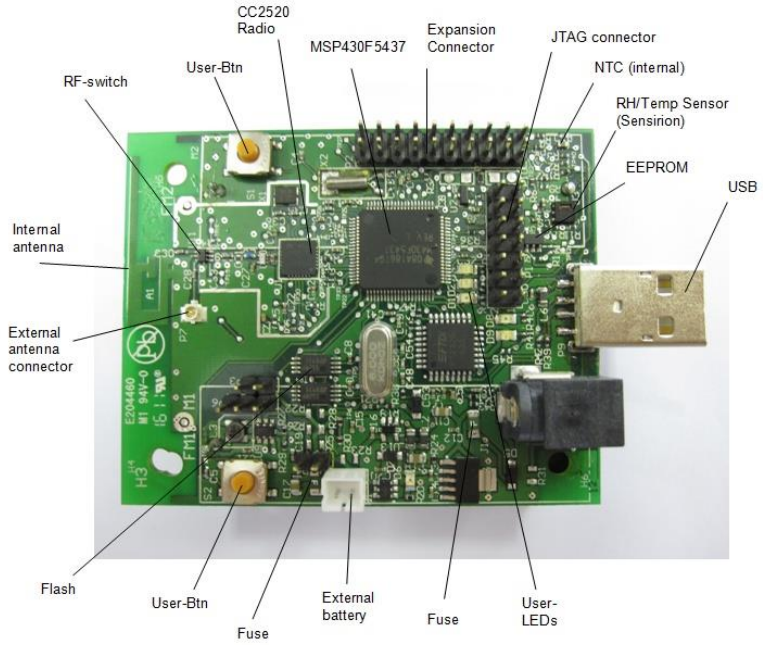


Figura 18. Exemple de mòdul 802.15.4, RMONI RM090 [124].

3.4.1.1. Microcontroladors

Un microcontrolador (abreujat µC, uC o MCU) és un circuit integrat programable, capaç d'executar les ordres gravades en la seva memòria. Està compost de diversos blocs funcionals, els quals compleixen una tasca específica. Un microcontrolador inclou en el seu interior les tres principals unitats funcionals d'un ordinador: unitat central de processament, memòria i perifèrics d'entrada / sortida.

A l'Annex XXXVIII es descriuen els MCUs més coneguts que s'empren actualment per a xarxes sense fils.

3.4.1.2. Processadors

Tot MCU porta dintre un processador. Com hem pogut a l'Annex XXXVIII, la gran part de MCUs de 32 bits incorporen un processador de la companyia ARM i, en concret, un model Cortex.

ARM fabrica quatre grans famílies de processadors:

- Cortex-A: destinats a telèfons mòbils, *netbooks*, tauletes digitals, TV digital, pasarel·les d'Internet, servidors i components de xarxa. D'entre tots els models disponibles, el més bàsic és el Cortex-A5 mentre que els modells superiors són el Cortex-A57 i el Cortex-A53.

- Cortex-R: destinats a aplicacions en temps real, com ara sistemes de frenada en automoció, controladors de dispositius d'emmagatzematge massiu, xarxes i impressió. Els models disponibles són el Cortex-R4, Cortex-R5 i Cortex-R7.

- Cortex-M: processadors de 32 bits destinats a microcontroladors, on es necessita una gestió d'interrupcions ràpida i altament determinista, al mateix temps que s'aconsegueix el menor nombre de portes i menor consum possibles. Les aplicacions van des de sensorització intel·ligents, *wearables*, automoció (per exempla *airbags*), etc. Els models disponibles són el Cortex-M0, M0+, M3, M4 i M7. Tal i com es pot veure a la taula de sota, el més adient per a sensors de xarxes IoT (per exemple BLE) és el Cortex-M0+. Un dispositiu que incoropori aquest processador pot aconseguir una vida útil de la bateria de fins a 15 anys, segons la pròpia ARM.

Cortex-M0	Cortex-M0+	Cortex-M3	Cortex-M4	Cortex-M7
Touchscreen controller	IoT sensor node	Activity tracker wearable	Smart metering	High-end audio headset or soundbar
Power management	Bluetooth smart transceiver	Wifi transceiver	High-performance motor control	Automotive (transmission, body electronics, low-cost infotainment)

Taula 7. Comparativa de models Cortex-M d'ARM.

- SecurCode: processadors per a aplicacions que necessiten alta seguretat. Els models disponibles són l'SC000, SC100 i SC300.

3.4.1.3. Sistemes en un Xip (SoC)

Un sistema en un xip (SoC o *System on a Chip*, en anglès) és bàsicament un circuit integrat – una placa amb components electrònics- que integra tots els elements propis d'una computadora, en un únic xip. Un SoC pot contenir tant funcions digitals, analògiques i RF en un mateix substrat de xip. Avui dia és molt comú fer servir SoC en dispositius electrònics mòbils degut al seu baix consum. La seva aplicació més típica són els sistemes encastats (*embedded systems*, en anglès).

Els components típics d'un SoC són:

- Un MCU, microprocessador o DSP – processador digital de senyal (o fins i tot varis),
- Blocs de memòria, incloent ROM, RAM, Flash i EEPROM,
- Fonts de temps, com ara oscil·ladors,
- Comptadors-temporitzadors, temporitzadors en temps real, generadors de *reset*, etc.
- Interfícies de comunicació amb l'exterior: USB, FireWire, Ethernet, UART, SPI, I^2C, etc.
- Conversors analògic-digital (ADCs) o digital-analògic (DACs),

- Reguladors de tensió i circuits de gestió de potència.

Els SOCs, entre d'altres aventatges –com ara el menor consum- també implifiquen poden "encastar" transceptors RFs en xarxes de sensors sense fils.

A la figura de sota tenim, a mode d'exemple, el diagrama funcional de blocs d'un SoC de l'empresa Analog Devices, en concret el model ADuCRF101. Al diagrama es poden observar tots els components descrits abans, com ara el transceptor RF (UHF), el microcontrolador (ARM Cortex M3), els diversos temporitzadors (*wake-up*, *watchdog*, genèric), el controlador d'interrrupcions, les memòries (RAM, Flash), un ADC de 12 bits, així com les interfícies de comunicació (sèrie cablejat, SPI, I2C, UART, etc).

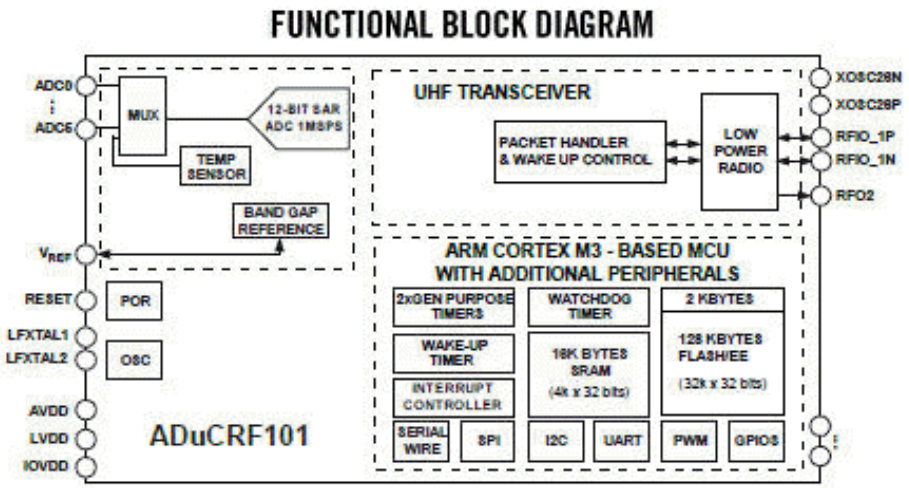


Figura 19. Diagrama de blocs del SoC AduCRF101

A l'Annex XXXIX es descriuen alguns exemples dels SoCs més comuns que hi ha actualment al mercat orientats a M2M/IoT, encara que n'hi ha moltíssims més, gairebé tants com fabricants.

3.4.1.4. Plataformes de desenvolupament

Una plataforma de desenvolupament acostuma a ser un SoC –placa amb tots els components necessaris per esdevenir un node/mota LLN- però orientat als àmbits de l'R+D (recerca i desenvolupament), educació i públic entusiasta, que volen aprendre i experimentar amb la tecnologia, fent servir les APIs (interfícies de programació d'aplicació) que els fabricants de la placa posen a disposició dels usuaris, per tal de que aquests darrers puguin crear i provar xarxes en entorns de laboratori. No obstant però, també es poden fer servir aquests plataformes per implementar xarxes que més tard es posaran en producció.

A l'Annex XL es descriuen les principals plataformes que hi ha actualment al mercat: Intel Galileo i Intel Edison, Arduino, Raspberry Pi B+, Beaglebone Black, Libelium Waspmote, TelosB, GINA i OpenMote.

3.4.1.4.1. Comparativa

Com a darrer apartat d'aquesta secció, s'inclou, amb efectes de comparació, una taula resum amb totes les plataformes de desenvolupament comentades als Annexos, incloent algunes de les seves característiques principals: MCU/processador, memòria, ràdio, consum, mida i preu.

Empresa i Nom	SoC o MCU	Memòria	Transceptor RF incorporat	Consum (*idle*)	Mida (mm)	Preu unitari
Intel Galileo	Quark X1000	256 MB RAM 512 KB SRAM 8 MB Flash	No	≈520 mA	107 x 74 x 23	55-60 EUR
Intel Edison	Tangier	1 GB RAM 4 GB Flash	No	≈50 mA	35.5 × 25 × 3.9	40 EUR
Arduino (TinyDuino)	Atmega168 Atmega328 Atmega1280 Cortex-M3	2 KB RAM 32 KB Flash	No	≈10 mA	20 x 20	20 EUR
Raspberry Pi B+	BCM2835	512 MB RAM	No	≈360 mA	85 x 56 x 17	35 EUR
BeagleBone Black	AM 335x	512 MB RAM 4GB Flash	No	≈280 mA	76.2 × 76.2 × 16	35-37 EUR
Libelium Waspmote	ATmega1281	8 KB SRAM 4 128 KB Flash	Múltiples opcions	≈9 mA	73.5 x 51 x 13	135-233 EUR
TelosB TPR2420CA	MSP430	10 KB RAM 48 KB Flash	CC2420	1 µA	65 x 31 x 6	55-57 EUR
GINA 2.2	MSP430	10 KM SRAM 10 KB Flash	AT86RF231	N/D	60 x 60	N/A
OpenMote	CC2528	32 KB RAM 512 KB Flash	CC2520	≈27 mA	24.5 x 27.6	90 EUR

Taula 8. Taula resum amb diverses plataformes de desenvolupament

Alguns comentaris sobre la taula anterior:

- El mode *idle* és aquell en que la mota està encesa, amb la ràdio activada, esperant rebre algun missatge però no rebent cap en concret; per tant, no s'ha de confondre amb el mode actiu i en recepció (RX). S'ha escollit aquest mode per comparar els consums de corrent ja que és en el que es poden trobar més disparitats entre plataformes, donat que en el mode *sleep*, la majòria de les plaques tenen un consum molt baix, per sota de 1ηA (el més normal és 0.07 ηA aproximadament) i seria més difícil comparar entre elles. Això no treu que el consum dels transceptors quan operen en aquest mode –*idle*- és gairebé el mateix que quan operen en mode RX i, per tant, està clar que el millor serà sempre apagar completament la ràdio i ficar la placa en mode *sleep*, en comptes de deixar-la en mode *idle*, per tal de reduir el consum tot el possible.

- La mida d'intel Edison correspon únicament al mòdul central (SoC), no a la placa de desenvolupament sencera.

- De plaques Arduino n'hi ha moltes al mercat, cadascuna amb una MCU, velocitat, memòria, mides i preus diferents. Per a la taula anterior s'ha escollit TinyDuino, ja que creiem que és el model més adient per a LLNs, on el que preval és tenir motes amb la menor mida, consum i preu possibles, a expenses d'altres variables com ara la potència de processament o la quantitat de memòria.

- Les plaques que a la columna "Transceptor RF incorporat" tenen el valor "No" no porten ràdio per defecte, tot i que es podria afegir una fent servir mòduls externs, per exemple a través d'un adaptador endollat al port USB.

- De la plataforma GINA no s'han trobat dades relatives al consum en mode *idle*, tot i que probablement aquest estarà entre 13-15 mA, d'acord amb els consums de corrent de l'MCU MSP430 i del transceptor AT86RF231 en mode RX. Tampoc s'ha pogut trobar el preu de la placa, probablement degut a que no es tracta d'un producte comercial sinó únicament a finalitats acadèmiques.

- Al web oficial d'OpenMote no s'han pogut trobar les mides de la placa (de fet, l'enllaç per veure el *Datasheet* no funcionava). La mida que apareix a la taula correspon a un factor de forma XBee amb PCB –placa de circuit imprès- ràdio 802.15.4.

Les conclusions que es poden treure de la taula anterior són:

- Si el que necessitem és la major potència i quantitat de RAM possibles per als nostres nodes però sense importar un alt consum, la mida, el preu o que no hi hagi ràdio incorporada per defecte, llavors les opcions adients són Intel Galileo i Intel Edison (40-60 EUR).

- Si el que necessitem és una computadora completa, amb ports Ethernet, HDMI, USB, etc. i a un preu assequible però no importa el consum ni la mida, llavors les millors opcions són Raspberry Pi+ i BeagleBone Black (35-37 EUR).

- Sí el que necessiten és el preu i la mida més petites, la millor opció és, sens dubte, TinyDuino (20 EUR, 20x20mm)

- Si el que es necessita és el menor consum possible, l'opció més adient és TelosB (TPR2420CA), seguida de Libelium Waspmote i TinyDuino.

- Si es necessiten motes que ja tinguin ràdio IEEE 802.15.4 incorporada, un baix consum i mida mitjana o petita, les opcions són Waspmote, TelosB, GINA i OpenMote.

- Si el que es necessita és una solució *plug & play* i la possibilitat d'instalar decenes de tipus de plaques de sensors ja predissenyades i provades, la millor solució és Waspmote (encara que el seu preu més entre 2.5 i 5 vegades més alt que altres opcions amb ràdio incorporada, fent que instal·lar una xarxa de centenars o milers de nodes sigui molt car).

- Com a millors opcions globals (relació entre mida Vs preu Vs consum) les millors opcions són TelosB, GINA i OpenMote. Entre aquestes tres, l'alternativa més equilibrada seria OpenMote, ja que disposa del triple de RAM que TelosB i GINA, així com 10-50 vegades més de memòria Flash, mentre que el preu únicament és 30 EUR superior al de TelosB (90 EUR Vs 57 EUR).

Per últim, es fa notar que totes les solucions de maquinari que incorporin una ràdio 802.15.4 poden, per tant, suportar 6LoWPAN i totes les tecnologies i protocols relacionats (RPL, UDP, CoAP) donat que el suport a aquestos vindrà determinat pel programari i, en concret, pel sistema operatiu que es faci servir, tal i com es podrà veure al següent apartat. Recordem que 6LoWPAN no és més que una capa d'integració que permet córrer IPv6 sobre ràdios que compleixin l'estàndard 802.14.5, sense haver de fer cap altra modificació a nivell de maquinari.

3.4.2. Programari

A l'apartat anterior –i als Annexos corresponents-- s'han vist els components de maquinari (MCUs, processadors, SoCs i plataformes de desenvolupament) més coneguts en l'actualitat per a R+D i prototipatge de xarxes de sensors sense fils, fent èmfasi en aquelles solucions més econòmiques, de menor mida i, sobretot, amb un consum de corrent més baix (a menor consum, més vida de les bateries); per tant, aquelles destinades a LLNs i M2M/IoT. Per la seva banda, pel que fa als sistemes operatius –programari- més coneguts per a IoT tenim: OpenWSN, Contiki, FreeRTOS, RIOT i TinyOS.

En línies generals, el que es buscarà en un sistema operatiu per a LLNs i aplicacions IoT és que accepti 802.15.4e (per exemple, TSCH), 6LoWPAN i tots els protocols de capa superior (RPL, CoAP). En altres paraules, que la pila de protocols implementi tot l'anterior.

A l'Annex XLI els pricinpicals SOs que hi ha actualment al mercat, així com els seus fabricants.

3.4.2.1. Comparativa

A continuació es mostra una taula resum amb tots els SOs vist fins ara, incloent algunes de les seves característiques principals: *footprint*, suport per a *multi-thread*, suport per a temps real, suport per a 6LoWPAN, suport per a TCP i modularitat.

SO	*Footprint (core)*	*Multi-thread*	Temps real	6LowPAN	TCP	Modularitat
OpenWSN	30 KB Flash 3.5 KB RAM	No	No	Sí	Sí	Sí (parcial)
Contiki	10 KB RAM 30 KB ROM	Sí (parcial)	Sí (parcial)	Sí	Sí	Sí
FreeRTOS	6-10 KB ROM	No	Sí	Sí	Sí	
RIOT	1.5 KB RAM 5 KB ROM	Sí	Sí	Sí	Sí (experimental)	Sí
TinyOS	400 bytes RAM	Sí (complet)	No	Sí	Sí (experimental)	No

Taula 9. Taula resum amb diversos SOs per a entorns IoT

Segons la taula anterior, les conclusions que s'extrauen són les següents:

- L'emprempta més petita és, de llarg, la de TinyOS, amb tant sols 400 bytes de RAM (únicament tenint en compte el *core* de l'SO; no es té en compte la implementació 6LowPAN). Per tant, en motes molt limitades a nivell de memòria i que tant sols necessiten IPv4, aquesta seria l'opció més adient.

- Si es necessita un SO amb suport complert de multi-fil (multi-tasca), llavors l'única opció adient és RIOT (TinyOS i Contiki també inclouen suport *multi-threading* però únicament parcial).

- Si es necessita un SO en temps real, les úniques opcions són FreeRTOS i RIOT.

- Si es necessita suport estable i complet per a TCP amb 6LoWPAN, les alternatives vàlides son OpenWSN, Contiki o FreeRTOS.

- Si es necessita suport per a TSCH (802.15.4e) l'única opció possible que l'implementa és, ara per ara, OpenWSN.

- En plaques que tan sols disposen de ROM i/o tenen molt poca RAM, l'SO a escollir seria FreeRTOS (ocupa molt poc i és *ROMable*).

- Si la manca de modularitat de l'SO i que no sigui *real-time* no és un problema, l'opció a escollir seria TinyOS, perquè el seu *footprint* en RAM és baixíssim.

- Si es necessita molt baix *footprint* però, a la vegada, temps real, multi-tasca i suport TCP (encara que aquest sigui experimental), la millor opció es RIOT.

- Si es necessita TCP estable amb 6LoWPAN i la RAM és molt límitada, s'ha d'escollir OpenWSN.

- Si es necessita TCP estable amb 6LoWPAN i tenim més RAM disponible o bé 30 KB de ROM, es pot escollir Contiki.

- Si no hi ha cap limitació, els "millors" SOs -els que tenen més prestacions- són Contiki i RIOT.

Per tant, a l'hora d'escollir un sistema operatiu o un altre per a les motes s'haurà de mirar, per un costat, les necessitats de les aplicacions que s'executaran a la xarxa (si necessiten temps real, si hi haurà vàries executant-se a la vegada, etc.) i, per altre costat, les limitacions de memòria del maquinari que tindrem al nostre abast (que moltes vegades, vindran determinades, al seu voltant, per limitacions de tipus econòmic o de consum de corrent elèctric).

4. Conclusions

En aquest treball, s'ha intentat donar una visió bastant ampla del concepte/paradigma d'Internet de les Coses i de tot allò que representa, tant a nivell de les tecnologies/protocols subjacents com dels àmbits d'aplicació on es pot fet servir aquesta nova forma de comunicació, així com els reptes de disseny que els enginyers i tècnics han d'afrontar per a la implementació de xarxes sense fils de cost i consum cada cop més baixos, amb milers o milions de nodes simultanis, operant en entorns difícils i desatesos.

Per un cantó, s'ha vist que la definició d'IoT transcendeix de la clàssica comunicació màquina-usuari i, fins i tot, d'una mera comunicació M2M -entre màquines- per passar a significar tota aquella comunicació entre "coses", ja siguin aquestes darreres persones, peces de roba, animals, ordinadors, etc. i fent servir Internet com a xarxa "aglutinadora" o intermitja entre les coses/objectes que es volen comunicar; a més, es pot fer servir, adicionalment i, de manera optativa, un servei de *cloud computing* per a emmagatzemar i processar les dades rebudes, si escau. Hem vist que aquest paradigma sorgeix com a evolució de l'actual tecnologia d'identificació d'objectes per etiquetes de radiofreqüència o RFID.

Per altra banda, s'ha vist que els àmbits d'aplicació de l'IoT són immensos: des d'usos militars fins a aplicacions industrials, passant per aplicacions domèstiques, agrícoles, *wearables*, gestió de la salut, ciutats intel·ligents, *smart grid*, previsió de temps, etc. En definitiva, el que el paradigma IoT pretèn és que qualsevol objecte quotidià que poguem imaginar pugui connectar-se a la Xarxa per tal d'enviar informació a altres objectes o centres de processament remots i actuar en conseqüència: des d'una simple ampolla de vi o un envàs de detergent, fins a una rentadora, un abric, un rellotge, un cotxe, un fanal o una grua poden tenir minúsculs nodes amb sensors incorporats que recullin i enviïn informació d'utilitat. D'aquesta manera, el que es busca és que aquesta informació, recollida com diem per mitjà de sensors incorporats als objectes, pugui ser útil per a l'usuari i, en definitiva, fer-li la vida més fàcil.

Els principals reptes a l'hora de dissenyar xarxes LLNs (aquelles amb dispositius de baix consum, baix cost i en entorns amb pèrdues) han estat fins ara múltiples, entre els quals cap destacar els següents: manca d'un estàndard –a ser posible, obert- ben definit i àmpliament adoptat pels fabricants per a la comunicació entre els nodes; necessitat de molt baix consum dels dispositius; bateries que durin anys sense necessitat de ser canviades; "resistència" a entorns difícils on pot haver-hi interferències; simplicitat en la comunicació entre nodes; manca d'adreces IPs suficients perquè tots els nodes d'una xarxa puguin ser visibles directament a Internet sense necessitat de fer mecanismes de traducció complexos; seguretat suficient per tal de garantir la integritat i confidencialitat de les dades transmeses.

Pel que fa als estàndards actuals per a la creació de xarxes sense fils de curt abast, està clar que els "reis" indiscutibles, avui per avui i si, parlem d'entorns domèstics, han estat i són encara Wi-Fi i Bluetooth. El principal problema d'aquests és que no estan optimitzats per a molt baix consum, ja que són tecnologies que presuposen que els dispositius estaran endollats contínuament al corrent elèctric o bé que les bateries dels mateixos es recarregaran periòdicament (per exemple cada un o dos dies). Per aquesta raó, han sorgit noves versions d'aquests estàndards, com ara Low-Power Wi-Fi o Bluetooth Low Energy (Bluetooth Smart) on s'intenta minimitzar el consum de bateria dels dispositius, fent servir determinades tècniques com ara MSC, TWT i TXOP (Low-Power Wi-Fi) o AFH i TSCH (BLE), per tal de disminuir el *duty cycle* o cicle de treball del node (posant-los a "dormir" si no estan emetent/rebent dades), disminuir la potència d'emissió de la ràdio i canvi de canal programat. Tot i així, aquestes dues tecnologies continuen estant més enfocades a entorns domèstics, on no hi hagi interferències extrenes i, de cara a IoT, el seu ús quedaria relegat a objectes com ara electrodomèstics, *smartphones*, ordinadors o *wearables*, així com BANs (xarxes d'àrea corporal).

Per la seva banda, per a xarxes en entorns industrials o agrícoles o simplement llocs oberts/extensos i més propensos a pèrdues i interferències, s'ha vist que hi ha altres tecnologies més adients, com ara ZigBee (l'estàndard de facto fins avui dia per a WSNs), WirelessHART, ISA 802.11a, wM-Bus, DASH7 o IEEE 802.15.4e. Igual que en el cas anterior de Low Power Wi-Fi i Bluetooth Smart, cada tecnologia intenta, a la seva manera, maximitzar la vida de les bateries, fent servir tècniques de canvi de canal, assignació de ranures temporals, disminució del *duty cycle*, etc. En qualsevol dels casos, tots aquests estàndars tenen els mateixos trets comuns: distàncies/rangs de cobertura màxims entre 50 i 100 metres; taxes de dades baixes, entre 40 i 250 Kbps; fan servir freqüències ISM (2.4 GHz o sub-1 GHz). Com ja hem dit abans, el concepte d'IoT és immés, com també ho són els seus àmbits d'aplicació. Per tant, en funció del problema concret a solucionar, serà més adient una tecnologia o una altra: per exemple, per a entorns oberts amb pluja o altres inclemències meteorològiques i aplicacions militars on s'hagin de cobrir grans distàncies, evitar interferències de la saturada banda de 2.4 GHz i es necessiti a més gran precisió de localització, probablemente DASH7 és l'opció més adient; en canvi, per a aplicacions de lectura de comptadors de gas, electricitat, aigua, etc. és molt adient wM-Bus; per la seva banda, com a estàndard *de facto* per a control de processos, tenim WirelessHART; per a comunicació entre aparalls electrònics esportius (rellotges, bicicletes, cotxes, etc.), potser ANT és la solució que més s'està implantant darrerament; per últim, com a solució "comodí", apta per a qualsevol tipus d'escenari, potser 802.15.4e-2012 és la més adient, per ser un estàndard obert, suportar per l'IEEE, força madur i amb una comunitat d'investigadors forta.

Si ens centrem en l'IEEE 802.15.4e (versió de l'any 2012) que, tot sembla indicar, serà el nou estàndard *de facto* per a LLNs, hem vist que es tracta d'una evolució de l'IEEE 802.15.4 original, on s'han afegit diverses tècniques que optimitzen molt més l'ús d'energia i serveixen per lluitar contra les interferències: DSME, TSCH (també present a WirelessHART), CLS i RIT. La finalitat és aconseguir que aquest estàndard sigui molt més adient per a entorns industrials que l'especificació original, apropant-lo al rendiment d'altres alternatives com DASH7 i WirelessHART.

Pel que fa al problema de la manca d'adreces amb IPv4, s'ha vist que la solució passa per fer servir estàndards que suportin de manera nativa IPv6; en concret, per a dispositius de mida petita, baix cost i baix consum, tenim l'alternativa de 6LoWPAN, que es "consagra" com a capa d'adaptació preferida per tal de permetre IPv6 en aquest tipus de dispositius limitats (per exemple, nodes basats en microcontroladors de 8 bits i amb molt poca memòria RAM). 6LowPAN "comprimeix" les capçalares dels paquets i, a més, permet fragmentació i reesamblatge, fent possible que la informació viatgi per xarxes on l'MTU és de 127 bytes (IEEE 802.15.4). D'aquesta manera, cada node de la nostra xarxa podrà tenir una adreça pública única i diferent i podrà ser accesible/visible directament des d'Internet.

Pel que fa als protocols de capa superior, al igual que passa amb els estàndards de capa PHY/MAC, ens trobem amb diverses opcions. Per exemple, pel que fa l'encaminament, hem vist que, per a WSNs, es pot escollir entre protocols reactius, proactius i híbrids, cadascun amb els seus avantatges i inconvenients (latència, *overhead*, etc.) essent RPL l'opció més avançada i adient avui dia, donat que és la que millor s'integra amb 6LoWPAN i els seus modes d'encaminament, tant a nivell 2 (*mesh-under*) i nivell 3 (*route over*). Per la seva banda, pel que fa als protocols de la capa d'aplicació, la majòria d'opcions es basen en transferència de missatges i esquemes de publicació/subscripció (MQTT, AMQP) tot i que l'opció més adient i lleugera per a aplicacions IoT sembla ser CoAP, que no és més que una "simplificació" del protocol HTTP clàssic i, per tant, compatible amb arquitectures web i que permet que la comunicació sigui possible quan hi ha elements de seguretat intermitjos, com ara tallafocs.

Pel que fa al maquinari disponible per als nodes, també hi ha mútiples possibilitats: existeixen des de SoCs i plataformes de desenvolupament basades en simples MCUs de 8 bits com també avançats processadors de 32 bits, cadascun amb freqüències de treball i quantitats de RAM/ROM molt diferents. L'elecció entre una plataforma i una altra dependrà bàsicament de les nostres necessitats de processament i del nostre pressupost, encara que també d'altres variables com ara el consum del node, tant quan està emetent com quan es troba *idle* o *sleeping*. Per exemple, si els requeriments de processament de les motes són molt baixos, probablement hi hagi prou amb un dispositiu senzill basat en l'MCU ATmega1281 de 8 bits (per exemple Libelium Waspmote, encara que aquesta es tracta d'una solució propietària que no es pot configurar *a priori*); si, pel contrari, es necessita un processador potent –per exemple, si el node, a més de recollir diverses dades simultàniament de varis sensors, les ha de processar abans d'enviar-les- s'haurà d'escollir llavors una plataforma més avançada, basada en una CPU de 32 bits, com ara OpenMote (SoC TI CC2538 amb CPU ARM Cortex-M3) o BeagleBone Black (ARM Cortex-A8); per la seva banda, una solució intermitja, pel que fa a processament, podria ser fer servir TelosB, amb una MCU TI MSP430 de 16 bits i un consum en estat *idle* molt baix. També s'ha de tenir en compte si el node pot funcionar, a més de com a *end-device*, com a *gateway*, és a dir, com a pasarel·la cap a una xarxa exterior, normalment Internet (per exemple, OpenMote ho permet de manera fàcil en conjunció amb OpenBase, un placa adicional que fa d'interfície amb l'exterior gràcies al seu port FE RJ-45).

Per últim, pel que fa al programari, l'elecció d'un sistema operatiu o un altre dependrà en gran mesura de les funcionalitats que volguem tenir disponibles i de la quantitat de RAM disponible al node. Per exemple, si necessitem la menor emprempta possible perquè la nostra MCU té molt poca RAM, l'opció més adient és fer servir TinyOS; per altra banda, si necessitem un SO en temps real i al mateix temps *multi-thread*, llavors l'única opció és RIOT; per la seva banda, si necessitem suport complet de l'IEEE 802.15.4e, incloent TSCH, l'opció a escollir seria OpenWSN (que també suporta 6LoWPAN, RPL, etc.)

En definitiva, podem concloure dient que l'àmbit d'aplicació de l'IoT és immens i presenta molts reptes, on moltes tecnologies i molts protocols es troben a l'abast dels enginyers i que permeten dissenyar xarxes més o menys escalables i eficients. Escollir una o altra tecnologia o protocol dependrà de la solució que s'hagi d'implementar i de l'escenari en el qual ens trobem; per tant, primer de tot, el que s'haurà de fer és determinar aquest escenari i els problemes que representa i llavors podrem escollir aquells protocols que millor els manegin. Com a solució per defecte i, segons el vist en aquest treball, es pot dissenyar una xarxa basada completament en estàndars oberts, formada per 802.15.4e per a les capes PHY/MAC, 6LoWPAN com a capa d'integració IPv6, RPL com a protocol d'encaminament, CoAP com a protocol d'aplicació, OpenMote o TelosB com a maquinari dels nodes i OpenWSN com a sistema operatiu basat en 802.15.4e.

Glossari

- 3GPP: *Third Generation Partnership Project*
- 6LoWPAN: *IPv6 over Low power Wireless Personal Area Networks*
- ABR: *Associativity Based Routing*
- ACK: *Acknowledgment*
- ACL: *Access Control List*
- ACOR: *Admission Control Enabled On-Demand Routing*
- ADC: *Analog-To-Digital Converter*
- AES: *Advanced Encryption Algorithm*
- AES-CTR: *AES - Counter Mode*
- AES-CBC-MAC: *AES - Cipher Block - Chaining Message Authentication Code*
- AES-CCM: *AES CTR and CBC-MAC*
- AFH: *Adaptative Frequency Hopping*
- AIDC: *Automatic Identification and Data Capture*
- AMI: *Advanced Metering Infrastructure*
- AMC: *Adaptative Modulation and Coding*
- AMQP: *Advanced Message Queuing Protocol*
- AODV: *Ad-hoc On Demand Distance Vector Routing*
- API: *Application Programming Interface*
- ARPANET: *Advanced Research Projects Agency Network*
- A-TSCH (IEEE 802.15.4e): *Adaptative TSCH*
- BAN: *Body Area Network*
- BAP (RFID): *Baterry-Assisted Passive*
- BI (IEEE 802.15.4): *Beacon Interval*
- BLE: *Bluetooth Low Energy*
- BPSK: *Binary-Phase Shift Keying*
- BR (Bluetooth): *Basic Rate*
- BS: *Base Station*
- CAP (IEEE 802.15.4): *Contention Access Period*
- CCA: *Clear Channel Assesment*
- CCSA: *China Communications Standard Association*
- CFP (IEEE 802.11e-2005): *Contention-Free Period*
- CGSR: *Clusterhead Gateway Switch Routing*
- CoAP: *Constrained Application Protocol*
- CoRE (grup): *Constrained Resource Environment*
- CPE: *Customer Premises Equipment*
- CPU: *Central Processing Unit*
- CR: *Cognitive Radio*
- CSL (IEEE 802.15.4e): *Coordinated Sampled Listening*
- CSMA/CA: *Carrier Sense Multiple Access with Collision Avoidance*
- CSMA/CD: *Carrier Sense Multiple Access with Collision Detection*
- CSS: *Chrip Spread Spectrum*

- CT (DECT): *Cordless Telephone*
- CTP: *Collection Tree Protocol*
- D2D: *Device-To-Device*
- DAC: *Digital-To-Analog Converter*
- DAFO (matriu): Debilitats, Amenaces, Fortaleses, Oportunitats
- DAG: *Directed Acyclic Graph*
- DAO: DoDAG Destination Advertisement Object
- DARPA: *Defense Advanced Research Projects Agency*
- DDS: *Data Distribution Service*
- DECT: *Digital Enhanced Cordless Telecommunications*
- DHCP: *Dynamic Host Configuration Protocol*
- DIO: *DODAG Information Object*
- DIS: *DODAG Information Solicitation*
- DoD: *Department of Defense of the USA*
- DODAG: *Destination Oriented DAG*
- DPSK: *Differential Phase-Shift Keying*
- DQPSK: *Differentiak QPSK*
- DSDV: *Destination-Sequenced Distance Vector*
- DSME (IEEE 802.15.4e): *Deterministic & Synchronous Multichannel Extension*
- DSP: *Digital Signal Processor*
- DS-UWB: *Direct Sequence Ultra-Wide Band*
- DSN: *Distributed Sensor Network*
- DSR: *Dynamic Source Routing*
- DSSS: *Direct-Sequence Spread Spectrum*
- DYMO: *Dynamic MANET On-Demand*
- E2E: *End-To-End*
- EB (IEEE 802.15.4e): *Enhanced Beacon*
- EBR (IEEE 802.15.4e): *Enhanced Beacon Request*
- EDR (Bluetooth): *Enhanced Data Rate*
- EEPROM: *Electrically Erasable Programmable ROM*
- EM: *Electromagnetic*
- EN (norma): *European Norm*
- ETSI: *Europen Telecommunications Standards Institute*
- EXI (XMPP): *Efficient XML Interface*
- FDD: *Frequency-Division Duplex*
- FFD (ZigBee): *Full-Function Device*
- FHSS: *Frequency-Hopping Spread Spectrum*
- FTP: *File Transfer Protocol*
- GAP (DECT): *Generic Access Profile*
- GDB: *Geolocation Database*
- GIFSI: *Global ICT Standardization Forum for India*
- GFSK: *Gaussian Frequency-Shift Keying*
- GPRS: *General Packet Radio Service*

- GPS: *Global Positioning System*
- GSC: *Global Standars Collaboration*
- GSM: *Global System for Mobile Communications*
- GTS (ZigBee): *Guaranteed Time Slot*
- HART: *Highway Addressable Remote Transducer*
- HDMI: *High-Definition Multimedia Interface*
- HDTV: *High Definition TV*
- HTTP: *HyperText Transfer Protocol*
- HVAC: *Heating, Ventilating and Air Conditioning*
- HW: *Hardware*
- IaaS: *Infrastructure as a Service*
- IANA: *Internet Assigned Numbers Authority*
- ICMP: *Internet Control Message Protocol*
- ID: *Identifier*
- IDC (empresa): *International Data Corporation*
- IE (IEEE 802.11): *Information Element*
- IEC: *International Electrotechnical Commission*
- IEEE: *Institute of Electrical and Electronics Engineers*
- IETF: *Internet Engineering Task Force*
- IoT: *Internet of Things*
- IP: *Internet Protocol*
- ISA: *International Society of Automation*
- ISM: *Industrial, Scientific and Medical*
- ISO: *International Organitzation for Standardization*
- IS-IS: *Intermediate System to Intermediate System*
- ITU: *International Telecommunication Union*
- LLC: *Logical Link Control*
- LLDN (IEEE 802.15.4e): *Low Latency Deterministic Network*
- LLN: *Low Power and Lossy Networks*
- LOAD: *6LoWPAN Ad-Hoc On-demand Distance Vector Routing*
- LoS: *Line of Sight*
- LR-WPAN: *Low Rate WPAN*
- LTE: *Long Term Evolution*
- M2M: *Machine-To-Machine*
- M2P: *Machine-To-People*
- MAC: *Medium Access Control*
- MACsec: *Media Access Control Security*
- MANET: *Mobile Ad Hoc Network*
- M-Bus: *Meter-Bus*
- MBWA: *Mobile Broadband Wireless Access*
- MC: *Multi Carrier*
- MCU: *Microcontroller Unit*
- MIMO: *Multiple Input - Multiple Output*

- MIoT: *Military Internet of Things*
- MIT: *Massachusetts Institute of Technology*
- MHR: *MAC Header*
- MQTT: *Message Queuing Telemetry Transport*
- MTU: *Maximum Transmission Unit*
- NAT: *Network Address Translation*
- NFC: *Near Field Communications*
- NHL: *Next Higher Layer*
- OASIS: *Organization for the Advancement of Structured Information Standards*
- OCR: *Optical Character Recognition*
- OFDM: *Orthogonal Frequency-Division Multiplexing*
- OFDMA: *Orthogonal Frequency-Division Multiple Access*
- OMA: *Open Mobile Alliance*
- OS: *Operating System*
- OSI: *Open Systems Interconnection*
- OSLR: Optimized Link State Routing
- OSPF: *Open Shortest Path First*
- O-QPSK: *Orthogonal QPSK*
- P2MP: *Point to Multipoint*
- P2P: *Peer to Peer/ Point to Point*
- PAN: *Personal Area Network*
- PBX: *Public Branch Exchange*
- PCB: *Printed Circuit Board*
- PDU: *Protocol Data Unit*
- PHY: *physical layer*
- PIB (xarxa): *PAN Information Base*
- QoS: *Quality of Service*
- QPSK: *Quadrature Phase Shift Keying*
- QR (codi): *Quick Response*
- RAM: *Random Access Memory*
- REST (arquitectura): *Representational State Transfer*
- RIT (IEEE 802.15.4e): *Receiver Initiated Transmission*
- RF: *Radio Frequency*
- RFC: *Request For Comments*
- RFD (Zigbee): *Reduced-Function Device*
- RFID: *Radio-Frequency Identification*
- ROM: *Read-Only Memory*
- RPL: *Routing Protocol for Low-Power and Lossy Networks*
- RTLS: *Real Time Location System*
- RX: recepció
- RZ Time (IEEE 802.15.4e): *Rendez-vous Time*
- R+D: *Research and Development*
- S1G (banda): *Sub-1 GHz*

- SALS: *Simple Authentication and Security Layer*
- SCTP: *Stream Control Transmission Protocol*
- SDMA: *Space-Division Multiple Access*
- SIG (Bluetooth): *Special Interest Group*
- SMTP: *Simple Mail Transfer Protocol*
- SNR: *Signal-To-Noise Ratio*
- SO*: Sistema Operatiu*
- SOA: *Services-Oriented Architecture*
- SoC: *System on a Chip*
- SRD: *Short Range device*
- SSL: *Secure Sockets Layer*
- SUN: *Smart Utility Networks*
- SW: *Software*
- SWOT: *Strengths, Weaknesses, Opportunities, Threats*
- TCO: *Total Cost of Ownership*
- TCP: *Transmission Control Protocol*
- TDD: *Time-Division Duplex*
- TIA: *Telecommunications Industry Association*
- TG: *Task Group*
- TLS: *Transport Security Layer*
- TORA: *Temporally Ordered Routing Algorithm*
- TSCH: *Time-Slotted Channel Hopping*
- TSMP: *Time Synchronized Mesh Protocol*
- TV: *Television*
- TX: *transmissió*
- UART: *Universal Asynchronous Receiver-Transmitter*
- uC: *microcontroller*
- UDP: *User Datagram Protocol*
- UHF: *Ultra High Frequency*
- ULE (DECT): *Ultra Low Energy*
- ULP (Bluetooth): *Ultra Low Power*
- URI: *Uniform Resrouce Identifier*
- USB: *Universal Serial Bus*
- UWB: *Ultra Wide Band*
- V2V: *Vehicle-To-Vehicle*
- VLC: *Visible Light Communications*
- VHF: *Very High Frequency*
- VoIP: *Voice over IP*
- WAN: *Wide Area Network*
- WG: *Working Group*
- WRAN: *Wireless Regional Area Network*
- Wi-Fi: *Wireless Fidelity*
- WiMAX: *Worldwide Interoperability for Microwave Access*

- WLAN: *Wireless Local Area Network*
- WMAN: *Wireless Metropolitan Area Network*
- wM-Bus: *Wireless M-Bus*
- WORM: *Write Once Read Many*
- WPA2: *Wi-Fi Protected Access 2*
- WPAN: *Wireless Personal Area Network*
- WRP: *Wireless Routing Protocol*
- WSN: *Wireless Sensor Networks*
- XML: *eXtensible Markup Language*
- XMPP: *eXtensible Messaging and Presence Protocol)*
- XSF: *XMPP Standards Foundation*
- ZAO (ZigBee): *ZigBee Aplication Objects*
- ZDO (ZigBee): *ZigBee Device Objects*
- ZRP: *Zone Routing Protocol*

Referències

Llibres, articles i tesis

[1] Yibo Chen, Jean-Pierre Chanel, Kun Mean Hou. "RPL Routing Protocol a Case Study: Precision Agriculture". First China-France Workshop on Future Computing Technology (CF-WoFUCT 2012). February 2012.
http://hal.inria.fr/docs/00/68/13/19/PDF/cf2012-pub00035236.pdf
[Data darrer accés: 11/01/2015]

[2] Thomas Watteyne, Xavier Vilajosana, Branko Kerkez, Fabien Chraim, Kevin Weekly, Qin Wang, Steven Glaser, Kris Pister. "OpenWSN: A Standards-Based Low-Power Wireless Development Environment". Transactions on Emerging Telecommunications Technologies.Volume: 23: Issue 5. 480–493. August 2012.
http://onlinelibrary.wiley.com/doi/10.1002/ett.2558/abstract
[Data darrer accés: 11/01/2015]

[3] Leila Ben Saad, Cedric Chauvenet, Bernard Tourancheay. "Simulation of the RPL Routing Protocol for IPv6 Sensor Networks: two cases studies". International Conference on Sensor Technologies and Applications SENSORCOMM 2011. August 2011.
http://hal.inria.fr/hal-00647869
[Data darrer accés: 11/01/2015]

[4] Ulrich Herberg, Thomas Clausen. "A Comparative Performance Study of the Routing Protocols Load and RPL with Bi-Directional Traffic in Low-power and Lossy Networks (LLN)". PE-WASUN 2011. November 2011.
http://www.herberg.name/downloads/pubs/PEWASUN_11.pdf
[Data darrer accés: 11/01/2015]

[5] Joakim Flathagen. "A routing and cross-layer approach for energy and bandwidth efficiency in Wiresless Sensor Networks".Norwegian University of Science and Technology, Faculty of Information Technology, Mathematics and Electrical Engineering. October 2013.
http://www.diva-portal.org/smash/get/diva2:662516/FULLTEXT02
[Data darrer accés: 11/01/2015]

[6] Jürgen Schönwälder. "Internet of Things: 802.15.4, 6LoWPAN, RPL, CoAP". Jacobs University. October 2010.
http://www.utwente.nl/ewi/dacs/Colloquium/archive/2010/slides/2010-utwente-6lowpan-rpl-coap.pdf
[Data darrer accés: 11/01/2015]

[7] Trang Tran Thi Thuy. “Routing protocols in Internet of Things”. Aalto University, School of Science and Technology. December 2011.
https://wiki.aalto.fi/download/attachments/59704179/trang-tran-routing-protocols-in-iot.pdf?version=1&modificationDate=1324369299000
[Data darrer accés: 11/01/2015]

[8] Ketan Devadiga. “IEEE 802.15.4 and the Internet of Things”. Aalto University, School of Science and Technology. December 2011.
https://wiki.aalto.fi/download/attachments/59704179/trang-tran-routing-protocols-in-iot.pdf?version=1&modificationDate=1324369299000
[Data darrer accés: 11/01/2015]

[9] Markku Laine. “RESTful Web Services for the Internet of Things”. Aalto University, School of Science and Technology. December 2011.
https://wiki.aalto.fi/download/attachments/59704179/laine-restful-web-services.pdf?version=2&modificationDate=1324369128000&api=v2
[Data darrer accés: 11/01/2015]

[10] Mikko Lampi. “Internet of Things. Ambient Energy Harvesting”. Aalto University, School of Science and Technology. December 2011.
https://wiki.aalto.fi/download/attachments/59704179/lampi-iot-ambient-energy-harvesting.pdf?version=1&modificationDate=1324369156000&api=v2
[Data darrer accés: 11/01/2015]

[11] Timo Töyry. “Self-management in Internet of Things”. Aalto University, School of Science and Technology. December 2011.
https://wiki.aalto.fi/download/attachments/59704179/toyry-self-management.pdf?version=1&modificationDate=1324369262000&api=v2
[Data darrer accés: 11/01/2015]

[12] Jon T. Adams. “An Introduction to IEEE STD 802.15.4”.Freescale Semiconductor Inc. Sonoma State University.
http://www.sonoma.edu/users/f/farahman/sonoma/courses/cet543/resources/802_intro_01655947.pdf
[Data darrer accés: 11/01/2015]

[13] Giuseppe Anastasi. “From IEEE 802.15.4 to IEEE 802.15.4e.Another Step towards the Internet of (Important) Things”. Sun Yat-Sen University. May 2014.
http://www.iet.unipi.it/g.anastasi/talks/2014-Guangzhou.pdf
[Data darrer accés: 11/01/2015]

[14] Qinghua Wang and Ilangko Balasingham (2010). ”Wireless Sensor Networks - An Introduction, Wireless Sensor Networks: Application-Centric Design”. Yen Kheng Tan (Ed.), ISBN: 978-953-307-321-7, InTech
http://www.intechopen.com/books/wireless-sensor-networks-application-centric-design/wireless-sensornetworks-an-introduction
[Data darrer accés: 11/01/2015]

[15] Nick Hunn. “Essentials of Short-Range Wireless”. Cambridge University Press.ISBN: 978-0-521-76069-0 Hardback. Uniked Kingdom, 2010.
[Data darrer accés: 11/01/2015]

[16] LAn Yushi, Jiang Fei, Yu Hui. “Study on Application Modes of Military Internet of Things (MIoT)”. China Electronics Technology Group Corporation. Naijing, China.
http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6273031
[Data darrer accés: 11/01/2015]

[17] César Sanz Álvaro. “El Internet de las Cosas y los nuevos riesgos para la privacidad”. Universidad Politécnica de Madrid. Julio 2012.
http://oa.upm.es/14543/
[Data darrer accés: 11/01/2015]

[18] Stefan Herbert Aust. “Advanced Wireless Local Area Networks in the Unlicensed Sub-1GHz ISM-bands”. Delf University of Technology.The Netherlands. June 2014.
http://www.es.ewi.tudelft.nl/phd-theses/2014-Aust.pdf
[Data darrer accés: 11/01/2015]

[19] Diversos autors. “Requirements for WiMAX Machine to Machine (M2M) Communication.WMF-T31-127-v01”. WiMAX Forum. 2011.
http://resources.wimaxforum.org/sites/wimaxforum.org/files/technical_document/2012/05/WMF-T31-127-v01_M2M_Requirements_Spec.pdf
[Data darrer accés: 11/01/2015]

[20] Levis, S. Madden, J. Polastre, R. Szewczyk, K. Whitehouse, A. Woo,
D. Gay, J. Hill, M. Welsh, E. Brewer, and D. Culler. “TinyOS: An Operating System for Sensor Networks”. Berkeley University.
http://www.cs.berkeley.edu/~culler/papers/ai-tinyos.pdf
[Data darrer accés: 11/01/2015]

[21] Anis Koubaa, Mário Alves, Eduardo Tovar. “GTS Allocation Analysis in IEEE 802.15.4for Real-Time Wireless Sensor Networks”. IPP-HURRAY! Research Group, Polyctechnic Institute of Porto. April 2006.
http://www.open-zb.net/publications/tr-hurray-060404.pdf
[Data darrer accés: 11/01/2015]

[22] Pedram Radmand, Alex Talevski, Stig Petersen, Simon Carlsen. “Comparison of Industrial WSN Standards”. 4th IEEE International Conference on Digital Ecosystems and Technologies IEEE DEST 2010).
http://praia.unik.no/images/1/16/Comparison_of_Industrial_WSN_Standards.pdf
[Data darrer accés: 11/01/2015]

[23] Stig Petersen, Simon. Carlsen, IEEE Industrial Electronics Magazine. “WirelessHART Versus ISA100.11a”. DOI 10.1109/MIE.2001.943023. December 2011.
https://noppa.aalto.fi/noppa/kurssi/as-74.3199/luennot/AS-74_3199_wirelesshart_vs_isa100.11a.11a_-_the_format_war_hits_the_factory_floor.pdf
[Data darrer accés: 11/01/2015]

[24] Feng Wang, Dou Li, Yuping Zhao. “Analysis and Compare of Slotted and Unslotted CSMA in IEEE 802.15.4” School of Electronics Engineering and Computer Science, Peking Unversity. September 2009.
http://ieeexplore.ieee.org/iel5/5300798/5300799/05303580.pdf?arnumber=5303580
[Data darrer accés: 11/01/2015]

[25] Peng Du. “Adaptive Time Slotted Channel Hopping for Wireless Sensor Networks”. Department of Computer Science and Information Systems, University of London. United Kingdom.
http://www.dcs.bbk.ac.uk/~gr/pdf/ceec12.pdf
[Data darrer accés: 11/01/2015]

[26] Harjeet Kaur, Varsha Sahni, Dr. Manju Bala. “A survey of Reactive, Proactive and Hybrid Routing Protocols in MANET: A Review”. International Journal of Computer Science and Information Technologies.Vol. 4 (3), 2013.
http://www.ijcsit.com/docs/Volume%204/vol4Issue3/ijcsit2013040326.pdf
[Data darrer accés: 11/01/2015]

[27] Malisa Vucinic, Bernard Tourancheau, Andrzej Duda. "Performance Comparison of the RPL and LOADng Routing Protocols in a Home Automation Scenario".CNRS Grenoble Informatics Laboratory, University of Grenoble. Grenoble, France
https://hal.archives-ouvertes.fr/file/index/docid/923851/filename/rpl-loadng-wcnc.pdf
[Data darrer accés: 11/01/2015]

[28] Omprakash Gnawali, Leonidas Guibas, Philips Levis. “A Case for Evaluating Sensor Network Protocols Concurrently”.WinTECH ’10, Chicago, USA. September 2010.
https://sing.stanford.edu/pubs/wintech10-gnawali.pdf
[Data darrer accés: 11/01/2015]

[29] Adam Dunkels. “The ContikiMAC Radio Duty Cycling Protocol”. SIC Technical Report T2011:13, ISSN 1100-3154. December 2011.
http://dunkels.com/adam/dunkels11contikimac.pdf
[Data darrer accés: 11/01/2015]

Llocs web

[30] OpenMote
http://www.openmote.com/
[Data darrer accés: 11/01/2015]

[31] Connecting Sensor Networks
https://www.youtube.com/watch?v=ikFosQd-stA
[Data darrer accés: 11/01/2015]

[32] UC Berkeley EECS - IEEE STD 802.15.4: Enabling Pervasive Wireless Access Networks
http://www.cs.berkeley.edu/~prabal/teaching/cs294-11-f05/slides/day21.pdf
[Data darrer accés: 11/01/2015]

[33] IETF – RFC7252 (CoAP)
http://tools.ietf.org/html/rfc7252
[Data darrer accés: 11/01/2015]

[34] AMQP - Examples
https://www.amqp.org/about/examples
[Data darrer accés: 11/01/2015]

[35] IETF - Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks
http://tools.ietf.org/html/rfc6282
[Data darrer accés: 11/01/2015]

[36] IEEE – IEEE Get Program
http://standards.ieee.org/about/get/802/802.15.html
[Data darrer accés: 11/01/2015]

[37] A Guide to Succeeding in the Internet of Things
http://www.slideshare.net/claropartners/a-guide-to-succeeding-in-the-internet-of-things
[Data darrer accés: 11/01/2015]

[38] OpenWSN
http://www.openmote.com/openwsn/
[Data darrer accés: 11/01/2015]

[39] TinyOS
http://www.tinyos.net/
[Data darrer accés: 11/01/2015]

[40] Towards an Interoperable, Scalable and Evolvable Internet of Things
http://www.slideshare.net/waltercolitti/iotgent-presentation-walter
[Data darrer accés: 11/01/2015]

[41] Instant Contiki
http://sourceforge.net/projects/contiki/files/Instant%20Contiki/
[Data darrer accés: 11/01/2015]

[42] 35 Open Source Tools for the Internet of Things
http://www.datamation.com/open-source/35-open-source-tools-for-the-internet-of-things-1.html
[Data darrer accés: 11/01/2015]

[43] IoT Barcelona
http://www.meetup.com/iotbarcelona/
[Data darrer accés: 11/01/2015]

[44] NXP JN5168-RD6040 IoT gateway
http://www.nxp.com/demoboard/JN5168-RD6040.html
[Data darrer accés: 11/01/2015]

[45] TST Sistemas
http://www.tst-sistemas.es/
[Data darrer accés: 11/01/2015]

[46] Intel Edison Module
http://www.intel.com/content/www/us/en/do-it-yourself/edison.html
[Data darrer accés: 11/01/2015]

[47] Goldman Sachs - What is the Internet of Things?
http://www.goldmansachs.com/our-thinking/outlook/iot-infographic.html
[Data darrer accés: 11/01/2015]

[48] Goldman Sachs - The Internet of Things: Making sense of the next mega-trend
http://www.goldmansachs.com/our-thinking/outlook/internet-of-things/iot-report.pdf
[Data darrer accés: 11/01/2015]

[49] Wind River –Security in the Internet of Things
http://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf
[Data darrer accés: 11/01/2015]

[50] Cisco Blogs - Milestone in Connecting the Internet of Things – RPL Routing Standard Completed
https://blogs.cisco.com/news/rpl-routing-standard-completed/
[Data darrer accés: 11/01/2015]

[51] Postscapes – Internet of Things Hardware
http://postscapes.com/internet-of-things-hardware
[Data darrer accés: 11/01/2015]

[52] Atmel – Single Chip Solutions
http://www.atmel.com/products/wireless/802154/single-chip_solutions.aspx
[Data darrer accés: 11/01/2015]

[53] HP – Cense
http://www8.hp.com/us/en/hp-information/environment/cense.html#.VCrkzPna5cY
[Data darrer accés: 11/01/2015]

[54] Postscapes – Internet of Things software
http://postscapes.com/internet-of-things-software-guide
[Data darrer accés: 11/01/2015]

[55] About Technology - Wireless Standards - 802.11a, 802.11b/g/n, and 802.11ac
http://compnetworking.about.com/cs/wireless80211/a/aa80211standard.htm
[Data darrer accés: 11/01/2015]

[56] Digi -Demystifying 802.15.4 and ZigBee
http://www.digi.com/pdf/wp_zigbee.pdf
[Data darrer accés: 11/01/2015]

[57] ThinkMind Digital Library - IEWMC 2012: Evaluation of Routing Protocols for Internet-Enabled Wireless Sensor Network
http://www.thinkmind.org/download.php?articleid=icwmc_2012_3_30_20243
[Data darrer accés: 11/01/2015]

[58] AnandTech – ARM announces 'mbed' IoT Device Platform
http://www.anandtech.com/show/8583/arm-announces-mbed-iot-device-platform
[Data darrer accés: 11/01/2015]

[59] Université d'Avignon – MindTeck: 6LoWPAN Technical Overview
http://projets-gmi.univ-avignon.fr/projets//proj1112/M1/p09/doc/6LoWPAN_overview.pdf
[Data darrer accés: 11/01/2015]

[60] Xataka – Intel Edison es el triunfo de la miniaturización para una nueva era de los "wearables"
http://www.xataka.com/otros/intel-edison-el-triunfo-de-la-miniaturizacion-y-la-nueva-era-de-los-wearables
[Data darrer accés: 11/01/2015]

[61] Sensor Networks – Security in 802.15.4 and ZigBee networks
http://www.sensor-networks.org/index.php?page=0903503549
[Data darrer accés: 11/01/2015]

[62] Wikipedia – Bluetooth Low Energy
http://en.wikipedia.org/wiki/Bluetooth_low_energy
[Data darrer accés: 11/01/2015]

[63] Bluetooth – Bluetooth Core Specification 4.1
https://www.bluetooth.org/en-us/specification/adopted-specifications
[Data darrer accés: 11/01/2015]

[64] Slideshare – An Introduction to IoT protocols
http://www.slideshare.net/vgholkar/io-t-protocolsoscon2014
[Data darrer accés: 11/01/2015]

[65] MDPI Open Access Publishing – Flexible Unicast-Based Group Communication for CoAP-Enabled Devices
http://www.mdpi.com/1424-8220/14/6/9833
[Data darrer accés: 11/01/2015]

[66] Electronic Design – Understanding The Internet of Things
http://electronicdesign.com/communications/understanding-internet-things
[Data darrer accés: 11/01/2015]

[67] Arc Advisory Group – The Internet of Things is much more than M2M
http://www.arcweb.com/strategy-reports/2014-03-07/the-internet-of-things-is-much-more-than-m2m-1.aspx
[Data darrer accés: 11/01/2015]

[68] RFID Journal – That 'Internet of Things' Thing
http://www.rfidjournal.com/articles/view?4986
[Data darrer accés: 11/01/2015]

[69] Global Information – M2M and Cloud as the Foundation for the Internet of Things
http://www.giiresearch.com/report/mar247059-m2m-cloud-foundation-internet-things.html
[Data darrer accés: 11/01/2015]

[70] Intelligent HQ – Guide to the Internet of Things Part 2: SWOT Analysis
http://www.intelligenthq.com/technology/guide-internet-things-part-2-swot-analysis/
[Data darrer accés: 11/01/2015]

[71] KTH University - IEEE 802.15.4, ZigBee , WirelessHARTWirelessHART, ISA SP-100, ROLL100, ROLL
https://people.kth.se/~carlofi/teaching/pwsn-2009/lectures/lec6.pdf
[Data darrer accés: 11/01/2015]

[72] Xataca – Telefonica lanza Thinking Thinks y se implica de lleno en la Internet de las Cosas
http://www.xataka.com/accesorios/telefonica-lanza-thinking-things-y-se-implica-de-lleno-en-la-internet-de-las-cosas?utm_content=bufferbf274&utm_medium=social&utm_source=linkedin.com&utm_campaign=buffer
[Data darrer accés: 11/01/2015]

[73] Silicon Labs – The evolution of Wireless Sensor Networks
http://www.silabs.com/Support%20Documents/TechnicalDocs/evolution-of-wireless-sensor-networks.pdf
[Data darrer accés: 11/01/2015]

[74] Nivis Wireless Sensor Networks – Evolution of Wireless Sensor Networks for Industrial Control
http://www.nivis.com/resources/Low_TIMReview_May2013.pdf
[Data darrer accés: 11/01/2015]

[75] eWeek – A look back at Internet of Things' origin, evolution
http://www.eweek.com/networking/slideshows/a-look-back-at-internet-of-things-origin-evolution.html/
[Data darrer accés: 11/01/2015]

[76] Internet-of-Things Architecture (IoT-A). Project Deliverable D3.1 – Initial M2M API Analysis
http://www.iot-a.eu/public/public-documents/d3.1/at_download/file
[Data darrer accés: 11/01/2015]

[77] IPSO Alliance – ETSI M2M workshop Nov 2013
http://docbox.etsi.org/Workshop/2013/201311_M2MWORKSHOP/S02_ENABLINGTECHNOLOGIES/IPSO_WETTERWALD.pdf
[Data darrer accés: 11/01/2015]

[78] Postscapes – Internet of Things Protocols & Standards
http://postscapes.com/internet-of-things-protocols
[Data darrer accés: 11/01/2015]

[79] Freie Universität Berlin - Embedded Internet and the Internet of Things
https://www.mi.fu-berlin.de/inf/groups/ag-tech/teaching/2012-13_WS/L_19528_Embedded_Internet_and_the_Internet_of_Things/06.pdf?1358508475
[Data darrer accés: 11/01/2015]

[80] CMS Wire – Collaboration and the Internet of Things
http://www.cmswire.com/cms/information-management/collaboration-and-the-internet-of-things-022988.php
[Data darrer accés: 11/01/2015]

[81] Silicon Labs – The Internet of Things
http://www.silabs.com/products/pages/internet-of-things.aspx
[Data darrer accés: 11/01/2015]

[82] Clarice Technologies – The Internet of Things: hype and potential
http://claricetechnologies.com/blog/2014/03/demystifying-the-internet-of-things/
[Data darrer accés: 11/01/2015]

[83] Libelium – 50 sensor applications for a smarter world
http://www.libelium.com/es/top_50_iot_sensor_applications_ranking/
[Data darrer accés: 11/01/2015]

[84] Wireless T/ICT4D Lab - Wireless Workshop for Science in Africa 2013
http://wireless.ictp.it/school_2013/schedule.html
[Data darrer accés: 11/01/2015]

[85] IoT World – Smart devices improve farm operations
http://www.iotworld.com/author.asp?section_id=3150&doc_id=561056
[Data darrer accés: 11/01/2015]

[86] Wikipedia – Anàlisi DAFO
http://es.wikipedia.org/wiki/An%C3%A1lisis_DAFO
[Data darrer accés: 11/01/2015]

[87] IRISA (Institut de Recherce en Informatique et Systèmes Alèatoires) – SWOT Analysis
http://www.irisa.fr/tipi/wiki/doku.php/probe-it_project
[Data darrer accés: 11/01/2015]

[88] Intelligent HQ – Guide to the Internet of Things Part 2: SWOT Analysis
http://www.intelligenthq.com/technology/guide-internet-things-part-2-swot-analysis/
[Data darrer accés: 11/01/2015]

[89] Publico - ¿Por qué no despega el 4G en España?
http://blogs.publico.es/kaostica/2014/06/17/telefonia-4g/
[Data darrer accés: 11/01/2015]

[90] Wikipedia – IEEE 802.11
http://en.wikipedia.org/wiki/IEEE_802.11
[Data darrer accés: 11/01/2015]

[91] EDN Network - Tiny low-power Wi-Fi module enables Internet of Things
http://www.edn.com/electronics-products/other/4373837/Tiny-low-power-Wi-Fi-module-enables-Internet-of-Things-4373837
[Data darrer accés: 11/01/2015]

[92] Wikipedia – IEEE 802.11n-2009
http://en.wikipedia.org/wiki/IEEE_802.11n-2009
[Data darrer accés: 11/01/2015]

[93] EE Times – How much transmit power do WiMAX nets need?
http://www.eetimes.com/document.asp?doc_id=1271732
[Data darrer accés: 11/01/2015]

[94] National Instruments – Introduction to WiMAX Transmitter Measurements
http://www.ni.com/white-paper/8976/en/
[Data darrer accés: 11/01/2015]

[95] Wikipedia – Differentiated Services
http://en.wikipedia.org/wiki/Differentiated_services
[Data darrer accés: 11/01/2015]

[96] Qualcomm – Developing for Bluetooth Smart Beacons
https://developer.qualcomm.com/blog/developing-bluetooth-smart-beacons-new-white-paper-and-limited-time-promotion
[Data darrer accés: 11/01/2015]

[97] Bluetooth – Bluetooth Low Energy
https://www.bluetooth.org/DocMan/handlers/DownloadDoc.ashx?doc_id=227336
[Data darrer accés: 11/01/2015]

[98] CSR – CSRmesh Development kit
http://www.csr.com/products/csrmesh-development-kit
[Data darrer accés: 11/01/2015]

[99] The Sensor Network Museum – Tmote Sky
http://www.snm.ethz.ch/Projects/TmoteSky
[Data darrer accés: 11/01/2015]

[100] MEMSICPoweful Sensing Solutions – TelosB wireless measurement system
http://www.memsic.com/userfiles/files/Datasheets/WSN/telosb_datasheet.pdf
[Data darrer accés: 11/01/2015]

[101] Wikipedia – Contiki
http://en.wikipedia.org/wiki/Contiki
[Data darrer accés: 11/01/2015]

[102] Texas Instruments - Zigbee Tree Addressing (Cskip) explained
http://e2e.ti.com/support/wireless_connectivity/f/158/t/17257.aspx
[Data darrer accés: 11/01/2015]

[103] The Network Simulator NS-2
http://www.isi.edu/nsnam/ns/
[Data darrer accés: 11/01/2015]

[104] OPNET - IT Guru Academic Edition
[Data darrer accés: 11/01/2015]
http://www.opnet.com/university_program/itguru_academic_edition/

[105] TETCOS - Netsim Platform for Network R&D
http://www.tetcos.com/netsim_comp.htm
[Data darrer accés: 11/01/2015]

[106] ANAREN – ZigBee channels
http://www.anaren.com/air-wiki-zigbee/Channel
[Data darrer accés: 11/01/2015]

[107] Cambridge Wireless – Essentials of Short Range Wireless Standards
http://www.cambridgewireless.co.uk/Presentation/Nick%20Hunn,%20WiFore.pdf
[Data darrer accés: 11/01/2015]

[108] EMCU - Wireless M-Bus Solutions SPIRIT1 & STM32L
http://www.emcu.it/WirelessMBUS/Wireless_M-BUS_Solutions_and_more.pdf
[Data darrer accés: 11/01/2015]

[109] Texas Instruments - Wireless M-Bus implementation with CC112x / CC120x High Performance Transceiver Family
http://www.ti.com/lit/an/swra423/swra423.pdf
[Data darrer accés: 11/01/2015]

[110] Silicon Labs - Wireless M-Bus Suite and Silabs specific documentation
http://www.silabs.com/Marcom%20Documents/Resources/wireless-m-bus-quick-start-guide.pdf
[Data darrer accés: 11/01/2015]

[111] Compass Security - Wireless M-Bus Security Whitepaper Black Hat USA 2013
http://www.csnc.ch/misc/files/2013/wmbus_security_whitepaper.pdf
[Data darrer accés: 11/01/2015]

[112] Slideshare – Benefits of DASH7 technology
http://www.slideshare.net/peburns/dash7-technology-2009-2011-seoul-briefing
[Data darrer accés: 11/01/2015]

[113] Z-Wave España – Enchufe controlador por Z-Wave con medición de consumos AEON LABS
http://zwave.es/AEO_ZW075-ZWEU
[Data darrer accés: 11/01/2015]

[114] Z-Wave Alliance – About Z-Wave Technology
http://www.z-wavealliance.org/about-z-wave
[Data darrer accés: 11/01/2015]

[115] Wikipedia – ANT (network)
http://en.wikipedia.org/wiki/ANT_(network)
[Data darrer accés: 11/01/2015]

[116] Embedded Computing Conference – DECT versus ZigBee, Bluetooth LE & Company.
http://www.embeddedcomputingconference.ch/pdf_2011/1A2-Rupp.pdf
[Data darrer accés: 11/01/2015]

[117] IETF – DECT ULE Introduction
http://www.ietf.org/proceedings/89/slides/slides-89-6lo-6.pdf
[Data darrer accés: 11/01/2015]

[118] LSR – A technical Overview of DECT ULE
http://www.lsr.com/white-papers/technical-overview-of-dect-ule
[Data darrer accés: 11/01/2015]

[119] IETF – ETSI-EN-300 Final Draft v2.4.0 (2011-2012)
http://www.etsi.org/deliver/etsi_en/300100_300199/30017505/02.04.00_40/en_30017505v020400o.pdf
[Data darrer accés: 11/01/2015]

[120] RFID INfosec - Lesson Title: RFID Modulation, Encoding, and Data Rates
http://rfidsecurity.uark.edu/downloads/slides/mod04_lesson04_slides.pdf
[Data darrer accés: 11/01/2015]

[121] Youtube - Reprogram Your TomorrowLand Bracelet - NFC Tag
https://www.youtube.com/watch?v=tq9hrTRmGMs
[Data darrer accés: 11/01/2015]

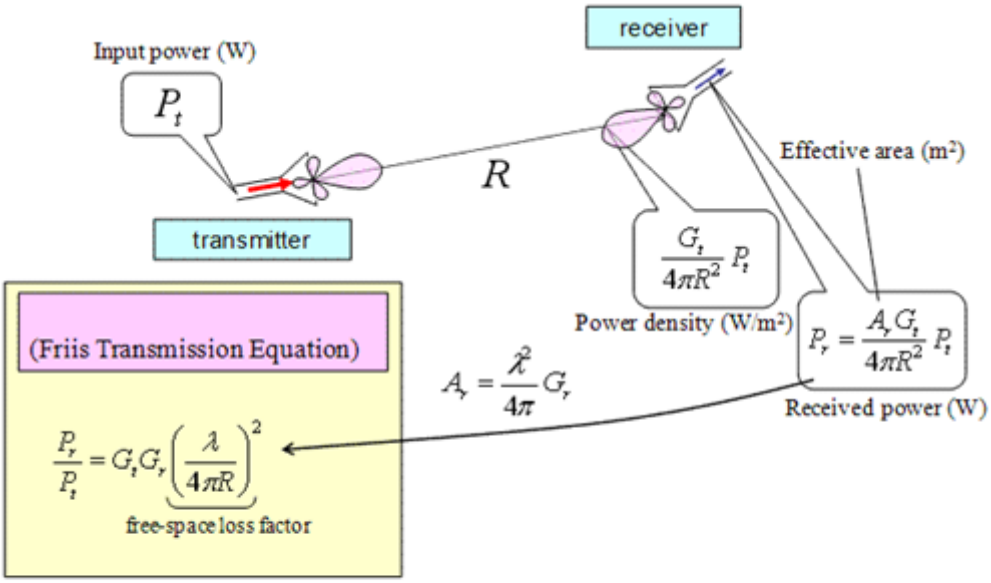
[122] Libelium – RFID/NFC 13.56 MHz Networking Guide
http://www.libelium.com/v11-files/documentation/waspmote/rfid_1356-networking_guide.pdf
[Data darrer accés: 11/01/2015]

[123] ATMEL Applications Journal - Considerations for RFID Technology Selection
http://www.atmel.com/images/secrerf_3_04.pdf
[Data darrer accés: 11/01/2015]

[124] RMONI Wireless Solutions - RM090 Ultra Low Powert IEEE 802.15.4 compliant wireless sensor module
http://www.rmoni.com/en/products/hardware/rm090
[Data darrer accés: 11/01/2015]

Annexos

Annex I. Equació de Transmissió de Friis.



$$P_r\big|_{dB} - P_t\big|_{dB} = G_t\big|_{dB} + G_r\big|_{dB} - 10\log_{10}\left(\frac{4\pi R}{\lambda}\right)^2$$

Figura 20. Esquema de comunicació emissor-receptor mostrant equació de Friis.

Annex II. Diferències entre IoT i M2M.

La següent figura mostra un resum prou visual de les diferències entre IoT i M2M i de la seva relació en el sentit de "comunicació remota entre dispositius" [67]:

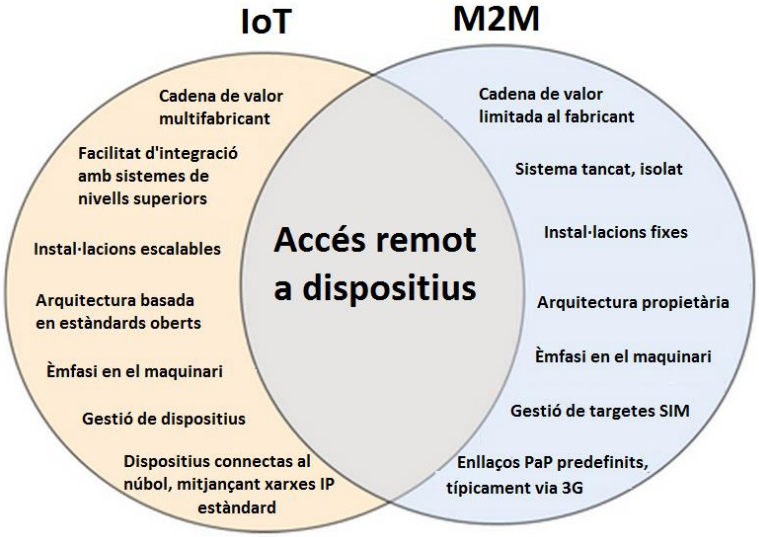


Figura 21. Interrelació entre els paradigmes IoT i M2M.

A la següent figura podem observar un diagrama d'una aplicació M2M bastant bàsica: una màquina de *vending* equipada amb un sensor de proximitat/presència, que s'activa quan el nivell d'ompliment de la màquina –quantitat de llaunes o ampolles- baixa per sota d'un nivell predefinit. Això fa saltar una alarma –paquet de dades- que s'envia a un centre de control fent servir una xarxa mòbil com ara GPRS, a través de una tarjeta mòbil SIM (*Subscriber Identity Module*) i un mòdem o encaminador –dibuixat com la "pasarel·la"- situats a l'interior de la màquina. En aquest sentit, l'únic que caldria tenir present és que la màquina s'hauria de situar en un lloc on hi hagués cobertura mòbil, per tal de poder enviar les dades al centre remot.

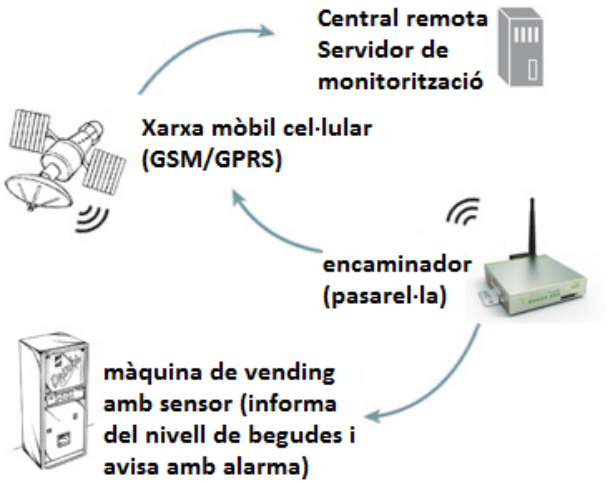


Figura 22. Aplicació típica M2M (màquina de *vending*).

Per la seva banda, la següent figura [5] mostra una aplicació típica de l'IoT, on una sèrie d'aparells (*appliances*) domèstics, com ara una bàscula electrònica, un medidor de pulsacions o un tensiòmetre (equipats amb una ràdio Wi-Fi o *Bluetooth Low Energy*) o bé un pot de pastilles intel·ligent (equipat amb una ràdio NFC – *Near Field Communication*) recullen les dades de l'usuari i les envien, fent servir una pasarel·la (típicament un *router* IP) a Internet, on aquestes dades es podrien emmagatzemar en un proveïdor de núvol públic, fent les dades accesibles a l'usuari en qualsevol moment i des de qualsevol dispositiu com para un *smartphone* o un PC portàtil:

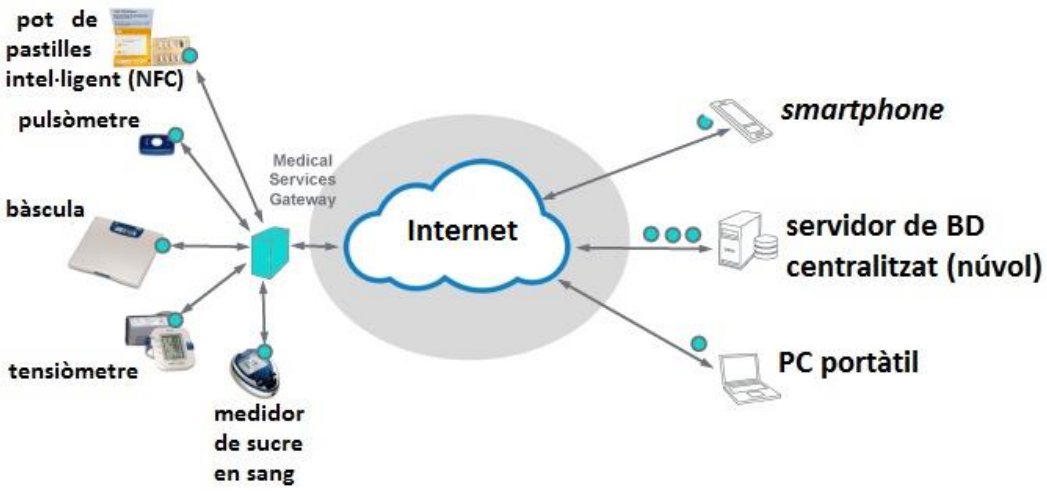


Figura 23. Aplicació típica IoT (electrodomèstics amb sensors i sense fils) [5].

Annex III. Principals estàndards i protocols M2M.

A dia d'avui, podem afirmar que els principals protocols per a M2M són els següents [76]:

- SCADA (*Supervisory Control And Data Adquisition*): els sistemes SCADA poden ser considerar els "ancestres" cablejats de les actuals WSNs. Avui dia, els SCADA es basen en comunicacions a llarga distància, per la qual cosa la transició d'SCADA cap a Internet és més que una simple tendència. Les seves característiques bàsiques són:

    - En alguns casos, les dades de sistema han de ser etiquetades amb la data actual (*timestamped* o *time-tagged*, en anglès). Això significa que la sincronització distribuïda dels rellotges en les RTUs (*Remote Terminal Units*) és un requeriment.

    - Tenen una tecnologia de comunicació de xarxa basada en trames que no es troba en els protocols Ethernet o TCP/IP (*Transfer Control Protocol/ IP Protocol*) i que les aplicacions M2M necessiten per a la determinació de missatges, sincronizatció, selecció de protocol i sostenibilidad de l'entorn.

    - Els sistemes SCADA estan convergint a tecnologies estàndard de xarxes. En concret, Ethernet i TCP/IP estan susbstituïnt els antics estàndards propietaris. L'àmplica majoria dels mercats ha acceptat les xarxes Ethernet al menys per a HUI (*Human Machine Interface*) amb SCADA.

    - Els sistemes SCADA s'estan incorporant paulatinament a tot arreu: des de clients lleugers (*thin clients*), portals web i productes basats en web estan guanyant popularitat amb la majoria dels fabricants.

- Modbus: es tracta d'un protocol de comunicacions en sèrie utilitzat de manera extensiva pels sistemes SCADA per establir la coomunicació entre els RTUs i els dispositius. Amb Modbus, la major part dels tipus de dades s'anomenen de forma especial: un únic bit de sortida s'anomena *coil*; un únic bit d'entrada s'anomena *discreteinput* o *contact*; les trames, tant de missatges de consulta des del node mestre com els missatges de resposta des dels esclaus, porten els següents dades: adreça del dispositiu, codi de funció, octets de dades i chequeig d'error.

- UPnP (*Universal Plug and Play*): es tracta d'una sèrie de protocols de xarxa, principalment dissenyats per a xarxes residencials i que habilita als dispositius de xarxa, com per exemple ordinadors, impresores, pasarel·les d'Internet (*routers*), punts d'accés Wi-Fi (*Wireless Fidelity*) i dispositius mòbils l'autodescobriment de la presència d'altres dispositius en la mateixa xarxa i l'establiment de serveis de xarxa per a entreteniment, compartició de dades i comunicacions. El concepte d'UPnP és una extensió del clàssic *plug-and-play* ("endollar i llestos"), tecnologia que permetia la

connexió dinàmica de dispositius a un ordinador, encara que amdues tecnologies no estan relacionades directament. Els dispositius UPnP "s'endollen i llestos" perquè, cuando es connecten a una xarxa, automàticament "col·laboren" amb altres dispositius (el que en anglès es demonina *zero-configuration*).

- NAT-PMP (*Network Address Translation – Port Mapping Protocol*): es tracta d'un RFC (*Request For Comments*) de l'EITF (Engineering Task Force Internet), introduït per Apple l'any 2005 com a alternativa del més comú *IGD* (*Internet Gateway Device*) *Standardized Device Control Protocol*, que es troba implementat a multitud d'encaminadors NAT. NAT-PMP permet que un ordinador en una xarxa privada (darrer un encaminador NAT) pugui configurar automàticament l'encaminador per permetre a dispositius externs a la xarxa privada contactar el primer. En concret, aquest protocol funciona sobre UDP (*User Datagram Protocol*) i bàsicament, el que fa, és automatizar el procés de reenviament de ports.
- DWPS (*Devices Profile for Web Services*): definex un conjunt mínim de restriccions d'implementació per permetre serveis web (missatgeria, descobriment, descripció i events) segurs en dispositius amb recursos restringits. Els seus objectius són similars a UPnP però, a més, es troba totalment alineat amb la tecnologia de serveis web (*Web Services*) i inclou numerosos punts d'extensió.

- Protocols XML (*eXtensible Markup Language*)

    - Tenim, per un cantó, BiTXml, que és un estàndard de comunicació obert, basat en XML, dissenyat per implementar el nivell de Presentació OSI (*Open System Interconnection*), amb la principal meta d'estandaritzar la manera que s'intercanvien les comandes i la informació de control per a l'objectiu específic dels requeriments de comunicació M2M (per exemple, comunicació amb dispositius genèrics amb o sense unitat de processament incorporada –com sensors, actuadors, aparells d'aire condicionat, ascensors, etc.- o una combinació d'ells.

    - Per altre cantó, tenim M2MXML, un altre protocol obert per comunicacions M2M, que té com principal filosofia de disseny la seva simplicitat. Una de les metes d'M2MXML és establir un estàndard obert que pugui ser adaptat pels fabricants de dispositius i els desenvolupadors d'aplicacions M2M, permetent d'aquesta manera una interoperativitat que avui dia gairebé no existeix. El projecte M2MXML també inclou el desenvolupament d'APIs (*Application Programming Interface*) per facilitar l'ús del protocol per part dels desenvolupadors. Fins ara, altres intents de desenvolupar protocols per a M2M han resultat en protocols que són difícils d'entendre i massa detallats per ser utilitzats en dispositius petits i amb limitacions d'amplada de banda, fent que la majoria de aplicacions M2M actuals estiguin completament "customitzades" (personalitzades) d'extrem a extrem, incloent el desenvolupament de protocols propietaris.

Per la seva banda, altres protocols que, encara que també vàlids per a M2M, s'associen comunament més amb el paradigma IoT són (s'anomenen els principals) [78]:

- IPv6: es tracta de la versió 6 de l'Internet Protocol, substitut de l'actual (i ja "antic") IPv4. Aquest protocol està destinat a l'interconnexió en xarxes de commutació de paquets, proporcionant transmissió de datagrames extrem a extrem a través de múltiples xarxes IPs. Amdós estàndards són molt similars en termes de funcionalitat encara que no pas en termes de mecanismes interns. Les diferències més importants entre IPv4 i IPv6 es resumeixen en la següent taula:

Característica	IPv4	IPv6
Estàndard des de	1974 (RFC 791)	1998 (RFC 2460)
Longitud (bits)	32	128
Màxim nombre d'adreces	2^{32}	2^{128}
Format d'adreces	Dotació decimal Ex: 192.168.100.1	Dotació hexadecimal Ex: 2001:0DB8:0234:AB00: 0123:4567:8901:ABCD
Adreça de *loopback*	127.0.0.1	::1
Adreçament dinàmic	DHCP*	SAAC**/DHCPv6
IPSec	Opcional	Obligatori
Longitud capçalera	Variable	Fixa
Mida mínim de paquet	576 byte (fragmentat)	1280 byte
Fragmentació	En els nodes finals i ens els encaminadors	Únicament en el punt final de la comunicació
Options de capçalera	Sí	No (mitjançant extensions)
Fluxe	No	Etiqueta de fluxe de paquet
Descobriment d'encaminadors	Opcional	Obligatori
Resolució d'adreces en capa d'enllaç	ARP*** (*broadcast*)	Missatges de descobriment de veïns *multicast*

Taula 10. Principals diferències entre IPv4 i IPv6.

*DHCP (*Dynamic Host Configuration Protocol*)
*DHCP (*Dynamic Host Configuration Protocol*)
** ARP (*Address Resolution Protocol*

- 6LoWPAN (*IPv6 over Low power Wireless Personal Area Networks*): es tracta d'una adaptació d'IPV6 per a enllaços que funcionen amb l'estàndard IEEE 802.15.4. En altres paraules, es tracta d'una capa d'adaptació que habilita l'ús d'IPv6 en xarxes sense fils (de radiofreqüència o RF), de baix consum i amb pèrdues (LLN). Aquest protocol opera únicament en el rang de freqüències de 2.4 GHz i amb una taxa de transferència màxima de 250 Kbps.

  Bàsicament, el que fa 6LoWPAN és comprimir tant la capçalera d'IPv6 com la UDP, per tal de que els datagrames d'IPv6 (que han de tenir una MTU o Unitat de Transmissió Màxima de al menys 1.280 byte) puguin viatjar per enllaços 802.15.4 (on la MTU estàndard es de 127 byte). 6LoWPAN ve definit inicialment per l'RFC4944 i va ser actualitzat més tard per l'RFC6282 [79].

- UDP (*User Datagram Protocol*): es tracta del mateix protocol de comunicació que ja es feia a IPv4 i IPv6. És un protocol pertanyent a la capa de transport (nivell 4 OSI), no orientat a connexió (per tant, no es pot garantir l'entrega de les dades) per a aplicacions client/servidor, basat en IP. UDP és una alternativa a TCP (Transmission Control Protocol) per a aplicacions que requereixen un comportament i rendiment en temps real (per exemple videoconferència, televisió IP –IPTV, veu per IP –VoIP).

  Bàsicament, en LLNs, es fa servir UDP per les característiques propies de la xarxa: com que parlem de xarxes amb pèrdues, la probabilitat d'error augmenta respecte a un medi cablejat, com ara fibra óptica. Una major probabilitat d'errors implicaria haver de reenviar els paquets defectuosos o que no han arribat a la destinació, la qual cosa implicaria, al seu voltant, un major consum de bateria degut a la major utilització de l'antena ràdio (i, com ja saben, a les LLNs, la durada de la bateria és un factor clau, que s'ha d'intentar maximitzar tot el possible). Això fa que sigui preferible l'utilització d'un protocol no orientat a connexió, que no garanteix l'entrega, ja que el fa més ràpid (entre d'altres, ens evitem el *three-way handshake* inicial) i menys "costós".

- UIP: bàsicament, es tracta d'una implementació de codi obert (*open source*, en anglès) de la pila TCP/IP, capaç d'executarse en microcontroladors de 8 i 16 bit.

- TLS (*Transport Layer Security*): protocol que assegura la privacitat entre aplicaciones i els usuaris a Internet. Quan un servidor i un client es comuniquen, TLS assegura que no pot haver-hi escoltes il·legals (*eavesdropping*) per part de tercers, ni poden modificar cap missatge (*tampering*). TLS es considera com el successor del protocol SSL (*Secure Sockets Layers*). Bàsicament, es composa de dues capes: *TLS Record Protocol* i *TLS Handshake Protocol*: la primera, proporciona seguretat a la connexió mitjançant algún mètode d'encriptació com ara DES (*Data Encryption Standard*), encara que TLS també es pot fer servir sense encriptació; per la seva banda, la segonda, permet al client i al servidor autenticar-se mútuament i negociar un algorisme d'encriptació i claus criptogràfiques abans de que les dades s'enviin. TLS es basa en SSL 3.0, encara que ambdós protocols no son interoperatius.

- DTLS (*Datagram Transport Layer*): protocol que es basa en TLS i que proporciona garanties de seguretat equivalents. DTLS proporciona privacitat per als protocols de datagrames, permetent que les aplicacions client/servidor es comuniquin de manera que no pugui haver-hi *eavesdropping*, *tampering* o falsificació de missatges.

- MQTT (*Message Queuing Telemetry Transport*): protocol que proporciona un model de missatgeria publicador/subscriptor, de manera extremadament lleugera, sent útil per connexions amb localitzations remotes on es requereix una emprempta de codi (*code footprint*) molt petita i on l'amplada de banda és limitat.

- Mosquito: un *broker* de codi obert per a MQTT v3.1 (un *broker* de missatgeria és un patró arquitectònic per a la validació, transformació i encaminament de missatges; es tracta d'un mecanisme mediador de la comunicació entre aplicacions, permetent minimitzar el grau de coneixement mutu que aquestes aplicacions necessiten tenir per poder intercanviar missatges, implementant així el seu desacoblament)

- CoAP (*Constrained Application Protocol*): com el seu propi nom indica, es tracta d'un protocol de la capa d'aplicació, dissenyat per ser utilitzant en dispositius amb recursos limitats, com per exemple nodes d'una WSN. CoAP "tradueix" a HTTP (*Hyper Text Transfer Protocol*) per tal de permetre una fàcil i simplificada integració amb la Web, al mateix temps que aconsegueix altres requeriments com ara support *multicast*, molt poca sobrecàrrega (*overhead*) i, sobre tot, simplicitat [65]. El Grup de Treball CoRE (*Constrained Restful Environments*) de l'IETF ha proposat les següents funcions per a CoAIP:

    - Disseny de protocol tipus RESTful (*Representational State Transfer*), minimitzant la complexitat del mapeig amb HTTP,
    - Baixa sobrecàrrega a la capçalera (*low overhead header*),
    - Baixa complexitat,
    - Suport per a URI (*Uniform Resource Identifier*) and *content-type,*
    - Suport per al descobriment de recursos provistos per serveis CoAP coneguts,
    - Subscripció simple a recursos i notificacions resultats tipus *push,*
    - Procés d'emmagatzamematge en memòria cau (*caching*) simple, basa en *max-age,*

- SMCP: una pila CoAP escrita en llenguatge C, flexible, adequada per entorns/dispositius encastrats (*embedded devices*).

- RPL (*Ripple*): bàsicament, es tracta d'un protocol d'encaminament específic per a IPv6 i xarxes LLN. El protocol ha estat creat pel RoLL (*Routing over LLN*), un Grup de Treball (*Working Group*) de l'EITF [71]. Aquest protocol d'encaminament era necessari bàsicament pels requeriments propis de les LLNs [31]:

    - Els enllaços entre nodes no són permanents i són "febles",

- Les LLNs normalment prioritzen l'estalvi d'energia (consum de bateria),

- Els patrons típics de tràfic no són simplement fluxes *unicast* (ja que en molts casos, sinó en la majoria, el tràfic es de tipus punt a multipunt),

- D'igual manera, en molts casos, les LLNs fan servir capes d'enllaç amb mida de trama restringit (p.ex. 802.15.4 té una mida de 127 byte màxima), que fa que els protocols d'encaminament hagin d'estar adaptats a aquest fet

- Els protocols d'encaminament LLN ha de ser molt curosos quan negocien eficiència per generalitat, ja que molts dels nodes no tenen recursos a malgastar.

- XMPP (*Extensible Messaging and Presence Protocol*): es tracta d'una tecnologia oberta –protocol de la capa aplicació- que permet comunicació en temps real, que dóna vida a un ampli espectre d'aplicacions com ara missatgeria instantània, presència, xat multipersona, trucades de veu i vídeo, col·laboració, *middleware* (programari que actua com a pont entre el sistema operatiu i les bases de dades o aplicacions, en una xarxa) lleuger, sindicació a continguts i encaminament generalitzat de dades XML. Inicialment s'anomenava Jabber.

- AMQP (*Advanced Message Queing Protocol*): protocol estàndard obert de la capa d'aplicació per a middleware orientat a missatges. Els trets característics d'aquest protocol són: orientació a missatges, encuament, encaminament (incloent punt a punt i publicació-subscripció), fiabilitat i seguretat.

- DDS (*Data-Distribution Service for Real-Time Systems*): es tracta del primer *middleware*estàndard obert a nivell internacional, dirigit a comunicacions de tipus publicació-subscripció, per a sistemeas encastrats en temps real.

Alguns d'aquests protocols (en concret, els utilitzats en l'estàndard IEEE 802.15.4) es veuran amb més profunditat als capítols següents.

En la següent taula podem observar les diferències, a nivell de protocols utilitzats, capa a capa OSI, entre la clàssica pila (*stack*) TCP/IP existent en l'actualitat per a entorns d'Internet i el nou paradigma IoT, utilitzat per objectes intel·ligents que fan servir IP:

Capa OSI	TCP/IP clàssica	IoT – Objectes
Capa d'Aplicació (nivell 7)	HTTP, FTP*, STMP, ..	CoAP
Capa de Transport (nivell 4)	TCP, UDP	UDP, DTLS
Capa de Xarxa (nivell 3)	IPv4, IPv6	6LoWPAN, RPL
Capa d'enllaç (nivell 2)	802.3 (Ethernet), 802.11 (WLAN**)	IEEE 802.15.4e

Taula 11. Comparativa entre les capes OSI pròpies de TCP/IP i les d'IoT

*FTP (*File Transfer Protocol)*
*WLAN (*Wireless Local Area Network)*

Annex IV. Àmbits d'aplicació d'IoT.

En la següent figura [66] podem veure l'evolució de les WSNs pel que fa als seus àmbits d'aplicació, constatant que el factor més important per a l'obertura de nous àmbits/mercats ha estat l'abaratiment progressiu del costs dels sensors (fet que ha anat unit a una miniaturització dels mateixos així com a un augment de la potència de procés dels microcontroladors o processadors dels nodes):

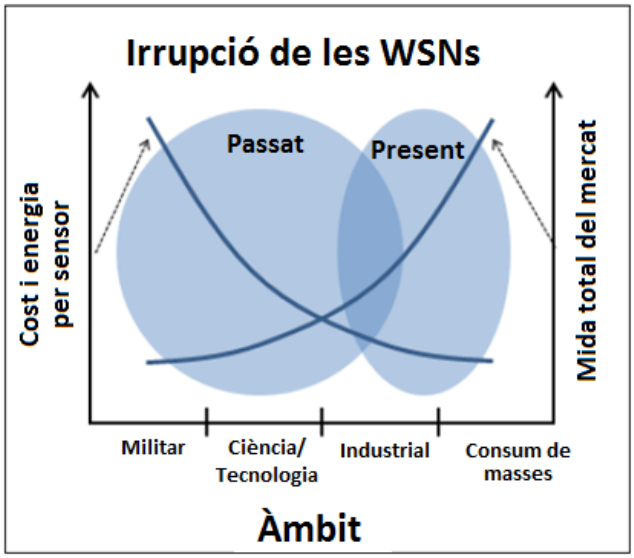


Figura 24. Evolució dels àmbits d'aplicació de les WSNs en funció del cost per sensor.

Repassem ara, un per un, els àmbits listats anteriorment per tal d'entreveure les possibles aplicacions d'IoT en cadascun d'ells:

- Militar: en aquest àmbit, potser moltes vegades no es podrà parlar pròpiament d'IoT sinó simplement de comunicacions M2M ja que, de fet, Internet no serà pas –per raons òbvies de seguretat- la xarxa que s'utilitzarà per comunicar remòtament els objectes/coses (persones, sensors, servidors, etc). En comptes de fer servir Internet, probablement es faran servir xarxes privades, normalment satel·litats (quan s'han de connectar escenaris de batalla amb centres de control remots ubicats a altres països) o xarxes WiMAX (*Worldwide Interoperability for Microwave Access*) o cablejades –fibr òptica- en cas de comunicacions entre centres militars en un mateix país.

  Per tant, aquí ja trobem la primera particularitat de l'àmbit militar: l'ús majoritari de xarxes privades i, en qualsevol cas, els fortíssims requeriments de seguretat, essent imprescindible fer servir tècniques d'encriptació com ara l'estàndard AES-256 o fins i tot criptografia quàntica.

  En qualsevol cas i, tal i com s'aprecia en la figura de sota, qualsevol applicació en l'ámbit militar hauria de constar de les següents capes (faci's notar que aquesta arquitectura es pot aplicar, en realitat, a qualsevol dels àmbits d'IoT):

- Capa de sensat, que inclue els "objectes" que monitoritzen l'entorn: càmeras, radars, telèfons mòbils, etiquetes RFID, sensors de moviment, llum, temperatura, etc. Aquests objectes poden estar ubicats en la roba dels soldats, vehicles militars, armament, etc. Els protocols utilitzats, a banda de RFD, podrian ser 802.15e, Wi-Fi, ...

- Capa d'accés: formada pels dispositius pasarel·la que envien les dades cap a la xarxa exterior. Aquests *gateways* poden ser des d'estacions base (*Base Stations* o BS, en anglès) o pasarel·les –encaminadors- de tipus IPv6/IPv4, etc.

- Capa de Xarxa: formada per la xarxa exterior, per on s'encaminen els paquetes fins a l'altre extre remot (centre de control). Pot ser Internet, una xarxa privada satel·litat, una xarxa cel·lular GSM/GRPS/LTE, etc

- Capa de servei: formada pel conjunt de servidors, computació en núbol, etc. que emmagatzemen la informació rebuda de la capa de sensat. Aquesta cap ha de estar redundada i ser altament disponible.

- Capa d'aplicació: en aquesta capa es troben les aplicaciones militars pròpiament dites, que poden ser mútliples:

    - Control d'armes (per exemple munició remanent),
    - Gestió de distribució física de les tropes,
    - Monitorarge del camp de batalla (tant visual, sonor, etc.),
    - Logística militar (enviament de material, menjar, armes),
    - *Drones* equipats amb sensors per monitoratge mòbil i execució d'accions.

Part d'aquestes aplicacions també es podrien extrapolar/aplicar a àmbits similars, com ara seguretat i defensa nacional (Policia) o d'altres relacionats, com Protecció Civil, Bombers, emergències mèdiques, etc.

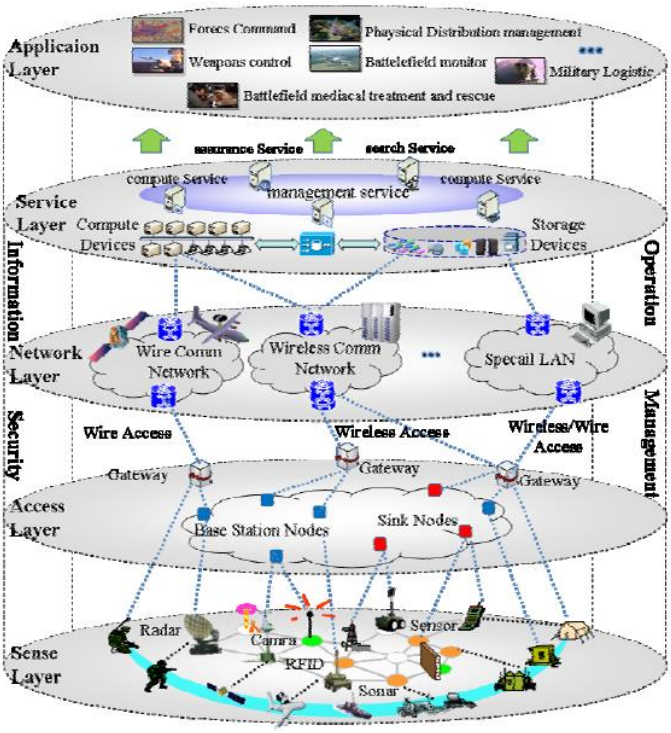


Figura 25. Arquitectura d'un sistema MIoT [16].

- Ciència i Tecnologia: aquest àmbit és molt genèric ampli i es podrien incloure dintre altres "sub-àmbits" com per exemple la gestió electrònica/remota de la salut –també coneguda com *eHealth*. Aquí podríem trobar diverses aplicacions com ara:

    - Detecció de la salut de persones malaltes o gent gran: mitjançant les peces de vestir amb sensors (wearables) es podrien control·lar aspectes del pacient com ara la tensió, ritme cardíac, temperatura, caigudes fortuïtes, etc. D'aquesta manera, aquests col·lectius podrien portar una vida més independent i alhora trobar-se més segurs.

    - Frigorífics mèdics: control de les condicions dels congeladors que emmagatzemen vacunes, medicines i, en general, qualsevol element orgànic.

    - Cura de l'esportista: monitoratge de les costants vitals, per exemple en proves d'esforç, centres d'alt rendiment o, en general, qualsevol centre/camp d'entrenament.

    - Radiació ultravioleta: mesurament dels rajos ultravioleta (UV) per avisar la gent de no exposar-se a certes hores del dia.

  Un altre àmbit relacionat amb la ciència pot ser el del medi ambient. Aquí podem trobar nombroses aplicacions:

    - Control de la fauna marina (per exemple, espècies que viuen fora del seu hàbitat o que es troben en perill d'extinció),

- Control del nivell de les aigües (p.ex. en llocs com Venècia és indispensable saber, d'avantmà, quan pot ocórrer el fenòmen conegut com a 'Aqua Alta' per així estar preparats i actuar en conseqüència),

- Control del nivell de precipitacions a una àrea concreta (també temperatura, humitat, vent, vent, etc),

- Control de gasos tòxics i de radiació (estudi de la ventilació i qualitat de l'aire en llocs concrets),

- Control de terratrèmols o erupcions de volcans (zones que es troben a prop de plaques tectòniques –amb activitat sísmica prèvia- o a prop de volcans actius o "dorments")

- Monitoratge de fauna (per tal d'entendre els seus hàbits, manera de viure, etc.)

Per exemple, la figura de sota mostra un mapa del nivell de radiació a Japó, tot just després del *tsunami* que va afectar a la central nuclear de Fukushima el passat març de 2011. L'organització Safecast recollia aquesta informació mitjançant sensors i la va fer disponible a Internet.

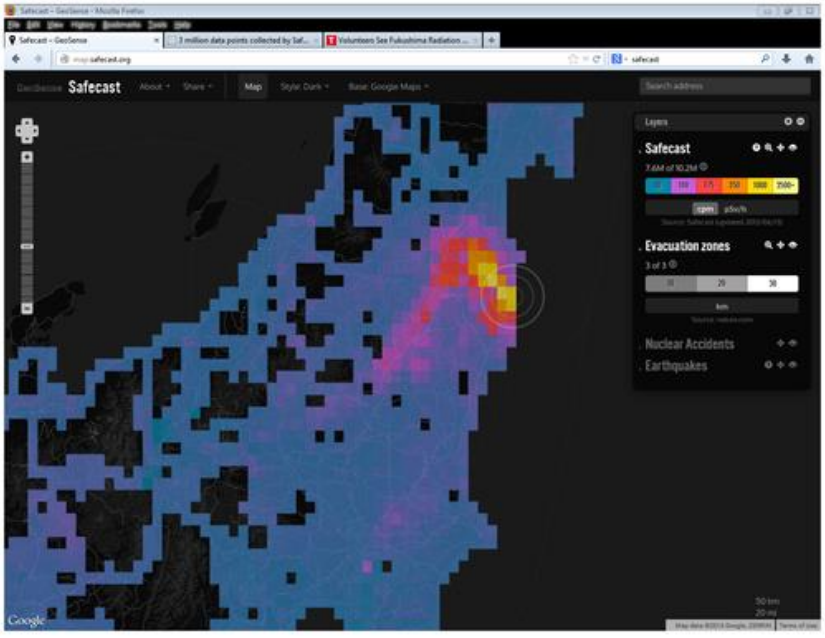


Figura 26. Mapa del nivell de radiació de Japó tras l'accident de Fukushima.

De manera similar, a la figura de sota podem veure una captura del lloc web de l'ISMAR (*Instituo di Scienze Marine*, en italià) que, conjuntament amb el CRN (*Consiglio Nazionale delle Richerche*) van crear portar a terme el projecte 'Acqua Alta' per tal de monitorar el fenòmen del mateix nom a la ciutat de Venècia, com ja s'ha comentat abans [84].

La informació es recull a través de dispositius localitzats tant sobre el nivell del mar com sota la superfície (des de radars fins a càmeres d'alta resolució en 3D, passant per sensors de temperatura i pressió). Tota aquesta informació és enviada a una estació base situada en una plataforma a 10 milles naútiques de la ciutat, on la profunditat de l'aigua és de 16 metres. A la plataforma hi ha un enllaç punt a punt, que envia finalmente les dades fins a un centre de control, on aquestes es processen i es fa accesiblenpúblicament a Internet, a través de qualsevol navegador web.

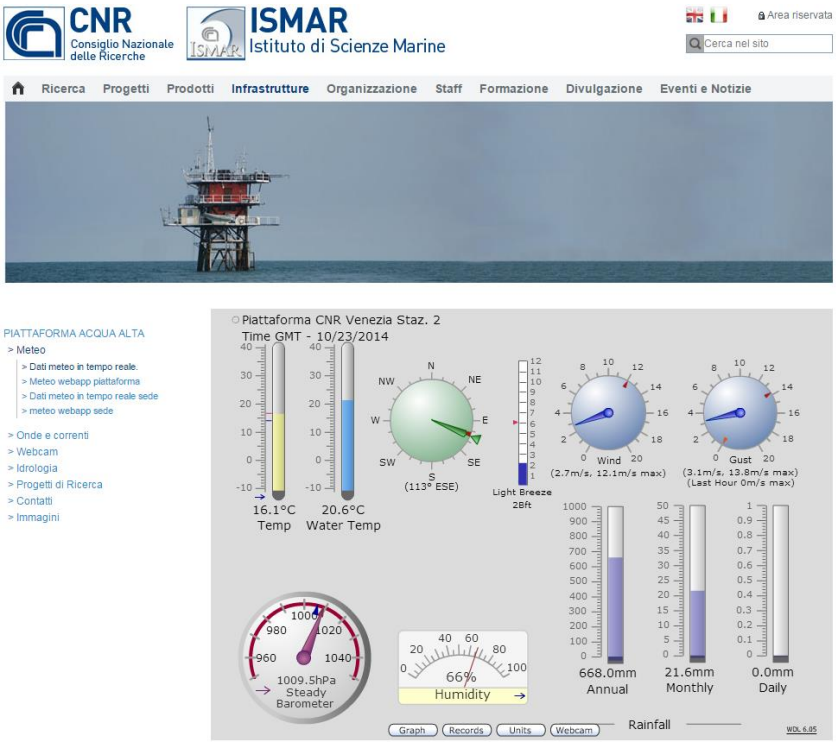


Figura 27. Secció del lloc web de l'ISMAR pertanyent al projecte 'Acqua Alta' [84]

- Industrial: aquest àmbit també es força ampli ja que es poden trober centenars d'aplicacions on les xarxes WSN poden ajudar en processos industrials, com per exemple:

    - Aplicacions genèriques M2M: sensors i robots/PLCs (*Programmable Logic Controler*) en una factoria – per exemple en una cadena de muntatge- que es parlen entre ells i executen accions en funció de les dades recollides pels primers: parar la cadena en cas de temperatura massa elevada, en cas de un "taponament" en una part de la mateixa, una peça defectuosa, manca de material, etc.

- Control de la qualitat de l'aire dins de la factoria (mesura de la qualitat de l'aire per assegurar la seguretat dels treballadors),

- Monitoratge de temperatura (en zones que requereixen unes condicions de freu o calor especials, com ara forns, càmeres frigorífiques, etc),

- Presència d'Ozó (monitoratge dels nivells d'ozó en processos de assecat de carn i, en general, en factories de productes alimentaris),

- Localització d'objectes (localització en tot moment dels actius de la companyia, fent servir etiquetes actives –ZigBee- o passives -RFID/NFC- i aplicable tant a oficines, magatzems o ports,

- Autodiagnosi de vehicles: els vehicles industrials poden incorporar sensors i enviar emergències en temps real als conductors –o, fins i tot, parar el vehicle- en cas d'un mal funcionament.

- Control de flotes/control de paquets: des d'un punt de vista logístic, es tracta de controlar les rutes que segueixen determinats bens delicats o d'alt valor, com per exemple medecines, joieria o substàncies perilloses.

- Agricultura i Ramaderia: dins d'aquest àmbit (*Smart Agriculture* i *Smart Farming*) podem trobar aplicacions molt diverses, també:

    - Monitoratge de la qualitat del sòl/terreny. Es poder monitorar variables com la humitat o el tronc dels vegetals -per exemple de les vinyes- per tal de controlar la quantitat de sucre en el raïm, així com la salut de la vinya i detectar la presència de possibles enfermetats causades per paràsits [85].

    - Control de hivernacles. Es poden monitorar i controlar les variables d'un microclima –temperatura, humitat, quantitat de llum- per tal de maximizar la producció de plantes, fruites i verdures, així com la seva qualitat).

    - Irrigació sel·lectiva de zones seques que necessitin aigua (això també poc aplicar a parcs i jardins públics, camps de golf, etc).

    - Control del compost (control de la humitat i la temperatura en alfalfa, palla, etc. per prevenir fongs o altres contaminants microbials).

    - Seguiment/localització d'animals (localització i identificació d'animals que pasturen en camps oberts o en estables molt grans).

    - Gasos tòxics (estudi de la ventilació i qualitat de l'aire en granjes, així com detecció de gasos perjudicials en els excrements dels animals).

- Control de les cries/descendència (controlar les condicions de creixement dels animals en les granjes per tal d'assegurar la seva supervivència i salut).

- Serveis Públics: dins d'aquest gran àmbit trobem el concepte de ciutats intel·ligents o *Smart Cities*. Les aplicacions en aquest camp són immenses:

  - Aparcament intel·ligent (monitoratge dels espais lliures en pàrquings –tant públics com privats- per tal d'assistir a l'aparcament)

  - Salut de les estructures (monitoratge de vibracions i condicions dels materials en edificis, ponts, monuments històrics, etc)

  - Mapa de soroll urbà (monitoratge del nivell de soroll en zones d'oci concurregudes –per exemple bars- o en zones de gran pas de vehicles, aeroports, etc.)

  - Nivell de camps electromagnètics (mesurament de la energia irradiada per elements de les xarxes mòbils com ara repetidors de televisió, antenes de telefonica, encaminadors Wi-Fi/WiMAX, etc.),

  - Congestió del tràfic (monitoratge del nivell de vehicles i peatons per optimitzar rutes)

  - Il·luminació intel·ligent (encesa i apagat de fanals en funció de la quantitat de llum natural i de la concentració de vehicles i persones a un àrea determinada, així com control de la intensitat d'il·luminació),

  - Gestió de residus (detecció dels nivells de brossa en els contenidors per optimitzar les rutes de recol·lecció)

  - Carreteres intel·ligents (autopistes amb senyalització dinàmica d'advertència en funció de les condicions climàtiques, embussos, accidents, etc.),

  - Monitoratge d'aigua potable (control de la qualitat de l'aigua que surt per les aixetes i fonts públiques de les ciutats),

  - Nivell de polució urbà (monitoratge i control en temps real dels nivells de concentració de gasos, principalment CO_2)

  - Xarxa intel·ligent (*Smart Grid*): monitoratge i gestió del consum d'energia de la ciutat o de zones concretes [53].

  - Transports urbans: monitoratge de la localització exacta de busos i tramvies durant les seves rutes i informació en panells informatius a les marquesines o

a través d'aplicacions mòbils per saber els temps d'espera exactes fins que arribi el proper transport.

- Control d'accés perimetral: control de l'accés a determinades àrees restringides de la ciutat (edificis governamentals, parcs i jardins que es tanquen a la nit, etc). També es pot aplicar a l'àmbit industrial/empresarial.

Per exemple, la figura de sota mostra una captura de pantalla de l'aplicació de gestió de recollida d'escombreries TSWASTE [45], de l'empresa TST Sistemas. Aquesta empresa es dedica, per un cantó, a comercialitzar plataformes de desenvolupament per a la creació de WSNs (TSgaTe, TSmoTe) que es poden programar fent servir llenguatge C estàndard i llibreries API pròpies; per un altre cantó, també comercialitzen solucions integrals com ara gestió de l'enllumenat o gestió de recogida d'escombreries, com ja hem dit. Aquesta solució fa servir sensors volumètrics –anomenats també TSwasTe- i que es col·loquen a l'interior dels contenidors. Els sensors tenen una interfície ràdio funcionant a 868 MHz; el sensat és basa en ultrasons i també disposa d'un sistema de detecció d'apertura de la tapa del contenidor per evitar falses mesures. La vida útil de cada sensor pot arribar fins a cin o set anys –fent servir simplement dues piles AAA d'1.5V i per a un promig de 8 medicions diàries- i tenen un abast de fins a 300-500 metres amb línia de visió (LoS o *Lineof Sight*, en anglès). Els sensors es connecten a repetidors –estacions base- situades a una certa altura i que poden incoporar interfícies Wi-Fi, Ethernet, ZigBee, 802.15.4 o cel·lular (GSM, UMTS) per a connexió amb un centre de gestió remot. A l'Annex XLII es mostren les especificacions tècniques dels sensors TWASTE, així com els components del repetidor.

Figura 28. Aplicació TSWASTE per a la gestió de recogida d'escombreries.

- Gran consum: aquest gran darrer àmbit abarca des d'oci fins a la domòtica o H*ome Automation*, passant per objectes com els *wearables* (literalment, "vestibles"). Algunes aplicacions poden ser:

- Consum de llum, aigua i gas (monitoratge del consum en temps real i consells sobre procediments/accions per gastar menys),

- Control remot d'electrodomèstics (*appliances*): aquesta implicació inclou desde apagar i encendre remòtament els nostres electrodomèstics (rentadora, robot de cuina, aspiradora, televisor, ordinador, etc) fins el monitoratge d'alguns d'ells (temps que manca perquè la rentadora acabi la bugada, nivell d'emplenament de la nevera, etc.),

- Sistemes de securetat/detecció d'intrusos (detecció de finestres i portes obertes, càmeres enfocades a un punt concret d'una estància, etc. amb la finalitat de prevenir robatoris)

- Preservació de material valuós (monitoratge de variables com la temperatura, humitat o quantitat de llum, per tal de controlar obres d'arts –per exemple quadres- o qualsevol altre tipus de bens a museus, magatzems, etc.),

- Pagament de compres (poder pagar sense tarjeta de crèdit ni billets/monedes, fent servir per exemple *smartphones* amb tecnologia NFC incorporada).

- *Wearables*: peces de roba que incorporen sensors de tot tipus (temperatura, humitat, moviment, pressió, etc.) com ara rellotges, cinturons, braçalets, sabatilles per córrer, gorres o fins i tot samarretes, pantalons o jaquetes. Els sensors capturen l'informació, que es rebuda per la unitat de processament (microcontrolador o processador de mida diminut) i enviada a Internet fent servir protocols com ara Bluetooh LE, ZigBee, 802.15e, etc. on és emmagatzemada i tractada per servidors remots i pot ser visualitzada en forma de gràfics per part de l'usuari, a través d'un ordinador, *smartphone*, etc. mostrant tot tipus d'informació com ara els kilòmetres recorreguts al dia, el pols, nivell de suor, calories cremades, pes, etc. Aquests sensors també poder servir en situacions d'emergència (per exemple per trobar un esquiador o alpinista que s'ha perdut a la montanya o es troba sota un allau, o bé un nadador, submarinista, windsurfista o nàufrag que s'ha perdut a alta mar).

Annex V. Teoria de l'anàlisi DAFO.

L'anàlisi DAFO (Debilitats, Amenaces, Fortaleses, Oportunitats), també conegut com a FODA o en anglès com a SWOT (*Strenghts*, *Weaknesses*, *Opportunities*, *Threats*) és una metodologia d'estudi de la situació d'una empresa o projecte, analitzant les seves característiques internes (Debilitats i Fortaleses), així com la seva situació externa (Amenaces i Oportunitats) [86]. A la pràctica, és una eina molt potent que es pot aplicar a gairebé qualsevol cosa: persones, serveis, productes, tecnologies, etc.

Bàsicament, a través de l'anàlisi DAFO, hem de poder contestar les següents preguntes:

- Com es pot destacar cada fortalesa?
- Com es pot disfrutar cada oportunitat?
- Com es pot defendre cada debilitat?
- Com es pot detenir cada amenaça?

De cara a l'anàlisi extern, s'han d'establir els fets o aconteixements que poden guardar cap relació amb l'empresa (en el nostre cas, amb el paradigma IoT) [87]. Aquests fets poden ser de caràcter polític (p.ex. restriccions a la importació), legal (per exemple, impostos), social (per exemple, creixement demogràfic) o tecnològic (per exemple, rapidesa dels avanços tecnològics o canvis en els sistemes). Un cop tenim aquests factors, es determina el grau d'influència que poder tenir per facilitar o restringir els objectius, en aquest cas de la tecnologia, esdevenent les oportunitats i les amenaces, respectivament.

Per la seva banda, de cara a l'anàlisi intern, s'han d'analitzar aspectes com la disponibilitat de recursos de capital, personal, actius, qualitat de la tecnologia (dels productes que la composen), estructura interna i de mercat, percepció dels consumidors, etc. Aquest anàlisi fixarà les fortaleses i debilitats del servei.

Al final, el resultat s'acostuma a mostrar en forma de taula/matriu, que ha de tenir aproximadament el següent aspecte i contingut [88]:

	Fortaleses	Debilitats
Anàlisi Intern	. Capacitats diferents . Avantatges naturals . Recursos superiors	. Recursos i capacitats escases . Resistència al canvi . Problemes de motivació del personal
	Oportunitats	**Amenaces**
Anàlisi Extern	. Noves tecnologies . Debilitament de competidors . Posicionament estratègic	. Alts riscos . Canvis en l'entorn

Taula 12. Matriu DAFO genèrica.

Annex VI. Anàlisi DAFO per a IoT.

Pasem a comentar cada cel·la de la matriu DAFO per a IoT exposada a la Memòria:

- Fortaleses

    - Per un cantó, tenim que diverses associacions de reconegut prestigi a nivel mundial com ara l'IEEE, IETF, 3GPP (*3GPP 3rd Generation Partnership Project*), etc. estan treballant/col·laborant conjuntament per tal de desenvolupar estàndards relatius a l'IoT (per exemple, d'aquí ha sorgit 6LoWPAN, RPL, CoAP, etc). Aquesta tasca és completament necessària si es vol arribar a un conjunt d'estàndards global que s'acabin imposant a la resta (protocols i plataformes propietàries que poden dificultar l'ascensió de l'IoT) [70].

    - Per altre cantó, el camp treball de les xarxes sense fils no és nou, ni tampoc el de les xarxes de sensors, que ja existeixen des de fa trenta anys. Podem parlar de tecnologies que, al menys des d'un punt de vista històric, ja són prou madures i han estat utilitzades extensivament en múltiples àmbits.

    - Per últim, un dels objectius finals de l'IoT es basar-se en estàndards i protocols oberts i flexibles, que permeten una fàcil interoperativitat/integració entre dispositius i plataformes. Aquest també és un gran punt a favor si el que es pretèn es crear una gran xarxa global completament interconnectada.

- Debilitats

    - La primera gran debilitat que trobem és que, fins ara, molts fabricants i grans companyies s'han dedicat a desenvolupar els seus propis protocols i estàndards per a solucions M2M, per un cantó per una manca d'estàndards globals i oberts en aquell moment i, per altra banda, probablement per raons estratègiques/comercials (protegir el seu mercat, intentar convertir-se en un referent en aquest tipus de solucions i poder desbancar a la competència, etc). Al final, però, aquest fet dificulta que diverses plataformes de diversos fabricants puguin comunicar-se entre elles o que la seva interconnexió sigui costosa i complicada, fet que pot fer enrera als consumidors (tant empreses com particulars) i, en definitiva, a llarg termini, suposen un entrebanc per al major creixement de l'IoT

    - A nivell tècnic, tenim que l'IoT, en basar-se en xarxes sense fils de sensors, necessiten disposar d'una font d'energia que duri el màxim de temps possible. Aquest font d'energia normalment acostumaran a ser bateries, donat que els dispositius no estaran connectats a la xarxa elèctrica. Aquest fet es podria solucionar dotant als sensors de sistemes de captació d'energia (*energy harvesting*) com ara panells solars però llavors apareix l'incertidumbre de si les condicions del medi –per exemple la quantitat de llum, és a dir, les condicions

meteorològiques- seran suficients per poder abastir les necessitats d'energia dels dispositius [10].

Per tant, es necessita saber d'avantmà quina serà la duració màxima de la bateria –i, per tant, la vida útil del dispositiu- amb la càrrega que porta de sèrie. Això dependrà tant del consum de la unitat sensora com de la unitat de processament però sobretot i, en gran mesura, per la unitat de comunicació (antena). Llavors, els esforços es troben actualment en fer servir l'antena el mínim possible (tant emissió com recepció) i apagar-la quan no es faci servir (d'igual manera, el microcontrolador/processaor també es fica en estat d'espera o *stand-by* quan no recolecta informació). Per tant, ens trobem, en definitiva, amb que la vida útil dels sensors (i, en concret, la durada de les bateries) és encara una debilitat que s'ha de salvar, per la qual cosa s'estan investigant nous algorismes/protocols –o millores els existents- per minitmizar l'ús de les mateixes.

- En tercer lloc i, tot que s'estan fent grans avenços pel que fa a la disminució del grau de complexitat necessària per a la implementació de solucions l'IoT (podem veure un exemple a l'Annex XLVIII, amb la plataforma 'Thinking Things' de Telefonica que permet posar en marxa una xarxa de sensat senzilla en uns segons), el cert és que, per a requeriments més complexes (per exemple solucions industrials, ramaderia, etc.) implementar una solució no és tan fàcil i fan falta molts més pasos com ara un estudi tècnic previ per determinar les necessitats de número de sensors, la seva ubicació (per garantir línia de vsió directa), potència d'emissió de l'antena), programació/configuració dels dispositius (microcontroladors) per a la captació de dades i el seu enviament, configuració de les pasarel·les, etc. Al final, acostumen a ser projectes llargs i personalitzats. Aquesta és una gran debilitat que s'ha de superar si es vol que el paradigma IoT tingui un desplegament massiu, no sols a nivell de consumidors individuals sinó de les empreses.

- Per últim, una possible debilitat que es pot trobar l'IoT és, tal i com es diu a la matriu, que els consumidors (finals, empreses) siguin reticents a acceptar i adoptar la tecnologia, bé per desconeixement de la mateixa o de les aplicacions que pot tenir (monitoratge de la salut, eficiència energètica , seguretat, simplificació de processos, etc.) o bé simplement perquè recelen d'ella (per exemple degut a qüestions de seguretat, ja que les persones i/o les empreses potser no volen que dades de caràcter sensible –p.ex. dades de salut- viatgin a través de mitjans sense fils, ni molt menys que aquestes dades s'emmagatzemin en llocs remots sobre els quals no es té cap coneixement ni control (i, el que podria ser pitjor, del tractament d'aquesta informació recollida i dels possibles usos que se'n podria fer de la mateixa, no sempre legítims i que al final podrien repercutir en contra del propi usuari)

- Oportunitats

    - Les oportunitats que s'obren a l'IoT són moltes, tants com camps/àmbits d'aplicació es puguin trobar. Com ja s'ha vist abans, es poden implementar solucions reals –i, el més important, realment beneficioses- en àmbits com la ramaderia, l'agricultura, el medi ambient, gestió intel·ligent de ciutats, optimització de processos industrials, estalvi energètic, etc. En aquest sentit, la demanda de dispositius i solucions IoT serà exponecialment creixent en els propers anys ja que, deixant de banda consideracions de seguretats o legals, els beneficis que se'n deriven són enormes.

    - Relacionat amb la primera gran oportunitat, tenit l'aparació de noves oportunitats de negoci, tant per a empreses ja existents que vulguin entrar a desevolupar i comercialitzar solucions i serveis IoT (p.ex. Telefonica, Google, Apple, Microsoft, etc.) com a oportunitats per a nous empresaris i emprenedors que troben que aquest és encara un mercat per descobrir i amb un altíssim potencial econòmic.

    - El cost total de una solució IoT (per exemple instal·lació de milers de sensors en un bosc o conreu) dependrà, en gran mesura, del cost dels components de maquinari, és a dir, dels nodes/motes. En aquest sentit i, gràcies a les economies d'escala (la producció de moltíssimes unitats d'un mateix producte deriva en una optimització i, per tant, reducció de costos) cada cop es poden oferir dispositius més barats i també més petits, fets que ajuden en gran manera a que empreses a pressupostos molt ajustats puguin permetre's iniciar projectes d'aquest tipus, al mateix temps que obre la tecnologia al consum massiu per part de consumidors/usuaris particulars.

    - Inversament amb el cost de producció, la potència de processament també ha anat augment paulatinament, seguint amb l'establert per la Llei de Moore (veure Annex XLIV) que indica que, aproximadament, el número de transistors d'un CI (circuit integrat) es duplica cada dos anys. Aquest fa viable que es puguin desenvolupar solucions cada cop més complexes (per exemple, fer que els dispositius no recollin únicament informació dels sensors de manera passiva, sinó que siguin capaços de tractar-la i processar-la en temps real i, fins i tot, que els dispositius puguin col·laborar entre ells per a executar tasques més ràpidament (computació paralel·la).

    - Per últim i, tal com ja s'ha deixat entreveure abans, podem considerar com a oportunitat per al creixement de l'IoT qualsevols dels beneficis últims que reporta per a les empreses i usuaris: millora de processos industrials, reducció de costos, control i millora de l'estat de salut, eficiència energètica, millora de l'atenció i satisfacció del client, oferiment de millors productes (carn, peix, fruta, ...) i, en definitiva, millora de la qualitat de vida de la societat.

- Amenaces

    - Pel que fa a les amenaces, probablement una de les més importants és a nivell legal/governamental. Els governs dels països podrian posar limitacions a l'ús de freqüències ja existents o de la potència d'emissió de les antenes, nombre de dispositius que es poden desplegar per m o Km^2, etc. En definitiva, es necessita, per un cantó que existeixi un marc legal ben definit i sense fisures o dobles interpretacions, però que al mateix temps no sigui massa restrictiu i impedeixi un major desplegament de solucions IoT (per exemple, en un escenari hipotètiu, es podria crear una agència pública que recaptés un "cànon" per cada dispositiu IoT que es fabriqués, situació que implicaria un augment del cost i, per tant, del preu final per al consumidor, fet que podria fer baixar la demanda d'aquest tipus de dispositius),

    - Molt relacionat amb el punt anterior, es necessita no únicament un marc regulatori ben definit i suficientment "flexible", sinó també que a nivell públic es suportin i promoguin aquest tipus de solucions, sobre tot a les empreses. Si a nivell governamental es posen entrebancs per al desenvolupament i, sobretot, implementació d'aquestes tecnologies, llavors els fabricants probablement aniran perdent interés en continuar desenvolupant nous productes i fins i tot les associacions que s'encarreguen de la definició d'estàndards podrien també deixar de crear millores/modificacions als protocols existents. És difícil que es doni aquesta situació però per exemple, a Espanya, ja tenim una certa experiència/jurisprudència en aquest temes, per exemple degut al problema d'asignació de l'espectre radioelètric amb el solapament de freqüències entre 4G i TDT, fet que es coneis com a "Dividend Digital" [89].

    - Un altra amenaça importatíssima (potser la que més) són els possibles riscos de privacitat amb que es poden trober les empreses/usuaris particulars [17], si no es prenen les mesures adequades d'avantmà. Per exemple, escollir quina informació es vol transmetre/emmagatzemar a Internet; fer servir una encriptació adequada com ara AES; fer servir infraestructures de clau pública (*PKI – Public Key Infrastructure*); limitar la potència d'emissió dels dispositius; etc. Si els entorns/plataformes no s'asseguren de manera correcta, s'està exposat a múltiples problemes, com per exemple:

        - Escolta/interceptació (*eavesdropping*) de dades per part d'usuaris externs, que tindrien accés a informació sensible/confidencial sobre temes de salut, estat d'infraestructures públices o privades, etc. i després fer un mal ús d'aquesta informació (per exemple traficar amb ella).

        - Injecció de dades incorrectes a les pasarel·les o directament als servidors remots (per exemple, es podrien injectar mesuraments incorrectes de temperatura, humitat, llum, vibracions, etc. que podrien fer que els servidors remots enviessin comandes errònies a les motes, per exemple des de parar/arrencar un sistema de rec a fins i tot parar per complet una cadena de muntatge, passant per l'enviament d'efectius (bombers, polícies) a llocs on no ha passat reso, el que és pitjor, no enviar-los quan sí ha passat quelcom. En definitiva, la injecció de dades malicioses pot resultar ser molt perillosa i fer-se servir, fins i tot, per enmascarar atacs físics.

    - Per últim, una possible amenaça que sobrevola el desplegament de l'IoT és que la pròpia indústria (en el sentit de fabricants i desenvolupadors de maquinari i programari) estigui disposada a acceptar i suportar els estàndards desenvolupats per les institucions com ara l'IEEE ja que, si això no passa i prefereixen continuant fent servir protocols i plataformes propietàries i tancades, a mig i llarg termini, probablement acabi desembocant en un estancament del grau d'implementació donat que, per defecte, els usuaris prefereixen quants menys estàndards millors (recordem antics escenaris similars, com ara la "batalla" entre els sistemes de vídeo VHS, Beta i 2000, on finalment va acabar guanyat VHS tot i no ser el pitjor sistema a nivel tècnic, on el millor fou 2000 seguit de Beta, però on 2000 no va aconseguir gairebé cap èxit degut a la seva aparició tardia i al poc suport per part dels fabricants i sobretot dels distribuïdors de pel·lícules).

Annex VII. Tipus de transmissió amb tecnologia MIMO.

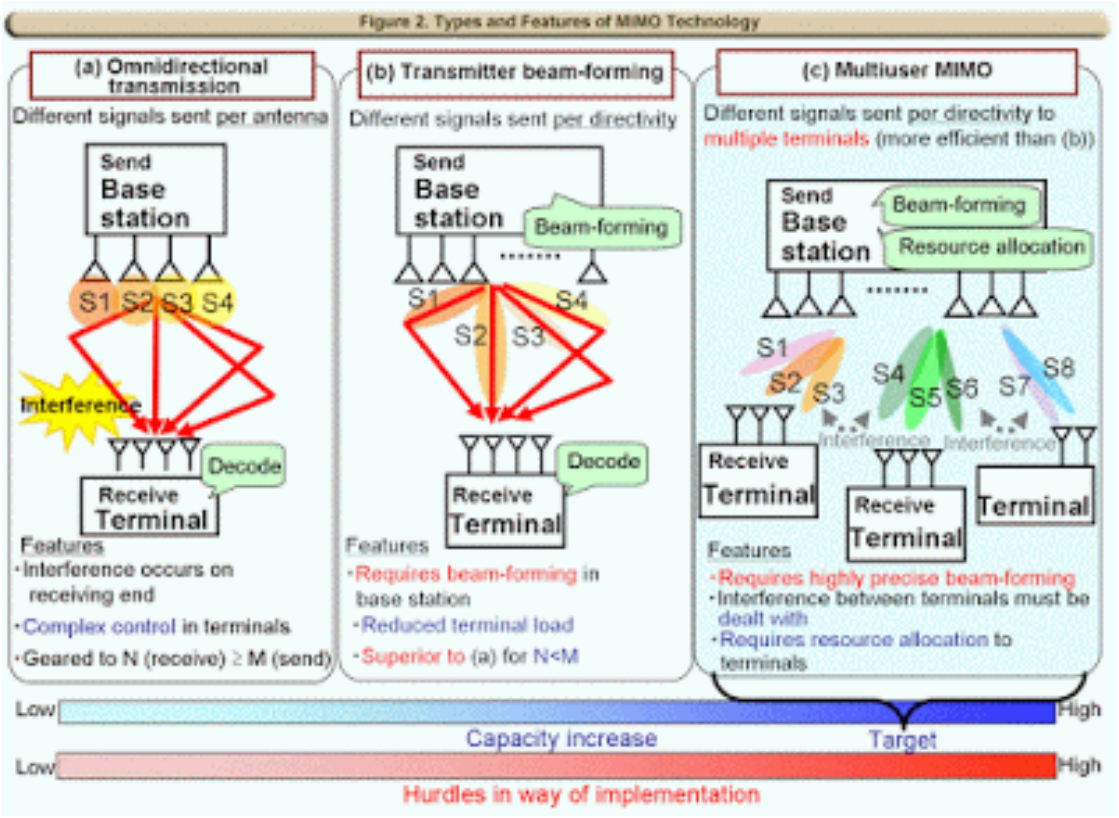


Figura 29. Esquema dels diferents tipus de transmissió MIMO.

Annex VIII. Característiques tècniques d'IEEE 802.11.

Freqüències

Pel que fa a les freqüències utilitzades, 802.11b, 802.11g i 802.11n-2.4 fan servir el rang freqüencial de 2.4-2.5 GHz, que és una de les bandes ISM (*Industrial, Scientific and Medical*); aquestes bandes freqüencials, que estan definides per l'ITU-R (*International Telecommunication Union – Radiocommunication Sector*) es troben obertes al seu ús per qualsevol persona, sense necessitat de licència, a nivell mundial (un resum amb les bandes ISM es pot veure a l'Annex XLV) [55]. Per la seva banda, 802.11a i 802.11n fan servir les bandes regulades -necessari licència- de 4.915-5.824 GHz. La primera banda és coneguda informalment com a 2.4 GHz mentre que la segona es coneix com 5 GHz. Cada rang es subdivideix en canals, cadascun amb una cert amplada de banda i freqüència central, de la mateixa manera que passa amb les retransmissions de ràdio i TV [90].

De fet, per ser correctes, el rang de 2.4 GHz es fa servir simultàniament tant per dispositius "sense llicenciar" (*unlicensed*) com per dispositius "llicenciats" (*licensed*). Això fa que, en aquesta banda (utitlizada per 802.11b i 802.11g) pugui haver interferències ocasionals amb altres dispositius que fan servir el mateix rang, com ara forns microones, telèfons sense fils i dispositius amb Bluetooth. A més, les freqüències utilitzades per certs canals (concretament del primer al sisè) cauen dintre de la banda 2.4 GHz de radioafeccionats (*amateur radio*). Per fer front a aquestes interferències, aquestes versions fan servir els mètodes de senyalització DSSS (802.11b) i OFDM (802.11g).

En el rang de 2.4 GHz, hi ha un total un de 14 canals, cadascun d'ells separats 5 MHz del canal contigu, amb un amplada de banda de 22 MHz i centrats a una freqüència de 2.412 GHz, com es pot veure a la figura de sota. Això implica que hi ha un cert grau de solapament entre els canals, amb l'excepció dels canals 1, 6 i 11 que són els únics tres que no es solapen:

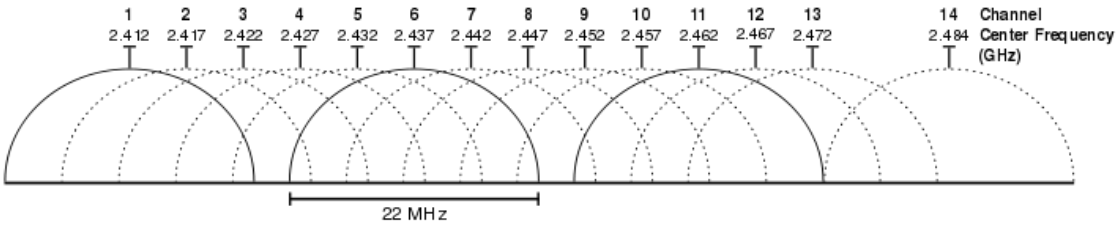


Figura 30. Representació gràfica de distribució de canals 802.11 al rang 2.4 GHz.

A la banda de 5 GHz, el tema és força més complicat i menys intuitiu, ja que l'amplada de cada canal pot ser de 20, 22, 40, 80 i fins i tot 160 MHz i, a més s'han de tenir en compte les diferents regulacions en funció del països.Per exemple, 802.11a fa servir la banda U-NNI (Unlicensed National Information Infrastructure) de 5 GHz que, per a la major part del món, offereix al menys 23 canals que no es solapen, a diferència dels únicament tres que s'ofereixen a 2.4 GHz.

Elements

Pel que fa als elements bàsics d'una xarxa 802.11, acostumen a ser els següents:

- Estacions (STA): són els nodes de la xarxa, que poden ser ordinadors, *smartphones* o qualsevol altre dispositiu amb la interfície de xarxa sense fils adequada,

- Medi de propagació: l'aire, fent servir ones d'RF,

- Punt d'accés (AP o *Access Point*): fa les funcions de pont entre dues xarxes, així com de concentrador (*hub*) de les connexions dels nodes. No és un element essencial en una xarxa Wi-Fi, ja que podem tenir comunicació directa entre nodes (*peer-to-peer*), tal i com es descriu sota.

- Conjunt de servei bàsic (BSS – *Basic Service Set*): grup d'estacions que s'intercomuniquen entre elles. Hi ha dos mètodes de comunicació: independient o *ad-hoc* (les estacions es comuniquen entre elles sense necessitat d'AP) o mode Infraestructura (els nodes es comuniquen a través d'un AP).

- Conjunt de servei extés (ESS – *Extended Service Set*): unió de diversos BSS i, per tant, de les seves LANs associades.

- Àrea de servei bàsic (BSA – *Basic Service Area*): és la zona on es comuniquen les estacions d'una mateixa BSS; per tant, indica la capacitat de poder canviar els terminals de lloc, variant així el BSS.

Codificacions

Per la seva banda, pel que fa a les tècniques de codificació utilitzades, tenim les següents:

- DSSS (*Direct Sequence Spread Spectrum* o Espectre Eixamplat per Seqüència Directa): també es coneix com DS-CDMA (Accés Múltiple per Divisió de Codi en Seqüència Directa. Es trata d'un dels mètodes de codificació de canal (pas previ a la modulació) en espectre eixamplat que més s'utilitza per a la transmissió de senyals digitals sobre ones RF. Tant DSSS com FHSS es troben definits per l'IEEE en l'estàndard 802.11. DSSS s'empra, amb alguna variació, en sistemes CDMA (*Code Divistion Multiple Access)* asíncrons, com per exemple UMTS (*Universal Mobile Telecommunications System*).

  En DSSS, es genera un patró de bits redundant per cadascun dels bits que composen el senyal. Com més gran sigui aquest patró, major resistència tindrà la senyal a interferències. IEEE 802.11 recomana un patró de 11 bit però l'òptim és de 100. En recepció, es realitza el procés invers per obtenir la informació original. La seqüència de bits utilitzada per modular els bits d'informació es coneix com seqüència de Barker (coneguda també com "codi de dispersió" o "pseudosoroll"). Es tracta d'una seqüència ràpida per tal de que apareguin, aproximadament, el matei nombre d'uns que de zeros.

Un cop aplicada la seqüència, hi ha dos tipus de modulació possibles: DBPSK (*Differential Binary Phase Shift Keying*) i DQPSK (*Differential Quadrature Phase Shift Keying*).

- FHSS (*Frequency Hopping Spread Spectrum* o Espectre Eixamplat per Salt de Freqüència): aquesta tècnica de codificació consisteix en transmetre una part de la informació en una determinada freqüència durant un interval de temps (*dwell time*) inferior a 400 ms. Passat aquest interval, es canvia de freqüència d'emissió i es segueix transmetent per una altra. D'aquesta manera, cada "tram" d'informació es transmet en una freqüència diferent durant un curt període de temps. Aquesta codificació vindria a ser un equivalent d'una multiplexació en freqüència.

  L'ordre de salts en freqüència ve determinat per una seqüència pseudoaleatòria emmagatzemada en unes taules i que tant emissor com receptor han de conèixer; per tant, si es manté la sincronització en els salts de freqüència s'aconsegueix que, encara que en temps es canvii de medi físic, a nivell lògic únicament es manté un canal. El nombre de salts està regulat a cada país (per exemple, a USA es fixa una taxa mínima de 2.5 salts per segon).

  Un cop aplicat FHSS, la modulació que s'aplicaria en aquest cas és FSK (*Frequency Shift Keying*).
- OFDM (*Orthogonal Frequency Divsion Multiplexing* o Multiplexació per Divisió de Freqüència Ortogonal): es tracta d'un mètode de codificació de dades en mútiples freqüències portadores. Aquest esquema ha esdevingut molt popular en comunicacions digitals de banda ampla, ja sigui en medis sense fils o en cablejat de coure i és utilitzats en aplicacions com ara broadcasting de TV digital, accés a Internet DSL (*Digital Subscribe Line*), xarxes a través del corrent elèctric (PLC – *Power Line Communication*) o xarxes 4G.

  Com ja s'ha dit, ODFM és una esquema FDM (multiplexació per divisió de freqüència); concretament, s'utilitza un llarg nombre de senyals subportadores ortogonals per transportar les addes, a través de diversos fluxes paralels de dades (anomenats "canals"). Que cada subportadora sigui "ortogonal" a la resta implica que s'elimina la diafonia (*cross-talk*) i que les bandes de guarda entre portadores no són necessàries, fet que simplifca el disseny tant del transmissor com el receptor. L'ortogonalitat requereix que l'espaiament entre subportadores sigui d' $\Delta f = \frac{k}{T_U}$ (Hz), on T_U és la durada útil de símbol (mida de finestra del costat receptor) i k és un enter positiu, típicament 1; per tant, amb *N* subportadores, l'amplada total passabanda és de B ≈ N · Δf (Hz)

  Cada subportadora es modula fent servir un esquema de modulació convencional, com per exemple QAM (*Quadrature Amplitude Modulation*) o PSK (*Phase-Shigt Keying*) a una taxa de símbols baixa. El principal avantatge de fer servir OFDM en relació a

esquemas d'una sola portadora és l'habilitat per fer front a condicions de canal severes (per exemple, atenuació a altes freqüències sobre cables de coure, interferències de banda estreta degudes a multicamí, etc) sense haver d'utilitzar complexos filtres d'equalització. L'equalització de canal es simplifica perquè OFDM es pot veure com una utilització de moltes senyals lentes de banda estreta, en comptes d'utilitzar un únic senyal de banda ampla modulat més ràpidament. La baixa taxa de símbol permet l'utilització d'un interval de guarda entre símbols assequible, fent possible l'eliminació d'interferències intersíbol (ISIS – *Intersymbol Interference*), al mateix temps que utlitza l'eco i el repartiment de temps per aconseguir guany en diversitat (és a dir, una millora de l'SNR –*Signal to Noise Ratio*)

Altres dades

A banda de les característiques anteriors, altres valors útilsd'una xarxa 802.11 són les següents:

- Nombre màxim de nodes per xarxa: formalment, el màxim nombre de nodes dintre d'una mateixa xarxa 802.11 és d'únicament 32 nodes.

- Consum promig de corrent: lògicament, dependrà de la potència amb la que emiti l'antena però típicament es troba sobre uns 220mA en transmissió (Tx) i 215mA en recepció (Rx) amb la versió 802.11n [92]. Cal tenir en compte que l'FCC (*Federal Communications Commission*) dels Estats Units imposa una potència màxima de transmissió (*output power*) amb la que s'alimenta l'antena de 30 dBM (1 Watt) mentre que, per defecte, acostuma a ser de 20 dBm (0.1 Watt).

- Possiblitat de de multi-salt: no es permet multi-salt, és a dir, reenviament de paquets de dades entre nodes. Les xarxes 802.11 presenten sempre una tecnologia d'estrella en mode Infraestructura o bé punt a punt en mode *ad-hoc* (la topologia *mesh*, present en altes estàndards, no és possible).

- Vida de la bateria: dependrà de diversos factors (òbviament, de la capacitat de la bateria); a banda d'això, dependrà pricipalment de la potència d'emissió/recepció de l'antena així com del temps en què aquesta es troba activa (nombre de missatges enviats). Típicament, la durada de les bateries d'un dispositiu amb Wi-Fi acostuma a anar entre mig dia i 5-7 dies.

- Mida de la pila (*stack size*): aquest valor indica els recursos de sistema necessaris per poder habilitar Wi-Fi en un dispositiu. Per a 802.11b és d'aproximadament 1 MB (quantitat necessària per carregar a memòria)

- Latència: també anomenada "temps d'enllaç", pot arribar a ser de fins a 3 segons (temps que triga un dispositiu en connectar-se/enllaçar amb una nova xarxa Wi-Fi)

- Mètodes de securetat: SSID, WEP (*Wired Equivalent Privacy*), WPA/WPA2 (*Wi-Fi Protected Access*). Avui dia, tots aquests mètodes s'han demostrat insegurs i es poden "crakejar" amb relativa facilitat.

A mode de resum, podem dir que 802.11 és un estàndard adient més aviat per a xarxes sense fils de mida petita, en qué tots els nodes es connecten directament a un AP (que farà de *gateway* cap a una altra xarxa) i on els dispositius es troben endollats sempre al corrent elèctric o es poden endollar periódicament (portàtils, telèfons, etc.) ja que el consum és força elevat (Wi-Fi asumeix que l'antena estarà funcionant sempre i que no es ficarà en mode repós quan no calgui enviar dades). En canvi, l'estàndard no seria adient per grans xarxes de sensors (milers de nodes) que necessiten estar desateses i on els dispositius no poden connectar-se a la xarxa elèctrica per les pròpies característiques de l'emplaçament (per exemple a un conreu, al bosc, al mar, etc.). A més, no es poden salvar grans distàncies perquè no es permet una topologia *mesh* o clúster, on els paquets de dades es puguin encaminar entre nodes.

Per altra banda, els mecanismes de seguretat implementats per defecte a Wi-Fi són insegurs i es poden trencar (hi ha multitud d'eines a Internet que fins i tot automatitzen aquest procés) per la qual cosa no seria adient per a xarxes on la confidencialitat i integritat de les dades són crucials. Per últim, la mida de la pila és força elevada si es compara amb altres estàndars sense fils i, per tant, no es podria carregar en microcontroladors de baix cost, que acostumen a tenir escasa RAM.

Annex IX. Característiques tècniques d'IEEE 802.11ah.

El que s'intenta amb Low-Power Wi-Fi és, per un costat, anar fins a xarxes de sensors que facin servir nodes MIMO i basats en Wi-Fi; aquests nodes estarien indicats per a *smart metering* (mesurament inte·ligent, on s'han de transferir bastant dades). Per altra banda, també seria possible una coexistència amb 802.15.4, deixant aquest darrer per a la xarxa de sensors (quan no hi ha moltes dades a transmetre), utilitzant 802.11ah per al *backhaul* (xarxa de transport que interconnecta amb la xarxa remota). Aquest escenari queda reflectit en la figura de sota:

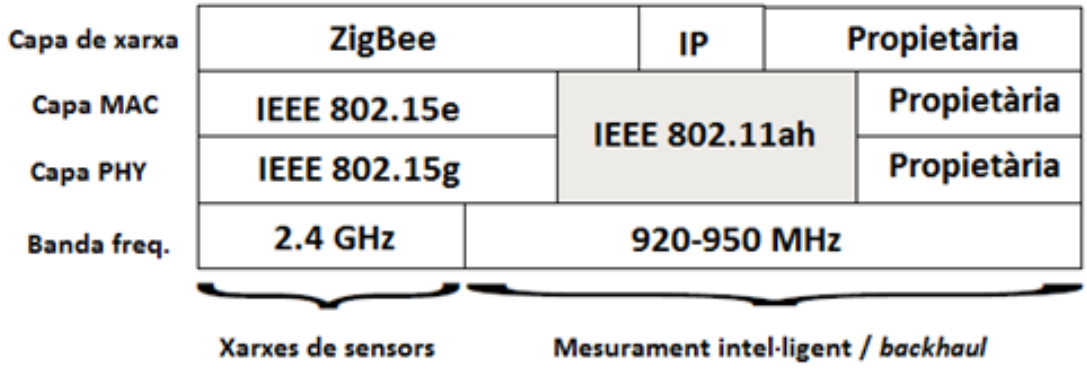


Figura 31. Piles de protocols de diferents WSNs.

De fet, 802.11ah es basa en tècniques que també es fan servir a 802.15.4, com ara el concepte de *relay*(reenviament) per poder cobrir distàncies més llargues o la utilització de períodes predefinits *wake*/*doze* (també anomenats *wake-up*/*sleep*, és a dir, despert/dormint) per estalviar reduir el consum d'energia.

En el primer cas, tenim que tant l'AP (anomenat *Relay AP*) com els STAs poden intercanviar trames entre ells. D'aquesta manera, les estacions que fan de *relay* també poden proporcionar connectivitat a altres estacions fora de l'abast de l'AP, agumentant la cobertura. El problema de fer servir les estacions reenviadores és que es presenta aquí es una sobrecàrrega en l'eficiència general de la xarxa i una complexitat superior; per tant, per limitart aquest overehad, la funció de *relay* ha de ser bidireccional i es limita a únicament dos salts.

Per la seva banda, per tal de baixar el consum d'energia, es consideren les següents opcions:

- Es fa servir MCS (*Modulation and Coding Schemes*), que redueix el temps que les estacions es troben en mode actiu, millorant d'aquesta manera la vida de les bateries.

- També existeix el concepte de 'Temps objectiu despertador' (*Target Wake Time* o TWT): aquesta funció permet a un AP definir un període o períodes de temps als quals les estacions poden accedir al medi (l´ús de TWT es negocia entre l'AP i les STAs). D'aquesta manera, les STAs i l'AP intercanvien informació que inclou una "durada esperada d'activitat" que permet a l'AP controlar la quantitat de contenció i solapament entre STAs que competeixen pel medi. D'aquesta manera, les estacions es troben "adormides" mentre no arriba el seu TWT.

- Divisió de les STAs en estacions TIM (*Traffic Indication Map*) no TIM. El primer tipus rep periòdicament informació sobre el tràffic emmagatzemat en els *buffers* de l'AP (en el que s'anomena "elements d'informació TIM"). Per la seva banda, el segon tipus fa servir el mecanisme TWT, que permet reduir la sobrecàrrega.

- Un altre mètode es la Finestra d'Accés Restringida (RAW - *Restricted Access Window*) que permet particionar les estacions d'una mateixa BSS en grups i restringir l'accés al canal únicament a les estacions que pertanyen a un determinat grup, en un període de temps concret. D'aquesta manera, s'ajuda a reduir la contenció i prenevir transmissions simultànies de un gran nombre d'estacions, ja que estarien "amagades" de la resta.

- També tenim el concepte d'Oportunitat de Transmissió (*Transmit Opportunity* – TXOP). D'aquesta manera, pot haver TXOPs bidireccionals entre un AP i un STA –entre parells d'estacions- per intercanviar una seqüència de trames ascendents o descendents, durant un temps reservat. Aquest mode d'operació està dirigit a reduir el nombre d'accés al canal basats en contenció, millorar l'eficiència de canal mitjançant la minimització del nombre d'intecanvi de trames requerides per a trames de dades ascendents o descendents i permet a les estacions extendre la vida de les bateries, mitjançant temps *Awake* curts. En versions anteriors, a aquest concepte se li deia Velocitat d'Intercanvi de Trames (*Speed Frame Exchange*).

  Com a conclusió, podem dir que aquest nou estàndard pot representar una alternativa a l'actual IEEE 802.15.4 –en alguns escenaris concrets- o bé ser una solució complementària. Probablement 802.15.4 es continuarà utilitzant en xarxes de sensors tradicionals, que necessiten un consum molt baix d'energia i una transferència de dades limitada; per la seva part, Low-Power WiFi s'utilitzarà en WSNs on s'hagi de transferir contingut multimèdia com aúdio/vídeo o bé a dispositius de consum massiu (per exemple electrodomèstics, televisors, domòtica, *wearables*, etc.)

Annex X. Característiques tècniques d'IEEE 802.16d.

Nivell PHY

A nivell de capa física, tenim que 802.16d fa servir OFDM pel transport de dades, suportant amplades de banda d'entre 1.25 i 20 MHz per canal (les típiques són 3.5, 7 i 10 MHz), aconseguint fins a 2048 portadores. Per la seva banda, Mobile WiMAX utiltiza OFDMA (versió multiusuari d'OFDM –accés múltiple-, que s'aconsegueix assignant subconjunts de subportadores a cada usuari individual) i les amplades de banda son 5, 7, 8.75 i 10 MHz.

802.16 suporta modulació i codificació adaptatives (*Adaptative Modulation and Coding* - AMC), és a dir, adequació de la modulació, codificació i altres paràmetres de la comunicació en funció de les condicions de l'enllaç ràdio (per exemple, pèrdues per propagació, interferències degudes a senyals d'altres transmissors, sensibilitat del receptor, marge disponible de potència al transmissor, etc). Això significa que, en condicions de bon senyal, es pot fer servir un esquema de codificació 64-QAM (*Quadrature Amplitude Modulation*), mentre que en condicions de senyal més pobre, es fa servir una codificació BPSK, més robusta (únicament en WiMAX fixe); en condicions intermitges, per la seva banda, es pot fer servir 16-QAM o QPSK, entre d'altres.

A la següent figura podem veure la relació que hi ha entre la cobertura –en Km- que es vol aconseguir i l'esquema de modulació que s'utilitza:

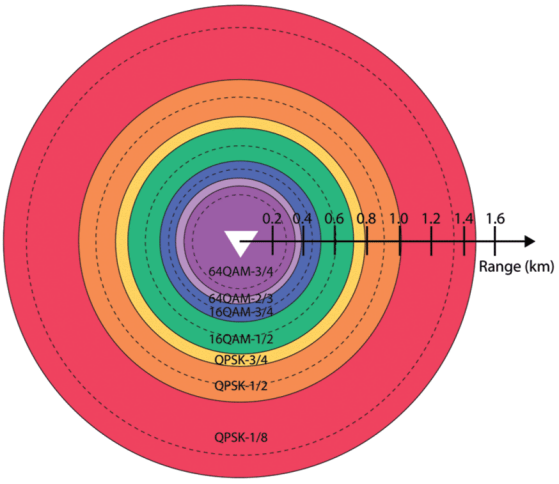


Figura 32. Relació entre abast i tipus de modulació utilitzada amb WiMAX.

Per que fa al tipus de multiplexació, WiMAX fixe fa sevir multiplexació per divisió temps (*Time-Division Duplexing* o TDD) o per divisió de freqüència (*Frequency-Division Duplexing* o FDD) mentre que la versió mòbil únicament fa servir TDD.

Pel que fa a l'espaiat entre subportadores, la versió fixa utilitza valors de 15.625, 31.25 i 45 MHz, mentre que la versió mòbil únicament proposa un espaiat fixe de 10.94 KHz.

Pel que fa potències, una BS acostuma a transmetre a un nivell aproximat de +43 dBm (20 W) mentre que un client mòbil típicament transmet a +23 dBm (200 mW) [93]. Tanmateix, hi una una gran diferència entre potència ascendent (*uplink*) i descendent (*downlink*), per la qual cosa, mentre que una estació -també anomenada*Susbscriber Station* o SS quan és fixa i *Mobile Subscriber Station* o MSS quan és mòbil- pot rebre fàcilment transmissions d'una BS, la relativa baixa potència de transmissió del mòbil fa difícil per a l'estació poder escoltar-ho. També és interessant destacar que, quan es transmeteix una trama, el 'preamble' sempre es transmet amb més potència que la resta, concretament a +3 dB (WiMAX fixe) o +9 dB (WiMAX mòbil) [94].

Per últim, WiMAX suporta MIMO per tal de permetre comunicació sense línea de visió directa (NLOS) i major amplada de banda, així com la tècnica *Hybrid Automatic Repeat Request* (HARQ) per a correcció avançada d'errors.

El radi de cobertura que WiMAX pot lograr és d'uns 70-75 Km com màxim, aproximadament. A més, WiMAX incorpora, a banda del típic mode punt a multipunt (P2MP), un altre mode/mecanisme per crear xarxes mallades multi-salt (*Multi-hop Mesh*) pel qual les BSes poden anar reenviant els paquets de dades entre elles per tal de salvar majors distàncies.

Per la seva banda, la màxima taxa de transferència –pic- depèn de la versió de 802.16 utilitzada (tradicionalment, la taxa típica ha estat de 25 Mbps per a pujada i 7 Mbps per a baixada):

- Amb 802.16.-2009 (*release* 1.5), la màxima taxa es troba al voltant dels 140 Mbps (en sentit baixada) i 135 Mbps (en sentit pujada), fent servir 2x2 MIMO, dos canals de 20 MHz amb multiplexació FDD i SOFDMA (*Scalable* OFDMA).

- Amb 802.16m (*release* 2), la màxima tasa és d'uns 375 Mbps en baixada i 365 en pujada, fent servir 4x4 MIMO, dos canals de 20 MHz amb FDD i SOFDMA. Les MSS que es mouen lentament poden fins i tot agregar canals i aconseguir així una taxa de baixada agregada de fins 1 Gbps.

Nivell MAC

A nivell de capa d'enllaç, una sèrie de "subcapes de convergències" (*Covergence Sublayers* – CS) descriuen com les tecnologies cableades (Ethernet, ATM – *Asynchronous Transfer Mode*, IP) s'encapsulen en el medi aire, com es classifiquen les dades, etc. També es descriu com s'entreguen comunicacions segures, utilitzant intercanvi segur de claus durant l'autenticació, basat en EAP (*Extensible Authentication Protocol*), així com encriptació AES o DES (*Data Encryption Standard*) durant la transferència de dades. Altres característiques de la capa MAC inclouen mecanismes d'estavil d'energia (modes *sleep* i *idle*) y mecanismes de traspàs (*handover*).

Per altra banda, una característica clau de 802.16 és que es tracta d'una tecnologia "orientada a connexió": el dispositiu final, també anomenat estació suscriptora (*Subscriber Station* - SS) no pot transmetre dades fins que l'estació base (*Base Station* – BS) li assigna un canal. Aquest fet permet que es pugui proporcionar una forta qualitat de servei (*Quality of Service* – QoS).

Al seu voltant, a cada connexió entre SS i BS ("fluxe de servei" o *Service Flow*) se li assigna una QoS específica. Hi ha cinc classes de servei a 802.16e:

- *Unsolicited Grant Service* (UGS): fluxex en temps real que comprenen paquets de dades de mida fixa, a intervals de temps periòdics (per exemple, circuits E1),

- *Extended Real-time Polling Service* (ertPS): fluxes de servei en temps real que generen paquets de dades de mida variable, a intervals periòdics (per exemple, VoIP),

- *Real-time Polling Service* (rtPS): fluxes de dades en temps real amb paquets de dades de mida variable, a intervals periòdics (per exemple, vídeo),

- *Non-real-time Polling Service* (nrtPS): fluxes de dades tolerants a retrasos amb paquets de dades de mida variable, pels quals es requereix una taxa mínima de dades o *throughtput* (per exemple, FTP amb taxa garantida),

- *Best Effort* (BE): fluxes de dades que no necessiten un nivell de servei mínim i, per tant, poden ser gestionats quan hi hagi temps/espai (exemple, HTTP).

Aplicacions

Al document "*Requirements for WiMAX Machine to Machine (M2M) Communication*" del WiMAX Forum [19], es descriuen diverses aplicacions -casos d'ús- de WiMAX, específicament de comunicació entre màquines. Aquests casos d'ús van des de la gestió de flotes de vehicles (per exemple per part d'una empresa de lloguer de cotxes), al monitoratge d'una màquina de *vending*, passant per l'*smart metering* (monitoratge i control del consum d'electricitat, aigua, gas), videovigilància, diagnòstic mèdic remot, informació del tràfic (per exemple a les parades de bus) o pagament mòbil.

A mode de resum, poder dir que 802.16 o WiMAX (anomenat informalment "WiFi amb esteroïdes") és un estàndard ja bastant madur amb dues versions diferenciades: fixa (802.16d) i mòvil (802.16e). La primera versió podria considerar-se com a reemplaç sense fils de tecnologies actuals d'accés cablejades, com ara coure (DSL – *Digital Subscriber Line*) o híbrides fibra-coaxial (HFC), sobretot en zones rurals o de difícil accés que encara no tenen infraestructura; per la seva banda, la versió mòbil podria considerar-se com una alternativa a tecnologies cel·lulars com ara UMTS o LTE, ja que les taxes de transferència i radis de cobertura aconseguits són similars o fins i tot superiors.

Per altra banda, existeixen dues versions –esmenes- encara en fase desenvolupament, per permetre aplicacions M2M (802.16b i 802.16p), que habiliten baix consum de potència, suport per xarxes amb gran número de nodes, etc. Tot i així, creiem que no espot considerar aquesta tecnologia com "plenament IoT", és a dir, com una alternativa a altres molt més enfocades a xarxes fixes de sensors de curt abast, com ara Low-Power Wifi, Bluetooth LE o 802.15.4, ja que aquestes darreres, com hem dit, es centren en xarxes on els nodes es troben molt més a prop entre ells i on les necessitats de transferència no són elevades (de l'ordre de Kbps); en canvi, 802.16 està molt més dirigit a xarxes punt a punt o punt a multipunt, on els nodes poden ser mòbils, estar separats fins i tot kilòmetres de distància i on es requereixen taxes molt més elevades (de l'odre de Mbps). Tal i com ja passava una mica amb Low-Power WiFi, podem considerar WiMAX més aviat per a la creació del *backhaul* amb la xarxa remota i mantenir 802.15.4 (o per exemple Bluetooth LE) per a la comunicació entre els nodes sensors i les pasarel·les.

Annex XI. Aprofundiment sobre IEEE 802.20.

A simple vista, es pot pensar en una gran semblança entre 802.16e i 802.20, en el sentit que ambdós estándars busquen proporcionar connectivitat sense fils de banda ampla i poden ser utilitzats per usuaris mòbils. Tot i així, en realitat 802.20 està enfocat a objectes que es mouen a gran velocitat (fins a 250 Km/h, per exemple trens d'alta velocitat), mentre que 802.16e s'utilitza més aviat per usuaris que van a velocitat vehicular (cotxe, moto, bicicleta) o caminant. També hi ha diferències pel que fa a com cada estàndard està implementat: per exemple, 802.16e opera en les bandes de 2 a 6 GHz mentre que 802.20 únicament fa servir bandes per sota de 3.5 GHz. En definitiva, 802.16e sembla indicat com estàndard d'última milla i *backhaul*per usuaris de telèfons mòbils i ordinadors portàtils i que pot ser vist com una extensió de la infraestructura sense fils actual, mentre que 802.20 fa servir antenes adaptatives i IP per proporcionar una alternativa a xarxes cel·lulars com ara 3G.

Per tant, la conclusió a la que arribem és bàsicament la mateixa a la que van arribar amb 802.16e: tot i aquests estàndars permeten crear xarxes sense fils, d'alta velocitat, amb mecanismes de qualitat de servei, etc. no els veiem adients per crear WSNs de baix consum (les antenes en principi han d'estar actives tota l'estona, sobre tot en entorns en moviment) ni baix cost, bàsicament perquè no estan orientades a aquest fi sinó, en tot cas, a comunicació M2M de dispositius en moviment (per exemple, dos trens d'alta velocitat que es comuniquen entre ells i decideixen i actuen en funció de paràmetres com la velocitat que porten, la via per la qual van, la climatologia, etc).

Annex XII. Característiques tècniques d'IEEE 802.22.

Les característiques principals d'aquest estàndard són:

- Modulació OFDMA,
- Rang de freqüències entre 54 i 790 MHz (espectre VHF i UHF),
- Radi de cobertura màxim d'uns 100 Km,
- Taxa de transmissió de 19 Mbps (a 30 Km de distància) ,
- Amplada de banda de 6-8MHz (amplada de banda d'un canal de TV),
- Possibilitat de fer *channel bonding* (ajuntar dos o més canals per aconseguir una major amplada de banda, és a dir, major taxa Tx/Rx),
- Capa MAC composta per dues estructures: trama (*frame*) i supertrama (*superframe*). Cada supertrama está formada per diverses trames. La supertrama tendrà una capçalera de control de supertrama (SCH) i un preamble. Aquestes eran enviades per la BS en cada canal que sigui possible, sense causar interferències. Quan un CPE es troba encés, aquest sensarà l'espectre i trobarà els canals que estan disponibles i rebrà la informació necessària per connectar-se a la BS (hi ha dos tipus de sensat: *in-band* i *out-of-band*: en el primer, es sensa únicament el canal actual utilitzat per la BS i el CPE; en el segon, es sensen també la resta de canals)
- Us de X.509v3 (infraestructura de clau pública i ús de certificats)
- S'utilitza EAP-TLS i EAP-TTLS per encriptació.

Com a resum podem dir que, aquest estàndard, tot i que força interessant a nivell tècnic, no està pensat per a xarxes de sensors, ja que els radis de cobertura amb el que es treballa són massa llunyans (en contraposició a les WSNs, on els sensors acostumen a estar a pocs metres els uns dels altres) ni incorpora mesures per a l'estalvi d'energia (per exemple mode *sleep* - apagat de l'antena quan no s'està emetent, compressió de capceleres per a disminució del volum de dades transmés, etc.) com tampoc passa amb els estàndars vist just abans però que altres estàndars com 802.15.4 sí que incorporen. L'exemple més clar el tenim amb el fet de que, amb 802.22, la BS ha d'emetre la supertrama a tots els canals lliures (fet que implicar la utilització de l'antena tota l'estona i, per tant, consum de bateria) i els CPEs també han d'anar sensant tots els canals, escenari que, des de el punt de vista de consum energètic, és altament ineficient.

Annex XIII. Característiques tècniques de Bluetooth.

Les xarxes que es creen fent servir Bluetooth s'anomenet *piconets* (picoxarxes). Una *piconet* consisteix en dos o més dispositius que ocupen el mateix canal físic –sincronitzats amb un rellotge comú i una seqüència de salt. Alguns exemples de picoxarxes són un telèfon mòbil connectat a un altre, un mòbil connectat a un PC portàtil, una càmera de fotos connectada a un PC, etc (tots ells amb interfície de xarxa Bluetooth). En una *piconet* pot haver-hi un únic dispositiu mestre (*master*) i fins a set dispositius esclaus (*slaves*); a més, pot haver-hi fins a 255 dispositius en estat inactiu ("aparcats"), que el mestre pot posar en estat actiu en qualsevol moment. Els dispositius poden canviar-se els rols, per acord mutu (un esclau pot convertir-se en mestre i a la inversa).

Tots els esclaus comparteixen el rellotge del mestre. L'intercanvi de paquets es basa en aquest rellotge, que fa "tic" a intervals de 312.5 µs; dos "ticks" de rellotge fan una ranura de 625 µs; dues ranures fan un parell de ranures (*slot pair*) de 1250 µs. En el mode més simple –ranures simples- el mestre transmet durant les ranures parells i rep en les ranures senars; els esclaus, per la seva banda, reben en les ranures parells i transmeten en les senars. Per la seba banda, els paquets poden tenir una llarga d'una, tres o cinc ranures.

Dos o més *piconets* poden connectar-se, formant una *scatternet* (xarxa dispersa) que permet que certs dispositius tinguin el rol de mestre en una de les picoxarxes i el d'esclau en les altres. En la figura de sota es pot veure una representació d'una *scatternet*, on els punts vermells representen dispositius mestres, els verds representen esclaus i els blaus representen dispositius "aparcats":

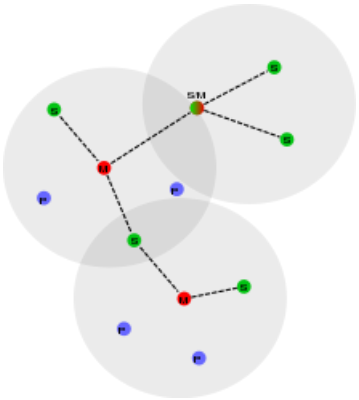


Figura 33. Exemple d'*scatternet* Bluetooth.

A grans trets, el mode de comunicació és el següent: en un moment determinat, es poden transferir dades des d'un mestre fins a un altre dispositiu (encara que també existeix un mode *broadcast* que gairebé no es fa server i que permet l'enviamenta diversos dispositius alhora). El mestre escolleix a qué esclau dirigir-se; llavors, canvia ràpidament d'un esclau a un altre seguint un esquema *round-robin* (algorisme de balanceig entre nodes, que assigna pesos a cada node i reparteix la comunicació entre ells, de forma seqüencial i circular). Donat que el mestre escolleix l'esclau amb què parlar, és més fàcil ser mestre que no pas esclau (en altres

paraules, és fàcil ser mestre de set esclaus però no es tàn fàcil ser esclau amb dos mestres, ja que se suposa que l'esclau ha d'estar escoltant en cada ranura de recepció).

Bluetooth està pensat com a reemplaç de protocols cablejats i està dissenyat per a un baix consum i xips transceptors de baix cost. Els dispositius no han de tenir línia de visió directa. Pel que fa a les cobertures efectives, depenen bàsicament de la potència d'emissió –encara que també de les condicions de propagació, configuracions de les antenes, condicions de les bateries, etc.- però, en la pràctica, son aquestes:

- Dispositius Classe 1: 100 mW potència màxima – Aprox. 100 m cobertura
- Dispositius Classe2: 2.5 mW potència màxima – Approx. 10 m cobertura
- Dispositius Classe 3: 1 mW potència màxima – Approx. 1m cobertura

Com podem veure, cada classe de dispositius ve determinada per la seva màxima potència d'emissió. A la pràctica, dos dispositius Classe 1 que es connecten entre sí, poden arribar a distàncies de comunicació de fins a 1 Km, quant tots dos tenen una alta sensitibitat i alta potència.

Avui dia hi ha diverses versions de les especificacions Bluetooth, essent les més importants les següents:

- Versió 1.2: incorpora AFH (*Frequency-Hopping Spread Spectrum*) per resistir millor a les interferències ràdio; velocitats de fins a 721 Kbps; introdueix control de fluxe; ratificat com a estàndard IEEE 802.15.1-2005.

- Versió 2.0 + EDR: introdueix EDR –de manera opcional- per a transferència de dades més ràpida, amb una taxa nominal de 3 Mbps teòrics (2.1 Mbps a la pràctica), utilitzant una combinació de GFSK i PSK amb les variants π/4-DQPSK i 8DPSK. Per altra banda, EDR també proporciona un consum més baix, gràcies a un cicle de treball -*duty cycle*- més reduït (recordem que el cicle de treball és el percentatge de temps d'un període en què una senyal està activa i s'expressa com a $D = \tau/P * 100$; a la pràctica, el terme s'utilitza per expressar el temps que la ràdio d'un dispositiu està activa).

- Versió 2.1 + EDR: igual que la versió 2.0 (mateixa velocitat màxima) però inclou, a més, emparellament segur simple (SSP), així com EIR (*Extended Inquiry Response*) per a un millor filtratge de dispositius abans de la connexió i *sniff subrating*, que redueix encara més el consum de dispositius que es treoben en mode de "baix consum".

- Versió 3.0 + HS: proporciona taxes de transferència màximes teòriques de fins a 24 Mbps, encara que no sobre un enllaç Bluetooth en sí mateix sinó sobre un enllaç 802.11, fent servir Bluetooth únicament per a la fase de negociació i establiment. Concretament, aquesta característica diferencial s'anomena AMP (*Alternative* MAC/PHY) i que, com el seu nom indica, especifica l'ús d'una capa PHY i MAC altenatives per transportar dades de perfil i que conté una part anomenada *High-Speed* que és opcional. Les dades de perfil i la connexió inicial continuen anant per

Bluetooth, mentre que quan s'han de transmetre grans quantitats de dades, s'utilitza MAC PHY 802.11 (típicament associades a Wi-Fi).

- Versió 4.0: aquesta especificació -també anomenada *Bluetooth Smart*- es va adoptar a partir de juny del 2010 i inclou *Classic Bluetooth* (protocols Bluetooth antics), *Bluetooh High Speed* (basat en Wi-Fi, com ja hem vist) i *Bluetooth Low Energy* o BLE (creat per Nokia en 2006 amb el nom de WiBree). Al igual que la versió 3.0, suporta velocitats de fins a 24 Mbps.

Annex XIV. Característiques tècniques de Bluetooth Smart.

Bluetooth Smart defineix diversos perfils –especificacions de com ha de funcionar un dispositiu en funció de l'aplicació particular que s'estigui fent servir- per a dispositius de baix consum (en realitat, l'existència de perfils ja existia a l'especificació Bluetooth original). Per la seva banda, els fabricants poden decidir incorporar, a un mateix dispositiu, implementacions de diversos perfils. Per un cantó, tenim perfils genèrics anomenats GATT (*Generic Attribute Profile*), especificació genèrica per rebre i enviar petites quantitats de dades sobre enllaços de baix consum. Per la seva banda, també tenim perfils BR/EDR. Per últim, també tenim perfils específics d'aplicació (cura de la salut, esport/*fitness*, sensat de promiximat, alertes i temps, etc.) basats en els anteriors.

A la taula de sota es pot veure una comparativa entre els valors de les característiques principal de la tecnologia *Bluetooth Classic* i la nova *Bluetooth Smart*:

Característica	Classic Bluetooth	Bluetooh Smart
Cobertura	1 Km (màxima) 100 m (típica)	250 m (màxima) < 100 m (típica)
Taxa de dades màxima	3 Mbps	1 Mbps
***Throughput*en aplicacions**	700 Kpps – 2.1 Mbps	100-260 Kbps
Esclaus actius màxims (escalabilitat)	7	No definit (depèn de la implementació)
Seguretat	56/128 bit i a nivell d'aplicació	128-AES CCM i a nivell d'aplicació
Latència (*connection set-up speed*)	100 ms (típica)	6 ms
Temps total en enviar dades	100 ms	3 ms
Suport de veu	Sí	No
Topologia de xarxa	*Scatternet*	*Scatternet*
Consum de potència	1 W (referència)	0.01 – 0.5 W
Consum de current (pic)	<30 mA	< 15 mA
Perfils d'aplicació	Sí	Sí
Cost	Baix	Molt baix (xips costen 20-40% menys)

Taula 13. Comparativa Bluetooth clàssic Vs Bluetooth Intel·ligent [63].

A grans trets, es veu que el consum d'un dispositiu *Bluetooth Smart* pot arribar a ser des de la meitat fins a 100 vegades menys que el d'un amb Bluetooth tradicional (0.01W Vs 0.5W).

Lògicament, el consum de corrent també es redueix a la meitat o més. L'incovenient és, llavors, que una reducció de potència implicaun radi de cobertura menor, així com una taxa màxima de transferència menor (3 Mbps Vs 1 Mbps), encara que això no hauria de ser un problema per xarxes de sensors que recullen i envien poca informació.

Per contra, tant la latència (temps que passa des de que el dispositiu s'activa fins que es connecta i envia dades d'ACK -reconeixement) com el temps que es necessita per començar enviar dades, són molt més baixos amb *Bluetooth Smart* (6 ms Vs 100 ms de latència) fet que redueix enormement el *duty cycle* i, per tant, allarga la durada de la bateria. De fet, dispositius com ara balises de proximitat (*proximity beacons*), que són nodes minúsculs -de la mida d'una ungla- que recullen informació de proximitat així com dades de temperatura, poden funcionar fins a dos anys amb una bateria de 1.000 mAh (la meitat de capacitat que una bateria de *smartphone* estàndard, mentre que si la mateixa balisa estigués encesa tota l'estona, la bateria es consumiria en poques hores. Per la seva banda, un dispositiu amb un consum diari de 100 µAh (per exemple, quan si'han de realitzar pocs sensats) significaria una vida de 4 anys amb una pila de botó.

Per últim, veiem que una xarxa BLE és més escalable ja que, a priori, no es té la limitació de 7 nodes esclaus per *piconet* (aquesta limitació vindrà, en tot cas, per part de la implementació específica) podent crear-se xarxes més grans. També és més segura, ja que fa servir encriptació 128-AES CCM (codi d'autenticació de missatges basat en xifrat de bloc encadenat). El cost dels xips també és menor (20-40% menys que un xip Bluetooth Classic; el preu pot arribar a ser d' 1 USD si es compra per volum).

CSRmesh

La companyia CSR ha desenvolupat un protocol propetari anomenat CSRmesh [98] i que, a grans trets, permet que una xarxa de dispositius BLE pugui no únicament enviar i rebre missatges entre mestres i esclaus, sinó també reenviar les dades entre dispositius, actuant per tant com a encaminadors intermedis, formant així una xarxa tipus malla i aconseguint extendre el rang de cobertura d'una xarxa *Bluetooth Smart* per salvar majors distàncies. En definitiva, aquesta tecnologia "copia" d'un manera o altra el mode *mesh* de les xarxes basades en 802.15.4 (Zigbee, 6LoWPAN). L'empresa ven fis i tot una placa de desenvolupament que consta d'un circuit integrat CSR1010, una antena ràdio, conector SPI per a programació i alimentació mitjançant dues bateries AA d'1.5V, tal i com es pot veure a la figura següient. Les aplicacions d'aquesta solució poden anar des d'enllumenat fins a xarxes de sensors, passant per domòtica (*home automation*). Aquesta seria, per tant, la solució més adient per a la creació de grans WSNs de baix consum i baix cost, tot i que *Bluetooth Smart* per sí mateix ja compleix les característiques d'un estàndard orientat a IoT (es pot incorporar a qualsevol electrodomèstic de casa, televisors, auriculars, altaveus, micròfons i fins i tot *wearables*, connectant-se directament a una pasarel·la Internet)

Figura 34. Placa de desenvolupament CSRmesh per a WSNs [98]

Annex XV. Característiques tècniques de ZigBee.

Els xips ZigBee venen usualment integrats amb ràdios i microcontroladors que tenen entre 60-250 KB de memòria *Flash*. La ràdio opera en la banda ISM de 2.4 GHz a la majòria de llocs del món; a més, a Xina opera als 784 MHz, a Europa als 868 MHz i a USA/Austràlia als 915 MHz. Per la seva banda, la taxa de dades varia des dels 20 Kbps –a la banda 868 MHz- fins als 250 Kbps –a la banda 2.4 GHz [56].

Les xarxes ZigBee soporten nativament les topologies d'estrella i arbre (en un arbre, hi ha un node pare sota el qual es creen dos fills, cada fill crea al seu cop dos altres fills, i així recursivament), així com xarxes de malla genèriques. Cada xarxa ha de tenir un dispositiu "coordinador", amb les tasques de la creació de la xarxa, control dels seus paràmetres i manteniment bàsic. Per exemple, en una topologia d'estrella, el coordinador ha de ser el node central o *hub*. Per la seva banda, en les tecnologies d'arbre i malla, es permet l'ús dels encaminadors (routers) per extendre la comunicació a nivell de xarxa.

Com s'ha dit abans, ZigBee es basa en l'estàndard IEEE 802.15.4 per la qual cosa va servir les capes PHY i MAC definides en aquest darrer [32]. La implementació inclou, a més, quatre components clau adicionals, de més alt nivell: capa de xarxa, capa d'aplicació amb objectes dispositiu ZigBee (*ZigBee Device Objects* – ZDO) i objectes d'aplicació definits pel fabricant, que permeten la personalització i afavoreixen una integració total. Per la seva banda, els ZDOs són responsables d'una sèrie de tasques, incloent mantenir la pista dels rols dels dispositius, gestionar peticions per associar-se a la xarxa, així com descobriment de serveis i seguretat.

A banda del ZigBee "clàssic", també existeix ZigBree PRO, també com ZigBee 2007, que és una versió millorada i totalment compatible amb els dispositius ZigBee tradicionals (ZigBee-2006v). Un dispositiu ZigBee PRO pot unir-se i operar en una xarxa ZigBee-2006v, i a la inversa. Tot i així, degut a diferències en les opcions d'encaminament, els dispositius ZigBee PRO han de ser forçosament dispositius no encaminadors (*ZitBee End-Devices* – ZED) en una xarxa 2006.

Altres millores de la versió PRO inclouen:

- Adreçament estocàstic: adreces de xarxa escollides aleatòriament,
- Gestió de dades de malla : els nodes no han de tenir una taula amb totes les rutes des d'un dispositiu fins a la pasarel·la sinó únicament la forma de com s'arriba a aquesta, reduïnt la quantitat de memòria necessària,
- Fragmentació: grans paquets de dades poden ser fàcilment fragmentats,
- Elecció dinàmica del millor canal: els nodes es mouen a altres canals si l'actual té interferències o soroll),

- Condicions asimètriques: els enllaços entre nodes no han de ser simètrics ja que la qualitat de la connexió entre A i B pot ser diferent a la d'entre B a A, per la qual cosa es creen sempre els millors camins, encara que aquestos siguin asimètrics,

- Seguretat (a més d'encriptació AES-128b, s'inclou una nova versió més complexa que deixa que cada parell de nodes tingui la seva pròpia encriptació P2P.

En definitiva, els protocols d'alt nivell ZigBee està dissenyats per a aplicacions encastrades, que requereixin baixes taxes de transmissió i baix consum d'energia. Les xarxes resultants faran ús, per tant, de quantitats globals d'energia molt petites. De fet, cada dispositiu individual ha de tenir una bateria que duri al menys dos anys per tal de poder passar la certificació ZigBee. Les aplicacions més usuals que es poden trobar amb aquesta implementació són:

- Domòtica (*home automation*) amb control intel·ligent d'iluminació i de temperatura, seguretat, control de *Home Theaters*, música, etc.
- Control industrial,
- Sistemes encastrats,
- Col·lecta de dades mèdiques,
- Automatització d'edificis,
- Avís de fum, escapaments d'aigua, intrussions, ...
- WSNs grans (més de 1.000 dispositius), amb sensors com per exemple Telosb, Tmote [99] i Iris.

A la següent figura podem veure l'exemple d' un node Iris amb una antena externa incorporada. Aquesta mota inclou un SoC XM2110CA, basat en un microcontrolador Atmel ATmega1281, amb 8 KB de RAM i 512 KB de memòria *Flash* (en aquesta darrera és on corre el sistema operatiu, MoteWorks). La freqüència de treball és de 2.4-2.48 GHz; la taxa de dades de 250 Kbps; el consum de corrent és de 8 mA (mota activa) o 8 µA (mode *sleep*); la potència típica RF 3 dBm (0,001995 W); el rang de cobertura és de més de 300 m en entorns exteriors i més de 50 m en entorns interiors (en ambdós casos, amb LOS i una antena dipol d'1/4 d'ona).

Figura 35. Sistema de mesurament sense fils IRIS.

Pel que fa al manteniment de l'especificació i, de manera semblant a com ja s'ha vist amb la Wi-Fi Alliance, amb ZigBee tenim la ZigBee Alliance, que és un grup de companyies que mantenen i publiquen l'estàndard. L'aliança també publica perfils d'aplicació que permeten als fabricants crear productes interoperables. Per exemple, l'aliança va crear el Perfil d'Energia Intel·ligent o *Smart Energy Profile* (SEP), primer la versió 1.0 i posteriorment la 2.0, amb la idea de permetre comunicacions M2M avançades i enfocar ZigBee cap a l'IoT (*smart grid*, *smart metering*, *smart homes*, etc.) .

El SEP són especificacions que defineixen un protocol basat en IP per monitorar, controlar, informar i automatitzar l'entrega i ús d'energia i aigua. La darrera versió, la 2.0, és una millora de la seva predecessora i inclou serveis com a càrrega de vehicles elèctrics (PEV), instal·lació/configuració i descàrrega de *firmware*, serveis de prepagament, informació d'usuari i missatgeria, control de càrrega, etc.

Per dotar als dispositius de funcions de mesurament avançades (intel·ligents),cal afegir-hi maquinari més potent però alhora, que segueixi sent barat i de mida petita. En aquest sentit, s'ha d'escollir sistemes en un xip (SoC) que tinguin un bon balanç entre funcionalitat, factor de forma, suport de programari i cost. D'aquesta manera, ens trobem amb MCUs (microcontroladors) de 32 bit, com ara Freescale Kinetis, STM32 [91] o TI Stellaris (amb *core* ARM Cortex-M) que ofereixen un bon grapat de característiques a un preu molt competitiu. Pel que fa al maquinari, SEP 2.0 es basa en una pila TCP/IP amb suport UDP; IPv6 amb serveis de descobriments com mDNS (*multicastDomain Name System*) i DNS-SD (*DNS Service Discovery*); protocol HTTP amb suport per a mètodes `GET`, `PUT`, `POST` i `DELETE`; seguretat mitjançant SSL (*Secure Socket Layer*) y TLS (*Transport Layer Security*), arquitectura RESTful, XML, etc. Totes aquestes tecnologies es troben disponibles amb Linux però com que els µC acostumen a tenir mides de RAM/memòria *Flash* molt petites (típicament de 96 a 128 KB) es fa impossible fer servir aquest SO, al menys en una distribució estàndard, fent necessari l'ús de distribucions amb un *footprint* molt més reduit, com ara Contiki (10 KB), TinyOS (1 KB) o FreeRTOS 10 KB).

Capes PHY/MAC 802.15.4

El disseny de la interfície ràdio en 802.15.4 ha estat curosament optimitzat perqué tingui un molt baix cost de producció quan es fabrica en grans volums; disposa de poques etapes anàlogiques i es fan servir circuits digitals sempre que és possible.

Per la seva banda, encara que les ràdios són barates, el procés de qualificació de la implementació ZigBee comporta una validació completa dels requeriments de la capa física. D'aquesta manera, totes les ràdios derivades del mateix conjunt de màsqueres de semiconductor haurien de tenir les mateixes característiques RF. Això és així perquè, d'altra manera, un dispositiu no certificat que fallés a nivell de capa física podria fins i tot mermar la bateria d'altres dispositius en la mateixa xarxa ZigBee. Per això, les ràdios han de tenir unes restriccions molt grans de potència i amplada de banda. D'aquesta manera, les ràdios ZigBee es proven amb les guies donades per la Claúsula 6 de l'estàndard 802.15.4-2004. Per la seva banda, la majoria de fabricants tenen intenció d'integrar la ràdio i el µC dins d'un únix xip –o ho han fet ja- fent que els dispositius siguin més petits.

Com ja s'ha explicat abans, l'estàndard 802.15.4 opera en la banda de 2.4 GHz a tot el món, 915 MHz a USA i Austràlia i 868 MHz a Europa, en tots els casos bandes ISM (sense necessitat de llicència). En concret, a la banda 2.4 GHz s'assignen 16 canals no superposats, amb 5 MHz de separació entre cadascun d'ells; en canvi, a la banda 915 Mhz s'assignen 10 canals, amb 2 MHz de separació entre ells; per últim, a la banda 868 MHz únicament s'assigna un canal. A la figura de sota es pot veure una representació gràfica dels canals en cada banda [106]:

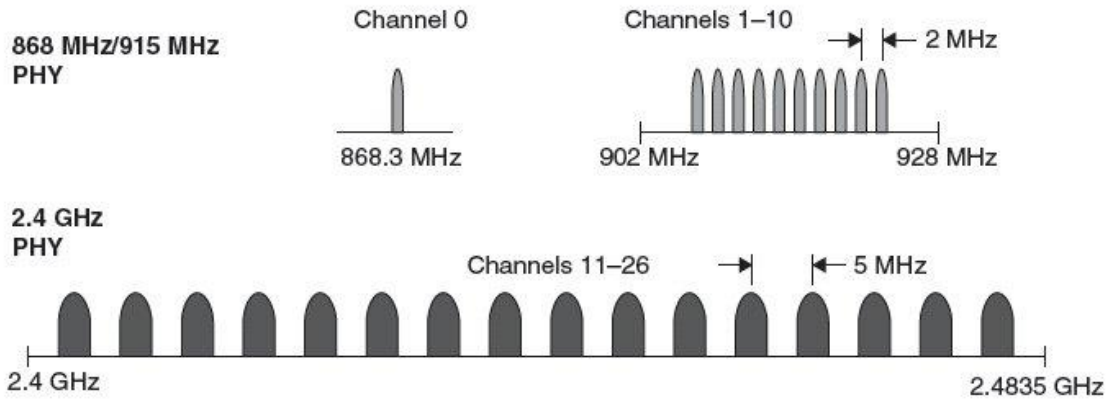


Figura 36. Canals PHY amb IEEE 802.15.4 segons banda de freqüències.

Pel que fa a la codificació que es fa servir,aquesta és DSSS: cada bit d'informació es modula en quatre senyals diferents, causant que el total d'informació a transmetre ocupi una amplada de banda més gran però utilitzant una menor densitat espectral de potència per cada senyal, fet que repercuteix en menys interferències en les bandes utilitzades i millora l'SNR (*Signal to Nose Ratio*).

Per la seva banda, les modulacions que es van servir són BPSK (*Binary Phase-Shift Keying*) en les bandes 868 i 915 MHz i O-QPSK (*Offset Quadrature Phase-Shift Keying*) en la banda de 2.4 GHz, transmetent dos bits per símbol. Això dóna com a resultat una taxa bruta de 250 Kbps per canal (banda 2.4 GHz), 40 Kbps per canal (banda 915 MHz) i 20 Kbps (banda 868 MHz). Per la seva banda, el rendiment o *throughput* real serà menor, degut a la sobrecàrrega (*overhead*) en els paquets així com a retrassos de processament. Pel que fa a la cobertura, en aplicacions *indoor* i en la banda 2.4 GHz, el rang sol ser de 10-20 m, depenent dels materials de construcció, parets i murs, etc.; per aplicacions *outdoor* amb LOS, el rang pot arribar fins els 1.500 m, depenent de la potència de sortida i les característiques ambientals, LOS, etc. La potència de sortida de les ràdios arriba fins als 20 dBm típicament (100 mW), igual que un dispositu Bluetooth de Classe 1 o la potència típica –no màxima- d'un dispositiu Wi-Fi.

Pel que fa a la unitat física de dades de protocol o PPDU (PHY *Protocol Data Unit*) de 802.15.4 –i, per tant, també de Zigbee- aquesta consisteix en: un preamble (4 byte), un delimitador (1 byte), la longitud del PPDU (1 byte) i una longitud variable de dades útils (*payload*). Per la seva banda, les estructures de dades dels protocols superiors s'encapsulen dintre del *payload* PHY. El màxim *payload* que defineix l'estàndard és de 127 byte.

Les xarxes 802.15.4 soporten xarxes amb balises (*beacons*) i sense balises:

- En xarxes sense balises, es fa servir un mecanisme d'accés al medi sense ranures, de tipus CSMA/CA (*Carrier Sense Multiple Access/ Collision Avoidance*) pel qual, a grans trets, els nodes comproven el medi abans de transmestre, és a dir miren que cap altre node no estigui transmetent ja i, si ho està, deixa pasar un temps aleatori abans de tornar a intentar-ho (a nivell tècnic, això significa que cada node escolta el medi i si el nivell d'energia trobat és superior a un nivell específic, llavors el node espera durant un temps aleatori –dintre d'un internaval- i ho intenta de nou). En aquest tipus de xarxes, els encaminadors tenen normalment les ràdios contínuament actives, requerint per tant més requeriments d'alimentació/bateria. En canvi, aquest modi permet xarxes heterogènies en les quals alguns dispositius reben permanentment, mentre que d'altres únicament transmeten quan es detecte un estímul extern.

  Un exemple típic de xarxa d'aquest tipus seria el d'un commutador de llum sense fils: un node situat a un làmpara pot rebre constanment, doncs es troba connectat a fonts d'energia com ara la xarxa elèctrica, mentre que un node situat a un llum alimentat per bateria hauria d'estar aformit fins que es pitja el conmutador. Llavors el commutador es desperta, envia un comand a la làmara, rep un ACK i torna a dormir. En aquest tipus de xarxes, el node a la làmpara hauria de ser, com a mínim, un encaminador i molt probablement també el coordinador, mentre que el node al commutador seria el ZED.

- Per la seva banda, en xarxes amb balises, els ZR envien balises periòdiques per confirmar la seva presència a altres nodes. Normalment, els nodes es troben adormits entre balises, abaixant per tant el cicle de treball i extenent la vida de les bateries. Les balises s'envien a intervals fixes predefinits (aquest internval entre dues balises es denomina *Beacon Interval* – BI) i no es fa servir CSMA. Per la seva banda, els ACK tampoc fan servir CSMA.

  Els intervals entre balises (BI) depenen de la taxa de dades i poden anar de 15.36 ms a 251.658 per a 250 Kbps, de 24 ms a 393.216 per a 40 Kbps o de 48 a 786.432 per a 20 Kbps. El problema és, llavors, que aquest cicle de treball baix amb llarg períodes entre balises necessita d'una temporització precisa (és a dir, que tos els dispositius tinguin exactament la mateixa hora, que es trobin sincronitzats) i això pot entrar en conflicte amb la necessitat de productes de baix cost. Aquesta problemàtica queda resolta amb l'estàndard 802.15.e-2012, tal i com podrem veure en el proper capítol.

Per altra banda, les xarxes amb requeriments de baixa latència i temps real poden fer servir la tècnica de "ranures de temps garantitzades" (*Guaranteed Time Slots* – GTS) que, per definició, tampoc fan servir CSMA. El funcionament de GTS és bàsicament el següent: un BI consta d'un període "actiu" i un període "inactiu" (aquest darrer és opcional). Al període actiu se li anomena *superframe* i es divideix en 16 ranures o *slots* idèntiques en temps, durant les quals les transmissions de trames estan permeses. Durant el període inactiu –si aquest existeix- tots els nodes es fiquen en mode *sleep* per estalviar energia. Llavors, el que es fa és que un node centralitzat –el coordinador- s'encarrega d'assignar ranures de temps –de les 16 comentades abans- a cada node, per tal que aquests darrers sàpiguin quan han de transmetre. En primer lloc, el node que vol transmetre ha d'enviar un missatge de tipus "petició GTS" al coordinador de la xarxa; com a resposta, el coordinador envia una balisa contenint la ranura assignada i el nombre de ranures que es poden fer servir [21].

Una altra tècnica que fa servir 802.15.4 és el *Channel Energy Scan* (petició PLME-ED). La idea principal que hi ha al darrera és saber quanta energia (activitat/soroll/interferències) hi ha en un o varis canals, abans de fer-los servir. D'aquesa manera es pot estalviar energia, escollint els canals que estiguin lliures quan es configura la xarxa. Hi ha tres comportaments diferents quan es tracta d'encarar un problema de detecció d'energia:

- Energia (*Transmit Power*): escaneja els canals i informa sobre l'energia trobada, sense importar si és causada per altres nodes ZigBee o qualsevol altra tecnologia o soroll; únicament reporta si l'espectre està sent utilitzat. Únicament es transmetrà quan el valor rebut estigui per sota d'un determinat llindar. Aquesta funcionalitat permet rebutjar certs canals, és a dir, posar-los a una "llista negra" (*blacklisting*).

- *Clear Channel Assesment* (CCA): s'escaneja el medi i s'informa si hi ha transmissions 802.15.4; per tant, el que es fa és sensar si hi ha alguna altra portadora del mateix estàndard al medi. Únicament es transmet quan el canal està lliure.

- CCA + Energia: escaneja el medi i informa si hi ha altres transmissions 802.15.4 per sobre del llindar d'energia especifica. Si no reporta, s'utilitzarà el canal.

En definitiva, podem dir que 802.15.4 minimitza el temps en que la ràdio es troba activa i, per tant, per tal de minimitzar el consum d'energia. En xarxes amb balises, els nodes únicament han de estar actius mentre la balisa s'està transmetent; en canvi, en xarxes sense balises, el consum és asimètric: alguns dispositius hauran d'estar sempre actius mentre que altres estaran la major part del temps dormint.

Topologia de xarxa ZigBee

Pel que fa la implementació ZigBee, podem trobar tres tipus de dispositius:

- Coordinador ZigBee (ZC): el dispositiu més versatil. El coordinador esdevé l'arrel de l'arbre de xarxa i pot "pontejar-se" amb altres xarxes. Hi ha únicament un coordinador per xarxa ZigBee donat que es tracta del dispositiu que comença originàriament la xarxa (hi ha una especificació però, anomenada *ZigBee LightLink*, que permet operar sense un coordinador però que està enfocada a productes de consum a nivell hogar). El coordinador emmagatzema informació sobre la xarxa, actuan com a Centre de Confiança i repositori de les claus de seguretat.

- Encaminador ZigBee (ZR): a més d'executar-se com a funció aplicació, un *router* actua com encaminador intermig, passant dades a altres dispositius.

- Dispositiu final Zigbee (ZED): conté únicament la funcionalitat de poder parlar amb un node pare (encaminador o coordinador) però no pot retransmetre dades d'altres dispositius. Aquesta relació permet al node poder "dormir" una quantitat de temps considerable, allargant per tant la vida de la bateria. Aquest tipus de node és el que requereix menys quantitat de memòria i, per tant, és menys costós de fabricar que un ZC o ZR.

Amb aquests tipus de dispositius, es poden crear xarxes amb topologia d'estrella, arbre o malla, tal i com es pot veure a la figura de sota, on els nodes verds representen els dispositius coordinadors, els nodes blaus representen els encaminadors i els nodes vermells representen els dispositius finals:

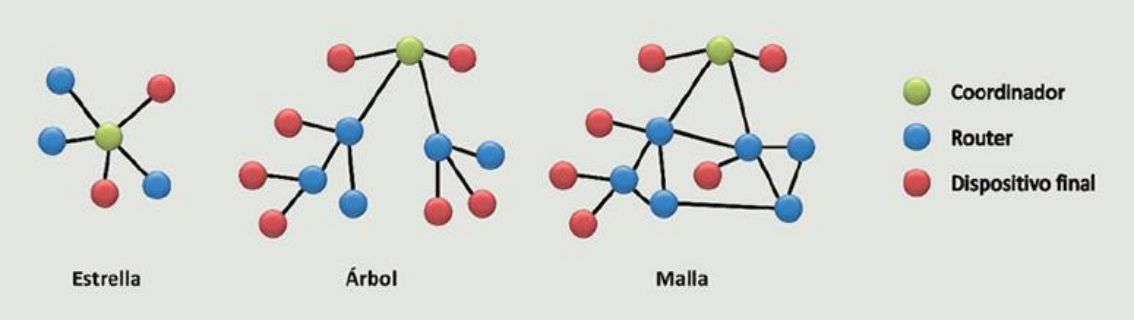


Figura 37. Tipus de topologies de xarxa amb ZigBee.

Per últim, pel que fa als mecanismes d'encaminament en una xarxa ZigBee, principalment en tenim dos (aquests procolos són genèrics de qualsevol xarxa WPAN): encaminament de tipus arbre i encaminament tipus malla. Dintre del primer grup tenim com a protocol més conegut el TR (*Tree Routing*), mentre que en la segona categoria tenim l'AODV (*Ad hoc On-Demand Distance Vector*).

- *Tree Routing*: és un mecanisme d'encaminament basat en jerarquies pel qual, a grans trets, les trames s'encaminen d'origen a destinació bé "cap amunt" –de nodes fills a nodes pares- o bé "cap avall" –de nodes pares a fills-,en funció de l'adreça de xarxa del dispositiu de destinació: si l'adreça de destinació es troba dintre de l'espai d'adreces del dispositiu, la trama s'encamina cap avall; en cas contrari, la trama s'encamina cap amunt. L'espai d'adreces de cada dispositiu es calcula inicialment mitjançant un senzill algorisme anomenat Cskip [102].

- AODV: aquest protocol és més complexe que l'anterior i es basa en la creació de taules d'encaminament entre nodes. A grans trets, tenim una xarxa que està en silencia fins que un node vol enviar una trama a una destinació. En aquest punt, el node difon una petició als seus nodes veïns, els quals, al seu voltant, reenvien el missatge i registren el node d'on han escoltat la petició, creant així una "explosió" de rutes temporals cap al node origen. Quan un node que ja té una ruta cap a la destinació rep un missatge, envia un missatge cap endarrere a trvés d'una ruta temporal cap al node origen. Llavors, el node origen comenza a fer servir la ruta fins a la destinació que tingui el menor número de salts intermitjos. Les entrades de les taules d'encaminament que no s'utilitzen es van reclicant periòdicament. Per la seva banda, quan un enllaç falla (per exemple perquè hi ha un node intermig caigut), un error d'encaminament s'envia al node origen i llavors es repeteix el procés.

L'encaminament a través d'un arbre és més senzill que mecanismes complexes com ADOV i té com a benefici que no es requereixen taules d'encaminament, per la qual cosa es pot fer servir en dispositius amb grans limitacions de recursos (potència de procés i sobretot memòria). En canvi, presenta un problema molt gran de disseny que, a la pràctica, el fa gairebé inservible en xarxes reals: aquest problema és que les adreces de dispositius són estàtitiques; és a dir, la posició en la jerarquia de l'arbre de un dispositiu queda fixada un cop aquest dispositiu es connecta a la xarxa, per la qual cosa és inflexible a qualsevol canvi en l'estructura de xarxa. D'aquesta manera, si un dispositiu falla o es cau, llavors es portarà per endavant –metafòricament- tots els dispositius per sota de la seva jerarquia, en el sentit de que no serà possible accedir a cap dispositiu que hi hagi per sota, essent la única manera de solucionar-ho que tots els dispositius tornessin a unir-se a la xarxa amb un parent que estigui viu. Un altre problema de disseny és que hi ha un punt únic de fallada, que és el coordinador: (vèrtex de l'arbre) si aquest cau, l'encaminament no funciona.

Per la seva banda, amb mecanismes d'encaminament de malla, si el coordinador cau, no passa res, perquè des del punt de vista de la malla, el coordinador és únicament un altre encaminador més en les taules d'encaminament. Per això s'acostuma a dir que aquest tipus d'encaminaments permeten l'auto-recuperació (*self-healing*, en anglès) de less xarxes en malla perquè, si un node cau, llavors simplement no participarà del procés de descobriment de rutes i, per tant, es descobrirà una altra ruta automàticament.

Per últim, podem dir que hi ha programari –tant per Windows com Linux- que permet simular xarxes 802.15.4 i ZigBee, com ara NS2 [103], OPNET [104] i Netsim [105]. Per exemple, a la figura següent es pot veure una captura de pantalla d'una petita ZigBee de laboratori simulada anb OPNET:

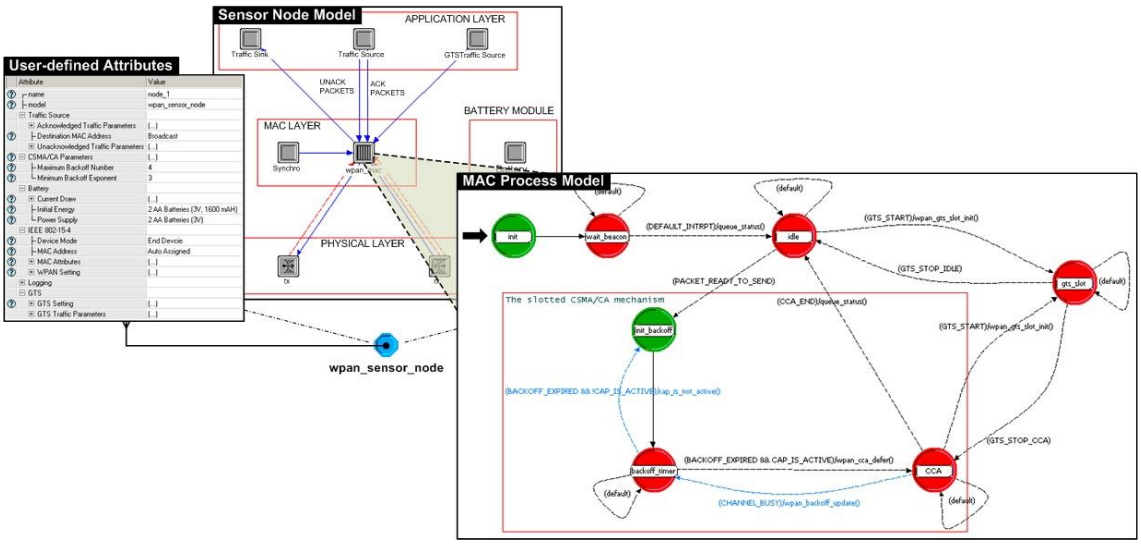


Figura 38. Simulació de xarxa ZigBee amb programari OPNET.

Annex XVI. Característiques tècniques de WirelessHART.

L'any 2010, WirelessHART fou aprovat per la Comissió Internacional d'Electrotècnica (IEC – *International Electrothecnical Commission*) de manera unànime, convertint-se en el seu primer estàndard internacional sense fils, amb la denominació IEC 6259.

Amb WirelessHART es fa servir, a nivell d'enllaç de dades, TDMA (*Time Division Multiple Access*) per arbitrar i coordinar la comunicació entre dispositius. Aquest nova capa d'enllaç estableix els enllaços especificant el *timeslot* (ranura temporal) i la freqüència que s'han de fer servir entre els dispositius. Els enllaços s'organitzen en supertrames que es repeteixen periòdicament per permetre comunicació tant cíclica com acíclica. Un enllaç pot ser dedicat o compartir, per pemtre una utilització "elàstica" de l'ample de banda de comunicació per assegurar el processament de dades amb la mínima latència.

Els dispositius clau d'una xarxa WirelessHART són els següents [22]:

- *Gateway* (pasarel·la): proporciona la connexió a la xarxa remota (*host network*). La interfície entre WirelessHART i el *host* principal és Modbus – Profibus – Ethernet. La pasarel·la proporciona a la xarxa, a més, el gestor de xarxa i el gestor de seguretat.

- *Network Manager* (gestor de xarxa): construeix i manté la xarxa de malla. Identifica els millors camins i gestiona la distribució dels accesos a les ranures temporals (cada segon es divideix en ranures de 10 ms).

- *Security Manager* (gestor de seguretat): distribueix les claus d'encriptació. També manté una llista dels dispositius autoritzats a unir-se a la xarxa.

- *Repeater* (repetidor): encamina els missatges. El seu ús principal és el d'extendre el rang d'una xarxa WirelessHART. Tots els instruments de mesura d'una xarxa WirelessHART tenen capacitats d'encaminament.

- *Adapter* (adaptador): s'endolla a un instrument HART i passa les dades des de l'instrument a la xarxa i cap al *host*. L'adaptador es pot localitzar en qualsevol lloc al llarg del cable 4-20 mA i pot tenir la seva font d'alimentació o alimentar-se a través del cable. Alguns adaptadors fan servir bateria i aquesta mateixa serveix també per a l'instrument de mesura.

- Terminal: s'utilitza per unir un nou instrument a una xarxa WirelessHART existent. El terminal té una connexió a la pasarel·la i després cap a un instrument que pot utilitzar-se per fer diagnòstics.

Pel que fa a la seguretat, és obligatòria a WirelessHART. La tecnologia proporciona mesures de seguretat tant extrem a extrem com salt a salt; en concret, encriptació i autenticació de missatges en les capes d'enllaç de dades i de xarxa (AES-128). Hi ha un conjunt de claus de seguretat que permeten una connexió segura: als nous dispositius, abans d'unir-se a la xarxa, se'ls hi proporciona una clau d'unió; la generació de la clau real i la seva gestió s'implementen per part del *Security Manager*. També es proporcionen claus de sessió i de xarxa per part del *Network Manager,* per a properes comunicacions. La clau de ssesió és utilitzada per la capa de xarxa per autenticar una comunicació extrem a extrem entre dos dispositius (la mateixa clau per cada parell). Per la seva banda la clau de xarxa s'utilitza per autenticar els missatges en un salt.

A mode de resum, podem dir que WirelessHART és una tecnologia WPAN multifabricant, basada en 802.15.4 a nivell de capa física i d'accés al medi, i que neix molt robusta (es basa en xarxes de malla, multisalt i amb tècniques de salt de canal) i que a més, especifica un nou enllaç de dades i aporta diferents mecanismes de seguretat (claus i encriptació forta), punts que fallen a les xarxes ZigBee originals -però que queden adreçats a ZigBee PRO. Per altra banda, la implementació d'una xarxa WiressHART sembla força més complicada que la de ZigBee.Per tant, creiem que ZigBee és una implementació més enfocada a xarxes de baix cost, baix consum i nodes petits (LR-WPAN) i de fàcil instal·lació, mentre que WirelessHART, per la seva pròpia història (compatibilitat amb dispositius i tecnologia HART) i per definició, està potser més orientada a xarxes d'instrumentació i sistemes de control (per exemple, sistemes de mesura en un entorn industrial o en laboratoris) on els factors claus són la seguretat i la fiabilitat.

Annex XVII. Característiques tècniques d'ISA-100.11a.

A nivell PHY i MAC, ISA-100 es basa en 802.15.4; en canvi, s'especifica un nou enllaç de dades, així com capes de xarxa, transport i aplicació. Per tant, també suporta -al igual que altres tecnologies similars- *Channel Hopping*, per evitar interferències amb altres dispositius RF operant en la misma banda, al mateix temps que proporciona robustesa per mitigar interferències multicamí. A més, ISA-100 facilita la coexistència amb altres sistemes RF i detecta canals ocupats i/o amb baix rendiment (baixa relació senyal-soroll).

De la mateixa manera, també fa servir una combinació de DSSS/FHSS i modulació O-QPSK. La taxa màxima de dades és també de 250 Kbps, la potència màxima de sortida de 10 mW i la cobertura màxima d'uns 100 m.

Per la seva banda, a nivell de capa d'enllaç, ISA-100 fa servir TDMA -igual que WirelessHart- que permet al dispositiu accedir al medi RF sense haver d'esperar a altres dispositius. ISA-100 també pot fer servir CSMA.

Com ja hem dit, la diferència entre aquest estàndard i altres basats en 802.15.4 es troba a partir de l'enllaç de dades i capa de xarxa. Per exemple, amb ISA.100 s'utilitzen formats de capçalera compatibles amb l'estàndard 6LoWPAN de l'IETF (que veurem en detall en el proper capítol) per tal de facilitar l'ús potencial d'aquest darrer com a *backbone* –troncal- de xarxa [23]. Tot i així, encara que les capçaleres siguin compatibles amb 6LoWPAN, no necessiten estar basades en IP; encara més, l'ús d'aquests formats de capçalera no implica que una xarxa ISA-100 estigui connectada a Internet sinó que, normalment, és més aviat al contrari (les xarxes ISA.100 no s'acostumen a trobar connectades a Internet i, per tant, no exposades a atacs externs).
Amb ISA100 també tenim diferents tipus de rols, com ja passaba amb WirelesHART:

- Entrada/Sortida (*Input/Output* – I/O): dispositiu que proporciona dades (sensor) o utilitza dades (actuador) d'altres dispositius,

- Encaminador (*Router*): dispositiu capaç d'encaminar dades des d'altres dispositius de la xarxa,

- Provisionador (*Provisioning*): dispositiu capaç de provisionar altres dispositius (habilitar-los per que s'uneixin a una xarxa determinada),

- Encaminador troncal (*Backbone Router*): dispositiu capaç d'encaminar dades des de/fins a una xarxa troncal.

- Pasarel·la (*Gateway*): dispositiu que proporciona una interfície entre la xarxa de la planta i una altra xarxa remota (per exemple, Internet) o entre la xarxa i una aplicació final en la pròpia planta,

- Gestor del Sistema (*System Manager*): una aplicació que governa la xarxa, els dispositius de xarxa i les seves comunicacions,

- Gestor de Seguretat (*Security Manager*): aplicació que, en conjunció amb el gestor del sistema, proporciona una operació segura del sistema. En aquest sentit, tant WirelessHART com ISA.100 basen els seus mecanismes de seguretat en aquest rol, per la qual cosa, si aquest rol cau, es perden els mecanismes de seguretat a la xarxa.

- Font de Temps de Sistema (*System Time Source*): dispositiu responsable per mantenir la font mestra de temps per al sistema.

Per la seva banda, la seguretat és una de les majors facetes en el disseny de l'estàndard ISA-100, ja que consideratot el cicle de vida de la xarxa al complet, incloent la seva configuració, operació i manteniment. La seguretat es considera en tot el sistema, no únicament a nivell de capa PHY i subcapa MAC. ISA-100 proporciona seguretat escalable per fer front a la major part d'amenaces industrial, fent ús de la seguretat proporcionada per 802.15.4-2006.

Els serveis de seguretat d'ISA-100 es seleccionen per política. Aquesta política es distribueix amb cada material criptogràfic creat, permetent aplicacions enfocades a polítiques. Donat que una única clau s'utilitza cada cop a nivell d'enllaç de dades –excepte per un breu període de traspàs de claus- la subxarxa al complet està subjecta a les mateixes polítiques a nivell d'enllaç de dades. Al igual que amb WirelessHART, el *Security Manage*r controla les polítiques de tots els materials criptogràfics que es generen.

Amb ISA-100, les claus de seguretat poden ser simètriques o asimètriques (si ho comparem amb WirelessHART, en aquest darrer únicament podien ser simètriques). Per la seva banda, les claus de sessió tenen un temps de vida limitat i s'actualitzen periòdicament, iniciant-se per part d'un dispositiu, per tal d'assegurar que la sessió es manté vida (s'envien *keep-alives*). El procés d'actualització de claus també pot ser iniciat per un dispositiu, encara que hauria de fer-se per part del Security Manager, entre el temps de vida *soft* i *hard* d'una clau de sessió.
A mode de resum, es pot dir que hi ha tant semblances comdiferències entre ISA-100 i WirelessHart i ZigBee:

- Tots ells persegueixen, en certa manera, objectius comuns, amb més o menys fortuna: baix cost, baix consum, interoperabilitat amb altres sistemes, escalabilitat, estalvi d'energia, compatibilitat amb dispositius industrials, fiabilitat en les comunicacions i seguretat.

- Tots tres es basen en 802.15.4 i, per tant, fan servir el mateix rang freqüencial de 2.4 GHz (és a dir, mateixa capa PHY).

- Per la seva banda, ISA-100, al igual que WirelessHart, suporta topologies tant d'estrella com de malla o una combinació d'ambdues, mentre que ZigBee suporta estrella, malla i arbre.

- Tots tres estàndards tenen la mateixa capa MAC, encara que WirelessHart i ISA-100 defineixen un nou enllaç de dades (els dos darrers fan servir TDMA i salt de canal/freqüència, en comptes de CSMA-CD i un únic canal estàtic, com utilitza el ZigBee tradicional).

- Per la seva banda, pel que fa la seguretat, WirelessHART i ISA-100 tenen resistència a la manipulació (*tampering*) de dades, degut a la criticitat dels entorns en els que treballen. Tant WirelessHART com ISA.100 fan servir claus (simètriques en el primer cas i simètriques o asimètriques en el segon).

- WirelessHART es va pensar més aviat com una evolució sense fils de l'antic HART, mentre que la idea d'ISA100.11 va més enllà i és proporcionar un entorn –marc de treball- que permeti l'adreçament i transport de dades, sense fils i entre diferents protocols, fins i tot cablejats (HART, Profibus, etc.), fent servir 6LoWPAN.

- En el mercat industrial, WirelessHART i, sobretot, ISA-100, són opcions molt més adients que ZigBee ja que, com hem vist, ISA.100 pot comunicar-se simultàniament amb la majoria de protocols cablejats, integrant-los, fet que ZigBee no suporta. A més, tant WirelessHART com ISA-100 incorporen mecanismes per permetre la coexistència amb altres usuaris de l'espectre 2.4 GHz, encara que siguin d'altres xarxes/estàndards. Per tant, ZigBee queda més relegat a àmbits d'aplicació comercials (amb implementacions més senzilles), no industrials (implementacions més complicades).

- WirelessHART incopora moltes característiques de seguretat que són obligatòries mentre que en ISA.100, moltes d'aquestes són opcionals, fet que aporta més flexibilitat a la xarxa.

- WirelessHART i ISA.100 són competidors directes en la lluita per convertir-se en l'estándard "de facto" per comunicació sensde fils d'instrumentació en factories industrials i processos d'automatització. Tot i així, alguns experiments en entorns de laboratori mostren que la taxa de pèrdua de paquets en WirelessHART és una mica superior quan es comparteix tràfic amb altres xarxes IEEE 802.11.

Annex XVIII. Característiques tècniques de wM-Bus.

Depenent de l'aplicació, existeixen diverses combinacions de modes de comunicació i dispositius de mesura. Aquests modes de comunicació són [110]:

- S1: en aquest mode (*Stationary*), el dispositiu de mesura –també anomenat "transceptor"- envia les seves dades diversos cops al dia. En aquest mode, el col·lector de dades pot estalviar energia donat que els dispositius de mesura envien un senyal de *wake-up* abans de començar a transmetre les seves dades.

- S1-m: com S1 però el col·lector de dades pot ser mòbil.

- S2: com S1 però amb comunicació bidireccional (el col·lector de dades pot demanar dades als dispositius de mesura).

- T1: en aquest mode (*Frequent Transmit*), els dispositius de mesura envien dades als col·lectors a intervals, configurables en termes de segons o minuts.

- T2: com T1 però bidireccional (el col·lector de dades pot demanar dades als dispositius de mesura).

- C1: aquest mode (*Compact*) és similar al T però més avançat, ja que permet la transmissió de més dades dintre amb la mateixa energia i mateix cicle de treball. És adequat per a lectures de tipus *walk-by*i/o*drive-by*. És possible la recepció de trames T i C amb un mateix receptor.

- C2: com C1 però bidireccional (el col·lector de dades pot demanar dades als dispositius de mesura).

- R2: aquest mode (*Frequent Receiver*), és similar a T2 –per tant, bidireccional- però des del punt de vista del col·lector de dades. El col·lector escola cada pocs segons la recepció d'un missatge de wake-up per part de l'equip de mesura.

- N1: aquest mode (*Narrowband VHF*) està optimitzant per a banda estreta.

- N2: com N1 però bidireccional.

- F1: aquest mode (*Frequent TX & RX*) és per als missatges de *wake-up* des d'un dispositiu de mesura, ja sigui fixe o mòbil.

- F2: igual que F1 però bidireccional.

Alguns dels modes pertanyen a l'especificació primera de l'estàndard de l'any 2005 (S, T, R), mentre que altres es van incorporar a la nova versión del 2011 (N, C, F).

La següent taula mostra un resum dels diferents modes, així com la banda que fan servir, la codificació que s'empra en cadascun d'ells i el cicle de treball (*duty cycle*) associat [108]:

Mode	Banda	Codificació	Cicle de Treball
S	868 MHz	Manchester	1%
T	868 MHz	Manchester i "3 de 6"	0,1%
R	868 MHz	Manchester	1%
C	868 MHz	NRZ	0,1%
N	169 MHz	NRZ	Sense dades
F	433 MHz	NRZ	Sense dades

Taula 14. Modes d'operació d'ISA-100.11a.

Recordem que la codificació Manchester (anomenada també bifase-L), és aquell mètode de codificació elèctrica d'un senyal binari en la que, en cada temps de bit, hi ha una transició entre dos nivels de senyal. Per la seva banda, la codificació NRZ (Non-Return-to Zero) és aquella en la que la tensió no torna a zero quan hi ha dos bits consecutius a '1'.

Un dispositiu wM-Bus acostuma a tenir una potència de transmissió de 10 mW (+10 dBm), encara que els que traballen a la banda de 169 MHz poden arribar fins a 1W (+30 dBm), amb la intenció d'aconseguir una cobertura més gran, com ja s'ha dit abans. Per la seva banda, si es fa servir un dispositiu que admeti el mode C -com el que es mostra a l'Annex XLVI [109]- que, recordem, pot enviar més dades amb la mateixa energia i *duty cycle* (0.1%), si es configura un interval entre transmissions de 16 segons llavors es pot aconseguir que la bateria del dispositiu duri fins a 13 anys. Per tant, això indica que aquest estàndard és ideal per a dispositius que s'han de deixar desatesos.

Per la seva banda, el rang de cobertura del transceptor depèn, com ja hem vist abans, de la potència de transmissió i pot arribar a 200 metres amb l'antena interna i fins a un kilòmetre amb una antena externa.Pel que fa a les taxes de dades, són molt modestes: habitualment és d'uns 32.6-38.4 Kbps -si es fa servir el mode S- i d'uns 100 Kbps –si es fan servir els modes T i C.

Per últim, pel que fa a les modulacions, es poden fer servir tant MSK (*Minimum Shift-Keying*) com ASK (*Amplitude Shift Keying*), OOK (*On-Off Keying*), GMSK (*Gaussing Minimum Shift Keying*), 2-GFSK i 4-GFSK, en funció de la taxa de dades que volguem aconseguir.

El gran punt feble d'aquesta especificació és, sens dubte, la seva manca de seguretat. Encara que wM-Busfa servir AES-128, alguns estudis [111] afirmen que l'estàndard és basicament insegur per les següents raons:

- Un ús inapropiat de les claus de seguretat i del vector d'inicialització (*Initialization Vector – IV*) permeten que es pugui saber els lectors on el consum és zero. Fent servir les mateixes tècniques, es poden saber els consums actuals de cada dispositiu, ja que la informació viatja en text clar (sense xifrar).

- Maca de protecció d'integritat, que permet manipular els valors dels consum que es troben en trànsit a la xarxa. També permet la manipulació de comandes obrir/tancar sobre vàlvules i interruptors.

- Manca d'autenticació amb actualitzacions de rellotge, que pot portar a una repetició de la clau de fluxe.

- Manca d'autenticació per a la gestió de la xarxa, quet permet a un atacant convertir-se en un reenviador (*relay*) de dades fraudulent.

- Les notificacions d'alama i error viatgen en text clar, la qual cosa permet a atacants saber si un conmutador manipulat ha estat activtat.

- La informació del fabricant del dispositiu, tipus d'aparell de mesura i ID de versió també viatja en text pla, fet que simplifica la identificació d'objectius vulnerables.

- El mecanisme d'actualització de clau és massa bàsic i pot portar a conèixer la clau.

- Tot i que la mida màxima de clau és de 128 bit, l'estàndard recomana fer servir la meitat per a cada dispositiu, el que redueix la mida a 64 bit únicament.

En resum, es pot afirmar que wM-Bus és un estàndard apte per a entorns on la seguretat no és primordial, normalment a nivell domèstic, per controlar el consum dels subministraments d'energia (aigua, llum, gas) dels consumidors. Les dades es poden enviar a un centre col·lector de dades que podria estar en les zones comuns dels edificis (per exemple en l'armari de comptadors) i d'aquí i, fent servir una pasarel·la, enviar les dades a Internet i la companyia subministradora. També es pot fer servir la banda de 169 MHz per aconseguir cobrir distàncies de 500 m i fins i tot 1 Km però no creiem que aquest estàndard sigui convenient per a entorns industrials, a menys que la manca de seguretat no sigui un problema. On sí es podria fer servir és en granjes, conreus, embalsos, etc, seguint la mateixa filosofiaque en el cas domèstic (lectura de registres). Òbviament, donat el seu enfoc, no es tracta d'un estàndard que es pugui considerar competència d'altres tecnologies sense fils més flexibles i amb més àmbits d'aplicació, com ara Low-Power WiFi, BLE o ZigBee.

Annex XIX. Característiques tècniques de DASH7.

Pel que fa al rang de cobertura de DASH7, tal i com passa amb altres protocols, aquest dependrà de molts factors, com ara la potència de sortida, la taxa de dades, el soroll, etc. Amb taxes de dades baixes (per exemple, 10 Kbps) es tindrà un canal més immune al soroll i, per tant, augmentarà l'SNR i la sensitivitat del receptor, millorant la cobertura; per contra, amb taxes altes (200Kbps), disminueix l'SNR i la cobertura empitjora. Per altra banda, pel que fa a l'absorció de potència, aquesta depèn en granmesura del cicle de treball (és a dir, de la quantitat de temps que està encesa la ràdio del MCU), com ja s'ha vist que passa amb els altres estàndars.

Pel que fa a la freqüència, el fet d'utilitzar la banda de 433 MHz (concretament, 433.92 MHz), una freqüència baixa en relació als 2.4 GHz o 5 GHz d'altres tecnologies, fa que el senyal pugui penetrar millor els murs de formigó dels edificis, així com parets internes de totxo i també penetra millor en l'aigua (incloent entorns amb pluja). Per la seva banda, els requeriments de potència son també menors, fent que els dispositius amb aquesta tecnologia puguin ser alimentats per petites piles de botó o bateries de pel·lícula molt primes, durant fins a 10 anys o més. A més, com que 433.92 MHz és múltiple de 13.56 MHz (32 vegades més), això significa que es poden fer servir les mateixes antenes que s'empren en altres estàndars com ara NFC, FeliCA, MiFare, etc.

Pel que va a la capa PHY de DASH7, tenim que:

- Fa servir d'un a cinc canals, amb una amplada de banda de 0.5 a 1.75 MHz cadascun.
- Com a modulació, es fa servir FSK o GFSK.
- El *throughput* (rendiment) típic és d'uns 27.8 Kbps.
- El consum de potència és d'uns 42 μW, per a una aplicació que enviï 10 missatges al dia de 256 byte cadascun. Això represeenta unes 10 vegades menys conum que ZigBee (414 μW), 13 vegades menys que Low-Power WiFi (570 μW) o un 15% menys que BLE (50 μW).

Un altre aspecte diferenciador de DASH7 respecte a altres tecnologies basades en RFID és que es permet comunicació d'etiqueta a etiqueta (*tag-to-tag*) fet que, combinat amb el grau de coebrtura i la freqüència de treball, fan que sigui una alternativa molt atractiva a tres tecnologies de xarxa de malla. A més, DASH7 soporta sensors, encriptació i IPv6.

DASH7 fa servir el concepte de "sessió" per transmetre dades: una transmissió és esporàdica, no contínua, per la qual cosa es fa servir en aplicacions on el baix consum és essencial, com ara telemetria. DASH7 fa servir la tecnologia BLAST (*Bursty*, *Light*, *Asynchronous*, *Stealth*, *Transitive*):

- *Bursty* (a ràfagues): les dades es transfereixen de manera abrupta i no inclouen contingut de vídeo, aúdio o altres formes de dades isocrones.

- *Light* (lleuger): per la major part d'aplicacions, els paquets de dades es limites a 256 byte (i, encara que es permet la transferència de múltiples paquets consecutius, s'intenta evitar en la mesura del possible)

- *Asynchronous* (asíncron): el principal mètode de comunicació es mitjançant ordre-resposta que, per disseny, no requereix de *hand-shaking* periòdic de sincronització entre dispositius.

- *Stealth* (sigilós): no es necessiten balises periòdiques per poder respondre a una comunicació

- *Transitive* (transitiu): un sistema DASH7 és, de manera inherent, mòbil o transicional. A diferència d'altres tecnologies, està centralitzat en la pujada de dades (*upload-centric*), no en la baixa (*download-centric*) per la qual cosa els dispositius no necessiten ser gestionats per una infraestructura fixa (estacions base).

DASH7 incopora un mode de treball (*Mode* 2) que incorpora integrat un protocol de consultes únic, que minimitza la quantitat de voltes (*round-trips*) que ha de donar un missatge en aplicacions de missatgeria, resultant en una menor latència i major rendiment de xarxa.

Pel que fa a les seves aplicacions comercials, tal i com s'ha dit abans, DASH7 va començar estant enfocat a l'àmbit militar -sector defensa- igual que altres tecnologies (per exemple, DARPA -*Defense Advanced Research Projects Agency* - va fundar Internet). Avui dia, entre els àmbits més importants podem trobar:

- Control d'accessos, *Smart Energy* i automatització d'edificis: les característiques de propagació permeten penetrar murs, finiestres, portes i qualsevol altre objecte que en la banda de 2.4 GHz representa un problema. Pel que fa a *Smart Energy* i automatitzaciód'edificis, es poden implementar xarxes amb molta menys infraestructura que altres tecnologies i, per tant, amb menor cost total de propietat (TCO – *Total Cost of Ownership*).

- Serveis basats en localització: es pot fer servir amb targetes intel·ligents (smartcards), clauers, tíquets, rellotges i, en definitiva, qualsevol altre producte convencional que pugui prendre avantatge de la petita emprempta de DASH7, així com del seu baix consum, llarga cobertura i baix cost, en comparació amb altres tecnologies menys convenients com Wi-Fi o Bluetooth. Per exemple, es pot fer servir DASH7 per indicar un registre (*check-in*) a un lloc determinat, en comptes de fer servir altres tecnologies com GPS, que gasten més energia i que no funcionen tant bé en entorns urbans. Aquest tipus d'aplicació ja el fan servir portals com Foursquare o Twitter.

- Publicitat mòbil: DASH7 es pot fer servir en cartells, posters, etc que poden ser accessibles des de molts metres (i fins i tot kilòmetres) de distància, creant noves oportunitats pel que fa al seguiment de l'efectivitat d'una publicitat però també creant noves oportunitats de negoci (*e-commerce*). El fet de que es puguin realitzar registres i sortides de localitzacions (*check-ins* i *check-outs*) fa possible proporcionar publicitat basada en la localització.

- Automoció: DASH7 es veu com la nova generació de sistemes per monitorar la pressió dels pneumàtics, donat que fa servir la mateixa freqüència que la majoia de sistemes TPMS (*Tire Pressure Monitoring System*) propietaris actuals. Es poden proporcionar lectures més acurades de la pressió, resultant en menys gast de combustible, reducció de rebentada de rodes i major seguretat.

- Logística: DASH7 ja s'està fent servir per rastrejar la localització de contenidors, palets, camions, vagons de tren, vaixells i, en general, qualsevol altre bens de la cadena de suministre, proveint a les empreses de molta més visibilitat de les seves operacions diàries. També es pot fer servir per a gestió/control de la cadena de fred (especialment últil en el transport i emmatzematge de vacunes, productes frescos, flors, etc).

DASH7 es fa servir de manera extensiva per part del Departament de Defensa (DoD – *Department of Defense*) d'EEUU i gran part de la seva base de sensors sense fils ja funciona –o està essent migrada- a aquesta tecnologia. Per la seva part, a Europa, l'OTAN també està implementant infraestructures basades en DASH7. De fet, les forces militars de l'OTAN han d'implementar infraestructures que puguin interoperar amb les xarxes DASH7 del DoD.

Per últim, en DASH7 existeix l'OpenTag, una llibreria de *firmware* de codi obert que proporciona als desenvolupadres d'un entorn en llenguatge C sobre el qual poden crear aplicacions DASH7 molt ràpidament. Per tant, a més de que DASH7 és un estàndard obert, OpenTag és una pila també open source que és única en relació a altres tecnologies d'WSN (ZigBee).

A mode de resum, podem dir que DASH7 és una opció més que viable com a alternativa a altres solucions 802.15.4 com ara ZigBee, ja que presenta més cobertura (tant en interiors com exteriors) i més penetració d'obstacles. De vegades, es diu que DASH7 és "6x" (sis vegades més) que ZigBee, en aquests aspectes mencionats [112]. L'únic inconvenient és, com acostuma a passar al treballar en aquests freqüències, que la seva taxa de dades és molt més limitada que altres opcions en la banda 2.4 o 5 GHz.

Annex XX. Característiques tècniques de Z-Wave.

Els transceptors Z-Wave acostumen a ser fabricants per les companyies Sigma Designs i Mitsumi tot i que existeixen opcions *open source*, amb transceptor d'altres fabricants (per exemple amb interfície USB); tanmateix, hi ha projectes com ara Open-Zwave, que estan dirigits a tothom que vulgui desenvolupar però sense la necessitat de costosos kits de programari; també hi ha altres projectes que integren una antena Z-Wave en plataformes Raspberry Pi.

Les xarxes Z-Wave fan servir una topologia de malla i poden ser tan simples com un únic dispositiu de tipus controlador i un dispositiu controlat o esclau, podent arribar a un màxim de 232 nodes, afegint posteriorment més controladors o esclaus (fins i tot es poden "pontejar" dues o més xarxes si és necessari un major nombre de dispositius). Al procés d'associar més nodes a la xarxa se li diu *pairing* -de manera semblant a altres tecnologies com ara Bluetooth- i normalment consisteix tan sols en pitjar un o varis botons tant en el controlador com en el nou node a afegir. Una particularitat d'aquest procés d'associació és que el controlador "aprèn" la potència del senyal del node que es vol afegir per tal de composar internament una arquitectura de la xarxa; això significa que s'espera que la localització dels dispositius sigui sempre la mateixa, un cop s'uneixen a la xarxa (per tal que la potència que rep el controlador no variï). A més, el controlador acostuma a portar una bateria interna que li permet ser desendollat temporalment de la xarxa elèctrica i ser ubicat a prop del dispositiu a emparellar.

Cada xarxa Z-Wave s'identifica pel seu ID de xarxa, així com cada dispositiu també té el seu propi ID de node. L'identificador de xarxa (també anomenat *Home ID*) és compartit per tots els nodes que pertanyen a la mateixa xarxa lògica Z-Wave i té una longitud de 32 bits, essent assignat a tots els nodes pel controlador primari quan el node s'associa a la xarxa. D'aquesta manera, dos nodes amb identificadors de xarxa diferents no poden parlar-se entre ells. Per altra banda, la longitud de l'identificador de node és de 8 bits i no es permet que, dins d'una mateixa xarxa lògica hi hagi dos dispositius amb el mateix ID de node.

Per altra banda, els nodes es poden configurar per retransmetre missatges per tal de garantitzar connectivitat en un entorn multicamí, per exemple en una casa residencial. El número màxim de salts entre nodes és quatre, que hauria de ser suficient per cobrir un rang màxim de 30 metres.

El mètode que fa servir Z-Wave per a l'encaminament de missatges és "encaminament a l'origen" (*source-routed*, en anglès). D'aquesta manera, es pot anar d'un node A a un node D passant per nodes intermitjos B i C (nodes preferits per fer l'encaminament). En cas de que cap d'aquests nodes encaminadors no estigui disponible, el node origen cerca una altra ruta amb nodes intermitjos "vius" que també permetin arribar a D.

Un inconvenient d'aquest tipus d'encaminament és que els nodes que fan d'encaminadors no poden posar-se mai en mode *sleep* –ja que en qualsevol moment els hi pot arribar un missatge d'un altre node per ser encaminat- i, per tant, aquests dispositius han d'estar connectats a una font d'energia contínua (no poden funcionar solament amb bateries degut al seu major consum). Un altre inconvenient és que, en tractar-se d'un encaminament en origen d'una xarxa estàtica, es suposa que tots els dispositius sempre estan en la mateixa posició, per la qual cosa dispositius mòbils com ara control remots no poden ser configurats com enrutadors.

En versions més noves de la tecnologia, s'han afegit mecanismes de descobriment de xarxa com ara trames d'exploració, que poden ser utilitzatdes per arreglar rutes "trencades" degut dispositius que s'han mogut o tret de la xara. En realitat, aquest mecanisme es tracta d'un missatge de *broadcast*, que se suposa a d'arribar a cada dispositiu de la xarxa. Per tant, aquesta opció es fa servir com a darrera alternativa, per part del dispositiu enviador, quan la resta d'intents d'encaminament han fallat.

A grans trets, es pot resumir que Z-Wave és una tecnologia sense fils pensada principalment per a automatització de llars, on els requeriments d'enviament de dades i cobertura són petits i on el nombre de nodes per xarxa no ha de ser molt gran. Les característiques més important de l'estàndard són:

- Taxa de dades de fins 100 Kbps, amb *throughputs* típics de 9.6 i 40 Kbps.
- Modulació GFSK (amb condificació prèvia Manchester).
- Rang màxim de 30 metres assumint espais oberts.
- Freqüència de 868.42 MHz (Europa), 908 MHz (USA), 916 MHz (Israel), 919.82 MHz (Hong Kong), 921.42 MHz (Australia i Nova Zelanda), 865.2 MHz (India).
- Seguretat mitjançantencriptació AES-128.
- Suport per a IPv6.

A l'Annex XLVII es pot trobar un exemple de dispositiu amb tecnologia Z-Wave encastrada: es tracta d'un simple endoll de corrent amb commutador ON/OFF que es pot activar remòtament i que a més incorpora lectura del consum elèctric [113].

Annex XXI. Característiques tècniques d'ANT.

Les aplicacions d'ANT són fonalmentalment aquelles on és necessarìa la transferència periòdica de petites quantitats de dades, en xarxes amb topologia punt a punt, arbre, estrella o malla. Aquestes aplicacions normalment tenen limitacions de cost –fabricació- i sobretot de potència, per la qual cosa els paràmetres que es medeixen normalment no canvien massa ràpidament (per exemple temperatura o humitat) per la qual cosa és més que suficient mesurar les actualitzacions cada pocs segons.

En una xarxa ANT, els nodes poden operar com a esclaus o com a mestres, la qual cosa significa que poden actuar com a transmissors, receptors o encaminadors de tràfic a altres nodes. A més, cada node és capaç de determinar quan ha de transmetre, basant-se en l'activitat dels node veïns. Per la seva banda, els dispositius, quan es troben en mode adormit, tenen un consum d'únicament uns µA i únicament es desperten per transmetre o rebre informació: quan transmeten el consum arriba a un pic d'uns 13.5 mA mentre que quan reben el consum té un pic de 22 mA. D'aquesta manera, el consum promig pot arriba a ser de tant sols 60 µA, en funció del període d'actualització.

En les xarxes ANT, els canals són bidireccionals, en el sentit de que en un mateix canal pot haver-hi un o més nodes enviant o revent dades, depenent de la topologia de xarxa. Els tipus de missatges que pot haver-hi son tres: difusió (*broadcast*), reconeixement (*acknowledgment*) i ràfaga (*burst*):

- El missatges de difusió són en un únic sentit, d'un node a un altre (o a molts). El node receptor no transmet cap justificant de recepció –reconeixement (encara que podria enviar, pel seu compte, missatge a altre node, incloent el node origen). Aquest tipus de missatge és el que es fa servir en aplicacions de sensors, essent el mètode d'operació més econòmic.
- El missatges de reconeixement confirmen la recepció dels paquets de dades; per tant, el transmissor és informat sobre l'èxit o fracàs, tot i que no hi haurà retransmissions. Aquesta tènnica es fa servir per a aplicacions de control.

- Els missatges de tipus ràfaga és una tècnica de transmissió multi-missatge que fa servir tot l'ample de banda de dades i que s'executa fins a transferir totes les dades. El node receptor envia llavors un ACK i informa dels paquets corruptes, que l'emissor tornarà a enviar. Aquests paquets es numeren per raons de traçabilitat. Aquesta tècnica s'utilitza per a transferències de blocs de dades on la integritat és primordial.

Les característiques principals d'una xarxa ANT, quan es compara amb altres alternatives com ara Bluetooth, BLE, Wifi o ZigBee, són:

- ANT està enfocada a xarxes sense fils de sensors a gran escala, amb baixa taxa de dades i que requereixen molt poc consum d'energia (els nodes s'han de alimentar amb bateries de botó). Altres tecnologies con Wi-Fi o Bluetooth no estan dissenyades per xarxes molt grans sinó de pocs nodes (32 o 8, respectivament). Els dispositius típics ANT són rellotges, equipament esportiu o, genèricament, xarxes de sensors.

- Amb ANT també es pot implementar via programari -al igual que a partir de Bluetooth 3.0- una opció per utilitzar Wi-Fi quan s'han d'enviar dades més ràpidament, per aquells dispositius que incorporin els dos protocols. Si es no fa servir aquesta tècnica, es pot sevir tanmateix l'especificació ANT *File Share* (ANT-FS) per transmetre dades fent servir únicament ANT, amb un rendiment d'uns 60 Kbps.

- ANT incorpora transmissió adaptativa isòcrona, de manera que es permeten molts dispositius ANT comunicant-se concurrentment sense interferències amb cap altre, la qual cosa permet construir, al menys potencialment, xarxes de desenes de milers de nodes (fent servir tècniques com els "canals compartits", "mode d'escaneig continu" o "escaneig en segon pla", que no consumeixen gairebé recursos adicionals, ni de memòria ni d'amplada de ràdio).

- Tot i que ANT, ZitBee, Bluetooth i Wi-Fi fan servir totes elles la banda de 2.4 GHz, ANT fa servir –tal i com ja hem dit abans- una tecnologia de xarxa adaptativa isòcrona per evitar interferències, en comptes de fer servir DSSS i FHSS com fan servir Wi-Fi, ZigBee i Bluetooth. Bàsicament, l'esquema d'ANT es basa en l'habilitat de que cada transmissió pot ocòrrer en una ranura de temps lliure –anomenada "interferència"- dintre de la banda de freqüència: la ràdio transmet durant menys de 150 µs per missatge, permetent que un únic canal pugui dividir-se en centenars de ranures de temps i que cada dispositiu pugui transmetre en una d'aquestes ranures (el nombre total de ranures depèn de l'*ANT Messaging Period*, que és el temps que hi ha entre cada node transmeten les seves dades).

- A més, aquest esquema isòcron no requereix d'un rellotge mestre (els tranmissors comencen a difondre a intervals regulars però poden modificar el temps de transmissió si es troben interferències d'un vei en una ranura de temps particular). Aquesta flexibilitat permet adaptar-se a entorns hostils al mateix temps que assegura que no hi haurà sobrecàrrega quan no hi ha interferències.

- Per últim, ANT té la capacitat de "saltar" a canals alternatives d'1 MHz –sempre en la banda de 2.4 GHz- en cas de que les condicions del canals actual siguin dolentes o aquest estigui molt saturat. A aquesta tècnica se li anomena *frequency agility*.

- Les característiques de Bluetooth Smart (BLE o simplement SMART) i ANT són molt similars a nivell de RF, per la qual cosa els fabricants poden decidir incorporar ambdues tecnologies fent servir el mateix xip. Tot i així, cap de les dues pot competir amb 6LoWPAN, ZigBee o WirelessHART per a aplicacions que requereixin grans xarxes multisalt, ja que tant ANT com SMART estan pensades per a xarxes amb un o pocs salts (per exemple connexió d'un rellotge o un pedal de bicicleta connectats a un PC o *smartphone*).

- ANT, al igual que SMART, fa pocs anys que està present al mercat de gran consum. Els primers telèfons intel·ligents amb ANT van sortir al mercat únicament a finals de 2010 i únicament fa un any que empreses con Samsung han decidir incloure aquest portocol al seus productes (el primer producte a suportar-lo va ser el Samsung Galaxy Note 3).

- ANT és entre un 10-50% més eficient que altres tecnologies com Bluetooth Smart per a dispositius com monitors de glucosa.

- La taxa màxima de dades (*over the air*) amb ANT és d'1 Mbps, en contraposició a ZigBee (250 Kbps) i igual a la d'SMART.

Per últim, cal afegir que darrerament ha aparegut al mercat ANT+, que no és més que una funció d'interoperabilitat i accés obert a dades que es pot afegir al protocol base ANT. Aquesta nova estandardització permet als dispositius ANT+ propers entre ells el poder recollir i interpretar dades dels mateixos.Per exemple, amb ANT+ es pot fer que dispositius de *fitness*, com ara monitors cardíacs, velocímetres, pedòmetres, ordinadors de bicicleta, etc. puguin treballar conjuntament per tal d'ensamblar i fer un seguiment de les dades –mètriques- de rendiment. Altres dispositius possibles poden ser mesuradors de pressió sanguínea, de glucosa, monitors de pressió de rodes, control d'enllumenat, etc. Per la seva banda, existeix l'ANT+ Alliance, amb més de 300 membres (incloent Adidas, Suunto, Garmin, Timex, McLaren, etc) i que promou dispositius i aplicacions que fan servir ANT+.

Annex XXII. Característiques tècniques de DECT/ DECT ULE.

DECT fa servir un perfil estandaritzat per a la interoperabilitat entre dispositius de diversos fabricants; aquest perfil s'anomena GAP (*Generic Access Profile*) i permet que els auriculars i bases de diferents fabricants puguin interactuar entre ells al seu nivell més bàsic de funcionalitat, és a dir, per fer i rebre trucades. També existeixen altres perfils menys coneguts, que es fan servir per a dades i serveis d'abonat local de ràdio. Cal dir però, que la versió DECT 6.0 no fa servir GAP per la qual cosa els dispositius de diferents marques no tenen garantida la seva interoperabilitat.

Les característiques bàsiques de l'especificació DECT són les següents:

- Rang freqüencial: 1880-1900 MHz (Europa i Hong Kong), 1920-1930 MHz (USA i Canadà), 1910-1930 (Sudamèrica), 1.893-1906 MHz (Japó).
- Taxa de dades: 1.15 Mbps.
- 10 canals en Europa, 5 canals en USA (espaiats 1.728 MHz).
- 24 ranures temporals (*timeslots*) per canal.
- Potència de transmissió Europa: 10 mW típica-250 mW pic (Europa), 4 mW típica - 100 mW pic (USA).
- Rang de cobertura: 25-100 metres (màxim teòric 300 metres amb LOS).
- Modulacions possibles: GFSK, 1/2 DPSK, 1/4 DQPSK, 1/8 D8PSK.
- Còdecs d'aúdio: G.726 (ADPCM, 32 Kbps), G.711, G.722 (banda ampla, 64 Kbps), G729.1 (banda ampla), MPEG-4 ER LD AAC (banda ampla i super banda ampla).
- Capa PHY: fa servir FDMA, TFMA i TDD (espectre ràdio dividit en freqüència i temps).
- Capa MAC: mode orientat a conexió, mode sense connexió i mode de serveis *broadcast*.
- Capa d'enllaç: fa servir LAPC (*Link Access Protocol Control*), una variant de LAPD per a XDSI (Xarxa Digital de Serveis Integrats), totes dues basades en HDLC (*High-Level Data Link Control*).
- Seguretat: es fa servir DSC (DECT Standard Cipher) a la capa de control d'acces al medi, un mode de xifrat bastant feble avui dia, que consta d'un IV de 35 bits i encriptació del fluxe de veu amb 64 bits.

La darrera revisió de DECT és DECT ULE (*Ultra Low Energy*). Aquest estàndard va ser definit el 2011 i els primers products comercials van aparèixer durant el mateix any. DECT ULE és la vesió de baix consum de DECT i fa servir la banda de 1.9 GHz, per la qual cosa pateix menys interferències que altres tecnologies com ZigBee, Bluetooth o Wi-Fi que fan servir totes elles 2.4 GHz (al igual que, per exemple, els forns microones). Aquesta versió va ser creada per permetre aplicacions d'automatització de llargs, seguretat, cura de la salut i monitoratge d'energia, allà on es requereixen dispositius de baix consum i que es puguin connectar fàcilment a Internet, fent servir el gran nombre de mòdems DECT existents actualment; aquestes aplicacions es podrian consultar a través de qualsevol dispositiu intel·ligent amb accés a la Web, com ara un PC o *smartphone* [117].

Les característiques bàsiques de DECT ULE són [118]:

- Topologia de xarxa: estrella (menys costosa d'implementar que en malla).
- Rang freqüencial: 1.8 GHz (Europa), 1.9 GHz (USA).
- Potència de transmissió màxima: 0.35 W (Europa), 0.1 W (USA).
- Consum de corrent promig: <20 uA.
- Cicle de treball baix: 0,5% (100 ms de transmissió de sensor cada 20 segons).
- Durada de les bateries fins a 10 anys (degut al cicle de treball baix i baix consum).
- Cobertura: 70 m (interiors), 600 m (exteriors).
- Canals: 10 (Europa), 5 (USA) amb separació de 1.724 MHz entre canals.
- Taxa de dades: 1.15 Mbps.
- Capa PHY: TDMA, FDMA, TDD, 24 ranures temporals, modulació GMSK.
- Capa MAC: selecció dinàmica de canal per evitar interferències i reduir consum, mida de *payload* de 40 o 80 bytes, modes circuit o paquet.
- Suport de repetidors per extendre rang de cobertura.
- Suport de diversitat d'antena.
- Baixa latència.
- Solució en un únic xip; baix cost de fabricació.

Amb ULE DECT, el consum de potència depèn del mode operacional del dispositiu:

- Mode síncron (*Locked Mode*): consisteix en un temps d'*sleep* predeterminant (entre 1-20 segons). En aquest mode, el node ULE comunica autònomament amb la base cada 1-20 segons.

- Mode asíncron (*Unlocked Mode*): es defineix un període *sleep* que pot anar des d'uns segons a varis dies.

Fent servir dues piles alcalines AA o dues piles de botó AAA, es pot aconseguir, en el mode síncron, una durada de les bateries de fins quatre anys (configurant un temps d'*sleep* de 20 segons); per la seva banda, en el mode asíncron, configurant un temps d'*sleep* de 2.5 min o 5-6 min, es poden aconseguir vides de bateria de 5 i 10 anys, respectivament.

La darrera versió de DECT ULE, la v3.0 –encara en fase d'esborrany per part de l'IETF- contempla la transmissió de paquets IPv6 fent servir 6LoWPAN. D'aquesta manera, DECT ULE es convertiria en un veritable competidor de tecnologies com ara IEEE 802.15.4, que ja suporten aquests protocols. Aquesta versió de DECT es consideraria, per tant, com la primerarealment enfocada a entorns M2M i IoT (*Smart Metering*, seguiment de dispositius, cura de la salut pública/privada); és a dir, a grans xarxes de sensors sense fils de baix consum. Això seria possible, entre d'altresm amb la incorporació de característiques com són la creació de sistemes multicel·la (fent servir repetidors) i la possibilitat de xarxes auto-organitzatives i amb auto-recuperació.

Annex XXIII. Característiques tècniques d'RFID.

Les etiquetes RFID es fan servir actualment a molts àmbits i en un gran nombre d'aplicacions: per exemple, poden ser enganxades a un cotxe durant el procés de producció per tal de fer un seguiment de la cadena de muntatge; els medicaments o qualsevol altre producte poden ser localitzats dintre d'un gran magatzem; les mascotes poden tenir una etiqueta injectada per tal de poder identificar l'animal, etc. Fins i tot, es podrien col·locar etiquetes a les persones, encara que en aquest cas ens trobaríem amb el típic debat sobre la privacitat de les dades personals i l'ús inadequat o sense consentiment de les mateixes.

Pel que fa a la mida de les etiquetes, darrerament s'ha aconseguit miniaturitzar moltíssim. Fins i tot s'ha pogut, en els darrers anys, col·locar transpondedors RFID a formigues per tal d'estudiar el seu comportament. La mida pot ser tan petita com 0.05 x 0.05 (mm). Aquestes etiquetes poden tenir una ROM de 128 bits i emmagatzemar una seqüència de fins a 38 dígits.

Per altra banda, les etiquetes poden ser únicament de lectura o bé de lectura/escritura: en el primer cas, tenen un número de sèrie que ve de fàbrica i que s'utilitza com a clau d'identificació en una base de dades; en el segon cas, es poden introduir, per part dels usuaris, dades relatives al producte que s'identifica. Aquest darrer tipus de targetes s'anomenen també "programables" i poden ser escrites una única vegada, encara que llegides totes les que es vulgui.

Les etiquetes RFID consten de dues parts:

- Un circuit integrat (CI): s'encarrega d'emmagatzemar i processar la informació, modular i demodular el senyal RF, recollir correct continu (DC) del senyal incident de l'interrogador, així com altres funcions especialitzades. Per la seva banda, la informació de l'etiqueta s'emmagatzema en una memòria no volàtil (ROM).

- Una antena: utilitzada per rebre i transmetre el senyal.

- Una bateria: en el cas de tractar-se d'una etiqueta BAP o activa.

Respecte als aspectes d'estandarització, l'ISO ha creat diversos estàndards que fan referència a l'RFID, essent els més coneguts els següents:

- ISO 14223: defineix l'RF per a la identificació d'animals, fent ús de transpondedors avançats.

- ISO/IEC 14443: estàndard per a 13.56 MHz. Els passaports electrònics i l'estàndard NFC (*Near Field Communication*) es basen en l'ISO/IEC 14443.

- ISO/IEC 15693: similar a l'anterior però enfocat al pagament fent servir targetes sense contacte.

- ISO/IEC 18000: es divideix en set parts; a grans trets, fa referència als paràmetres de la interfície aire per a determinades freqüències (135 KHz, 13.56 MHz, 860-960 MHz i 433 MHz).

- ISO 18185: estàndard industrial per a seguiment de contenidors de càrrega, fent servir les bandes de 433 MHz i 2.4 GHz.

Dels estàndars anteriors, potser el més important és ISO/IEC 18000-6C, creat l'any 2006, que recull les característiques de RFID Gen 2, és a dir, la segona generació de etiquetes RFID. A aquest estàndard també se li anomena EPC Gen 2. Aquesta versió treballa únicament en el rang UFH 860-960 MHz. En la nova versió, es defineixen cinc classes d'etiquetes:

- Classe 0: UHF; únicament lectura; etiquetes passives preprogramades; escriptura una única vegada però lectura múltiples vegades (WORM – *Write Once, Read Many*).

- Classe1: HF o UFH; com la Classe 0 però les etiquetes poden ser llegides per lectors d'altres companyies diferents.

- Classe 2: etiquetes passives de lectura/escritura que poden ser escrites a qualsevol punt de la cadena de suministre.

- Classe 3: etiquetes semi-passives, tipus BAP (assistides per bateria), amb capacitats de sensorització, capaces d'enregistrar paràmetres com temperatura, pressió i moviment.

- Classe 4: etiquetes actives de lectura/escriptura, amb transmissors integrats; es poden comunicar amb altres etiquetes i amb lectors.

- Classe 5: similar a la classe 4 pèro amb funcionalitats adicionals; poden proporcionar energia a altres etiquetes i comunicar-se amb altres dispositius que no siguin lectors.

Les Classes 0 i 1, les més senzilles, són compatibles amb dispositius RFID de primera generació, mentre que la resta de classes són pròpies de la segona generació.

Pel que fa a la capa PHY, les característiques fonamentals de RFID Gen 2 són:

- Modulació ASK (*Amplitude-Shift Keying*) o PSK (Phase-Shift Keying).

- Codificació FM0 o Miller.

- Taxes de dades variable: 40-640 Kbps amb codificació M0; 10-640 Kbps amb codificació Miller; 60-70 Kbps taxa típica amb Miller M=4.

Pel que fa a les freqüències i rangs associats que fa servir RFID (incloent Gen 1) són les següents:

- 120-150 KHz (baixa freqüència): banda no regulada; el rang de cobertura és d'únicament uns 10 cm; pot atravessar més fàcilment aigua o altres materials; la taxa de transferència de dades és baixa; el cost aproximat d'una etiqueta (comprant per volum) és d'1 USD; es fa servir normalmente per identificació d'animals i recollida de dades a fàbriques/magatzems.

- 13.56 MHz (alta freqüència): banda ISM; el rang d'acció és de 10 cm fins a 1 metre; la taxa de dades és de baixa a moderada; el cost unitari comprant per volum és de 0.50 USD; es fa servir per a targetes intel·ligents (*smartcards*).

- 433 MHz (ultra alta freqüència): banda pròpia del SRD (*Short Range Devices*) [107]; el rang és d'1 a 100 metres; la taxa de dades és moderada; el cost unitari és d'uns 5 USD; es fa servir per aplicacions de defensa i etiquetes actives.

- 865-868 o 902-928 MHz (ultra alta freqüència): banda ISM; el rang és d'1 a 12 metres; la taxa de dades és de moderada a alta; el cost aproximat unitari és d'uns 0.15 USD; es fa servir per a EAN (identificació per codi de barres).

- 2.4-5.8 GHz (microones): banda ISM; el radi d'acció és d'un a dos mestres; la taxa de dades és alta; el cost unitari aproximat és de 25 USD; es fa servir per als estàndars 802.11 i Bluetooth.

- 3.1 – 10 GHz (microones): li afecta la regulació de l'ultra banda ampla; el rang de cobertura és de fins a 200 metres; la taxa de dades és alta; el cost unitaro aproximat és d'uns 5 USD; es fa servir per a etiquetes actives o semi-actives degut al major consum d'energia.

A les figures de sota es poden veure dos exemples de tecnologia RFID: en el primer cas, es tracta d'un xip i antena de fil a l'interior d'una tarjeta de plàstic (típic cas de tarjeta d'accés a edificis); en el segon cas, el xip i l'antena (tipus espira) venen "encastrades" a la part de darrera d'una enganxina convencional.

Figura 39. Exemples d'antenes i xips RFID integrats.

Per la seva banda, a la figura de sota podem veure la classificació dels diferents sistemes RFID que existeixen actualment, principalment en dos tipus: actius i passius.

- En el cas dels sistemes actius, tenim per un cantó les etiquetes per a sensors i altres tipus d'etiquetes actives.

- Per altra cantó, en el cas dels sistemes passius, tenim per un cantó les etiquetes EAS (*Electronic Article Surveillance*), típiques ens els comerços-per evitar robatoris dels articles. També tenim sistemes de baixa freqüència (LF) i alta freqüència (HF), i també d'ultra alta freqüència (UHF) i de microones. En el cas d'LF i HF, l'acoblament entre els dispositius és del tipus inductiu, mentre que en el cas d'UFH i microones, l'acoblament és de tipus *backscatter*, com ja s'ha comentat abans.

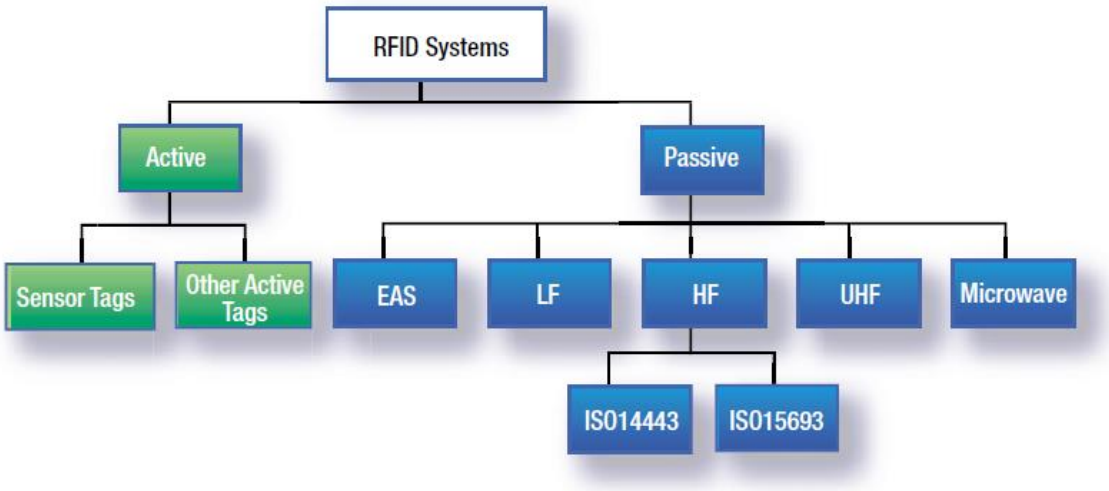


Figura 40. Arbre amb tipus de sistemes RFID.

En resum, podem dir que la tecnologia RFID és una manera molt econòmica –probablement la que més, avui dia- de dotar de certa "intel·ligència" a qualsevol objecte quotidià, anant des de simples capses, contenidors, targetes de crèdit o peces de roba i arribant fins i tot a animals i persones, permetent que la informació emmagatzemada en les etiquetes es pugui llegir remòtament.

És per aquest fet que RFID es considera el "precursor" del concepte/paradigma de l'IoT, encara que dista bastant de assemblar-se a tecnologies molt més complexes com ara IEEE 802.15.4, ja que aquestes darreres incorporen mecanismes de seguretat avançats (encriptació, claus), topologies de xarxa en malla amb milers de nodes, auto-encaminament i auto-recuperació, 6LoWPAN, etc.

Per un cantó, tenim les etiquetes passives, que poden emmagatzemar des d'únicament 64 bits fins a 1 Kb (en una EEPROM, normalment) mentre que, per altre cantó, tenim les etiquetes actives (més grans, amb bateries, utilitzades per exemple en aplicacions militars) i que poden emmagatzemar fins a 128 Kb. Les etiquetes BAP i les actives, com que disposen de bateria, poden utilitzar-se per oferir un major rang de cobertura, per emmagatzemar més dades i per afegir capacitats de *logging*, com per exemple en sensors de temperatura, humitat, etc. A més, el seu rang temperatures de treball (-25ºC a 70ºC) les fan adequades per tot tipus d'usos, tant a nivell de gran consum, com industrial i militar (algunes poden arribar a funcionar fins i tot amb temperatures de 250ºC).

Per últim, la segona generació d'etiquetes (Gen2) i, en especial, les classes 4 i 5, estan dirigides a xarxes de sensors, on es poden recollir variables i enviar-les no únicament a un lector sinó també a altres etiquetes, obrint així la possibilitat de formar topologies de xarxa tipus malla o arbre i acostant-se més a altres tecnologies com ara 802.15.4. De fet, l'IEEE, en el seu estàndard 802.15.4f-2012, defineix la capa PHY per a RFID actiu, per tal de poder crear WPANs de baixa velocitat (LR-WPANs).

Annex XXIV. Característiques tècniques d'NFC.

L'estàndard especifica la presència de dos tipus de nodes: un dispositiu iniciador (*initiator*) i una destinació u objectiu (*target*): l'iniciador genera, de manera activa, un camp RF que pot posar en funcionament un "objectiu" passiu. Això significa que, al igual que amb RFID passiu, podem trobar dispositius destinació molt senzills com ara engaxines, targetes, etiquetes, etc. que no requereixen bateries. La novetat respecte a RFID clàssic és que ara també es permet una comunicació bidireccional de tipus P2P, sempre i quan els dos dispositius rebin energia.

Al igual que amb RFID, les etiquetes són típicament sols de lectura (en dispositius simples), encara que també es poden sobreescriture (en dispositius més avançats). La quantitat d'informació que es pot guardar va de 96 byte a 4 Kb. Pel que fa a la distància/rang de cobertura, típicament és de 4 cm de separació entre dispositius, encara que es pot arribar als 20 cm màxims. Pel que fa al cost d'una etiqueta NFC, és fins i tot inferior al de RFID, ja que pot arribar a ser d'únicament vuit cèntims d'euro si es compren per volum.

Pel que fa a la capa PHY i, en concret, a la modulació emprada, és sempre ASK, igual que RFID. Com a pas previ (codificació), es fa servir o bé Manchester (amb *ratio* de modulació 10%) o bé Miller modificat (amb *ratio* de modulacio 100%). En el darrer cas –codif. Miller- la taxa de dades que s'aconsegueix és de 106 Kbps mentre que amb Manchester, la taxa és de 212 o 424 Kbps. Això permet un consum de potència per sota de 15 mA (en mode lectura), valor semblant al que s'obté amb BLE.

En referència al temps de preparació/configuració (*setup time*), aquest és molt ràpid, ja que no arriba als 0.1 segons, bastant més ràpid que Wi-Fi o Bluetooth però més lent que per exemple BLE, que té un temps de configuració inferior a 0.006 segons.

NFC, de manera semblant a altres tecnologies, disposa de la seva pròpia associació, denominada NFC Forum, que compta actualment amb uns 190 membres i que té com a finalitat desenvolupar estàndars basats en NFC (permetent interoperabilitat entre productes de diversos fabricants), així com potenciar el desenvolupament d'aplicacions i productes basats en NFC. Alguns dels seus membres són Broadcom, Google, Intel, NEC, Nokia, Qualcomm, NXP Semiconductors, Visa, Mastercard, etc

Els usos d'NFC poden ser molt variats i entre ells destaquen els següents:

- Comerç: es pot fer com a forma de pagament *contactless*, amb dispositius encastrats dintre de targetes de crèdit, telèfons mòbils, claures, etc. Pot fer-se servir en targetes de fidelitat d'hotels, benzineres o supermercats, pagamentde peatges, etc.

- Com a “llançadora” d’altres tipus de connexió: de manera semblant a com Bluetooth Smart permetia llençar una connexió Wi-Fi quan es volien transmetre grans quantitats de dades de manera ràpida, NFC pot fer el mateix, és a dir, pot iniciar una comunicació Bluetooth per transmetre dades entre dos dispositius emparellats i acte seguit deshabilitar Bluetooth (també es pot aplicar a Wi-Fi). D’aquesta manera es poden aconseguir transferències de l’ordre de 100 o 300 Mbps iniciades de manera simple mitjançant NFC (un exemple el tenim amb la funcionalitat Android Beam que incorporen alguns mòbils amb aquest sistema operatiu).

- Jocs: es poden vendre joguines (per exemple, figures) que tinguin dintre un xip NFC i on es pugui escriure informació sobre el tipus de personatge del joc, les seves habilitats (força, resistència, sabiduria), etc. Aquesta informació s’escriu i llegeix per part d’una consola amb NFC. D’aquesta manera, les joguines “guarden” la informació dels objectes, que llavors es poden transportar a un altre lloc (a una altra consola). Per exemple, la consola Wii-U ja incorpora aquesta funcionalitat.

- Com a sistema d’identitat i d’accés: aquesta funcionalitat és la mateixa que ja es va veure amb RFID; és a dir, es pot fer servir com a identificador de la persona a l’hora d’accedir a un edifici o recinte restringit. L’avantatge d’NFC és que com que el radi de cobertura és menor i suporta encriptació, ara és molt més segur que no pas quan es fa servir RFID.

- Automatització de tasques en dispositius mòbils: un smartphone pot emparellar-se amb una etiqueta NFC i aquesta li darrera li pot donar informació al móbil sobre un text a mostrar, una aplicació per ser llençada, una sèrie de comandes a ser executades, etc. Com a exemple, tenim que molts festivals de música, en comprar l’entrada, donen a l’usuari una polsera amb un xip NFC integrat. Quan la polsera es troba a prop del telèfon, es mostra en aquest informació sobre el festival, les propere actuacions, mapes del recinte, on es troben els bars o els lavabos, etc. Al mateix temps, la polsera serveix com a sistema d’identitat al recinte (ús explicat anteriorment).

- En xarxes socials: es pot fer servir per compartir fotografies, vídeos, música, etc. així com a iniciador de partides multijugador en dispositius mòbils.

A mode de resum, es pot dir que NFC és una evolució/extensió de RFID però treballant ara amb distàncies més curtes, amb una taxa de dades típica més alta, amb major seguretat i on tots dos dispositius poden intercanviar informació entre ells (mode P2P). Es un estàndard molt enfocat a pagaments sense contacte i per a accés a recintes, per la qual cosa no es veu com una veritable alternativa per a xarxes de sensors sense fils. Per les seves característiques, els seus competidors més directes són RFID (per a identificació, autenticació i seguiment d’objectes) i BLE (per a transferència de dades). La major part de telèfons mòbils actuals i moltes tabletes ja disposen de funcionalitat NFC per la qual cosa és una tecnologia ja present, encara que el seu ús es troba encara una mica restringit, donat que al final són les empreses les que han de saber buscar usos per a la mateixa.

Annex XXV. Capes PHY i MAC d'IEEE 802.15.4.

A la figura de sota es pot apreciar gràficament el que s'ha comentat a la Memòria sobre sobre les diferents bandes de freqüència i els canals de 802.15.4:

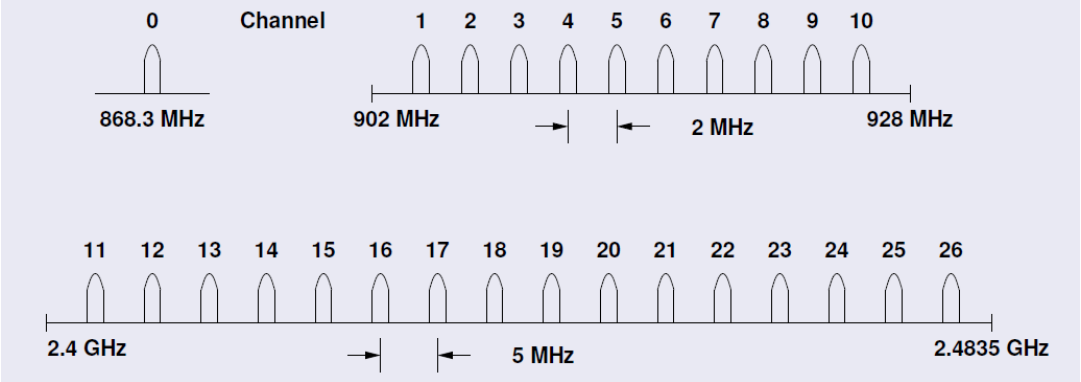


Figura 41. Característiques dels canals ràdio amb 802.15.4.

Per la seva banda, a la figura de sota es pot veure l' esquema d'un paquet a nivell PHY i una trama de tipus balisa a nivell MAC. Com es pot apreciar, tota la trama MAC s'encapsula dins del *payload* PHY (també anomenat PSDU o *PHY Service Data Unit*).

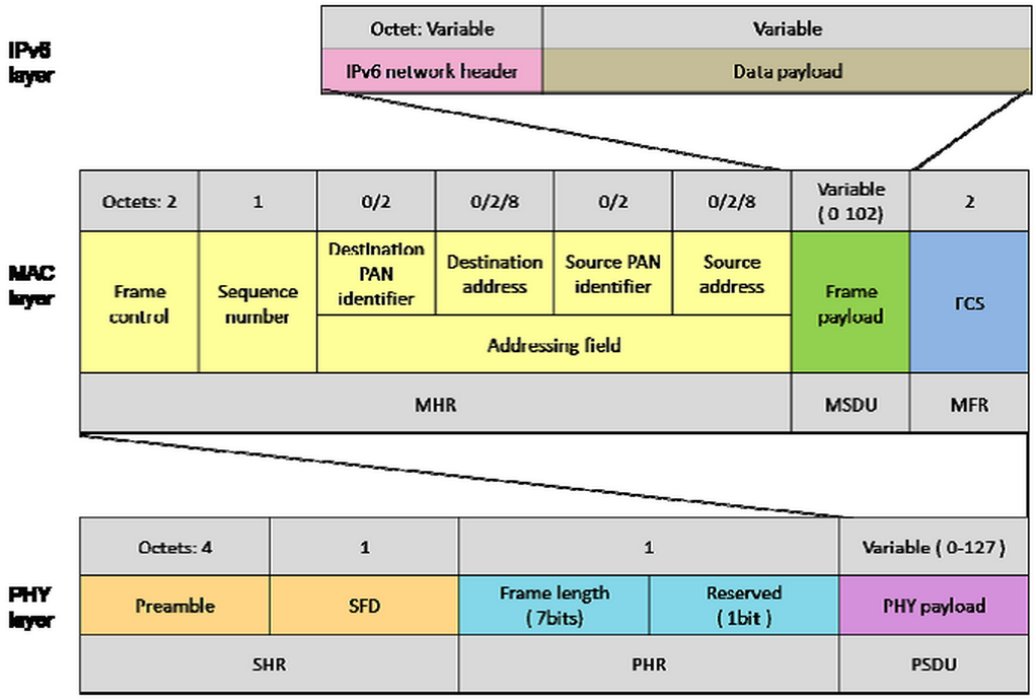


Figura 42. Esquema d'un paquet PHY i trama MAC amb IEEE 802.15.4.

A nivell PHY, el preamble ocupa 4 octets (bytes) i l'SFR (*Start of Frame Delimiter* – Delimitador de començament de trama) 1 byte, formant tots dos l'SHR (*Synchronization Header*– Capçalera de Sincronització). Per la seva banda, el PHR (*PHY Header*– Capçalera Física) ocupa únicament 1 octet i està format pel *Frame Length* o Longitud de Trama (7 bits) i un bit reservat (opcional). Per últim, el *payload* (dades d'usuari pròpiament dites) és l'únic camp dins del PSDU, sent aquest variable (de 0 a 127 bytes).

Per la seva banda, a nivell MAC, tenim l'MHR (*MAC Header*) format pels següents camps: *Frame Control* - Control de Trama (2 bytes), *Sequence Number* - Número de Seqüència (1 byte), *Destination PAN identififern* - Identificador de Xarxa Personal de Destinació (0 o 2 bytes), *Destination Address* - Adreça de Destinació (0, 2 o 8 bytes), *Secure PAN Identifier* – Identificador de xarxa personal Segura (0 o 2 bytes) i *Source Address* – Adreça Origen (0, 2 o 8 bytes). A més, tenim l'MRF (*MAC Footer* – Peu de MAC) que consta del camp FCS (*Frame Check Sequence* – Seqüència de xequeig de trama). Per últim, tenim l'MSDU (*MAC Service Data Unit*) que és el *payload* –dades d'usuari- i que té una longitud variable de 0 a 102 bytes.

També es pot veure que, en cas de fer servir IPv6 (amb 6LowPAN) tot el paquet IP aniria encapsulat dins del MAC SDU.

Encara que ja queda prou clar a l'explicació anterior, és important fer notar que l'estandàr 802.15 no fa servir 802.1d o 802q, és a dir, no hi intercanvi de trames Ethernet estàndard, com passa a les xarxes LAN tradicionals. De fet, tal com s'ha pogut veure, la capa PHY únicament suport trames fins a 127 bytes (encara que hi ha capes d'adaptació com 6LoWPAN que permeten fragmentar paquets més grans per poder-los transportar amb 802.15.4).

Annex XXVI. Transport de dades amb IEEE 802.15.4.

Amb 802.15.4 tenim dos tipus de CSMA/CA: *slotted* (amb ranures) i *unslotted* (sense ranures). El primer funciona fent servir balises mentre que el segon no les fa servir.

- Amb el mode sense ranures o *unslotted*, com s'ha dit, no es fan servir balises. En aquest escenari, quan un node –transmissor- vol enviar dades a un altre node -receptor- o a un coordinador, fa servir CSMA/CA i llavors el receptor envia un ACK si l'emissor ho va demanar (donat que l'ACK és opcional) [24]. Això implica que el receptor ha d'estar escoltant contínuament el canal, per la qual cosa no pot "dormir", situació que implica, al seu voltant, un consum molt més elevat, que faria que, en un dispositu alimentat per bateries, aquestes s'esgotessin molt ràpidament, en qüestió d'hores. Per la seva banda, una situació semblant es dóna quan el coordinador PAN ha d'enviar dades a un node: suposem que un receptor pregunta al coordinador PAN si hi ha dades disponibles; llavors, el coordinador envia un ACK seguit d'una trama de dades; al seu voltant, el node receptor envia un ACK (si el demana l'emissor); d'aquesta manera, tenim que el coordinador també ha d'estar contínuament actiu, escoltant el canal.

- Per la seva banda, el mode *slotted* (amb ranures) es basa en balises, que el coordinador PAN envia periòdicament a la xarxa per identifcar-la i llavors sincronitza els nodes associats a la mateixa. Concretament, el mode amb ranures fa servir el concepte de supertrama. Aquestes darreres es defineixen pel coordinador PAN. Una supertrama es divideix en 16 ranures (*slots*) dividides amb el mateix temps, que poden ser agrupades, al seu torn, en una part "activa" i una part "inactiva". De fet, una supertrama es divideix en tres períodes:

    - Període CAP (*Contention-Access-Period*): el canal pot ser accedit fent servir CSMA/CA, com es faria normalment amb el mode sense balises.

    - Període CFP (*Contention-Free-Period*): en aquest període, el coordinador assigna ranures de temps garantizades (GTS – *Guaranteed Time Slots*) a cada node. Això vol dir que cada node únicament pot transmetre en el GTS que li ha estat assignat. En una supertrama pot haver-hi fins a set GTS la qual cosa significa que únicament fins a set nodes poden transmetre mentre dura la supertrama. De la mateixa manera, en cas de ser necessari, a un únic node se li pot assignar més d'un GTS, per tal de que pugui completar la transferència de totes les dades en la durada de la supertrama.

    - Període IP (*Inactive-Period*): com el seu nom indica, aquest període és la part inactiva de la supertrama, on el canal no es fa servir i tots els nodes, incloent el coordinador, es fiquen en mode *sleep* (estalvi d'energia). Lògicament, el coordinador es posa en aquest mode quan no necessita controlar la xarxa.

Per la seva banda, el coordinador delimita dues supertrames fent servir trames balisa. L'interval que hi ha entre dues balises s'anomena BI (*Beacon Interval*). A grans trets i, en general, l'interval entre balises és el mateix que la durada de la supertrama. En IEEE 802.15.4, la durada mínima de supertrama correspon a 960 símbols (cada símbol són 4 bits). Per tant, assumint que es treballa en la banda de 2.4 GHz i amb una taxa de dades de 250 Kbps, això significa que la durada mínima de supertrama és de 15.36 ms.

En la figura següent s'aprecien gràficament els tres períodes d'una supertrama (`CAP`, `CFP`, `INACTIVE`), així com els *beacons* que delimiten cada supertrama. Val a dir que entre dues supertrames, la contenció es realitza mitjançant CSMA/CA estàndard.

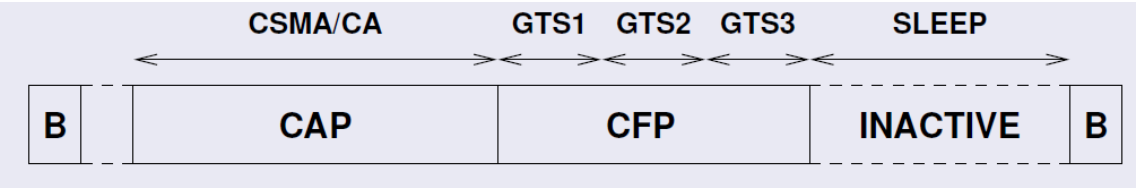


Figura 43. Períodes d'una supertrama IEEE 802.15.4.

El mode *slotted*és el que es fa servir per a aplicacions crítiques i que necessiten qualitat de servei (QoS). A més, en aquest mode, com que tots els nodes es fiquen en mode *sleep* en el període inactiu i cada node únicament transmet en el GTS que li toca, s'aconsegueix reduir moltíssim el consum de bateria; en altres paraules, disminueix el seu *duty cycle*.

Per altra banda, les supertrames s'utilitzen també en el contexte de dispositius amb necessitats de baixa latència, on les associacions han de mantenir-se fins i tot si els nodes estan inactius per llargs períodes de temps.

Annex XXVII. Subcapa MAC d'IEEE 802.15.4e.

Com es pot veure a la Memòria, una la trama 802.15.4.e es divideix en tres parts, de manera semblant a 802.15.4: *MAC Header* (MHR), *MAC Payload* o *MAC SDU* i *MAC Footer* (MFR):

- A l'MHR existeixen els següents camps: *Frame Control* (encarregat d'especificar el tipus de trama); *Sequence Number* (per especificar el número identificador únic de trama); *Addressing Fields* (conjunt de camps que especifiquen l'identificador destinació de la PAN, l'adreça de destinació, l'identificador origen de la PAC i l'adreça d'origen); *Auxiliary Security Header* (camp opcional utilitzat per a donar seguretat); *IEs Header* (on es troben les capçaleres dels IEs, que es descriuen més endavant).

- Per la seva banda, a l'*MAC SDU* es transporten les dades d'usuari dels IEs i el *payload* propi de la trama.

- Per últim, l'MFR conté dos octets per al FCS, amb el qual es verifica la integritat de les dades rebudes.

En definitiva, la diferència respecte a la trama 802.15.4 radica en la presència dels camps variables per als IEs, que a la versió original no apareixen.

Annex XXVIII. Possibles millores per a IEEE 802.15.4e.

Sincronització de temps entre nodes

Com hem vist a la Memòria, l'estàndard 802.15.4 es basa en tècniques com ara TSCH per a una major fiabilitat i menor consum de potència. Amb aquesta tècnica, se suposa que tots els nodes d'una xarxa es troben sincronitzats a nivell de temps i aquest es dividideix en ranures de 10 ms típicament, on aquestes s'agrupen en supertrames que es repeteixen contínuament al llarg del temps. Una programació diu a cada mota què fer a cada ranura de temps: enviar a un veí, rebre d'un veí o dormir. La diversitat de canals s'obté especificant, per a cada ranura, quin canal –freqüència- fer servir. La comunicació fent servir el salt de canals permet reduir l'impacte d'interferències externes i l'esvaniment multicamí.

El problema d'aquesta tècnica és que, com s'ha dit, se pressuposa que tots els nodes estan sincronitzats, però a la pràctica això no passa si no hi ha cap mecanisme que "forci" una sincronització entre els nodes.

Avui dia, els microcontroladors que fan servir comunament els nodes, incorporen oscil·ladors de cristall com a rellotge intern. Aquests oscil·ladors suposen un bon compromís entre consum de potència, estabilitat de freqüència i cost. Tot i així, la freqüència del cristall pot veure's afectada per variables com ara diferències entre els fabricants, temperatura i tensió d'entrada, entre d'altres. Per altra banda, un oscil·lador de cristall es valora segons la seva freqüència d'estabilitat: per exemple, un cristall de 32 KHz valorat amb 30 ppm (parts per milió) tindrà un pols entre 32768.99 Hz i 32.767.01 Hz. Si ara suposem dues motes equipades amb aquest mateix cristall, això significaria que aquestes poden variar (*drift*) 30 ppm +30 ppm = 60 ppm com a màxim, l'una de l'altra (una perquè vagi més depressa i l'altra perquè vagi més lenta); en altres paraules, aquestes dues motes es desincronitzaran 60 µs cada segon, com a màxim.

Aquest fet implica que les motes han de ser resincronitzades periòdicament, si volem fer servir mecanismes com TSCH, donat que aquesta tècnica es basa en que tots els nodes transmissors estiguin programats per a transmetre en el mateix moment en una ranura (típicament 2ms en una ranura). Per permetre certa desincronització entre nodes, els receptors comencen a escoltar una mica abans de l'instant de transmissió i segueixen escoltant després del mateix. A aquest interval se li anomena "temps de guarda".

Per tant, si s'assumeix, per exemple, un temps de guarda d'1 ms i dos nodes equipats amb cristalls de 30 ppm cadascun, llavors això implicaria que les motes es desincronitzarien un segon cada 16 segons i, donat que aquestes no es poden comunicar si es desincronitzen passat el temps de guarda, això implica que s'han de resincronitzar periòdicament. En aquest cas el que es faria és, o bé realitzar una resincronització cada 16 segons o bé realitzar-la aprofitant quan es transmeten les dades d'usuari.

La següent equació serveix per determinar el màxim període per realitzar una sincronització (τ_{ka}) que es defineix com la relació entre el temps de guarda (T_g), dividit entre la variació o deriva entre els nodes (Δ_v):

$$\tau_{ka} = T_g/\Delta_v$$

Si es resincronitzen les motes en un període inferior a τ_{ka}, llavors significa que aquestes estaran sincronitzades dintre del temps de guardaT_g. En altres paraules, com major és el temps de guarda o menor és la deriva entre motes, major serà el valor de τ_{ka}, la qual cosa significa que les motes necessiten ser sincronitzades menys freqüentment. El problema d'augmentar el temps de guarda o bé de sincronitzar les motes més freqüentment del que es necessita (sobre-sincronització) és que, com que això implica tenir la ràdio encesa i aquesta consumeix potència, això farà augmentar el *duty cycle* i, per tant, la vida de les bateries minvarà. Per tant, el que s'ha d'aconseguir és que els nodes veïns estiguin sincronitzats però sense necessitat d'enviar paquets de sincronització; és a dir, sense necessitat de tener la ràdio encesa.

Una tècnica proposada per alguns investigadors és el que s'anomena "sincronització adaptativa" i que ja s'inclou en algunes implentacions de l'IEEE 802.15.4e, com per exemple en la pila de protocols del sistema operatiu OpenWSN. Aquesta tècnica consisteix, a grans trets, en mesurar, mitjançant un algorisme, la variació/deriva de rellotge que hi ha respecte del node veí i utilitzar aquesta informació per actualitzar –modificar- periòdicament el propi rellotge intern. Per exemple, un cop una mota calcula la deriva que hi ha respecte al seu veí, pot decidir "alentir" o "accelerar" el seu rellotge, depenent de si el rellotge intern va més ràpid o més lent que el del veí, respectivament. La deriva entre els nodes es calcularà entre dos missatges consecutius de *keep-alive* (per saber si el node veí segueix viu) entre els nodes, que poden succeir, per exemple, cada 60 segons.

D'aquesta manera, els dos rellotges estaran sincronitzats i no caldrà fer resincronitzacions tant freqüentment, fet que comportarà un cicle de treball més baix i major durada de les bateries. De fet, amb la sincronització adaptativa, s'aconsegueix reduir el temps de guarda deu vegades (per exemple, de 660 µs a tan sols 60 µs, prenent com a referència un interval entre *keep-alives* de 60 segons). Això comportarà, al seu voltant, una reducció del cicle de treball –quan les motes estan en mode espera o *idle*- en un factor de 10.

Altre apropament similar és per exemple l'ús de TASA (*Traffic Aware Scheduling Algorithm*), un algorisme per a IEEE 802.15.4 que permet configurar programacions d'enviament de dades depenent de la topologia de la xarxa i de la càrrega de tràfic de cada node [25]. D'aquesta manera, creant programacions *traffic-aware* (conscients del tràfic de dades que hi ha a la xarxa) s'aconsegueix reduir el nombre de vegades que les ràdios de les motes estan enceses i, per tant, disminuir el *duty cycle*.

Recolecció/escombrat d'energia

Tot i que no es tracta d'una millora de la subcapa MAC pròpiament dita, decidem explicar aquí una altra tècnica per a l'augment de la vida dels sensors, mitjançant el que s'anomena recolecció (*harvesting*) o escombrat (*scavening*) d'energia per part de les motes. La idea bàsica és senzilla: recollir energia des de l'exterior, per tant de poder carregar les bateries dels nodes i que aquests puguin treballar perpètuament, sense supervisió humana o canvi de bateries, o fins i tot poder treballar, sota certes condicions, sense cap tipus de bateria (amb condensadors o supercondensadors).

Per un cantó, podem diferenciar entre *Energy Harvesting* (quan la recol·lecció d'energia es fa des de fons d'energia regulars, ben caracteritzades i predictibles) i *Energy Scavening* (quan la font d'energia és desconeguda i/o altament irregular). En ambdós casos però, estaríem parlant sempre de recolliar l'energia present en l'entorn, per exemple l'energia ambiental, i transformar-la en energia elèctrica que pugui ser utilizada per les motes. Hi ha molts tipus de fonts d'energia que es poden fer servir per aquest fi i que es poden dividir en quatre grans grups:

- Solar: absorbir un gran nombre de fotons fent servir materials fotovoltaics. El major problema d'aquesta opció és que hi ha una gran dependència de l'exposició solar (per exmple, durant la nit o en dies ennuvolats no es pot garantizar una recol·leció d'energia el suficientment gran).

- Termal: la recol·lecció termoelèctrica es basa en les diferències de temperatura (per exemple en entorns amb grans diferències de temperatura entre el dia i la nit o en forns industrials, etc). Aquest tipus de dispositius poden ser molt petits i treballar en entorns difícils.

- Moviment: es pot fer servir aquesta opció quan els nodes estan subjectes a moviments, oscil·lacions i vibracions (electromagnètiques, piezoelèctriques, electroestàtiques). Els exemples són múltiples: en cas de terratrèmols; nodes situats en ponts per on passen vehicles; nodes en túnels per on passen trens; nodes que estiguin al mar -afectats pel moviment de les onades; nodes en vehicles en moviment; nodes en *wearables*, quan el propi cos humà es mou; fluxos d'aire, etc. L'energia és llavors recollida a través de la llei de Faraday referent a la inducció electromagnètica. L'avantatge d'aquest mètode és que, en certs escenaris, pot propocionar una energia constant.

- Electromagnètica: quan un node està exposat a un camp electromagnètic, l'energia radiant pot ser recollida fent servir inductors (bobines). Aquesta és una de les tècniques amb més futur i que s'està desenvolupant actualment, ja que ens trobem amb grans quantitats d'energia electromagnètica al voltant nostre, gairebé a tot arreu (per exemple, senyals RF de televisió, xarxes sense fils com ara Wi-Fi, torres de telefonia mòbil, etc.). Una antena receptora rep aquestes senyals i les bobines –un circuit generador de potència- les converteix en tensió contínua que es pot fer servir per alimentar els nodes.

La figura de sota mostra l'aspecte genèric d'un node amb sensors incorporats i amb una unitat de recol·lecció d'energia externa. Bàsicament, trobem cinc elements: un microcontrolador o processador del node; la memòria; el/s sensor/s que mesuren les variables –temperatura, humitat, llum, pressió, etc.; l'antena per enviar/rebre dades a altres nodes; per últim, el mòdul de recol·lecció d'energia (que pot ser des d'una altra antena fins una petita placa o pel·lícula solar, un microgenerador hidroelèctric, petits aeromotors, etc.)

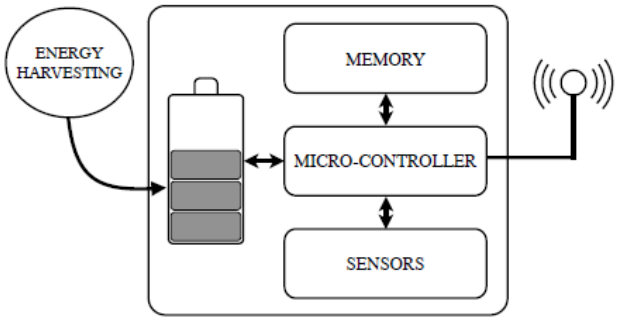


Figura 44. Components d'una mota amb sensors i mòdul de recol·lecció d'energia.

L'avantatge principal de la recol·lecció d'energia és que, si s'ha fet un estuti previ de l'energia present a l'ambient i aquesta és més o menys contíua/predictible llavors, en condicions normals, la bateria del node trigarà molt menys en carregar-se del que després trigaria en descarregar-se quan l'antena està activa. D'aquesta manera, ens asseguraríem una vida il·limitada de la mota pel que fa a energia.

Annex XXIX. Característiques tècniques de 6LoWPAN.

Compressió de capçaleres

Com ja s'ha comentat a la Memòria, IPv6 requereix que l'MTU sigui d'al menys 1280 bytes. Per la seva banda, la capa PHY de l'estàndard 802.15.4 definex una mida de màxima de paquet de 127 byte, incloent el *payload*.

- Com que la sobrecàrrega (*overhead*) per capçaleres MAC que té 802.15.4 és de 25 bytes, això deixa 127 – 25 = 102 bytes útils. Aquests 25 bytes provenen de*: Frame control* (2 bytes) + *Sequence Number* (1 byte) + *Source/Destination PAN IDs* i *Source/Destination addresses* (20 bytes) + FCS (2 bytes).

- D'aquest valor de 102 bytes, hem de treure fins a 21 bytes adicionals, necessaris per a les capçaleres de seguretat MAC (per exemple, AES-CCM-128 fa servir 21 bytes, AES-CCM-64 fa servir 13 bytes i AES-CCM-32 fa servir 9 bytes), deixant llavors 102 – 21 = 81 bytes útils.

- A nivell IPv6 hi ha 40 bytes de capçaleres, deixant el total llavors en 81 – 40 = 41 bytes.

- Per últim, s'han de treure les capçaleres de les capes TCP i UDP (20 bytes en el primer cas o 8 bytes en el segon). Això ens deixa un total útil per a *payload* de la capa d'aplicació de 41 – 20 = 21 bytes (TCP) o 41 – 8 = 33 bytes (UDP). Aquests valors, òbviament, són molt menors del que es desitjaria que es veu que, a cada paquet 802.15.4, tenim un 83.5% de capçaleres i únicament un 16.5% de dades útils. Faci's notar que, en LLNs, es farà servir per defecte UDP, per ser un protocol no orientat a connexió i que per tant comporta un menor consum d'energia i un menor cicle de treball dels nodes, al no ser necessaris els ACKs.

Per tant, per tal de transportar IPv6 de manera eficient sobre LLNs, les capçaleres IPv6 s'han de comprimir. L'objectiu d'aquesta compressió es impedir que es transmeti informació que es coneix de manera implícita o que es por recuperar d'alguna altra manera. Alguns exemples d'aquesta compressió són:

- El camp *Version* que indica la versió del protocol és sempre IPv6; per tant, aquest camp és pot ometre.

- Els camps *Traffic Class* i *Flow Label* no són d'aplicació en LLNs de malla i per tant es poden ometre; també es pot decidir deixar-los en un únic bit, si els dos camps tener valor 0.

- El camp *Payload Lenght* és redundant i es pot ometre ja que aquesta informació ja es pot extreure de la trama IEEE 802.15.4.

- El camp *Next Header* es pot ometre si no hi ha cap altra capçalera següent a la trama. En altres casos, es pot comprimir a 2 bits (si els paquets que es transporten són TCP, UDP o ICMPv6).

- El camp *Hop Limit* no es pot comprimir i ha de ser transportat en la seva totalitat.

- Els camps *Interface Identifier* (IID) per a les adreces d'origen i destinació, que són de 64 bits cadascun, s'ometen si la destinació els pot derivar de l'adreça de la capa de xarxa a la trama 802.15.4 o del *Mesh Addressing Header*.

- Els camps d'adreça IPv6 d'origen i destinació poden ser ja coneguts (per exemple, si els dos nodes estan a la mateixa xarxa local –`FE80::`- i es fa servir el mateix prefix per a tota la xarxa). En aquest cas, el prefix s'escurça fins a 1 únic bit per a cada camp.

En general, un datagrama IPv6 encapsulat en LoWPAN es "prefixa" amb una pila de capçalera d'encapsulació (*Encapsulation Header Stack*). Cada capçalera de la pila comença amb un camp *Header Type* seguit per cap o més camps de capçalera. A la següent figura es mostra l'exemple més senzill, on es pot veure el *payload* IPv6 "prefixat" per la capçalera IPv6 (que porta dintre els seus propis camps) i abans, per un camp anomenat *IPv6 Distpach*:

```
+---------------+-------------+---------+
| IPv6 Dispatch | IPv6 Header | Payload |
+---------------+-------------+---------+
```

Figura 45. Format genèric de trama IPv6 en LoWPANs.

El contingut del camp *IPv6 Dispatch* indica el tipus de capçalera o *Header Type* que està emetent. Els valors més comuns d'aquest camp són:

- 01 000001: indica que la capçalera són adreces IPv6 sense comprimir,
- 01 000010: indica que la capçalera IPv6 porta compressió HC1,
- 01 010000: indica una capçalera de difusió (*broadcast*) BC0,
- 01 111111: indica que segueixen més bytes de *distpach* adicionals,
- 10 xxxxxx: indica que s'envia una capçalera d'encaminament de malla (*mesh routing*),
- 11 000xxx: indica que s'envia una capçalera de fragmentació (la primera),
- 11 100xxx: indica que s'envia una capçalera de fragmentació (després de la primera).

La figura de sota mostra un datagrama IPv6/UDP encapsulat en LoWPAN, en el pitjor escenari possible, és a dir, quan no es pot comprimir res:

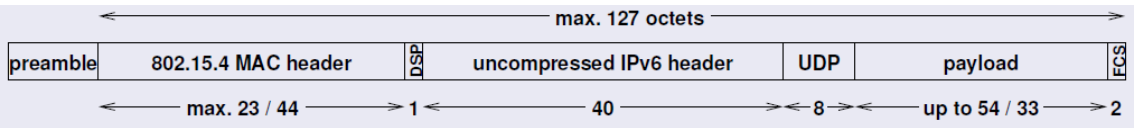


Figura 46. Format de trama 6LoWPAN quan no es pot comprimir res [35].

Per la seva banda, la figura de sota mostra la millor situació possible, quan el datagrama IPv6/UDP es pot comprimir:

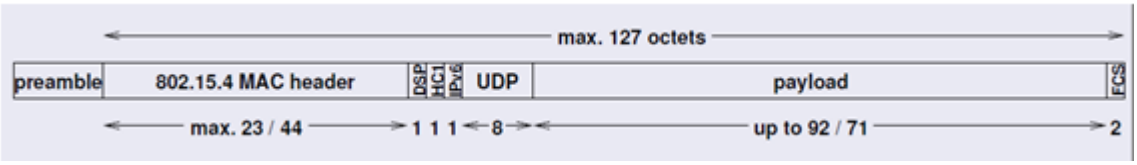


Figura 47. Format de trama 6LoWPAN quan es pot comprimir la capçalera IPv6 [35].

En el primer cas (sense compressió), veiem que únicament queden 33 o 54 bytes disponibles per a dades d'usuari, en funció de si es fa servir seguretat o no. Això significa que el contigut del camp DSP (*IPv6 Distpach*) serà 01 000001. Per la seva banda, en el segon cas (amb compressió), pot haver-fi fins a 71 o 92 bytes de *payload*, en funció de si es fa servir seguretat o no. Això significa que el camp DSP tindrà el valor 01 000010, indicant que la capçalera IPv6 porta compressió HC1. Fixem-nos que, parlant amb propietat i, tal i com s'ha vist abans, en realitat no es "comprimeix" la capçalera sinó que es codifica d'una altra manera, per tal d'ocupar menys espai; per això de vegades es parla de "codificació" en comptes de "compressió", indistintament.

Adicionalment, després d'una codificació HC1 (compressió de la capçalera IPv6) pot venir una codificació HC2 (compressió de la capçalera UDP). Qualsevol camp de capçalera que no es pugui comprimir s'inclou després de les etiquetes HC1 i HC2.

Per altra banda, aquests formats de compressió són els definits per l'RFC4944, mentre que el nou RFC6282 parla, en canvi, de compressions HC (*IPv6 Header*) i NHC (*Next-Header*). Aquest darrer RFC també incorpora compressió per a extensions IPv6 i compressió d'adreces *multicast* compactes.

Fragmentació/reensamblatge

A més de comprimir les capçaleres, 6LoWPAN també s'encarrega de fragmentar els datagrames IPv6 que siguin més grans del màxim *payload* permès, enviant-los en diverses trames 802.15.4. Òbviament, també s'encarrega del seu reesamblatge a la destinació. Aquest procediment es realitza a la capa d'enllaç. En concret, el primer fragment incorpora una capçalera que inclou la mida del datagrama (11 bits) i una etiqueta de datagrama (16 bits). Tots els fragments que s'envien després del primer inclouen una capçalera amb la mida del datagrama, l'etiqueta de datagrama i un *offset* o desplaçament (8 bits). A més, es defineix un temps límit de 60 segons per a reensamblar tots els fragments. A la figura de sota es pot veure l'estructura d'aquesta capçalera de fragment, per a fragments *N* amb *N* > 1:

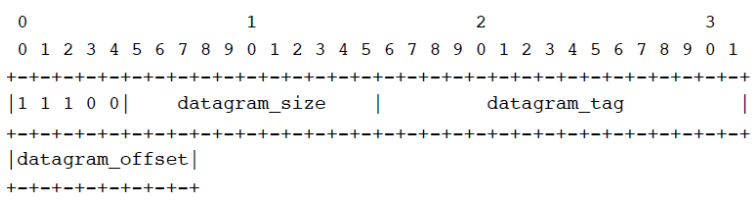


Figura 48. *Fragment Header* per a datagrames fragmentats (segon fragment i més).

Per la seva banda, a la figura de sota es pot veure un exemple de datagrama IPv6 que es fragmenta en *N* trames 802.15.4:

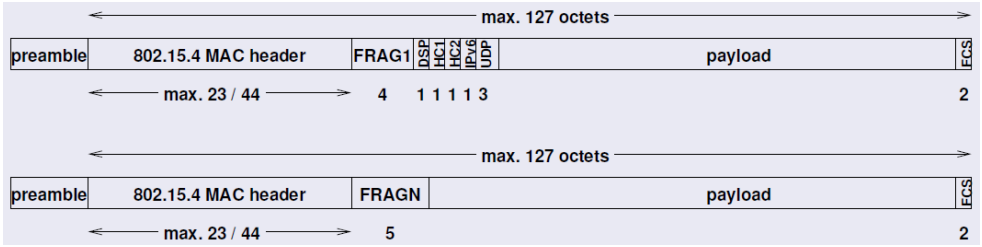


Figura 49.Format de trama 6LoWPAN quan es pot comprimir la capçalera IPv6 [35].

Com es pot apreciar, el primer fragment té una capçalera de 4 bytes en total, anant seguidament el camp *Dispatch IPv6* que ja s'ha vist a l'apartat anterior (i que indica el tipus de capçalera que s'està enviant), així com les capçaleres comprimides IPv6 (HC1) i UDP (HC2). Per la seva banda, la trama *N* –que inclou el fragment *N* del datagrama IP- té una primera capçalera que ocupa un byte més -5 bytes en total- ja que s'ha d'incloure el desplaçament en relació al fragment original; en canvi, no s'han d'incloure de nou les capçaleres DSP, HC1, HC2, IPv6 i UDP, per la qual cosa queda més espai per al *payload*.

Per tant, en general, un datagrama IPv6 fragmentat amb LowPAN i amb capçalera IPv6 comprimida, tindrà la següent estructura de trama:

Figura 50.Format de trama 6LoWPAN quan el datagrama IPv6 està fragmentat.

El principal problema de la fragmentació és que el rendiment global disminueix. En general, el rendiment en l'enviament de paquets IPv6 grans que s'han de fragmentar sobre xarxes LLN és bastant pobre: per un cantó, degut a que els fragments que es perden/no arriben a la destinació causen que s'hagi de retransmetre el datagrama IPv6 sencer; per altra banda, degut al baix ample de banda i el retard propis del canal sense fils. És per aquesta raó que els protocols d'aplicació –capa superior- haurien d'evitar a tota costa la fragmentació, per exemple comprimit el *payload* IP.

D'aquesta manera, si anomenen p a la probabilitat incorrelada de pèrdua de paquets i n al nombre de fragments del datagrama IPv6, llavors tenim que la probabilitat de pèrdua de datagrames és de $1-(1-p)^n$. Si grafiquem aquesta funció per a diferents valors de p (0.1, 0.2, 0.3) s'obté el següent [57]:

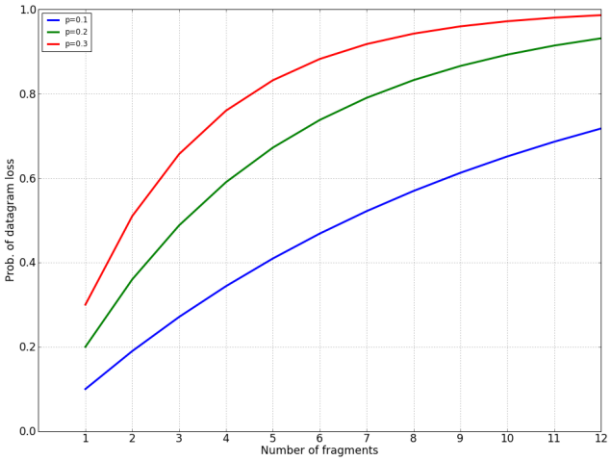


Figura 51. Funció de probabilitat de pèrdua de datagrames IPv6.

Segons la gràfica, s'observa visualment que, amb una probabilitat de pèrdua d'un paquet d'únicament un 10%, si el nombre de fragments del datagrama és de 12, llavors la probabilitat d'haver de retransmetre el mateix és superior al 70%. De la mateixa manera, si la probabilitat de pèrdua d'un paquet augmenta fins el 30%, llavors amb quatre fragments ja s'arriba a una probabilitat de retransmissió del datagrama del 80%.

Reenviament a nivell 2

Com s'ha dit abans, 6LowPAN permet el reenviament (*forwarding*) de *payloads* 6LoWPAN sobre múltiples salts de ràdio, a nivell dos (capa d'enllaç); és a dir, sense fer ús de les funcionalitats d'encaminament (*routing*) pròpies del nivell 3 (capa de xarxa). Per poder aconseguir això, es fa ús de una capçalera anomenada *Mesh Addressing Header* (capçalera d'adreçament de malla), que inclou tres camps: *Hop Limit* (Límit de Salts), *Source Address* (Adreça origen) i *Destination Address* (Adreça Destinació). El primer camp és anàlog al d'IPv6 amb el mateix nom i serveix per limitar el nombre de salts per al reenviament; cada cop que es passa per un node, el valor del camp decrementa en una unitat, fins que s'arriba a zero, moment en el qual la trama no es reenvia més i es perd. Per la seva banda, les adreces d'origen i destinació indican els extrems (*endpoints*) d'un salt IP. Aquestes adreces són del tipus 802.15.4 (nivell d'enllaç) i poden ser tant curtes com exteses.

A la figura de sota es pot veure l'estructura d'aquesta capçalera:

1	0	O	F	Hops left (4 bits)	Originator address (16-64 bits)	Final address (16-64 bits)

Figura 52.Estructura estàndard del *Mesh Addressing Header*.

Els dos primers bits (10) corresponen al tipus de capçalera o *Header Type*. Seguidament, el tercer i quart bits indican quin mode d'adreçament fer servir per a les adreces d'origen i destinació. Per la seva banda i, per defecte, amb 4 bits en el camp *Hop Limit* es pot configurar un màxim de fins a 15 salts –valor que hauria de ser més que suficient per a gairebé qualsevol xarxa- encara que, si fos necessari, es podrien configurar 4 bits adicionals –fent un total de 8 bits- per permetre un màxim de 255 salts. Això es pot fer afegint el valor 0xF (que significa *All Nodes*) després del quart bit de la capçalera. D'aquesta manera, el *mesh header* quedaria així:

1	0	O	F	0xF	Hops left (8 bits)	Originator address (16-64 bits)	Final address (16-64 bits)

Figura 53. *Mesh Addressing Header* ampliat per a 255 salts màxims.

Per tant i, a mode de resum, en la figura següent es pot veure:

- PDU a nivell PHY (127 bytes màxims de *payload*),
- PDU a nivell MAC i com s'encapsulaaquesta dins del *payload* PHY,
- Encapsulació, amb 6LowPAN, d'un datagrama IPv6 dins del *payload* MAC:
    - En el primer cas, s'encapsula un *payload* IPv6 i una capçalera IPv6 comprimida,
    - En el segon cas, s'encapsula el*payload* IPv6, amb una capçalera comprimida IPv6 i, a més, una altra capçalera indicant que es tracta d'un datagrama fragmentat,
    - En el tercer i darrer cas, s'encapsula el *payload* IPv6, la capçalera IPv6 omprimida, la capçalera indicant datagrama fragmentat i una altra capçalera indicant el reenviament de datagramal entre nodes a nivell 2,

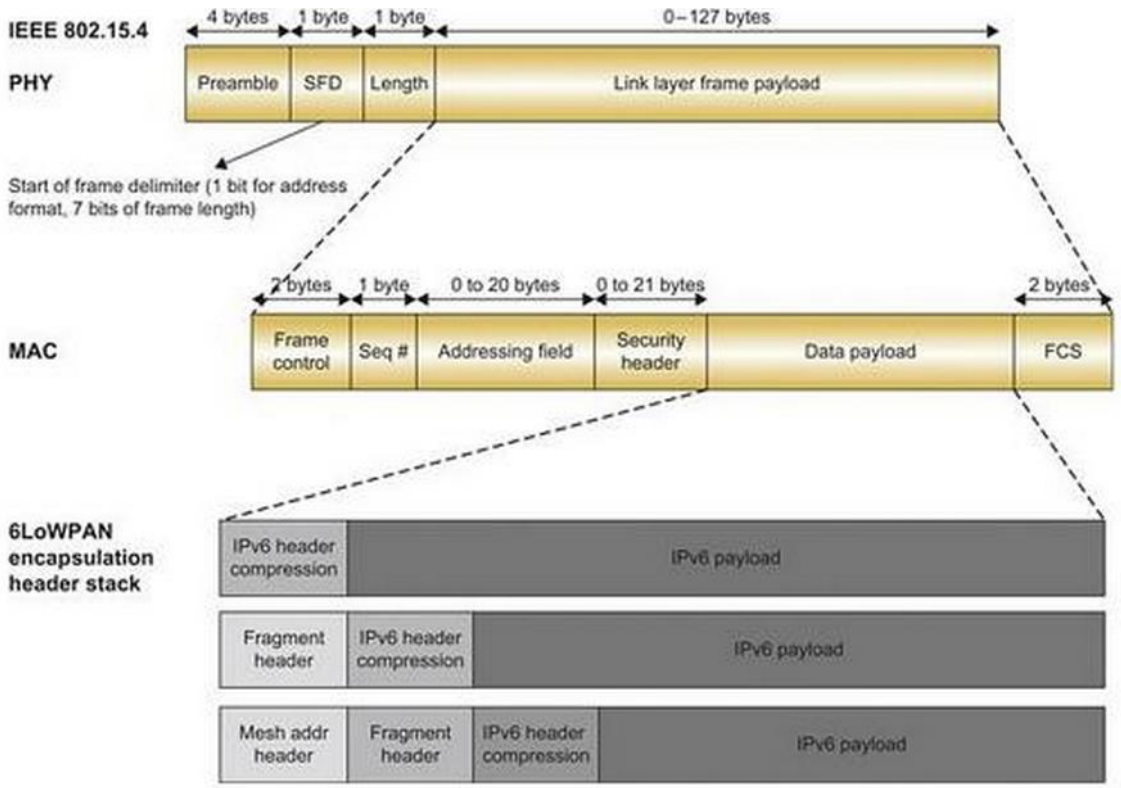


Figura 54. PDUs a nivell PHY i MAC i possibles encapsulacions 6LoWPAN.

Cal destacar, un cop més, que aquest reenviament de trames entre nodes es produeix a nivell dos -en la capa d'enllaç- en contraposició a l'encaminament tradicional, que es produeix a nivell tres –en la capa de xarxa. De fet, 6LowPAN, com que té un rol de capa d'adaptació entre l'enllaç i la xarxa, pot suportar els dos tipus d'encaminament, a qualsevol de les dues capes. La figura de sota mostra aquests dos apropaments:

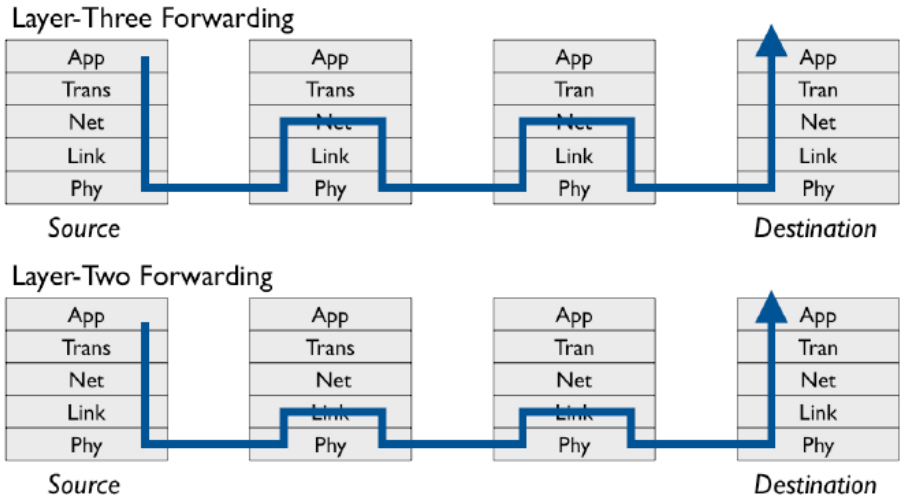


Figura 55. Reenviament a nivell d'enllaç i a nivell de xarxa.

En el primer cas (reenviament a nivell 2) es parla de mode *Mesh-Under* mentre que en el segon cas (reenviament a nivell 3) es parla de mode *Router-Over*. Amb el primer mètode, la pila de xarxa no realitza cap encaminament IP dintre de LoWAN; en canvi, la capa d'adaptació busca "emmascarar" la manca d'una difusió completa a nivell PHY mitjançant un reenviament i encaminanent transparent de paquets dintre de LoWAN. El desafiament es troba en que l'emulació de l'enllaç lògic és significativament més complexa que en infraestructures tradicionals basades en topologies 802.11. Les topologies de malla requereixen un reenviament sobre múltiples salts ràdio; a més, ha d'haver-hi un *multicast* a nivell d'enllaç local que permeti entregar els paquetes a tots els nodes de la LoWPAN sencera. Molts dels mecanismes que existeixen per formar, mantenir i diagnosticar l'encaminament han de ser recreats a la capa d'enllaç perquè la malla pugui operar de manera confiable.

De manera alternativa, però, en el segon cas (*Route-Over*) tenim que l'encaminament pot ser efectuat a la capa IP, amb cada node actuant com un *router* IP. De fet, es pot veure com una colecció d'enllaços d'abast local sobreposats, amb cada enllaç local definit per la seva connectivitat ràdio. De manera diferent al mode *Mesh Under*, ara es suportan mecanismes de reenviament de nivell 3 dins de la LoWPAN que poden fer servir les capacitats pròpies d'IP, com ara encaminament IPv6 i ICMPv6 per a configuració i gestió. El mode *Route-Over* també deixa que els protocols d'encaminanent IP abastin diferents tecnologies d'enllaç, permetent una millor integració en xarxes més capaces. També deixa que els protocols basats en IP limitin la comunicació IP a un abast ràdio local, en comptes de a tota la xarxa.

Annex XXX. Principals protocols d'encaminament reactiu.

AODV

AODV són les sigues d'*Ad-hoc On Demand Distance Vector Routing (*encaminament específic sota demanda de vector de distància). Es tracta d'un protocol d'encaminament reactiu molt utilizat a MANETs (*Mobile Ad Hoc Networks*) i altres xarxes sense fils; de fet, és el protocol d'encaminament que fa servir ZigBee.

Quan un node rep aquest missatge i ja té una ruta cap al node destinació, llavors envia un missatge cap enrrere a través d'una ruta temporal, cap al node peticionari. Llavors, el node origen comença utilitzant la ruta que conté el menor número de salts a través d'altres nodes. Per la seva banda, les entrades de la taula d'encaminament que no s'utilitzen es reciclen al cap d'un temps (s'eliminen si no es fan servir).

Quan un node falla/cau –i per tant no funciona la ruta- llavors s'envia un error d'encaminament cap al node transmissor i el procés es repeteix de nou amb altra ruta que no faci servir aquest node.

La complexitat d'aquest protocol radica en intentar minimitzar el nombre de missatges que s'envien per la xarxa, per tal de preservar la capacitat de la mateixa (és a dir, s'intenta evitar tot l'*overhead* que es pot). D'aquesta manera, cada petició de ruta té un número de seqüència; els nodes fan servir aquest número de tal manera que no han de repetir les peticions de ruta que jan han deixat passar abans.

Altra característica és que les peticions de ruta tenen un TTL (*Time To Live* – Temps de Vida) que limita quantes vegades es poden retransmetre. Una altra característica és que si una petició de ruta falla, llavors no es pot enviar la mateixa petició fins que no ha passat el doble de temps des del *timeout* de la primera petició.

Els principals avantatges d'AODV són:

- No crea tràfic extra per a comunicació entre enllaços ja existents.

- Donat que l'encaminant Vector Distància és simple, no requereix molta memòria ni potència de càlcul (un altre exemple de protocol Vector Distància és RIP -*Routing Infromation Protocol*- que fins l'any 1988 va ser l'únic protocol d'encaminament a Internet).

- Les rutes s'estableixen sota demanada i els números de seqüència s'apliquen per trobar la darrera ruta cap a la destinació.

Per la seva banda, els inconvenients principals d'aquest protocol són:

- Tal i com s'ha dit abans, AODV necessita més temps per establir una connexió que un protocol d'encaminament proactiu.

- La comunicació inicial per establir una ruta és més "pesada" que altres alternatives d'encaminament (hi ha un retard inicial més gran que comporta un major *duty cycle*)

- Els nodes intermitjos poden portar rutes inconsistents si el número de seqüència de l'origen és molt antic i els nodes intermitjos tenen un número de seqüència més alt – pero no el darrer- de la destinació, tenint per tant entrades antigues/inservibles (*stale entries*, en anglès).

- Múltiples paquets de tipus *RouteReply* (resposta de ruta) en resposta a un únic paquet de tipus *RouteRequest* (petició de ruta) poden portar a un gran *overhead* de control.

- Es consumeix ample de banda innecesari degut a la necessitat de balises periòdiques.

Als diagrames de la pàgina següent es pot veure un senzill exemple del funcionament d'AODV: en la primera figura, es veu com un paquet de Petició de Ruta (RREQ) es propaga per tota la xarxa, a través dels nodes intermitjos, fins arribar al node de destinació; per la seva banda, la segona figura mostra com s'envia un paquet de tipus Reposta de Ruta (RREP) des de la destinació fins a l'origen, passant pels nodes intermitjos.

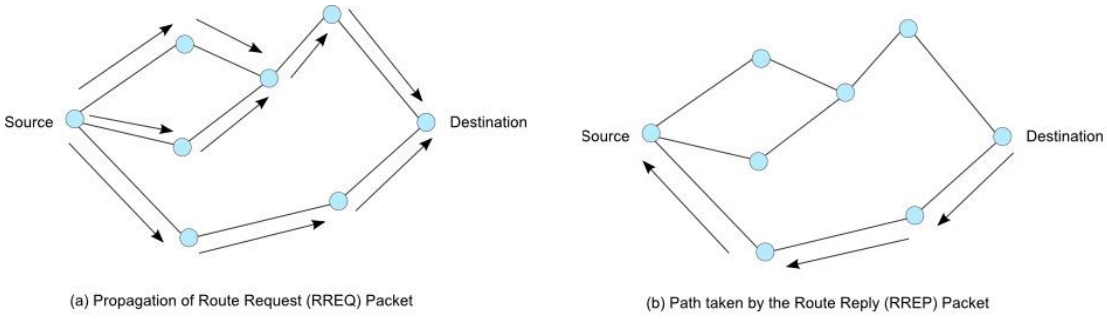


Figura 56. Exemple d'encaminament amb AODV.

Per últim, existeixen diverses implementacions/modificacions d'AODV, com ara TinyAODV (inclosa en el sistema operatiu TinyOS) i AODVjr (ADOV *Junior*), que són simplificacions d'AODV i que estan dissenyades específicament per executar-se en dispositius amb restriccions de memòria i potència de càlcul, com ara les motes d'una LLN.

DSR

DSR són les sigues de *Dynamic Source Routing* (Encaminament d'Origen Dinàmic). Igual que AODV, és un protocol d'encaminament reactiu per a xarxes sense fils de malla. És similar a AODV pel fet de que ambdós formen rutes sota demanda quan un node emissor fa una petició d'una. La diferència principal és que DSR fa servir encaminament fixat a l'origen (*Source Routing*) en comptes de basar-se en una tabla d'encaminament en cada dispositiu intermig.

Determinar rutes des de l'origen suposa haver d'acumular l'adreça de cada dispositiu intermig entre l'origen i la destinació, durant el procés de descobriment de ruta. Aquesta informació acumulada de la ruta s'emmagatzema en una cau (*cache*, en anglès) en els nodes que processen els paquets de descobriment de ruta. Llavors, les rutes apreses s'utilitzen per encaminar els paquets. Per acomplir l'encaminament a l'origen, els paquets encaminats contenen l'adreça de cada dispositiu que el paquet atravessarà, la qual cosa resulta en una sobrecàrrega molt alta per a camins molts llargs o adreça de xarxa llargues, com passa per exemple a IPv6. Per evitar aquesta situació, es pot fer servir una opció que defineix un *Flow ID* (identificador de fluxe) de manera que els paquets es reenvien únicament salt a salt, no fent servir per tant l'encaminament a l'origen.

Com que aquest protocol es basa veritablement en *source routing*, això significa que tota la informació d'encaminament es manté i actualitza constantment als nodes origen. El procés té, a grans trets, dues fases únicament: *Route Discovery* (descobriment de ruta) i *Route Maintenance* (manteniment de ruta). Per la seva banda, els missatges *RouteReply* únicament es generen quan un missatge ha arribat al node destinació. Per a poder retornar aquest *Route Reply*, el node destinació ha de conèixer la ruta al node origen: si aquesta ruta es troba ja en la cau d'encaminament del node, aquesta es fa servir; en cas contrari, la destinació mira el registre de ruta que s'ha trobat en la capçalera del missatge *RouteRequest* i fa servir la mateixa ruta pero al revès (això requereix que tots els enllaços siguin simètrics).

En cas d'error en la transmissió, la fase de *Route Maintenance* s'inicia allà on es generen els paquets *Router Error*; d'aquesta manera, s'elimina el sat de la cau d'encaminament del node.

DSR va de ser dissenyat per tal de limitar l'ample de banda consumit pels paqutes de control, mitjançant l'eliminació des missatges periòdics d'actualització de taules d'encaminament que es fan servir en els protocols –proactius- impulsats per taules (*table-driven*) com ara OLSR i DSDV, que veurem més endavant.

A més, com ja s'ha comentat abans, DSR no fa servir balises i per tant no necessita transmetre paquets balisa (HELLO) periòdics, que són utilitzats per un node per informar de la seva presència als nodes veïns (aguns exemples de protocols que fan servir balises són ZRP i OLSR). En canvi, el que sí que fa DSR –i, de fet, tots els protocols d'encaminament sota demanda- és establir les rutes a través de la inundació de la xarxa amb missatges *RouteRequest*. Llavors, el node destinació, en rebre aquest missatge, respon amb un paquet *RouteReply* a l'origen, que inclou tota la ruta atravessada pel paquet *RouteRequest*.

Els principals avantages d'aquest mètode d'encaminament són:

- No es necessita inundar la xarxa periòdicament amb missatges d'actualització de taules d'encaminament.

- Únicament es determina la ruta quan aquesta es necessita (no es necessita saber la ruta a tots els altres nodes de la xarxa si mai no s'ha d'enviar cap paquest a cap d'aquests nodes)

- Els nodes intermitjos fan servir la informació de la seva cau d'encaminament, reduïnt l'*overhead* de missatges de control.

Per la seva banda, els inconvenients de DSR són:

- El mecanisme de manteniment de ruta no repara un enllaç trencat, sinó que es calcula tota una nova ruta sencera.

- Informació desactualitzada en la cau d'encaminament pot resultar en inconsistències durant la fase de reconstrucció de ruta.

- Al igual que AODV, el retard durant la configuració de la connexió és superior al dels protocols proactius impulsats per taules.

- El protocol es comporta bé en entorns estàtics o amb baixa mobilitat però el rendiment decau ràpidament si la xarxa és molt canviant (nodes que es treuen contínuament, nodes mòbils, etc.

- Durant el mecanisme de *source-routing* es produeix una sobrecàrrega considerable, directament proporcional a la longitud de l'enllaç (ineficient quan s'han de fer molts salts).

ABR

ARB són les sigles de *Associativity Based Routing* (Encaminament Basat en Associativitat). Aquest protocol defineix una nova mètric per a encaminament coneguda com a "grau d'estabilitat d'associació". És un protocol lliure de bucles, punts morts i paquets duplicats. Amb ARB, es selecciona una ruta en funció dels estats d'associativitat dels nodes. Les rutes selecciones d'aquesta manera acostumen a ser, per tant, de llarga durada.

Amb ABR, tots els nodes generan balises periòdiques per indicar de la seva existència (aquí ja veiem una gran diferència amb AODV i DSR). Quam un node veí rep una balisa, llavors actualitza les seves taules d'associativitat. Per cada balisa rebuda, un node incrementa el seu comptador d'associativitat respecte del node d'on rep la balisa. Estabilitat d'associacióp significa, en realitat, estabilitat de la connexió d'un node respecte d'altre node, tant en temps com en espai. Un valor alt del comptador d'associativitat indica que el node veí es poc mòbil, mentre que un valor baix d'associativitat indica que el node és molt mòbil. Els comptadors d'associativitat es posen a zero quan un node veí o el mateix node és mouen fora de la zona de proximitat. Per tant, el principal objectiu d'ABR és trobar rutes de llarga durada en xarxes mòbils sense fils (MANETs).

En ABR es distigueixen tres fases: *Route Discovery*, *Route Reconstruction* (RRC) i *Route Deletion*.

- La primera fase és una cicle compost per una consulta de difusió i una espera de resposta (BQ-REPLY). El node origen fa una difusió d'un missatge BQ en busca de

nodes que tinguin una ruta a la destinació. Un node no reenvia una petició BQ més d'una vegada. Quan un node intermig rep un missatge BQ, afegeix la seva adreça i els seus comptadors d'associativitat al paquet de consulta. El proper node que rep el paquet elimina els comptadors d'associativitat del seus veïns "de pujada" (en la direcció d'arribada a la destinació) i únicament deixa l'entrada corresponent a ell mateix i el seu node directe de pujada. D'aquesta manera, cada paquet que arriba a la destinació contindrà els comptadors d'associativitat de tos els nodes de la ruta, des de l'origen fins a la destinació. La destinació pot, llavors, seleccionar la millor ruta de tornada, mitjançant l'examinació dels comptadors d'associativitat de cadascun dels camins. Si hi ha diversos camins amb el mateix grau total d'estabilitat d'associació, es seleccionarà la ruta amb el menor nombre de salts. Un cop s'ha escollit una ruta de tornada, la destinació envia un paquet REPLY cap a l'origen. Els nodes del camí que reben el paquet REPLY marquen les seves rutes com a vàlides. Tota la resta de rutes esdevenen inactives i, per tant, s'evita la possibilitat de paquets duplicats a la destinació.

- Per altre cantó, la fase RRC consisteix en un descobriment parcial de ruta, esborrat de rutes invàlides, actualitzacions de rutes vàlides i descoberiment de noves rutas, depenent de quins nodes de la ruta es mouen. Per exemple, si el node origen es mou, això resulta en un nou BQ-REPLY perquè el protocol d'encaminament s'inicia a l'origen. S'utilitza el missatge Route Notification (RN) per esborrar les entrades de ruta associades amb els nodes "de baixada" (de la destinació a l'origen). Per la seva banda, quan la destinació és la que es mou, el node de pujada més proper esborra la seva ruta.

- Per últim, quan una ruta ja descobera no es necessita més, llavors el node origen inicia una difusió de RD (esborrat de ruta). Tots els nodes de la ruta esborren de la seva taula d'encaminament esborren l'entrada corresponent a aquesta ruta.

Es pot concloure que ABR és un protocol d'encaminament reactiu (únicament es mantenen les rutes que realment es necessiten/desitgen), especialment indicat per a xarxes sense fils amb dispositius mòbils, ja que es basa en el grau d'associativitat d'un node amb els seus nodes veïns. Es tracta d'un protocol d'encaminament iniciat a l'origen (*source-initiated routing*) i representa un compromís entre un encaminament per difusió i un encaminament punt a punt. ABR no fa servir reconstrucció de rutes basada en informació de rutes alternatives sinó que les decisions d'encaminament s'efectuen a la destinació, que selecciona i fa servir únicament la millor ruta i deixa tota la resta de possibles rutes com a passives/inactives, evitant per tant paquets duplicats. La ruta escollida tendeix a ser de llarga durada, degut al seu alt grau d'associativitat.

DYMO (AODV v2)

DYMO són les sigles de *Dynamic MANET On-Demand* (MANET dinàmica sota demanda). Es tracta del succesor del protocol AODV, ja explicat abans (de fet, la denominació oficial actual del protocol és, en realitat, AODVv2). Per tant, DYMO opera de manera molt similar a AODV, amb la particularitat de que no afegeix cap característica extra ni extèn el protocol original sinó que, ans al contrari, el simplifica, mantenint el mateix mode d'operació bàsic. DYMO es troba en fase d'esborrany per l'IETF i es preveu que a curt termini esdevingui formalment un estàndard per la qual cosa passarà a ser el protocol més utilitzats a les MANETs.

Com en qualsevol altre protocol d'encaminament reactiu, DYMO consisteix en dues operacions o fases principals: *Route Discovery* i *Route Maintenance*. Les rutes es descobreixen únicament sota demanda, quan un node origen vol enviar un paquet a un node destinació que encara no té en la seva taula d'encaminament. Llavors, un missatge *RouteRequest* (RREQ) inunda tota la xarxa fent servir multidifusió i, si el paquet arriba a la destinació, un missatge de resposta o *RouteReply* (RREP) és enviat de tornada cap a l'origen, contenint el camí acumulatiu descobert.Per tant, quan el missatge RREP és rebut ler l'origen, ja s'ha registrar una ruta ens ambdós sentits, que queda gravaba als nodes intermitjos, i l'intercanvi de dades pot començar. Per la seva banda, el manteniment de rutes es realitza per prevenir purgar prematurament rutes actives de la taula d'encaminament o bé per esborrar rutes trencades –bé perquè incorporen un node caigut o que ja no està a la xarxa- prevenint per tant la pèrdua de paquets.

Cada entrada en la taula d'encaminament consta dels següents camps: *Destination Address*, *Sequence Number*, Hop Count, *Next Hop Address*, *Next Hop Interface*, *Is Gateway*, *Prefix, Valid Timeout*, *Route Delete Timeout*.

La principal diferència entre AODVv2 i AODV és que, amb la nova versió, l'origen (node que envia el RREQ) rep no únicament la informació d'encaminament de tots els nodes intermitjos, en contraposició a AODV, on únicament es rebia la informació sobre el salt següent. Aquesta diferència queda clarament ilustrada a la següent figura:

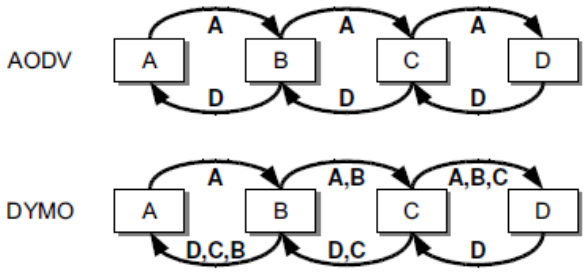


Figura 57. DYMO Vs AODV.

Per la seva banda, també existeix una extensió al protocol, denominada DT-DYMO (*Delay-Tolerant* DYMO) que proporciona un tercer mecanisme, apart del *Route Discovery* i *Route Maintenance*, pel qual es pot entregar un paquet fins i tot quan hi ha desconnexions regionals/temporals a la xarxa.Per aconseguir això, es necessiten camps adicionals als missatges RREQ i RREP (als primers, s'afegeix un camp amb la mínima probabilitat de trobar la destinació; als segons, s'afegeix un camp amb la probabilitat actual d'encontre del node i un altre per indicar el node buscat). A més, els paquets que no es poden entregar temporalment s'han d'emmagatzemar en una llista de dades; en el moment que es troba la destinació, són alliberats al canal.

També existeixen altres propostes d'extensió, com ara EA-DYMO (*Energy-Aware DYMO*) on, a més, es considera la càrrega mitjana de tràfic a la xarxa, així com el factor d'energia, per a cada ruta que s'ha de calcular.

Per últim, existeix una darrera versió de DYMO, anomenada DYMO-low, focalitzada a 6LoWPAN, és a dir, a encaminament de paquets IPv6 en LLNs. Bàsicament, es tracta d'una simplificació de DYMO, amb la finalitat d'estalviar energia en els nodes. Algunes de les modificacions que conté són:

- No existeix acumulació de ruta.
- Únicament el node destinació pot respondre.
- Es limita el nombre de missatges de control.
- S'utilitza LQI *(Link Quality Indicator*) com a mètrica per calcular el cost total de la ruta; no s'utilitzen missatges HELLO ni números de seqüència.
- S'obvien els missatges UERR (*Unsupported Element Error*; s'envien quan l'element rebut no s'entèn o no pot ser manegat pel node que el rep)
- Es permeten múltiplesmissatges RE (*Routing Element*) dins d'un mateix paquet, reduïnt possiblement d'aquesta manera el número de missatges de control, per agregació.
- S'inserta el camp *Error Code* dins dels missatges RERR.

ACOR

ACOR són les sigles d'Encaminament Sota Demanda amb Control d'Admissió Habilitat (*Admission Control Enabled On-Demand Routing*). Es tracta d'un protocol d'encaminament reactiu per a MANETs dissenyat per a suportar QoS en una ruta extrem a extrem.

ACOR es basa, per un cantó, en funcions de cost locals a cada node i, per altre cantó, en una funció de cost global; d'aquesta manera, es representa el cost total extrem a extrem d'una ruta. A més, s'incorpora un mecanisme simple de control d'admissió per a reserva implícita de recursos, adaptat a canvis freqüents en la topologia de xarxa. Aquesta ruta amb QoS i sota demanda es crea sense haver de mantenir informació actualitzada sobre encaminament o sense haver d'intercanviar periòdicament taules d'encaminament entre nodes –com fan els protocols proactius- ni sense haver d'introduir pesades funcions de senyalització.

De manera anàloga a la resta de protocols reactius, el mètode de funcionament d'ACOR és el següent: quan un node origen necessita una ruta, llavors fa un *broadcast* d'un paquet *RouteRequest* cap a la destinació. Un cop s'arriba a aquesta darrera, llavors contesta amb un paquet *unicast* de tipus *RouteReply* cap al node origen. Com a diferència respecte a altres protocols sense QoS, per proporcionar qualitat de servei, a cada node existeix un paràmetre de qualitat, representat per una funció de cost local. Per tant, cada node rep un paquet de petició de ruta, que transporta una funció de cost global així com aspectes relatiu a la QoS sol·licitada; llavors, implícitament, el node reserva els recursos requerits i afegeix la seva funció de cost local a la funció global, abans de reenviar el paquet fins al proper node. D'aquesta manera, la funció global serà l'acumulada a través de tota la ruta, des de l'origen fins a la destinació, representant una qualitat extrem a extrem. Aquest valor *end-to-end* de la funció de cost global s'enregistra i s'envia cap a l'origen dins del paquet *RouteReply*. Quan el node origen rep aquest paquet de resposta, llavors escull la ruta que conté el millor valor de funció de cost global.

La funció de cost local (F_b) és defineix com el *ratio* entre l'ample de banda requerit per una aplicació (B),dividit entre el màxim ample de banda suportat per l'enllaç (B_{max}) menys la suma de l'ample de banda total i un ample de banda residual (B_{res}). Llavors, tenim:

$$F_b = \frac{B}{B_{max}-(B_{res}+B)}.$$

En la funció anterior, s'ha de complir que $B_{res} + B < B_{max}$.
Per altre cantó, hi ha altra funció de cost local (F_d) que es defineix com el *ratio* entre el retard requerit per una aplicacio (D) dividit entre el retard màxim torerable (D_{max}) menys la suma del retard requerit per l'aplicació i el nombre de retards acumulats salt a salt ($sumD_i$). Per tant, tenim:

$$F_b = \frac{D}{D_{max}-(sumD_i+D)}.$$

En la funció anterior, de manera semblant a com passava abans, s'ha de complir que $sum\ D_i + D < D_{max}$.

D'aquesta manera, tenim que les funcions de cost locals es troben hiperbòlicament limitades per B_{max}i D_{max}, essent paral·leles a l'eix d'ordenades.

Per últim, la funció global d'extrem a extrem (F_g) es definex com la suma de les funcions locals F_b i F_d evaluades a cada node que participa en el descobriment de ruta. Per tant: $F_g = F_b + F_d$.

A mode de resum, podem dir que aquest protocol d'encaminament està més enfocat a xarxes sense fils amb nodes en moviment, on la topologia de xarxa és canviant, degut a nodes que entren o surten del ràdio d'acció de la xarxa (que s'associen/desassocien de la mateixa).

LOAD

LOAD són les sigles de *6LoWPAN Ad-Hoc On-demand Distance Vector Routing*. Es tracta d'una versió simplificada d'AODV, específicament dissenyada per a LLNs (amb nodes que es troben en estat *idle* –espera- la major part del temps). LOAD està dissenyat per operar per sobre de la capa d'adaptació 6LoWPAN, en comptes de a la capa de transport, creant una topologia de xarxa de malla per sota i sense coneixement per a IPv6, que veu 6LowPAN com a un únic enllaç. En ser una evolució d'AODV, es tracta d'un protocol reactiu, que és ideal per a LLNs ja que un protocol proactiu generari molt *overhead* innecesari (ja que si fos així, estaria demanant actualitzacions de rutes periòdicament i per tant el *duty cycle* augmentaria). La darrera versió de LOAD s'anomena LOADng (LOAD *Next Generation*) i actualment es troba en fase d'esborrany per l'IETF [27].

Com s'ha dit abans, LOAD està enfocat a LLNs i, en concret, únicament hauria d'executar-se en dispositius de funció completa (FFDs). A diferència d'AODV, LOAD no utilitza el número de seqüència que es fa servir en el primer. Per altra banda, únicament el node destinació pot generar un missatge RREP. A més, LOAD fa servir mètriques LQI –igual que DYMO-low- i nombre de salts de l'origen a la destinació. D'aquesta manera, es selecciona sempre la ruta que tingui el menor nombre d'enllaços dèbils totals, així com menys salts d'origen a destinació.

A més, LOAD no va servir una funcionalitat d'AODV anomenada "llista de precursors" i que servia per reenviar misttages *Route Error* (RERR) en cas d'un enllaç trencat o si el proper salt no podia ser trobat en la tabla d'encaminament. D'aquesta manera, amb LOAD, quan un enllaç està trencat, el node "cap amunt" (*upstream*) en l'enllaç ha d'intentar reparar la ruta localment, utilitzant mecanismes de descobriment (multidifusió de RREQ i RREP *unicast*).

Per altra banda, LOAD fa servir els ACKs de la capa MAC, en comptes de missatges balisa (HELLO) com fan servir altres protocols, de manera que s'estalvia energia, al mateix temps que es fa un seguiment de la connectivitat de la ruta; en concret, LOAD demana ACKs MAC per cada missatge que envia (això s'anomena LLN o *Link Layer Notification*).

A la figura de sota es clarifica l'intercanvi de missatges entre nodes fent servir LOAD:

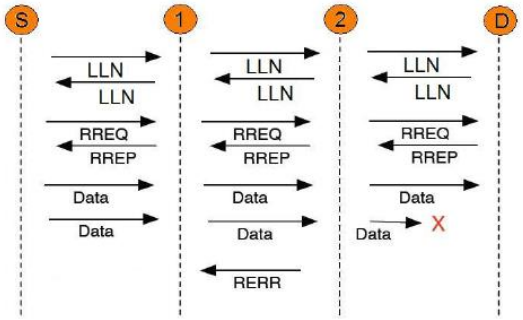


Figura 58. Intercanvi de missatges amb protocol LOAD.

Un dels majors inconvenients de LOAD i LOADng és, igual que passa amb la resta de protocols reactius, el retard durant el procés de descobriment de ruta. En aquesta fase, els paquets sortints s'han de col·locar en una memòria intermija o *buffer* i això podria originar pèrdues de paquets en nodes amb limitacions de memòria. A més, la tècnica d'inundació és altament ineficient a nivell energètic, per la qual cosa els nodes poden veure com s'esgoten les seves bateries o, si més no, com disminueix la mateixa considerablement únicament per haver de descobrir les rutes. Per últim, altre problema és el de les col·lisions de missatges de control degut precisament a les inundacions, fet que pot portar a retransmissions innecesàries i, de nou, a un major cicle de treball i, de retruc, un major consum de bateria.

En resum, LOAD és un protocol reactiu orientat a LLNs que es pot veure com una alternativa a RPL (protocol que es descriu just a continuació) per a LLNs que fan servir 6LowPAN, encara que alguns experiments en entorns de laboratori han mostrat que RPL es comporta millor a nivell general. En concret, LOAD mostra un rendiment acceptable en xarxes amb pocs nodes i amb tràfic de baixa prioritat.

Annex XXXI. Principals protocols d'encaminament proactiu.

OSLR

OSLR són les singles d'Encaminament per Estat d'Enllaç Optimitzat (*Optimized Link State Routing*), protocol d'encaminament definit a l'RFC3626.Es tracta d'un protocol proactiu, per la qual cosa les rutes a totes les destinacions possibles dins d'una xarxa són descobertes i mantingudes en una taula, tant si la ruta es necessita (si cap node l'ha demanat) com si no. Per tant, les rutes es descobriexen abans que cap paquet sigui enviat d'un origen a una destinació. OSLR és un protocol optimizat per a MANETs, encara que també es pot fer servir en altres tipus de xarxes sense fils.

OSLR fa servir missatges HELO i TC (*Topology Control*) per descobrir i difondre periòdicament informació d'estat d'enllaç a través de tota la xarxa. Els nodes reben aquesta informació de la topologia i computen el seu proper salt disponible –veïns directe. Els missatges HELLO permeten descobrir informació de veïns localitzats a dos salts i seleccionen un conjunt de reenviaments multipunt (MPRs). Aquests darrers són responsables de la transmissió de misstages de *broadcast* i de construir l'estat de l'enllaç. Per altra banda, també existeixen misstages HNA (*Host and Network Association*) que es fan servir per disseminar anuncis de rutes de xarxa, de la mateixa manera que els missatges TC anuncien rutes de *hosts*.

OSLR inunda amb dades de la topologia de manera el suficientment freqüent, a tota la xarxa, per assegurar-se que tots els nodes estan sincronitzats amb la informació d'estat d'enllaç.

Els protocols d'encaminament per estat d'enllaç, com ara OSPF (*Open Shortest Path First*) o IS-IS (*Intermediate System to Intermediate System*), escullen un encaminador designat per a cada enllaç, per tal de realitzar la inundació de la informació de topologia. En canvi, a les MANET, el concepte d'enllaç és diferent ja, que per exemple, els paquets poden sortir –i surten- per la mateixa interfície per la qual han entrat; per tant, és necessita un apropament different per poder optimizar el procés d'inundació. Fent servir, missatges HELO, el protocol descobreix informació sobre veïns localitzats a dos salts i llavors realitza una elecció distribuïda d'un conjunt de reenviadors multipunts (MPRs). Els nodes selecionen els MNRs de manera que existeix un camí a cadascun dels seus veïns a dos salts a través d'un node escollit com a MPR. Aquests darrers llavors originen i reenvien missatges TC que contenen selectors MPR. Aquest funcionament dels MPRs fa que OSLR sigui diferent d'altres protocols d'encaminament per estat d'enllaç, per diverses raons: el camí de reenviament de missatges TC no es comparteix entre els nodes sinó que varia depenent de l'origen; únicament un sobcnjunt de nodes originen informació d'estat d'enllaç; no tots els enllaços d'un node són anunciats sinó únicament aquells que representen seleccions MPR.

Donat que l'encaminament per estat d'enllaç requereix que la taula (base de dades) de la topologia estigui sincronitzada a tota la xarxa, protocols com OSPF i IS-IS realitzen una inundació de la topologia fent servir un algorisme confiable. En canvi, un algorisme d'aquesta mena és molt difícil de dissenyaer per a xarxes sense fils mòbils, per la qual cosa OSLR no es preocupa de la confiabilitat, ja que simplement inunda amb les dades de topologia de xarxa de manera freqüent, per assegurar-se que la taula no es troba desincronitzada durant massa temps.

Aquest protocol presenta diversos inconvenients per a la seva implementació en xarxes sense fils, especialment aquelles que tenen nodes amb recursos limitats. Alguns d'aquests problemes són:

- La definició original d'OSLR no inclou cap mecanisme per sensar i determinar la qualitat d'un enllaç. De fet, simplement s'asumeix que un enllaç està *up* –funcionant-si s'ha rebut un cert nombre de paquets HELLO recentment. Això assumeix que els enllaços són bimodals (és a dir, que únicament tenen dos modes possibles: actius/funcionant, en fallada), situació que no s'ha de donar necessàriament en el cas de xarxes sense fils, on els enllaços normalment funcionen però amb una capacitat degrada –no a la taxa màxima de dades- o amb pèrdua de paquets. Aquest problema queda resolt en implementacions més actuals, com ara OLSRd (la que porta el sistema operatiu Linux) que ja incorporen capacitat de sensar la qualitat de l'enllaç.

- En tractar-se d'un protocol proactiu, s'utilitzen bastants recursos (potència de processament i ample de banda) per tal de propagar les dades, fins i tot de rutes que no es faran servir. Mentre que això no representa un problema per a xarxes cablejades o xarxes sense fils d'alta velocitat, sí que és un gran inconvenient per a xarxes de sensors sense fils que se suposen que han d'estar en mode *sleep* la major part del temps, és a dir, estalviant energia. En aquest sentit, un protocol reactiu seria més convenient, ja que en aquests darrers les rutes únicament es creen sota demanda i tant sols les que es necessiten, mantenint la xarxa en silenci quan no hi ha tràfic per encaminar, evitant l'overhead dels protocols *proactius*.

- Com que es tracta d'un protocol d'estat d'enllaç, OSLR requereix bastant ample de banda i potència de processament per poder competurar els camins òptims a la xarxa. Això pot no ser un problema en xarxes petites de pocs centenars de nodes però sí que ho és quan la xarxa creix per sobre del miler de nodes. En aquest sentit, potser seria millor opció fer servir protocols com AODV o DSDV, que no fan servir l'estat de l'enllaç i per tant no requereixen d'aquest tipus de sincronització de la base de dades, o protocols com DSV, que no necessàriament construeixen camins òptims.

- OSLR fa servir MPRs per inundar informació de la topologia, la qual cosa elimina part de la redundància del procés d'inundació. Tot i que això pot semblar un avantatge, pot ser un problema en certes xarxes sense fils, on les taxes de pèrdua de paquets poden ser moderades o fins i tot altes.

El passat Abril del 2014 l'IETF va publicar la segona versió del protocol, l'OLSRv2. Aquesta nova versió manté les característiques principals del protocol original (selecció i disseminació d'MPRs) mentre que s'afegeixen noves característiques, com ara el disseny modular basat en components compartits (format de packet *packetbb*, descobriment de veïns amb el protocol NHDP). També hi ha diferències en la manera que es magenen els nodes amb múltiples adreces i interfícies.

DSDV

DSDV són les sigles de Vector Distància Seqüenciat a Destinació (*Destination-Sequenced Distance Vector*). Es tracta d'un protocol proactiu (per tant, *table-driven*) que es basa en l'agoritme Bellman-Ford (veure Annex XLVIII) per calcular rutes entre un origen i una destinació. Bàsicament, les millores sobre l'algorisme original són que DSDV proporciona rutes lliures de bucles i que s'inclou un senzill mecanisme d'actualització de rutes.Fins el dia d'avui, DSDV ha estat, junt amb AODV, OLSR i DSR, els quatre protocols més "prominents" per a MANETs i un dels primers en aparèixer, concretament l'any 1994.

Amb DSDV, cada node actua com a *router*, on es manté una taula d'encaminament i s'intercanvien actualitzacions periòdiques d'encaminament, encara que les rutes no es necessitin. La capçalera d'un missatge DSDV conté sempre aquests tres camps, de 32 bits cadascun: *Destination Address*, *Hop Count* i *Sequence Number*. Per tant, la capçalera ocupa en total 12 bytes. Després, els missatges DSDV s'encapsulen en segments UDP que posteriorment s'encapsularan en datagrames IP.

La mètrica de cost que fa servir DSDV és el *hop count* o compte de salts que hi ha entre un origen i una destinació. Per tant, es troba sempre el camí més curt o *shortest path*. Com que és un protocol proactiu, totes les entrades –rutes- per a tots els nodes de la xarxa es mantenen en una taula d'encaminament, no únicament per als veïns d'un node concret. Qualsevol canvi en la xarxa es propaga a través de dos mecanismes: actualitzaciones periòdiques o bé actualitzacions activades per disparador (*trigger*). D'aquest dos mètodes d'actualització, el basat en *triggers* envia missatges significativament més petits, per la qual cosa aquesta tècnica pot fer-se servir per a actualitzacions incrementals, de manera que no cal transmetre tota la taula d'encaminament per a cada canvi en la topologia de xarxa.

Tot i així i, al igual que altres protocols proactius com ara OLSR, DSDV és ineficient per a LLNs degut al requeriment d'haver de transmetre actualitzacions periòdiques, independentment del nombre de canvis que hi hagi hagut a la xarxa, la qual cosa comporta una sobrecàrrega (més procés per part dels nodes, més consum de bateria i més ample de banda requerit). Aquesta ineficiència limita el nombre de nodes que poden connectar-se a la xarxa, donat quela complexitat de sobreccàrrega esdevé quadràtica, amb $O(n^2)$.Per tant, es tracta d'un protocol orientat a xarxes petites, de pocs nodes, altrament, l'*overhead* seria massa gran.

Degut a aquestes actualitzacions, podrien aparèixer bucles a la xarxa. Per tal d'eliminar-los, cada actualització d'un node s'etiqueta amb un número de seqüència. Aquest número és escollit independentment per cada node pero ha de ser incrementat cada cop que es fa una actualització periòdica sobre un node. El número de seqüència d'una actualització normal ha de ser un número parell, donat que cada cop que es realitza una actualització periòdica el node incrementa la seva seqüència en 2, afegint l'actualització al missatge d'encaminament i per últim, transmetent el missatge. Per altra banda, cap node no pot canviar el número de seqüència dels altres nodes. Si un node vol enviar als seus veïns una actualització degut a una ruta expirada, llavors únicament incrementa el seu número de seqüència en 1. Els nodes que reben aquesta actualització miraran el número de seqüència i, com que serà senar, eliminaran l'entrada corresponent de la seva taula d'encaminament.

Per últim, en escenaris altament mòbils, hi ha una alta probabilitat de fluctuacions en els encaminaments, per la qual cosa amb DSDV existeix el concepte de "temps d'estabilització ponderat" (*weighted settling time*) pel qual una actualització amb un canvi en la mètrica no serà publicat immediatament als veïns, sinó que el node esperarà a que passi aquest temps d'estabilització per assegurar-se que no va rebre l'actualització per part dels seus antics veïns, abans d'enviar-la.

CGSR

CGSR són les sigles d'Encaminament per Commutació de Pasarel·la de Cap d'Agrupació (*Clusterhead Gateway Switch Routing*). Es tracta d'un protocol d'encaminament proactiu que, tot i que també es basa en tenir totes les rutes cap a una destinació abans de que un node les necessiti, difereix dels ja vistos abans en que fa servir un esquema d'organització de xarxa jeràrquic; és a dir, a diferència d'altres protocols, que fan servir un esquema de xarxa "plana", CGSR és un protocol agrupat –clusteritzat- multisalt per a xarxes sense fils, que pot seguir diversos esquemes heurístics d'encaminament. El principal avantatge de tenir un cap d'agrupació (*cluster head*) controlant un grup de nodes, és que s'aconsegueix un marc de treball que permet separar tant el codi, l'accés al canal, l'encaminament i l'assignació d'ample de banda entre els clústers. Per exemple, a cada clúster se li podria assignar una banda de freqüències diferents en diferents codis CDMA o FDMA.

A la figura de sota es pot apreciar una petita xarxa sense fils dividida entres clústers, cadascun d'ells amb el seu propi cap de clúster (en color verd):

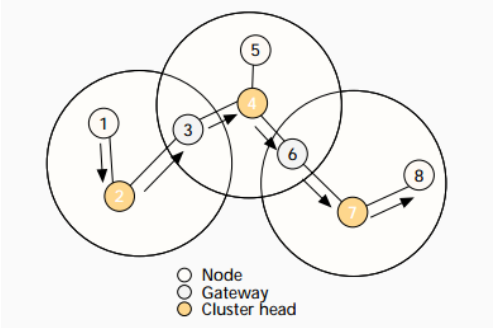


Figura 59. Exemple d'organització de xarxa amb CGSR.

El principal desavantatge de tenir un esquema basat en cap de clúster és que si hi ha canvis freqüents d'aquests això pot repercutir negativament en el rendiment de l'encaminament donat que els nodes estaran ocupats escollint el seu cap de clúster en comptes de reenviant els paquets. Per tant, en lloc d'invocar una reselecció del cap d'agrupació cada cop que canvia l'afiliació al clúster, s'introdueix un algorisme anomenat *Last Cluster Change* (LLC), que el que fa és que canvia els caps d'agrupació únicament quan dos caps entren en contacte o quan un node és mou fora del contacte de tota la resta de caps de clúster.

CSGR fa servir en realitat DSDV com a esquema d'encaminament subjacent i, per tant, també arrossega la major part d'*overhead* que aquest darrer provocava. No obstant això, CSGR modifica DSDV utilitzant l'apropament jeràrquic *cluster-head-to-gateway* (cap d'agrupació cap a pasarel·la) per encaminar les dades de l'origen a la destinació. Així, tenim les pasarel·les, que són nodes que es troben dins del rang de comunicació de dos o més caps de clúster. D'aquesta manera, un paquet que s'envia per un node, s'encamina primer al seu cap de clúster i després s'encamina des d'aquest darrer fins a la pasarel·la i, d'aquesta, fins a altre cap de clúster d'un altre clúster, i així succesivament fins que s'arriba al cap de clúster del node destinació, moment en el qual el paquet es reenvia d'aquest darrer cap al node destinació. Aquesta forma d'encaminament ja quedava reflectida a la figura de la pàgina anterior.

Fent servir aquest mètode, cada node ha de mantenir una "taula de membre de clúster", on s'emmagatzema el cap de clúster de destinació per a cada node de la xarxa. Aquestes taules són difoses per cada node periòdicament fent servir DSDV. Els nodes actualitzen les seves taules quan reben les d'un veí. A més, cada node ha de mantenir la típica taula d'encaminament, on es determina el proper salt per poder arribar a una destinació. Llavors, quan es rep un paquet, un node haurà de consultar totes dues taules per determinar, per un cantó, el cap de clúster més proper en la ruta cap a la destinació i, per altre cantó, el proper salt per arribar al cluster head seleccionat. Únicament després d'haver consultat les taules es transmet el paquet cap aquest node.

Cada clúster pot tenir diversos "fills" i formar així una estructura tipus arbre, com es pot veure a la figura anterior. Per la seva banda, un clúster que es troba més amunt en la jerarquia ha d'enviar els paquets al clúster que es troba més avall en la jerarquia.

L'algorisme CSGR determina, per un cantó, els nodes que s'agregen a un clúster; per altre cantó, selecciona el node que farà de cap de clúster dins d'una agrupació (aquest node és el que "parla" amb altres caps de clústers adjacents); per últim, també selecciona el *gateway* o pasarel·la (node que té comunicació directa tant amb el seu cap de clúster com amb el d'altra agrupació). Per tant, poden tenir tres tipus de dispositius: nodes "a seques", caps de clústers i pasarel·les.

Les funcions del cap de clúster són:

- Programar, de manera dinàmica, els camins/rutes
- Controla un grup de *hosts*/nodes mòbils
- Monitoritza la difusió dins del clúster
- Reenvia missatges a altre cap de clúster (a través d'una pasarel·la)

Pel que fa a les fases en que es pot dividir el funcionament del protocol CSGR, aquestes són tres: descobriment de rutes i emmagatzematge en memòria cau (caching); manteniment d'actualitzacions; distribució d'actualitzacions.

Els principals avantatges de fer servir CGSR són bàsicament dos:

- En fer servir un esquema jeràrquic, més eficient en condicions normals, s'aconsegueix una millor utilització –i, per tant, reducció- de l'ample de banda.

- Es redueix la mida de la taula vector distància perquè l'encaminament es realitza únicament a través del cap d'agrupació.

Per la seva banda, els inconvenients principals d'aquest protocol són:

- Com ja s'ha comentat al començament, es pot perdre més temps en seleccionar el cap de clúster i les pasarel·les que en enviar la informació.

- En nodes que facin servir CDMA/TDMA pot portar un temps aconseguir permís per enviar paquets.

- Canvis en un cap d'agrupació poden portar a múltiples trencaments de camins.

WRP

WRP són les sigles de Protocol d'Encaminament Sense FIls (*Wireless Routing Protocol*). Es tracta d'un altre protocol d'encaminament proactiu, bassat en vector distància, dissenyat per a MANETs. Aquest protocol bàsicament modifica i millora els protocols bàsics de vector distància de tres maneres:

- Quan no hi ha canvis en un enllaç, WRP intercanvi periòdicament missatges HELLO (apropament típic dels protocols reactius), en comptes d'intercanviar tota la taula d'encaminament, com acostumen a fer els protocols proactius. Si es percep un canvi en la topologia de xarxa, llavors únicament les tuples camí-vector contenen la destinació, distància i l'ID de node del predecessor (salt del segon al final).

- Per millorar la fiabilitat en l'entrega de missatges d'actualització, es requereix que cada veí enviï ACKs per als paquets d'actualització rebuts. Les retransmissions tenen lloc únicament si no es reben ACKs positius dintre d'un període de *timeout*.

- La informació d'ID de node predecessor permet al protocol calcular recursivament el camí sencer, d'origen a destinació.

A diferència d'altres protocols com ara AODV, OLSR o RPL, DSVD no disposa de cap RFC que serveixi per guiar al compliment de l'estàndard.

Com que WRP és proactiu, també pertany a la categoria de protocols *table-driven*; per tant, és molt similar a DSDV –vist just a l'apartat anterior- i, per tant, també exhibeix les propietats de l'algorisme Bellman-Ford distribuït. En concret, amb WRP tots els nodes intermitjos que participen en la comunicació han de enviar missatges HELLO periòdics als veïns per tal d'assegurar la connectivitat. Si cap dels nodes no envia HELLOs, llavors es declara com a node "mort" i així queda actualitzat en els veïns. La diferència entre WRP i DSDV és que el darrer manté únicament una tuala mentre que WRP manté un conjunt de taules. Per tant, WRP presenta una informació més precisa sobre la xarxa i efectua encaminament més ràpidament, encara que a costa de ser més complex. Al igual que amb DSDV, un dels avantatges de WRP és que s'eliminen els possibles loops a la xarxa (*loop-free*), evitant qualsevol tipus de problema d'enviament o *overhehad* per inundacions.

Per la seva banda, les diferents taules que manté WPR són aquestes quatre:

- Taula de distàncies: especifica el nombre de salts entre nodes a la seva destinació.

- Taula de rutes: conté un registre de tots els camins factibles des d'un node a la destinació.

- Taula de cost d'enllaç: proporciona informació sobre el retard associat amb un enllaç particular a la xarxa. El cost d'un enllaç trencat és infinit.

- Taula d'informació de retransmissió de missatges: aquesta taula (també anomenada MRL) conté el número de seqüència dels missatges actualitzats. La taula especifica quines actualitzacions han de ser retransmeses.

Tot i les petites diferències en el nombre de taules que es fan servir per a l'encaminament i com la informació es manté en aquests taules, tots els protocols proactius com ara DSDV, CGSR i WRP s'assemblen bastant, en el fet de que són protocols de vector distància basats en trobar el camí més curt; per tant, tots ells tenen el mateix grau de complexitat durant fallades en els enllaços i noves incorporacions de nodes.

MultihopLQI

MultihopLQI és un protocol d'encaminament de vector distància que es classifica dins del grup de protocols de "col·lecta d'informació". Bàsicament es tracta de protocols que s'enfoquen en estimar i monitorar els enllaços, així com la qualitat de les rutes. En WSNs, els protocols de col·lecta d'informació proporcionen un servei *best-effort* (millor esforç) de tipus *anycast*, on un o més nodes de la xarxa actuen com a *sink nodes* (nodes receptors, també anomenats estacions base en les xarxes sense fils). Quan un node envia un paquet, la capa de recol·lecció automàticament encamina el paquet fins el *sink* més proper. Aquesta operació és *anycast* perquè el protocol normalment no sap quin és el node receptor més proper i usualment és *best-effort* perquè la recol·lecció no proporciona cap tipus de fiabilitat extrem a extrem.

Les restriccions de RAM en els dispositius d'una WSN comporten que es prefereixin els protocols de vector distància enfront els protocols d'estat d'enllaç (aquests darrers fan servir taules molt més grans i necessiten també més recursos de CPU). Cada node que no sigui una BS manté una taula amb els propers salts candidats, cadascun amb un cost associat, on una BS té un cost zero. Llavors, un node envia paquets al proper salt que tingui el menor cost, formant d'aquesta manera un "bosc" amb arbres de mínim cost, amb arrel als *sinks*.

A les WSNs tenim diversos protocols de col·lecta d'informació com ara MintRoute, Dozer, MultihopLQI, Cent-Route o CTP. Tots ells construeixen arbres de mínim cost encara que difereixen en la manera com computen el cost. En el cas que ens ocupa, MultihopLQI computa el cost de ruta basant-se en mesuraments de les balises de control (*beacons*) de la capa PHY. Amb aquest percentatge de balises rebudes es calcula l'LQI (*Link Quality Indicator*), és a dir, es calcula un valor de qualitat per al canal.

Aquests protocols normalment estan pensats per a xarxes amb dispositius fixes, sense mobilitat, ja que en aquest tipus de xarxes, tot i que diferents dinàmiques d'enllaços, si els nodes no es mouen, la qualitat d'un enllaç normalment és sempre la mateixa o varia molt menys que si el node fos mòbil. Aquesta assumpció fa que els protocols de recol·lecció siguin vàlides, ja que val la pena perdre temps en estimar la qualitat d'un enllaç de llarga durada però no quan la qualitat canvia constantment. D'aquesta manera, aquests protocols aconsegueixen taxes d'entrega de paquets de fins el 97-99% amb molt baix cost, tot i que no existeixin ACKs extrem a extrem. Una de les implicacions d'aquesta assumpció és que aquests protocols reaccionen lentament en cas de canvis significatius en la topologia de xarxa, que es donen amb nodes en mobilitat. Per exemple, el MultihopLQI envia balises d'encaminament cada 30 segons, imposant una latència promig per canvi de ruta de 15 segons per salt. A més, aquests protocols normalment es basen en tècniques de promigjat de temps en les estimacions d'enllaços i actualitzaciosns de mètriques d'encaminament. Tot això fa que l'actualització d'estats d'encaminament locals sigui molt lenta, a més de que ralentitza la propoagació de nous estats d'encaminament. Per la seva banda, això comporta informació d'encaminament inconsistent entre els nodes de la xarxa, causant bucles i pèrdua de paquets.

Al sistema operatiu TinyOS es pot trobar una implementació del protocol MultihopLQI, potser la més coneguda i utilitzada actualment.

HybridLQI

Aquest protocol bàsicament és una proposta de millora de MultihopLQI però enfocat a xarxes amb enllaços asimètrics, on el canal de pujada no és igual –no té la la mateixa qualitat- que el canal de baixada. Aquesta situació és molt típica en xarxes de sensors, on alguns dels nodes (per exemple estacions base o pasarel·les) emeten amb una potència més elevada que la resta de nodes.

És important fer notar que encara que el protocol s'anomeni HybridLQI no es considera un protocol híbrid (reactiu i proactiu al mateix temps) sinó que s'anomena "híbrid" perquè fa servir dos indicadors de qualitat per a un mateix enllaç, tal i com veurem a continuació.

El principi de funcionament del protocol és el següent:

- Cada node de la xarxa envia balises cap a un node destinació. Aquest darrer node calcula el percentatge de balises rebudes –del total que esperaria rebre- i així es calcula l'LQI o indicador de qualitat del canal. Aquest és l'apropament que fa servir MultihopLQI.

- Per altra banda, amb HybridLQI, el node origen també manté un percentatge de paquets rebuts, en aquest cas dels reconeixements (ACKs) que rep del node destinació, del total de balises que ha enviat. Aquest indicador s'anomena PLP (*Packet Loss Percentage*).

- D'aquesta manera, es tenen dos indicadors de la qualitat del canal: LQI, que determina la qualitat per al sentit de "baixada" i PLP, que determina la qualitat en el sentit "pujada" (els termes "pujada" i "baixada" són relatius ja que depenen de quin node es considera client i quien es considera servidor)

Per tant, la millora sobre MultihopLQI és que mentre que el primer assumeix la mateixa qualitat en tots dos sentits de la comunicació, HybridLQI permet definir indicadors diferents per a cada sentit i així actuar en conseqüència. Aquesta millora no suposa cap cost adicional sobre el protocol adicional (més tràfic de xarxa) ja que simplement es fan servir les balises i ACKs propis dels paquets de control que són necessaris a la xarxa.

Amb dos indicadors de la qualitat del canal, es poden definir millor les polítiques d'encaminament i evitar situacions que es donen en els protocols que únicament disposen d'un indicador per enllaç, on acostuma a passar que els nodes que emeten amb més potència acaben esdevenint de manera temporal els caps d'una agrupació o on els diferències en la potència de transmissió entre nodes propicia l'increment de pèrdua de paquets. A més, protocols com MultihopLQI són massa sensibles a qualsevol moviment dels nodes o bé degut a factors externs com ara objectes o gent que es mou al voltant dels nodes; amb HybridLQI s'alleuja aquesta situació.

CTP

CTP són les sigles de Protocol de Col·lecta d'Arbre (*Collection Tree Protocol*). Al igual que MultihopLQI, es tracta d'un protocol d'encaminament per a WSNs, en concret enfocat en aquelles que tenen els nodes fixes. També s'engloba dins dels protocols de col·lecta d'informació. Aquest protocol ha servit per al desenvolupament d'altres protocols més recents, com ara RPL, que s'explicarà en el proper apartat.

CTP es pot veure com una millora respecte a MultihopLQI. En concret, s'incorporen tres mecanismes destinats a superar els desafiaments propis dels protocols de vector distància en xarxes sense fils altament dinàmiques:

- Mentre que MultihopLQIfa servir únicament la informació de les balises de control de la capa PHY, CTP fa servir un estimador híbrid d'enllaç, que calcula el cost mesurant el *ratio* de balises de control entregades, així com les transmissions de dades. En concret, es fa servir un estimador de 4 bits, que té en compte la informació rebuda tant pels missatges de la capa PHY, la capa d'enllaç i la capa de xarxa, proporcionant d'aquesta manera una estimació molt més acurada de la qualitat de l'enllaç.

- Per altra banda, CTP també realitza validació del camí de dades, per tal de detectar, en questió de poques desenes de milisegons, problemes com ara canvis de qualitat en els enllaços, bucles que poden causar congestió -i per tant malbaratament d'energia en els nodes, etc. Això s'aconsegueix mitjançant l'ús dels paquets de dades transmesos i rebuts com a sondes de la topologia; d'aquesta manera, es detecta ràpidament quan els paquets no arriben a la destinació.

- Balises adaptatives: els protocols d'encaminament fan difusió de paquets a intervals fixos concrets (per exemple, MultihopLQI ho fa cada 30 segons). Aquest interval presenta un compromís bàsic, donat que un interval més petit (balises més freqüents), fan el protocol més sensible a canvis en la xarxa però fa servir més ample de banda i més energia; per altra banda, un interval més llarg (menys *beacons*) fa servir més ample de banda i energia però pot fer que els problemes relatius a la topologia persisteixin per més temps. Per aquesta raó, CTP fa servir balisament adaptatiu, per tal de trencar aquest compromís: quan la topologia és inconsistent i té problemes, s'envien balises més freqüentment; en canvi, quan la xarxa està estable, el *ratio* de balises disminueix. D'aquesta manera, s'aconsegueix respondre ràpidament a les dinàmiques adverses de la xarxa, al mateix temps que es manté la sobrecàrrega a un nivell baix a llarg termini.

CTP ha esdevingut l'estàndard *de-facto* per encaminament basat en col·lecta d'informació en WSNs i s'utilitza acutalment per investigadores com a "línia base" sobre la qual nous protocols o dissenys són desenvolupats. Per exemple, RPL incopora dos mecanismes propis de CPT: el balisament adaptatiu i la validació cal camí de dades.

Alguns estudis experimentals [29] han demostrat que CTP fa servir fins un 73% menys de paquets de control que MultihopLQI (tal i com es pot veure al gràfic de sota), al mateix que també s'augmenta la taxa de paquets entregats (fins al 99.9%). Aquests mateixos estudis demostren que CTP reacciona a problemes en la topologia en únicament 64 ms, en contraposició als 30 segons de MultihopLQI (és a dir, un 99,8% menys de temps):

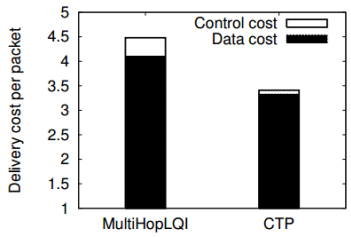


Figura 60. Cost d'entrega de paquets (control/data) en MultihopLQI i CTP [28].

RPL

RPL és un protocol d'encaminanemt per a LLNs que funcionen amb 6LowPAN. RPL és la manera com es pronuncia, en anglès, la paraula *Ripple* (ris). Aquest protocol existeix com a estàndard IETF, definit als RFC 6550 i 6553 [1]-

L'IETF va reconèixer, fa uns anys, la necessitat de formar un nou group de treball (WG) per estandaritzar una solució d'encaminament per a les xarxes IP de petits objectes intel·ligents (IPSO – IP *Smart Objectes*) que funcionessin amb IPv6 [77]. Aquest WG, creat l'any 2008, va anomenar-se ROLL (*Routing Over Low Power and Lossy networks*). El grup va portar a terme un anàlisi detallat dels requeriments d'encaminament d'algunes aplicacions com ara: xarxes urbanes de tipus *smart grid* (RFC5548), automatització industrial (RFC5673), automatització de llars/domòtica (RFC5826) i automatització d'edificis (RFC5867). Aquest conjunt d'aplicacions és el suficientment ampli com per cobrir la majoria d'aplicacions actuals de l'Internet de les Coses.

Per tant, l'objectiu del grup de treball va ser dissenyar un protocol per a xarxes sense fils de baix cost, baix consum i amb pèrdues, amb milers de nodes que poden tenir limitacions de memòria, potència de processament, etc. i suportant una varietat de capes d'enllaç però totes elles compartint les característisques comuns de poc ample de banda, poc consum, potencialment inestables i amb pèrdues. Per tant, això significa que el protocol d'encaminament no havia d'estar lligat específicament a una capa d'enllaç concreta, poden ser aquesta des de IEEE 802.15.4.4 fins a 802.15.4g, Low-Power WiFi, PLC (*Power Line Communcation*) amb IEEE P1901.2, etc. El resultat del group de treball va ser l'especificacióm junbtament amb especificacions de suport per a mètriques d'encaminament, funcions objectiu i seguretat.

Cal posar èmfasi en que, com que RPL opera a nivell de capa IP, permet l'encaminament a través de múltiples tipus de capes d'enllaç, en contrast amb altres formes d'encaminament (*forwarding*) que ja s'han vist abans i que treballaven a nivell 2 (capa d'enllaç) per la qual cosa únicament es poden reenviar paquets d'una mateix estàndard de capa d'enllaç (IEEE 802.15.4).

RPL es defineix com un protocol de Vector Distància, que especifica com construir un graf acíclic dirigit orientat a destinació (DODAG – *Destination Oriented Directed Acyclic Graph*) amb una funció objectiu definada i un conjunt de mètriques i restriccions. RPL fa servir un apropament proactiu: troba i manté rutes sense consideracions de tràfic (és a dir, es creen rutes fins i tot sense necessitar-se).

La funció objectiu opera amb una combinació de mètriques i restriccions per tal de computar el "millor" camí. Pot haver-hi diverses funcions objectius dins d'un mateix node o xarxa de malla perquè els desplegaments poden variar enormement amb diferents objectius i, a més, una mateixar xarxa pot necessitar transportar tràfic amb diferents requeriments de qualitat. Per exemple, es podrien utilitzar diversos DODAGs amb l'objectiu de trobar camins amb el millor valor transmissió esperada o ETX (mètrica) i que no fessin servir enllaços encriptats (restricció), o bé es podrien trobar els millors camins en termes de latència (mètrica) i evitant els nodes que operin amb bateries (restricció).

Aquestes funcions objectiu no especifiquen necessàriament unes mètriques/restriccions sinó que dicten les regles per formar un DODAG (per exemple, el nmombre de pares o fills, ús de balanceig de càrrega, etc). D'aquesta manera, s'aconsegueix un graf que és una topologia lògica d'encaminament, construïda sobre una xarxa física, i que compleix uns criteris especifics; d'aquesta manera, un administrador de xarxa pot decidir tenir múltiples topologies de xarxa (grafs) actius al mateix temps i utilitzats per enviar tràfic amb diversos requeriments. Un node de la xarxa pot participar i unir-se a un o diversos grafs (anomenades formalment "instàncies RPL") i llavors marcar el tràfic d'acord amb les característiques del graf per suportar encaminament amb QoS i basa en restriccions. El tràfic marcat flueix "cap amunt" o "cap avall" entre les vores del graf.

Creació del graf

El procés de creació d'un graf comença a l'arrel o LRB (LoWPAN *Border Router*) que es configurar per part de l'administrador de la xarxa. Pot haver-hi més d'una arrel configurada en el sistema. RPL especifica un nou conjunt de missatges de control ICMPv6 per tal d'intercanviar informació relativa al graf. Aquests missatges s'anomenen DIS (DODAG *Information Solicitation*), DIO (DODAG *Information Object*) i DAO (DODAG *Destination Advertisement Object*).

L'arrel comença publicant la informació sobre el graf, fent servir un missatge DIO. Llavors, els nodes veïns de l'arrel que estiguin escoltant rebran i processaran aquest DIO i decidiran, basant-se en certes regles (d'acord amb la funció objectiu, caraterístiques del DAG, cost de ruta anunciat i política local), si unir-se al graf o no. Un cop un node s'ha unit al graf llavors té una ruta cap a a l'arrel del graf. D'aquesta manera, l'arrel es coneix com al "pare" d'aquest node. El node computa el seu propi "rang" (*rank*) dintre del graf, que indica les "coordenades" del node en la jerarquia del graf, tal i com es pot apreciar a la figura de sota:

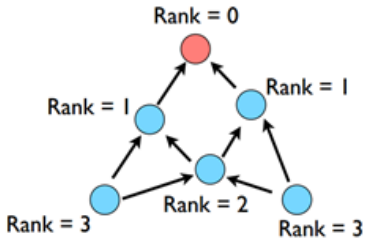


Figura 61. DODAG amb el rang de cada node indicat [50].

Si un node es configura per fer d'encaminador, llavors començarà a anunciar la informació del graf amb la nova informació que s'acaba d'afegir del node que ha rebut, a la resta de nodes veïns. En canvi, si el node és del tipus "fulla" llavors simplement s'uneix al graf i no envia cap missatge DIO. Els companys –*peers*- veïns repetiran el procés i faran la selecció del node pare, afegiment de ruta i anunciament de la informació del graf, fent servir missatges DIO. Aquest efecte de "ris" (*rippling*) d'ona fa que es construeixin els vèrtexs del graf, des de l'arrel fins els nodes fulla, on el procés termina. En aquesta formació, cada node del graf conté una entrada d'encaminament cap el seu pare (o múltiples pares, depenent de la funció objectiu), salt a salt; d'aquesta manera, els nodes fulla poden enviar paquets de dades a través del graf i cap a l'arrel, simplement reenviat el paquet als seus pares immediats.

Aquest model representa una topologia o patró de reenviament de tràfic MP2P (multipunt a punt), on cada node del graf té capacitat d'arribar a l'arrel. De vegades, aquest model també s'anomena "encaminament cap amunt", on cada node del graf té el seu rang relatiu i representa una coodenada incrementada de la posició relativa del node respecte de l'arrel en una topologia de graf. Aquesta noció de "raqng" es fa servir per RPL per a diversos propòsits, incloent la prevenció de bucles. Per la seva banda, el fluxe de tràfic MP2P també s'anomena sentit *up* (cap amunt) en el DODAG.

Per altra banda, els missatges DIS es fan servir proactivament per part dels nodes per sol·licitar informació del graf (via misstages DIO) als nodes veïns, seguint un model *pull*.

De manera similar al tràfic en sentit "cap amunt", que va des de les fulles fins a l'arrel, també hi ha un trafic *down*, en sentit "cap abaix". Aquest tràfic es pot originar bé des de fora de l'LLN, bé a l'arrel o a qualsevol node intermedi i va dirigit als nodes fulla. Això requereix un estat d'encaminament construït a cada node i un mecanisme per "poblar" aquestes rutes. Això s'aconsegueix mitjançant els missatges DAO, que es fan servir per anunciar prefixos d'accesibilitat cap als nodes fulles i que transporten informació de prefix, temps de vida vàlid i altra informació relativa a la distància del prefix. Alternativament, un node o l'arrel podem demanar missatges DAO al sub-DAG, a través d'una indicació en els missatges DIO. Llavors, quan cada node rep un missatge DAO, processa la informació de prefix rebuda per diversos nodes en el sub-DAG i enviar un missatge DAO al conjunt de parents. Aquest procés continua fins que la informació de prefix arriba a l'arrel i es configura un camí complet cap al prefix.

Modes *storing*/*non-storing*

Aquest mode d'operació tot just comentat s'anomena *storing* perquè als nodes intermitgos s'emmagatzemen taules d'encaminament (sempre i quan els nodes tinguin memòria disponible per a aquesta finalitat). També es suporta un altre mode, anomenat *non-storing,* on els nodes intermitjos no emmagatzemen cap ruta i que pot ser d'utilitzat en entorns on els nodes estan limitats per la quantitat de memòria que tenen (LLNs). Hi ha un compromís entre els dos modes de funcionament (a nivell de memòria, CPU i potència): en el mode *storing* es requereixen taules d'encaminament i, per tant, es fa servir més memòria a cada node, mentre que en el mode *non-storing*, encara que no hi ha taules d'encaminament -perquè aquestes no s'emmagatzemen- els paquets augmenten de mida per poder portar informació d'encaminament, la qual cosa acabat implicant un major consum i una major utilització de l'enllaç (es necessitat més ample de banda).

A més del patró de tràfic M2PL, RPL també suporta comunicació P2P (punt a punt) d'un node del graf a qualsevol altre. Quan un node envia un paquet a altre node de l'LLN, el paquet viatja "cap amunt" a un ancestre comú, punt en el qual és reenviat en sentit "cap avall" a la destinació.

A mode de resum, es pot dir que quan la comunicació és multipunt a punt (de les fulles a l'arrel) llavors el sentit és sempre cap amunt; quan la comunicació és punt a multipunt (de l'arrel a les fulles) llavors el sentit és sempre cap avall; per últim, en tràfic punt a punt (per exemple entre dues fulles), el sentit pot ser tant cap amunt com cap avall.

Múltiples encaminaments

RPL també proporciona l'habilitat de realitzar encaminament multitopologia (MTR), tal i com ja s'ha comentat abans, gràcies al concepte d'instància DODAG identificada per un *Instance*-ID. La idea bàsica és la de construir i identificar múltiples DODAGs sobre una mateixa topologia física (instància), fet que proporciona una via per proporcionar diversos camins amb diferents objectius d'optimització. Un node pot unir-se a un únic DODAG o a varis, estant llavors associat a diversos *instance*-IDs simultàniament (però els DODAGs d'una mateixa instància són disjunts, és a dir, no comparteixen nodes). Per exemple, tràfic no crític pot seguir un camí –potser evitant nodes que facin servir bateries- mentre que el tràfic crític podria seguir un altre camí, basant-se en obtenir la mínima latència. Per tant, veiem que ara les decisions d'encaminament són més complexes, ja que fan servir una sèrie de mètriques i restriccions, que poden canviar dinàmicament. El fet de poder crear diverses instàncies en funció del tipus de tràfic proporciona una gran flexibilitat i escalabilitat al sistema. De fet, el protocol d'encaminament permet el moviment ("salt") d'un node entre un DODAG i un altre, sempre que es segueixin unes regles fonamentals: per exemple, si un node es mou a un altre graf, llavors ha d'abandonar el seu conjunt de pares i tornar a computar el seu rang basant-se en la seva nova posició, així com haver de seleccionar un nou pare.

En definitiva, una instància RPL consisteix en un o múltiples DODAGs, amb tràfic que es mou "cap amunt" (*up*) o "cap abaix" (*down*), en funció de si els paquets van dirigits a l'arrel o a les fulles. Els DODAGS d'una mateixa instància són disjunts (no comparteixen nodes). La instància RPL té un objectiu d'optimització, per la qual cosa múltiples instàncies tenen objectius d'optimització diferents i per tant poden coexistir. A la següent figura es veu una clara presentació gràfica d'aquest concepte, amb els nodes *root* representats en color verd:

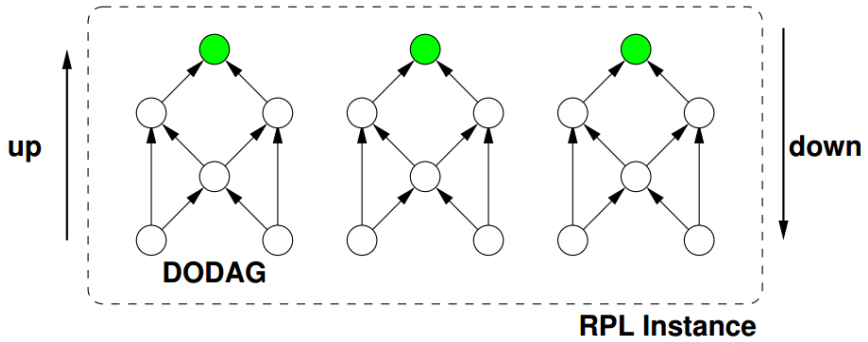


Figura 62. Instància RPL formada per tres DODAGs.

Mètriques i restriccions

Pel que fa a les mètriques i les restriccions, són els mecanismes que té el protocol per a proporcionar estratègies d'encaminanet sofisticades. Una mètrica és una quantitat escalar utilitzada com a variable d'entrada per seleccionar un millor camí, mentre que una restricció s'utilitza com a criteri adicional per descartar enllaços o nodes que no compleixen uns certs requeriments. Tant les unes com els altres es defineixen a nivell de node. Exemples de mètriques a nivell de node són, per exemple, l'estat del node, estat d'energia del node, etc. Per la seva banda, exemples de mètriques a nivell d'enllaç són la latència, confiabilitat, etc.

Tant mètriques com restriccions són dinàmiques; per tant, el protocol reacciona suaument als canvis en els valors d'aquestes. A més, les mètriques es poden acumular, node a node, al llarg d'un camí.

Detecció i prevenció de bucles

RPL també incopora mecanismes per detectar i evitar bucles (*loops*), aspecte que el diferencia d'altres protocols presents en xarxes tradicionals. En aquestes darreres, es poden formar bucles temporals deguts a canvis en la topologia i manca de sincronització entre nodes. Aquests bucles s'han de detectar el més ràpid possible, per tal d'evitar pèrdues de paquets (per exemple degut a expiració del temps de vida o TTL), evitar congestió de l'enllaç, etc. Per això s'han de proposar mecanismes d'optimització, per tal d'evitar aquest micro-bucles.

S'ha de fer notar que, mentre que en les xarxes tradicionals –cablejades- les velocitats són molt més elevades, en les LLNs la taxa de dades és bastanta baixa, la qual cosa implica que els efectes d'un bucle temporal probablement tindran un impacte limitat, la qual cosa aconsella no sobre-reaccionar, donat que les condicions que han propiciat aquest bucle poden ser transitòries. A més, si es reacciona massa ràpida, podria portar a oscil·lacions d'encaminament adicional i, per tant, a un major consum d'energia en els nodes, per tal de poder processar els paquests de control. Per tant, RPL no garantitza l'absència de bucles sinó que més aviat intenta evitar-los i especifca els mecanismes per detectar-los mitjançant la validació del camí de dades.

RPL especifica dues regles per evitar bucles, basades en el "rang" dels nodes:

- En primer lloc, com a part d'una regla anomenada *max_depth* (màxima profunditat), un node no té permès seleccionar com a pare un node veí que és més profun (que té un rang superior). Per altra banda, no es permet que un node sigui "cobdiciós" i intenti moure's més avall en el graf per tal d'incrementar el seu nombre de pares.Per altra banda, si un node fulla no disposa de cap node pare amb un rang inferior, llavors s'enverina la ruta cap aquest node amb un *INFINITE_RANK*, que indica que el node no és assolible (no es pot arribar a ell perquè s'ha especificat un rang infinit).

- Altra via d'intentar evitar bucles és especificant nous bits addicionals a la capçalera d'encaminament RPL (RH4) i processant aquests bits com a part de la validació del camí de dades. La idea és configurar i processar aquests bits quan el paquet es mou cap amunt o cap avall entre les vores dels graf i xequejar per anomalies en els valors per tal de detectar bucles. Per exemple, els bucles en un camí DAO poden ser detectats fent servir un bit *down* en la capçalera d'encaminament RPL. Quan un node envia un paquet destinat a un altre en el sentit "avall", llavors configura el bit *down* i reenvia el paquet al proper node.

  Un cop es rep un paquet que té aquest bit configurat, i la taula de cerca d'encaminament del node receptor indica que el paquet s'ha de reenviar cap en sentit "cap amunt" (*up*) llavors això indica una incosistència o un bucle i llavors el paquest es descarta (de fet, quan això passa, es dispara un event de reparació local). També es permeten altres tipus d'accions/optimitzacions.

Reparacions locals i globals

La reparació és una altra característica clau de qualsevol protocol d'encaminament, que es refereix a l'habilitat de reparar la topologia de xarxa quan ocorreix un error. En concret, RPL suporta mecanismes de reparació in cas de fallade dels nodes o dels enllaços. Tot i així, s'ha de tenir especial curar de no disparar una reconstrucció en condicions transistòries com les que s'han explicat abans. RPL especifica dues tècniques, complementàries entre elles tant en natura com accions, anomenades reparació local i reparació global.

- Quan es detecta una fallada en un node veí o en un enllaç –indisponibilitat- i el node no té cap altra ruta en en sentit "cap amunt", llavors es dispara una reparació local amb la finalitat de trobar ràpidament un camí alternatiu al pare. Aquesta reparació no té implicacions globals en el DODAG sencer.

- Per la seva banda, quan una reparació local té lloc llavors el graf pot començar a divergir de la seva forma òptima, punt en el qual pot ser necessari fer una reconstrucció sencera del graf, mitjançant el mecanisme de reparació global. Aquest darrer el que fa és reconstruir el graf tot sencer, des del començament. Es tracta, doncs, d'una tècnica d'optimització però implica un cost. La reparació global pot ser disparada únicament des de l'arrel i el seu cost és de tràfic adicional en la xarxa. Cada node del graf tornarà a executar la seva funció objectiu per a la secció del seu pare preferit.

Temporitzador degoteig

Un altra àrea on RPL difereix d'altres protocols d'encaminament que operen en entorns menys restringits és la de gestió del temporitzador (*Timer Management*). En LLNs, especialment aquelles amb dispositius que han d'estalviar energia, és imperatiu limitar el tràfic al pla de control. La major part de protocols d'encaminament fan ús de *keepalives* periòdics tant per mantenir l'adjacència d'encaminament com per mantenir les tables d'encaminament actualitzades. El problema és que aquestes tasques serien costoses en una LLN, on els recursos

són escasos. És per això que RPL fa ús d'un mecanisme de temporitzador adaptatiu anomenat "temporitzador degoteig" (*trickle timer*). Aquest mecanisme controla la taxa d'enviament de missatges DIO. L'algorisme tracta la construcció d'un graf com un problema de consistència i fa ús d'aquests temporitzadors per decidir quan fer multidifusió de missatges DIO. Certs events són tractats com inconsistències a la xarxa. Per exemple, quan un node detecta un bucle a la xarxa això es considera una inconsistència; quan un node s'associa a la xarxa o es mou dins d'aquesta, també es considera una inconsistència a la xarxa.

L'interval del temporitzador degoteig s'incrementa a mesura que la xarxa s'estabilitza, la qual cosa resulta en menys missatges DIO enviats a la xarxsa. De la mateixa manera, a mesura que es van detectant inconsistència, els nodes resetejen el seu temporitzador i envien missatges DIO més sovint. Fent servir aquest mecanisme, la freqüència de missatges DIO dependrà, llavors, del grau d'estabilitat de la xarxa, augmentat la freqüència en els nodes veïns quan es detecta cap inconsistència. En altres paraules, a mesura que la xarxa esdevé esatble, el nombre de missatges RPL disminueix; en canvi, quan es detecta un problema (bucle o canvi en els paràmetres DODAG) els temporitzadors es posen a zero per tal d'arreglar el problema ràpidament.

Un dels avantatges d'aquesta implementació de temporitzador és que no requereix d'un codi complex per la qual cosa és força fàcil d'implementar, tema especialment important en dispositius amb operació limitada.

RPL en xarxes 6LoWPAN

L'any 2005, l'IETF va engegar 6LowPAN, grup de treball per estandaritzar adaptacions de l'IPv6 sobre xarxes sense fil de malla de baix consum i de baix cost. D'aquesta manera, es va aconseguir encapsular i fragmentar datagrames IPv6 a trames IEEE 802.15.4. Així mateix, es van definir nous mecanismes per al descobriment de veïns IPv6 com per exemple resolució d'adreces a la capa d'enllaç i detecció d'adreces duplicades. Tot i que encara 6LoWPAN anava digirit inicialment a xarxes 802.15.4, el grup de treball també va tenir curar de permetre altres tecnologies, com ara Wavenis i PLC, perquè poguessin fer servir els mateixos mecanismes. Per tant, quan es parla de xarxes 6LoWPAN, es parla genèricament de LLNs que no tenen perquè ser necessàriamente IEEE 802.15.4.

Un problema de llarga durada pel que fa a adaptar IPv6 a qualsevol tecnologia de capa d'enllaç és si s'ha de suportar o no un únic domini de difusió, on tota la comunicació és transitiva dins d'una subxarxa (si A pot enviar a B i B pot enviar a C, llavors A pot enviar a C) i cada interfície pot arribar a qualsevol nombre d'interfícies dintre de la xarxa, mitjançant l'enviament de datagrames IP individuals. Emular un únic domini de *broadcast* dins d'una xarxa 6LoWPAN requereix d'encaminament i reenviament a nivell d'enllaç, mètode referit com a *mesh-under*, tal i com ja vam veure i explicar, on la topologia de malla multi-sant s'abstrau sota IPv6 per aparèixer com una xarxa completament connectada. Tot i així, l'IETF no va especificar cap protocol d'encaminament *mesh-under* per fer-se servir amb xarxes 6LoWPAN. En canvi, el que sí van especificar són arquitectures d'encaminament de capa 3 (*route-over*) on les tasques d'encaminament i reenviament es fa a nivell de xarxa, seguint l'arquitectura IP. Tenim llavors

que, mentre que en una arquitectura *mesh-under* es defineix l'abast d'un enllaç IPv6 com tots els nodes dins de la maitexa malla multi-salt, en una arquitectura *route-over* l'abast és simplement els veïns immediats als quals es pot arribar amb un sol salt/enllaç de transmissió (abast ràdio en enllaços sense fils). En altres paraules, una xarxa 6LoWPAN *route-over* estaria composada per múltiples abasts sobreposats d'enllaços locals, amb cada node definint el seu propi abast d'enllaç local, que inclou els veïns immediats.

Per tant i, a mode de resum, l'apropament *mesh-under* fa que les funcions de *routing* es portin a terme a la capa d'enllaç per emular un únic domini de difusió, on tots els dispositius apareixen com a veïns immediats. En canvi, amb l'apropament *route-over*, totes les funcions de *routing* es porten a terme en la capa de xarxa [3].

Un possible –i esperat- cas d'ús de RPL és en xarxes 6LoWPAN amb configuració *route-over*. Amb RPL, els encaminadors 6LoWPAN actuen com encaminadors IPv6 i formen rutes. Per la seva banda, els encaminadors de vora (*border routers*), que serveixen per connectar amb altres xarxes IP, operaran típicament com a arrels DODAG. Els nodes fan servir RPL per formar una o vàries topologies i així poder reenviar els datagrames IPv6 a la seva destinació.

De manera típica, una xarxa 6LoWPAN no configura cap prefix d'enllaç degut a la connectivitat variable i relacions de veïnatge comunes en una LLN. Per tant, els nodes han d'explicitar la seva presència als encaminadors veïns d'una de dos possibles maneres:

- Com a primera opció, un node pot operar una subxarxa de RPL, mitjançant la recepció de missatges DIO, escollint diferents pares basant-se en les mètriques publicades i les restriccions i comunicanat missatges DAO a l'arrel. Un node habilitat amb RPL no transmet missatges DIO perquè aquest no proveeix cap funcionalitat d'encaminament.

- Per altra banda i, de manera alternativa, un node 6LoWPAN pot ser "agnòstic" pel que fa al protocol d'encaminament, fent servir el protocol 6lowpan-nd per descobrir encaminadors veïns, escollir encaminadors de fixació i notificant a un o més d'aquests de la seva existència.

És important tenir present la interacció entre el procés de descobriment de veïns i RPL, especialment amb 6LoWPAN, on les optimitzacions fetes al procés d'ND (*Neigbor Discovery*) canvien el model d'interacció i l'arquitectura de xarxa LoWPAN demanda més d'aquest procés en una topologia *route-over*. Els nodes juguen un rol especial en LoWPAN donat que l'arrencada del procés ND permet a aquests afegir-se a la xarxa sense haver de participar en l'encaminament i, per tant, reduïnt la complexitat. Els encaminadors 6LoWPAN (anomenats 6LRs) que actuen bé com a encaminadors RPL o com a nodes fulla, responen a les sol·licituds d'encaminador (RS) dels nodes 6LoWPAN (anomenats 6LNs, ja siguin altres *hosts* o encaminadors) amb un missatge de publicació de ruta (RA). Aquests darrers contenen els prefixos necessaris i la informació de context perquè un node descobreixi la xarxa i autoconfiguri les seves adreces. A una xarxa LoWPAN, la informació dels veïns es manté per mitjà del registre dels nodes amb els seus encaminadors de proper salt per defecte. Això es fa mitjançant l'intercanvi de missatges unidifusió de tipus *Neighbor Solicitacion* (NS) o *Neighbor*

Advertisement (NA), que porten dades de tipus *Address Registration Option*. Aquests intercanvis del procés ND –entre un node i un encaminador- es mostren a la següent figura, on 'uc' indica un missatge *unicast* mentre que 'mc' indica un missatge *multicast* [4]-

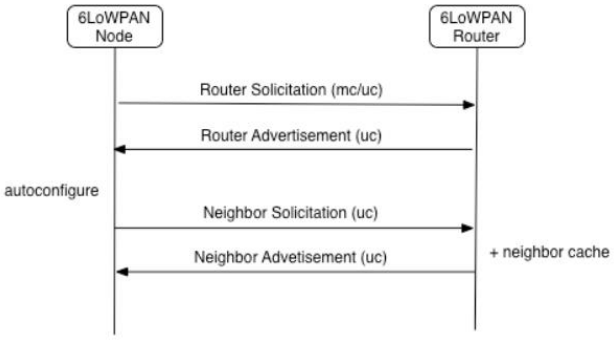


Figura 63. Intercanvi de missatges de *bootstrap* amb 6LoWPAN.

De la mateixa manera, els 6LRs fan servir ND per "arrencar" en la xarxa amb un encaminador veí i llavors registrar-se amb ells. En la figura de sota es veu un altre cop el mateix intercanvi que acabem de veure però, a més, ara es veu l'ND entre l'encaminador i un *border router* (LBR) on, a l'altre extrem –xarxa remota- hi ha un node IPv6 però que no és 6LoWPAN i on, eventualment, s'estableix una comunicació directa entre el node 6LowPAN i el node IPv6.

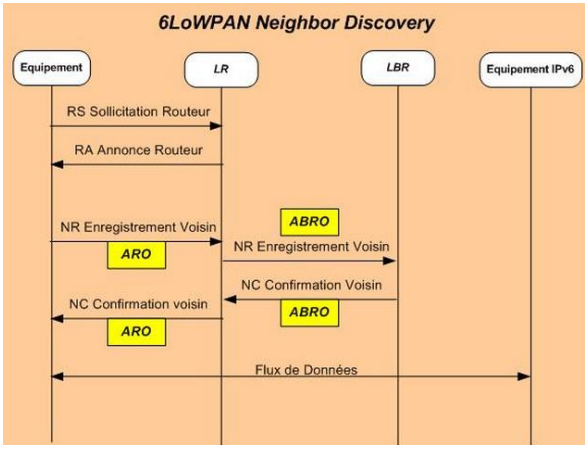


Figura 64. Intercanvi de missatges de *bootstrap* amb 6LoWPAN.

Una xarxa LoWPAN funciona correctament únicament quan la seva informació prefix i el conjunt de contexts de compressió -en cas que hi hagi- utilitzats per la compressió d'adreces, es troba sincronitzada per a totes els nodes de la xarxa. En un enllaç IPv6 això és trivial donat que tots els nodes de l'enllaç poden rebre missatges RA del mateix encaminador. En una LoWPAN *route-over* l'enllaç no és transitiu i, per tant, cada 6LR de la xarxa necessita un nou conjunt de prefixos i informació de context. Aquesta informació és llavors inclosa en l'RA enviat com a resposta a un RS d'un node veí. Això s'aconsegueix mitjançant la utilització de mecanismos de distribució de prefixos multi-salt. Aquí, el 6LBR origina el conjunt de prefixos i informació de context per a la LoWPAN. A mesura que hi ha intercanvis d'RS i RA pe part dels 6LRs, aquesta informació es distribueix lentament per tota la xarxa.

Seguint un conjunt senzill de regles, el 6LBR pot actualitzar el conjunt d'informació al mateix temps que manté tots els nodes de la xarxa LoWPAN sincronitzats.

Al seu voltant, els encaminadors RPL que fan d'encaminadors de fixació han d'injectar rutes de nodes al domini RPL, incloent informació sobre els darrers que s'han registrat via 6lowpan-nd en missatges DAO.

El resum que es pot treure és que aplicar RPL a una xarxa 6LoWPAN no requereix de cap consideració especial que sigui diferent de cap altra tecnologia d'enllaç. Des d'un punt de vista tècnic, permet la formació d'un únic graf d'encaminament cohesiu que no sofreix d'interaccions no desitjades entre protocols o entre capes. Des d'un punt de vista operatiu, executar un únic protocol d'encaminament a través de diferents tecnologies d'enllaç redueix la càrrega de l'operador d'haver d'entendre i gestionar un protocol d'encaminament per cada tecnologia d'enllaç específica. Dins d'un domini RPL, es configuren un o más encaminadors RPL per servir com arrels i iniciar el procés de creació del graf. Altres encaminadors RPL participar en el procés iteratiu de creació del graf i generen DAOs cap a l'arrel per publicar prefixos assolibles dins dels seus subgrafs. A més, en el mode *storing*, els encaminadors RPL mantenen l'estat dels prexies del seu subgraf.

Annex XXXII. Principals protocols d'encaminament híbrid.

ZRP

ZRP són les sigles de Protocol d'Encaminament de Zona (*Zone Routing Protocol*). Es tracta d'un protocol híbrid per a xarxes sense fils, que combina característiques dels protocols proactius i reactius. ZRP va de dissenyat per accelerar l'entrega de missatges i per tant reduir la sobrecàrrega, per mitjà de la selecció del protocol més adient en cada moment de la ruta.

Bàsicament, el funcionament de ZRP és el seguient: si la destinació d'un paquet es troba en la mateixa "zona" que l'origen, llavors s'utilitza un protocol proactiu, fent servir una taula d'encaminat prèviament emmagatzemada. D'aquesta manera, el paquet s'entrega immediatament. En canvi, si la ruta s'estén fora fora de la zona on s'ha originat el paquet, llavors s'utilitza un porotocol reactive, que comprova si la destinació es troba en la propera zona de la ruta. Aquest apropament disminueix l'*overhead* per aquest tipus de rutes. Un cop es confirma que una zona conté el node destinació, llavors passa a prendre el control el protocol proactiu (taula d'encaminament emmagatzemada) per entrega el paquet.

Fent servir aquest mètode, els paquets que s'envien a una destinació en la mateixa sona que l'origen, s'entregen immediatament fent servir una taula de rutes pre-emmagatzemada. En canvi, els paquets que s'envien fora de la zona s'estalvien haver de comprovar la taula de rutes, fent servir un protocol reactiu que mira si la propera zona conté el node destinació. D'aquesta manera, per a rutes llargues, s'evita la sobrecàrrega que tindríem si es fes servir únicament un protocol proactiu, eliminant al mateix temps els retards relatius al procés de descobriment de rutes propis dels protocols reactius, quan la destinació es troba en la mateixa zona que l'origen. En concret, com a mètode proactiu es fa servir IARP (*Intra-Zone Routing Protocol*) mentre que com a mètode reactiu es fa servir IERP (*Inter-zone Routing Protocol*). El primer es basa en una taula de rutes mentre que el segon es basa en el descobriment de ruta sota demanda.

IARP i IERP no són protocols d'encaminament específics sinó que són famílies de protocols. En concret, IARP és una família de protocols proactius basats en estat d'enllaç i amb profunditat limitada, on es manté la informació d'encaminament dels nodes que es troben dintre de la maeixa zona. Per altra banda, IERP és una família de protocols reactius que ofereixen descobriment de ruta avançat i serveis de manteniment de rutes basats en connectivitat local, monitoritzada per IARP.

Pel que fa a la definició de zones, es fa mitjançant el concepte de *k-neighborhood* (*k*-veïnatge). Bàsicament, una zona es defineix al voltant d'un node, consistint en tots els nodes dins d'un radi de *k* salts d'aquest primer node. Per exemple, una zona de grau 3 significaria una zona que inclou tots els nodes que es troben fins a tres salts del node escollit. Per altra banda, s'anomenen nodes vora (*border nodes*) els que es troben exactament a *k* salts del node origen (en una zona de grau 3, els nodes vora serien els que es troben exactament a tres salts del node origen).

Fora de la zona local, ocorreix el procés de descobriment de ruta: el node origen envia un *RouteRequest* als nodes vora de la seva zona, contenit la seva adreça, l'adreça de destinació i un número de seqüència únic. Cada *border node* comprova la seva zona local per veure si la destinació es troba inclosa en ella: si no és així, llavors el node vora afegeix la seva pròpia adreca al *RouteRequest* i llavors reenvia el paquet als seus border nodes; en canvi, si la destinació es troba a la mateixa zona que el node vora, llavors envia un *RouteReply*, en la ruta reversa, cap a l'origen. Els nodes origen fan servir llavors el camí guardat en el *RouteReply* per contactar amb la destinació.

A la figura de sota podem veure un exemple de zona amb ràdio *k*=2, centrada en el node *S*:

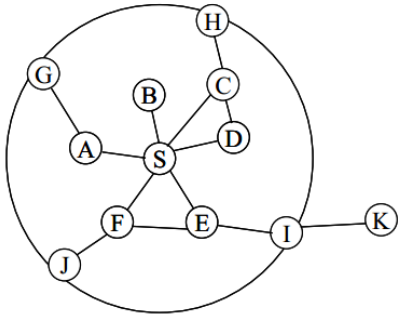


Figura 65. Exemple de zona ZRP amb *k*=2.

Per altre cantó, ZRP fa servir concepte de *bordercasting* (difusió a la vora) en contraposició al concepte de *broadcasting* (difusió a tots els nodes): el *bordercasting* fa servir la informació de la topologia proporcionada per IARP per així poder dirigir les peticions de consulta al *border node* d'una zona. En concret, un paquet de tipus *bordercast* s'entrega fent servir BRP (*Bordercast Resolution Protocol*). BRP es val d'un mapa estès d'una zona d'encaminament per construir arbres de *bordercast* per a paquets de peticions. De manera alternativa, es fa servir encaminament a l'origen basat en la zona normal d'encaminament. Per mitjà de la utilització de mecanismes de control de consultes, les peticions de ruta poden ser dirigides fora de les àrees de la xarxa que ja han sigut cobertes (que ja es coneixen). D'aquesta manera, fent servir *bordercasting*, es redueix la quantitat de tràfic quan es necessita un descobriment de ruta global.

S'ha de fer notar que, tot i fer ús de zones, aquest protocol, al igual que molts altres, disposa duna visió "plana" de la xarxa. Per tant, no s'ha de confondre amb l'estructura jeràrquica d'altres protocols d'encaminament com ara CGSR, explicat en apartats anteriors. El fet de disposar d'una topologia plana evita la sobrecàrrega/congestió que pot sorgir en els protocols jeràrquics quan s'ha d'escollir un cap d'agrupació o una pasarel·la. A més, ZRP es considera un protocol "pla" perquè les zones es sobreposen; per tant, es pot detectar una ruta òptima i es redueix la congestió de xarxa.

Per últim, ZRP és adaptatiu, en el sentit de que el seu comportament depèn de la configuració actual de la xarxa, així com del comportament dels usuaris. Per exemple, el radi d'una zona pot variar dinàmicament segons les condicions del tràfic: quan el radi d'una zona és més baix de l'òptim i hi ha més tràfic ZRP de l'òptim, llavors dominen les consultes IERP; en canvi, quan el

radi és més gran de l'òptim i el tràfic és també més gran del que seria òptim, llavors dominen les actualitzacions de ruta IARP. D'aquesta manera, tenim que el *ratio*/taxa de tràfic IERP i IARP es pot comparar amb un valor llindar; llavors, la mida de la zona es pot incrementar si el valor d'IERP/IARP és més gran que el llindar o es pot reduir si és menor que aquest darrer. Per altra banda, un valor d'histèresi es fa servir per millorar l'estabilitat. Fent servir aquest esquema, únicament es fa servir les mesures que es recol·lecten en un únic interval, millorant d'aquesta manera el rendiment en xarxes que canvien freqüentment.

TORA

TORA són les sigles d'Algorisme d'Encaminament Temporalment Ordenat (*Temporally Ordered Routing Algorithm*). Es tracta d'un algorisme d'encaminament distribuït per a WSNs de malla i MANETs multisalt. La darrera versió que hi ha del protocol és un esborrany de l'IETF que data de l'any 2001. Actualment ja no es desenvolupa activament.

L'algorisme subjacent de TORA no es basa ni en vector distància ni en estat de l'enllaç sinó que és membre del que s'anomena "algorismes d'enllaç invertit". El protocol aconsegueix crear un encaminament multicamí i lliure de bucles que s'utilitza com a base per al reenviament de tràfic a una destinació donada. Per altra banda, el protocol pot suportar simultàneament un apropament reactiu (encaminament sota demanda) i proactiu (iniciat per la destinació), segons la situació. Cal dir que l'encaminament que es crea entre un origen i destinació no té perquè ser òptim sinó que el que es busca més aviat és la preservació de l'ample de banda i alta reactivitat (baixa latència).

TORA, al igual que altres protocols semblants, fa servir una topologia de xarxa plana, no jeràrquica, amb el que s'aconsegueix un alt grau d'escalabilitat. L'objectiu principal de l'algorisme és que intenta suprimir el màxim possible la propagació de missatges de control d'abast llunyà (*far-reaching control messages*). Per aconseguir-ho, no es fa sevir la típica solució del camí més curt (*shortest path*) sinó l'algorisme d'enllaç invertit comentat al paràgraf anterior.

En altres paraules, tot i que TORA manté l'estat d'una ruta per a cada destinació (com passa amb qualsevol altre protocol de vector distància), no s'executa contínuament una computació del camí més curt i per tant la mètrica que es fa servir per establir l'estructura d'encaminament no representa una distància (això també comporta que el camí que es troba no té perquè ser l'òptim). En concret, durant l'operació reactiva del protocol, l'origen inicia l'establement de rutes a una destinació determinada, sota demanda, mode que pot ser avantatjós per a xarxes dinàmiques amb pocs patrons de tràfics definits, donat que no és necessari –ni desitjable- mantenir rutes per a cada parell origen/destinació possible. Al mateix temps, però, per a certes destinacions seleccionades es pot iniciar un mode d'operació proactiu, de manera semblant als protocols *table-driven*, la qual cosa permet que les rutes es mantinguin proactivament per a destinacions per les quals s'envia molt tràfic de manera contínua (per exemple quan les destinacions són servidors o pasarel·les) .

TORA es basa en la construcció d'un DAG (graf acíclic dirigit) dirigit cap a la destinació, de manera semblant com ho fa RPL. Una particularitat és que dos nodes no poden tenir el mateix pes dins del grap. La informació viatja dels nodes amb pesos més alts fins als nodes amb pesos més baixos. Llavors, es pot imaginar que les dades flueixen com un líquid que pot anar únicament en sentit "cap avall". Per mitjà del manteniment continu d'un conjunt de pesos totalment ordenats, TORA permet un encaminament multicamí lliure de bucles, donat que la informació no pot fluir "cap amunt" i, per tant, no pot creuar-se pel mateix camí per on ha vingut.

Els principal concepte de disseny de TORA és la localització de missatges de control en un únic petit conjunt de nodes a prop d'on ocorreix un canvi de topologia, per tal d'evitar l'*overhead* global el màxim possible. El protocol és distribuït, la qual cosa significa que els encaminadors necessiten mantenir informació dels encaminadors adjacents (que es trobern a un salt de distància). D'aquesta manera, tenim que el protocol pot realitzar tres funcions bàsiques: creació de ruta, manteniment de ruta i esborrat de ruta.

Durant les fases de creació i manteniment de ruta, els nodes fan servir una mètrica "d'altura" per establir un DAG dirigit cap a la destinació. Per tant, els enllaços s'assignen en funció d'aquesta mètrica d'altura relativa dels nodes veïns. Per altra banda, durant possibles períodes de mobilitat dels nodes, el graf es trenca i llavors comença el procés de manteniment de ruta, per tal de reestablir-lo de nou.

- Quan un node requereix una ruta cap a una destinació, envia un paquet de tipus QRY (*query*) que conté un *flag* RR (*Route Required*) activat. El paquet QRY conté, a més, l'identificador del node de edstinació.

- La resposta a un missatge QRY és un paquet de tipus UPD (*update*), que conté un vector de cinc elements (quintupla), entre ells la mètrica d'altura del node veí que contesta a la consulta, així com un camp de destinació que ens diu per a quina destinació es demana l'actualització.

- Quan un node rep un QRY amb el *flag* de RR activat, no reenvia aquest QRY cap a un altre node ja que el mateix node receptor ja ho haurà fet abans per compte propi; per tant, es descarta el paquet rebut per tal de prevenir una sobrecàrrega de missatges. En canvi, si el node que rep el QRY no té nodes més cap avall i el *flag* RR no estava activat, llavors sí que retransmet el missatge QRY rebut.

- Un exemple clar el tenim quan un node *C* requereix una ruta cap a un node *F*. El que fa *C* és difundir un missatge QRY. Aquest QRY arriba al node intermig *D*, que propaga/reenvia el missatge fins que arriba a un node que tingui una ruta cap a la destinació (per exemple, fins que arriba a un node *E*). Aquest node amb ruta cap a la destinació envia un missatge UPD, que es propaga cap endarrera.

- Per últim, pel que fa a la fase d'esborrat de ruta, essencialment es basa en la difusió/inundació d'un paquet d'esborrat (*Clear Packet* – CLR) a través de la xarxa per tal d'eliminar rutes invalides.

Per tant, podem concloure dient que TORA té els següents avantatges:

- Funciona com a protocol sota demanda (només crea el DAG quan es necessita).
- És eficient per a xarxes denses.
- Està enfocat en reduir la complexitat temporal (és a dir, té una alta reactivitat).
- Evita l'*overhead* mitjançant la focalització de missatges de control en un grup reduït de nodes.

En canvi, el protocol presenta aquests greus inconvenients:

- Latència inicial quan es demana una ruta, deguda al seu enfocament reactiu.
- No s'utilitza gairebé avui dia ja que hi ha protocols semblants com ara DSR i AODV que són més ràpids i eficients que TORA.
- No es tracta d'un protocol escalable.
- La ruta entre un origen i una destinació no té perquè ser l'òptima (la més curta).

Annex XXXIII. Aprofundiment sobre REST.

Com s'ha dit a la Memòria, un concepte important de REST és l'existència de "recursos", elements d'informació que poden ser accedits fent servir un identificador global o URI. Per poder manipular aquests recursos, els components de la xarxa (clients i servidors) es comuniquen mitjançant una interfície estàndard (per exemple HTTP) i intercanvien "representacions" d'aquest recursos (els fitxers que es descarreguen o s'envien). Per la seva banda, una petició pot ser transmesa per qualsevol número de "connectors" (per exemple clients, servidors, túnels, etc.) però cadascun d'ells ho fa sense veure "més enllà" de la seva pròpia petició (això és el que es coneix com a *stateless* o "sense estat").
D'aquesta manera, una aplicació pot interactuar amb un recurs coneixent l'identificador del recurs i l'acció requerida, sense necessitat de conèixer si existeixen caus, *proxies*, tallafocs, túnels o qualsevol altre element entre el client i el servidor que emmagatzema la informació. L'aplicació, en canvi, ha de comprendre el format de la informació que rep (la "representació) que, per norma general, es tracta d'un document HTML o XML, encara que també pot ser una imatge o qualsevol altre contingut binari/multimèdia.

REST es pot veure com una arquitectura semblant a RPC (*Remote Procedure Call* – Trucada a Procediments Remots) que es fa servir a entorns Windows i UNIX, encara que l'enfoc que es fa servir és diferent. Amb RPC, l'èmfasi es posar en la diversitat d'operacions disponibles en el protocol, també anomenades "verbs". Per exemple, una aplicació RPC podria definir operacions/funcions com ara: `trobaUsuari()`, `afegeixUsuari()`, `esborraUsuari()`, `llistaUsuaris()`, `trobaAdreca()`, etc. En canvi, amb REST, l'èmfasi es posa en els recursos (també anomenats "substantius"), especialment en els noms que s'assignen a cada tipus de recursos. Per exemple, una aplicació REST podria definir alguns tipus de recursos assignant els següents noms: `Usuari()`, `Adreca()`. LLavors, un recurs té el seu propi identificador (per exemple, `http://www.exemple.com/adreces/cat/Martorell`). Llavors, els clients poden treballar amb aquests recursos mitjançants els mètodes estàndard d'HTTP, com ara GET per descarregar una còpia del recurs o PUT per postejar/pujar un contingut al servidor.

Per exemple, el registre d'un usuari podria tenir el següent aspecte:

```
<usuari>
 <nom>Joan</nom>
 <estat>solter</estat>
 <adreca href="http://www.exemple.com/adreces/cat/Martorell">Martorell, CAT,
EU</adreca>
</usuari>
```

D'aquesta manera, si es vol actualitzar l'adreça d'aquest usuari, un client REST hauria primer de descarregar el registre anterior, en forma de fitxer XML, fent servir el mètode GET. Llavors, es podria modificar el fitxer i després pujar-lo al servidor fent servir el mètode PUT.

Un problema de REST és que cap dels verbs/mètodes HTTP (POST, GET, PUT, DELETE) no proporciona cap mecanisme estàndard per descobrir recursos (per exemple, no existeixen mètodes LIST o FIND, que són operacions que sí existeixen amb el protocol RPC). Això es resol tractant una col·lecció de resultats de cerca com si fos un altre tipus de recurs, el que requereixen que elsp rogramadors de l'aplicació coneguin les URLs per mostrar o cercar cada recurs. Per altra banda, REST proporciona algunes indicacions sobre com realitzar aquest tipus d'accions, que suggereix l'ús d'un llenguatge de formularis (per exemple un formulari HTML) per tal de poder especificar consultes parametritzades.

Donat que la definició de REST és molt àmplia, és possible afirmar que existeix un gran nombre d'aplicacions de xarxa que fan servir aquesta arquitectura (realment, qualsevol "cosa" que es pugui accedir mitjançant una petició HTTP GET). Alguns exemples són: les pàgines de blogs (fitxers XML que contenen llistats d'enllaços a altres recursos); Amazon ofereix una API –interfície per a desenvolupadors- en format REST; eBay, Amazon, Facebook, Twitter, MEGA, MercadoLibre i molts altres portals web també ho fan; etc.

Annex XXXIV. Aprofundiment sobre MQTT.

A grans trets, l'esquema d'un missatge/paquet MQTT és el següent:

- Introdueix una capçalera fixa de 2 bytes, on el primer byte inclou els seguents camps: *Message Type* (4 bits), *DUP* flag (1 bit), *QoS Level* (2 bits), *RETAIN* (1 bit). Per la seva banda, el segon byte conté el camp *Remaining Lenght*. Per tant, l'*overhead* que introdueix el protocol és molt petit:

    - El camp *Message Type* (tipus de missagte) pot adoptar qualsevol d'aquests valors (mnemònics): Reserved, CONNECT, CONNACK, PUBLISH, PUBACK, PUBREC, PUBREL, PUBCOMP, SUBSCRIBE, SUBACK, UNSUBSCRIBE, UNSUBACK, PINGREQ, PINGRESP, DISCONNECT. D'ells, els més comuns són PUBLISH (indica un missatge de publicació), SUBSCRIBE (petició de subscripció per part d'un client), UNSUBSCRIBE (petició de desubscripció per part d'un client), DISCONNECT (client que es desconnecta), PINGREQ (petició de paquet *ping*).

    - El camp *DUP Flag* indica si s'ha de duplicar una entrega. En altres paraules, el flag s'activa quan un client o servidor intenta entregar un altre cop un missatge PUBLISH, PUBREL, SUBSCRIBE o UNSUBSCRIBE.

    - El camp *QoS Level* indica quin nivell de qualitat de servei es configura; en altres paraules, quin nivell d'assegurança es configura per a l'entrega d'un missatge de tipus PUBLISH. Els valors possibles són:

        - QoS 0: el missatge s'entrega com a molt una vegada (també s'anomena *Fire & Forget*, en anglès). En altres paraules, els missatges s'envien d'acord amb el millor esforç possible de la xarxa TCP/IP subjacent, on poden ocórrer pèrdua de missatges o duplicacions. Aquest nivell de QoS es podria fer servir, per exemple, en un sensor de temperatura, o no importa si es perd una lectura individual ja que la propera lectura es publicarà en poc temps.

        - QoS 1: el missatge s'entrega al menys una vegada (també s'anomena *Acknowledged Delivery*). Aquí s'assegura la recepció del missatge per part del susbcriptor però podria ocórrer que arribessin duplicats.

        - QoS 2: el missatge s'entrega exactament una vegada (*Assured Delivery*). És el nivell més alt de qualitat, on s'assegura que el missatge tan sols es rep una vegada. Aquest nivell podria ser adient, per exemple, per sistemes de facturació on no es pot permetre ni que hagi pèrdua de missatges ni que aquestos arribin duplicats, ja que això significar potser no cobrar a un client o bé cobrar-li més d'una vegada.

- El camp RETAIN tan sols es fa servir en missatges PUBLISH. Quan un client envia un PUBLISH a un servidor, si el valor d'aquest camp es posa a '1' (s'activa el *flag*), això significa que el servidor ha de retenir el missatge un cop aquest ha estat entregat als suscriptors actuals.

- Per últim, el camp *Remaining Lenght* representa el nombre de bytes que queden dins del missatge actual, incloent les dades de la capçalera variable i el *payload* (dades d'usuari).

- A més de la capçalera fixa de 2 bytes, també es pot introduir una capçalera variable, que aniria entre la capçalera fixa y el *payload*. Aquesta capçalera només es fa servir per part d'alguns missatges d'ordres MQTT. Els camps que pot incloure aquesta són: *Protocol Name*, *Protocol Version*, *Clean Session Flag*, *Will Flag*, *Will QoS*, *Will RetainFlag*, *Username and Password Flags*, *Keep Alive Timer*, *Connect Return Code*, *TopicName*.

- Per últim, tenim el *payload* o dades d'usuari, que amb la darrera versió de MQTT pot contenir cadenes codificades en UTF-8. Els missatges que poden portar *payload* són CONNECT, SUBSCRIBE i SUBACK.

MQTT és un protocol que ja s'està fent servir en una àmplia varietat de sistemes encastrats: molts aparells hospitalaris fant servir el protocol per a la comunicació amb marcapassos i altres dispositius mèdics; per altra banda, les multinacionals de petroli i gas fan servir MQTT per monitorar milers de kilòmetres de canalitzacions.

Per últim, també existeix una nova versió de MQTT especialment dissenyada/adaptada per a xarxes de sensors sense fils, que s'anomena MQTT-S o MQTT-SN (*MQTT for Sensor Networks*). Básicament es tracta gairebé del mateix protocol, però orientat a dispositius que passen la major part del temps en mode *sleep* (amb MQTT els nodes poden ficar-se en mode "adormit" però no el 95% de seu temps, bàsicament per temes de persistència de sessió i *keep-alive*). Amb aquesta nova versió es fa servir UDP en comptes de TCP, la qual cosa significa un augment potencial de fins a 10 vegades en el nombre de dispositius en la xarxa (major escalabilitat, fins a desenes de milers de nodes). El major problema que es planteja amb aquesta versió és el fet de que UDP no acostuma a "atravessar" massa bé alguns tallafocs o *proxies*, principalment perquè el NAT (*Network Address Translation*) no funciona correctament: com que el protocol no està orientat a connexió, els tallafocs no poden portar un control de les sessions (paquets sortints) i, per tant, no esperen cap resposta del servidor i no deixen entrar moltes vegades les respostes.

A banda del protocol UDP, bàsicament, les diferències entre MQTT-SN i MQTN són les següents:

- Els missatges de tipus CONNECT es divideixen en tres sub-missatges, per facilitar la seva transmissió.

- Com que els missatges han de ser més curts en WSNs (degut a l'ample de banda limitat i les limitacions de mida dels protocols de capa d'enllaç), el nom de l'assumpte dels missatges PUBLISH es substitueix per una versió més curta (*topic ID*) d'únicament dos bytes, existint un procedimetn de registre que que permet als clients registrar els seus noms d'assumpte amb el servidor/pasarel·la i obtenir el seu corresponent *topic ID*. A més, existeixen alguns topic IDs ja predefinits, que es coneixen d'avantmà i que no necessiten registre previ.

- Un procediment de descobriment ajuda als clients que no tenen una adreça preconfigurada de servidor/pasarel·la per tal de descobrir-la.

- Amb MQTT, únicament les subscripcions de client poden ser persistents; ara, en canvi, també els missatges de tipus *Will Topic* i *Will Message* també poden ser-ho.

- Es defineix un nou procediment de *keep-alive* per als nodes clients en mode "adormit". D'aquesta mnera, els dispositius amb bateria poden quedar-se en mode sleep, període durant el qual els missatges destinats a ells es queden en una memòria intermitja o buffer en el servidor/pasarel·la per tal de ser entregats més tard, quan es despertin.

A la figura de sota es pot veure un diagrama amb l'arquitectura típica d'una xarxa que fa servir MQTT-SN. Bàsicament tenim per un costat els clients (nodes sensors); pe altra banda tenim els nodes *forwarders* o reenviadors (motes configurades per encaminar els missatges) i, per últim, tenim les pasarel·les, que es comuniquen amb el component *broker* fent servir MQTT tradicional.

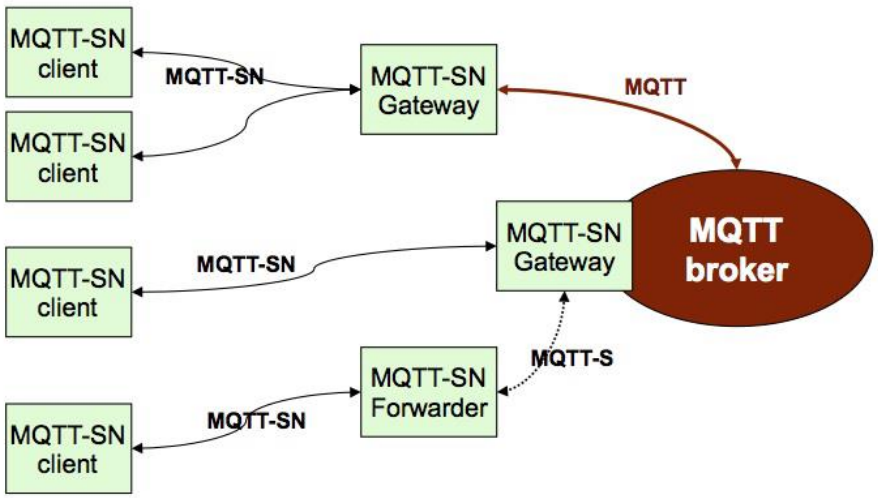


Figura 66. Arquitectura de xarxa amb MQTT-SN.

Annex XXXV. Aprofundiment sobre AMPQ.

L'especificació AMPQ es defineix en vàries capes:

- Un sistema tipus (*type-system*),
- Un protocol asíncron i simètric per a transferència de missatges d'un procés a un altre,
- Un format estàndard i extensible,
- Un conjunt de capacitats de missatgeria estandaritzades però extensibles.

A nivell de transport, tenim els *type-system*, que s'utilitzen per definir el format dels missatges, permenent que les metadades (estàndars i exteses) puguin ser expressades i enteses per les entitats de processament. També es fa servir per definir les primitives de comunicació a través de les quals s'intercanvien els missatges entre aquestes entitats (anomenades AMQP *frame bodies*). Aquest esquema d'auto-descripció serveix per permetre la interoperativilitat, pel que fa a la representació d'un ampli rang de tipus de dades comuns, a més de permetre anotar un significat adicional a les dades (per exemple, un mapa de valors que contingui parells de clau-valor com ara 'adreça', 'nom', etc. es podria anotar com una representació del tipus 'client'). En concret, existeixen els següents "tipus" AMQP:

- Tipus primitiva: valors escalars com ara booleà, números integrals i en coma flotant, marques de temps (*timestamps*), UUIDs, caràcters, cadenes, dades binàries i símbols. Per la seva banda com a colecció de tipus tenim les matrius, les listes i els mapes.

- Tipus descrits: es tracta de tipus personalitzats definits pel programador. Es basen en un 'descriptor', que el que fa és una associació entre un tipus personalitzat i un tipus primitiva.

- Tipus compostos: es fan servir per codificar dades estructurades com per exemple *frame bodies* (cossos de trames). Cada tipus inclou una seqüència ordenada de camps, cadascun amb un nom específic, tipus i multiplicitat. La definició d'aquest tipus també inclou un o més descriptors, al igual que els tipus descrits, per tal d'identificar les seves representacions.

- Tipus restringits: un nou tipus derivat d'un tipus existent on únicament es permeten una sèrie de valors que siguin subconjunt dels valors del tipus existent. Aquest tipus es fan servir normalment per a enumeracions, que en AMPQ són restriccions de tipus primitiva integrals, encara que també pot haver-hi, per exemple, tipus restringits que siguin una URL, que pot ser vist com una restricció d'un tipus primitiva cadena de caracters.

La unitat bàsica de dades amb AMQP és la trama (*frame*). Hi ha nou tipus de trames definides, anomenades *performatives*, que es fan servir per iniciar, controlar i tallar la transferència de missatges entre dos nodes. Aquests "cossos de trama" són: *open*, *begin*, *attach*, *transfer*, *flow*, *disposition*, *detach*, *end*, *close*. Per exemple, *attach* es fa servir per iniciar un nou enllaç (*link*) mentre que *detach* es fa servir per cancelar-lo. Els enllaços s'han d'establir per tal de poder

enviar o rebre missatges. Aquests missatges fan servir la trama *transfer* (els missatges flueixen en una única direcció). Per la seva banda, les transferències estan subjectes a un esquema de control de fluxe basat en crèdits, que es gestiona fent servir trames *flow* (això permet a un procés protegir-se d'una saturació deguda a un volum massa alt de missatges o simplement es fa servir per permetre a un enllaç agafar missatges quan vulgui).

Per altra banda, cada missatge que s'envia ha de ser finalment "col·locat" (*settled*). Aquest pas assegura que tant el transmissor com el receptor es posen d'acord en l'estat de la transferència, proporcionant garanties de confiabilitat. Els canvis en l'estat i la "col·locació" dels missatges en una transferència o grup de transferències es comuniquen entre els companys (*peers*) fent servir una trama *disposition*. Les garanties de confiabilitat es configuren segons les opcions que s'han comentat abans de "com a molt una vegada", "al menys una vegada" i "exactament una vegada".

Per últim, múltiples enllaços es poden agrupar en una sessió, que és una conversació bidireccional entre dos nodes que s'inicia amb una trama *begin* i s'acaba amb una frama *end*. Per la seva banda, una sessió pot contenir múltiples sessions multiplexades, cadascuna d'elles lògicament indenpendent de les altres. Les connexions s'inicien amb una trama *open* i es termien amb una trama *close*.

A nivell de missatges, AMQP en defineix dos tipus de formats:

- *Bare message* (missatge nu): és el missatge tal i com el proporciona el transmissor. Consta de tres seccions: propietats estàndards (*message id*, *user id*, *creation, time*, etc.), propietats d'aplicació (opcionals; també anomenades 'exteses') i dades d'aplicació (el "cos" o *payload* del missatge). Aquest missatge és immutable dintre de la xarxa AMQP en el sentit de que cap secció pot ser modificada per cap node AMQP que faci d'intermediari.

- *Annotated message* (missatge anotat): és el missatge tal i com el veu el receptor. Consisteix en el *bare message* més altres seccions per anotacions tant al començament (*header*) com al final (*footer*) del *bare message*. Hi ha dues classes d'anotacions: les que poden viatjar amb el missatge indefinidament i les que es consumeixen en el següent node.

A la figura de la pàgina següent es mostra un esquema del format d'un missatge AMQP:

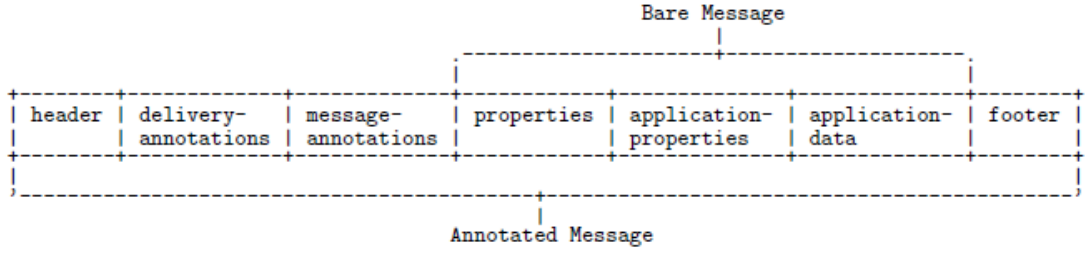


Figura 67. Estructura d'un missatge AMQP.

Per últim, a nivell de transaccions de missatges, amb AMQP aquestes s'han de declarar en primer lloc (quan comença el treball transaccional) i descarregar (*discharge*) quan el treball transaccional ha terminat. Durant el treball transaccional, les operacions a realizar poden ser publicar (*post*) un missatge, adquirir-lo (*adquire*) o retirarl-lo (*retire*). Aquestes accions es realitzen sempre per part d'un recurs de la transacció (*transactional resource*) quan així ho demana un controlador de transacció (*transaction controller*). Totes les transaccions tenen un idenficador de fins a 32 bytes.

L'ISO 19464 especifica la integració d'AMQP amb altres protocols per a una major flexibilitat i reducció de costos, com ara:

- DNS (*Domain Name System*) per a resolució de noms,
- SCTP (*Stream Control Transmission Protocol*) per a connectivitat,
- LDAP (*Lightweight Directory Access Protocol*) per a autorització a través d'un directori centralitzat,
- Kerberos per autenticació,
- XML com a format d'intercanvi de dades,
- FPML, FIXML i XBRL com a llenguatges comercials.

Per últim, si es compara AMQP amb el protocol vist a l'apartat anterior (MQTT), veiem que aquest segon té una sèrie de macances en relació amb AMQP, com ara: no hi ha cues (la qual cosa significa que tant transmissor com receptor han d'estar actius al mateix temps); no hi ha persistència, durabilitat, arxivat o recuperació de missatges; no hi ha compatibilitat amb APIs com ara JMS o WCF (*Windows Communication Foundation)*; no hi ha control de fluxe o ACKs selectius per prevenir bloquejos a nivell d'aplicació; no hi ha multiplexació (que permeti per exemple atravessar un tallafocs de manera fàcil); no es suporta autenticació via Kerberos; etc. Per tant, podem dir que AMQP és potser un protocol més "integrable" que no pas MQTT.

Algunes implementacions d'AMQP conegudes són: OpenAMQP, Apache Qpid, AMQP Infrastructure, RabbitMQ, ZeroMQ i Zyre. Per la seva banda, algunes companyies que fan servir AMQP són, a banda de JPMorgan, la Borsa alemana, la NASA (pla de control del projecte Nebula Cloud computing), Red Hat (pla d econtrol dels seus serveis de Cloud), VMware, Google, AT&T, el Govern de l'Índia (per al seu projecte d'identificador únic de persones), etc. [34].

Annex XXXVI. Aprofundiment sobre XMPP.

Una particularitat de la xarxa XMPP és que utilitza una arquitectura client-servidor, segons la qual els clients no poden parlar directament entre ells. Aquest model és decentralitzat, en el sentit de que qualsevol persona por córrer un servidor, encara que aquest no pot ser anònim ni de tipus P2P; és a dir, per disseny, no existeix cap servidor central autoritatiu, com passa amb serveis de missatgeria del tipus AOL Instant Messenegr o Windows Live Messenger (aquest darrer ja desaparegut).

En una xarxa XMPP, cada usuari té el seu propi identificador, anomenat JID o *Jabber ID*. Per tal de no haver de requerir un servidor central que mantingui tota la llista d'identificadors, el JID s'estructura com una adreça de correu electrónic, amb un nom d'usuari i un nom de domini (o adreça IP) per al servidor on resideix l'usuari. Per altra banda, donat que un usuari pot desitjar iniciar una sessió en múltiples localitzacions, llavors han d'especificar un "recurs": aquest identifica un client en particular que pertany a l'usuari (per exemple telèfon de casa, de feina o mòbil). Aquest recurs es pot incloure al JID afegint una barra (`/`) seguida del nom del recurs (per exemple, `username@exemple.com/mobil`). A més, a cada recurs se li pot assignar un valor numèric anomenat "prioritat". D'aquesta manera, els misatges enviats simplement a un usuari-sense especificar cap prioritat- aniran al client que tingui definida la major prioritat, mentre que un missatge dirigit a `/mobil` anirà dirigit únicament a aquest client. Per últim, els JIDs que no tenen nom d'usuari també són vàlids, donat que es fa servir per a missatges de sistema així com control de característiques especials en el servidor; de la mateixa manera, en aquestos JIDs l'especificació d'un recurs és també opcional.

Avui dia, els JIDs fan servir Stringprep, un format definit a l'RFC 3454 per poder manegar caracters Unicode, fora del rang ASCII estàndard, encara que en un futur proper es començarà a utilitzar la tecnologia creada pel Grup de Treball PRECIS de l'IETF.

A la pràctica, el fet de poder encaminar missatges basant-se en un identificador lògic d'un punt de terminació en lloc d'haver d'especificar una adreaça IP es presenta om una oportunitat per fer servir XMPP com una capa *overlay*, per damunt de differents topologies de xarxa subjacents.

Com ja s'ha comentat, XMPP es "ven" com una plataforma extensible intermitja orientada a missatges (xMOM – *eXtensible Message Oriented Middleware*). De fet, multitud d'aplicacions fan servir aquest protocol, sobretot aquelles relacionades amb la missatgeria instantània i distribució de dades de presència. També es pot fer servir com a protocol de descobriment i estat de disponibilitat de serveis, tant locals com serveis en xarxa, de manera similar a serveis ja existents com a Zeroconf o SLP (*Service Location Protocol*). De fet, degut a aquesta capacitat de suport de descoberta de serveis al llarg de múltiples dominis de xarxa local (en el que s'anomena "federació entre dominis"), XMPP és perfecte per a aplicacions de computació en el núvol, on les màquines virtuales, servidors d'emmagatzematge, tallafocs i altres dispositius poden suposar obstacles a altres serveis de descobriment alternatius. Tot això es deu, en part, a la capacitat d'intercanviar, de manera nativa, contingut en format XML, podent d'aquesta manera "orquestrar" l'intercanvi d'altres formes de contingut com per exemple fluxes binaris, vídeo, aúdio, transferència de fitxers, etc.

Per tant, com es pot veure, moltes de les aplicacions d'XMPP no estan relacionada amb la comunicació entre humans sinó M2M o P2P, a través de diferents conjunts de xarxes. Això fa al protocol adequat per a aplicacios IoT.

En l'especificació original, es defineixen dues maneres de comunicació via HTTP: *polling* (consulta) i *binding* (unió). El primer mètode ja està obsolet i essencialment implica que els missatges s'emmagatzemin en una base de dades en un servidor i aquests són "buscats" de manera regular per un client XMPP per mitjà dels mètodes GET i POST propis d'HTTP. Per la seva banda, el mètode de *binding* s'implement fent servir BOSH (*Bidirectional-Streams Over Synchronous HTTP*), que permet als servidors "empenyer" els missatges cap als clients tan aviat com són enviats.

Aquest model de notificació tipus *push* és més eficient que el model de consulta o *polling*, ja que en el darrer moltes de les consultes poden no retornar cap nova dada. L'únic inconvenient és que el port definit per l'IANA per a BOSH no és el 80/tcp (ja assignat a HTTP) sinó el 5280/tcp.

Per últim, una darrera alternativa, potser més convenient per a l'enviament de dades per a missatgeria en tempos real és WebSocket, una tecnologia web que permet canals de comunicació bidireccional i full duplex sobre una única connexió TCP. De fet, XMPP sobre Websocket està definit en l'RFC 7395, estàndard proposat per l'IETF.

Pel que fa als exemples d'utilització, tenim que XMPP es fa servir com a protocol de missatgeria per part de moltes aplicacions, essent l'exemple més conegut Google Talk. Altres companyies com Nokia (plataforma OVI) o DreamHost també ofereixen serveis XMPP com a alternativa als tradicionals serveis de web i correu electrònic. Adicionalment, també s'ofereixen servidors XMPP com a part de *Cloud Computing*, amb companyies com Cisco fent-lo servir en la seva plataforma WebEx. Per últim, també existeixen implementacions no relacionades directament amb missatgeria instantània, com ara sistemes *smart grid* (aplicacions demanda-resposta) així com a substitut del servei SMS per a missatgeria de text entre dispositius mòbils.

Segons tot l'anterior, XMPP s'ha vist moltes vegades com a competidor de SIMPLE (*Session Initiation Protocol for Instant Messaging and Presence Leveraging*), un protocol SIP (Inici de Sessió) i com estàndard "de facto" per a missatgeria instantània i notificació de presència. Algunes extensions d'XMPP fan possible que es pugui fer servir per a aplicacions de multi-xat (podria ser, per tant, un competidor del mític IRC) mentre que altres extensions de publicació-subscripció proporcionen les mateixes característiques que protocols vists abans com AMQP.

Algunes implementacions de programari servidor que fa servir XMPP són: iChat Server, jabberd2, Metronome, M-Link, Mongoose IM, Openfire, Prosody, Sun Java Communications Suite, Tigase. Per la seva banda, alguns dels clients que utilitzen el protocol són: AIM, Lotus Sametime, eBuddy, ICQ, Nimbuzz, Skype, etc.

Si ens centrem en les LLNs, el gran problema d'aquest protocol és -al igual que també passa amb la resta dels exposats abans- que es basa en TCP i per tant, en estar orientat a connexió, la sobrecàrrega que es pot produir degut a retransmissions és força elevada (ja es va veure anteriorment que, per a xarxes de sensors, és millor fer servir UDP perquè l'entrega d'un paquet individual no sol ser indispensable). Per altra banda, un altra problema afegit d'XMPP és l'*overhead* extra que s'afegeix pel fet que les dades que ens transmeten són en texte pla. Tot i així, la seva gran escalabilitat i la possibilitat d'afegir seguretat són aspectes a favor de fer servir aquest protocols en WSNs de mida gran.

Annex XXXVII. Aprofundiment sobre CoAP.

A la figura de sota es mostra un diagrama bàsic d'una xarxa de sensors que fa servir 6LoWPAN com a capa d'adaptació IPv6, RPL com a protocol d'encaminament, UDP com a protocol de transport i CoAP com a protocol d'aplicació. S'aprecia que el node que fa de gateway (a vegades anomenat proxy) s'encarrega de "traduir" CoAP a HTTP (de fet, sabem que CoAP és un "subconjunt" d'HTTP) de cara als dispositius remots que es troben en l'altra banda i que treballen amb IPv6, TCP i HTTP.

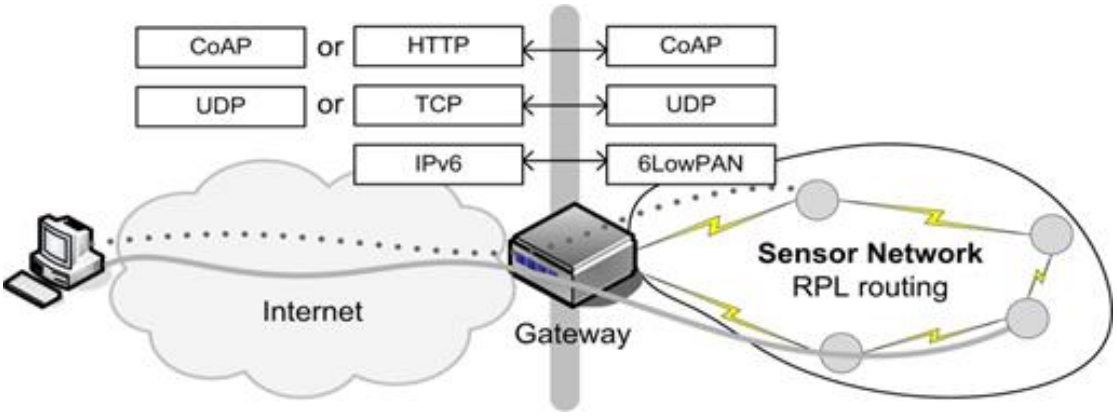


Figura 68. Diagrama de xarxa de sensors 6LowPAN/CoAP i xarxa IPv6 remota.

CoAP fa ús de dos tipus de missatges: peticions (*requests*) i respostes (*responses*), fent servir un format de capçalera en base binària bastant simple (de mida fixa 4 bytes). La capçalera, que inclou, entre d'altres camps, un anomenat *Message ID* (2 bytes) –destinat a evitar missatges duplicats- pot estar seguida o no d'unes opcions, en un format optimitzat *Type-Length-Value* (la mida d'aquestes opcions adicionals pot anar de 0 a 8 bytes). Després de les capçaleres i opcions, qualsevol byte adicional és considerat com a cos del missatge o *payload*. La longitud d'aquest cos ve implícita per la longitud del datagrama. Quan es fa servir UDP, el missatge sencer ha de cabre forçosament dins d'ún únic datagrama. Això significa que, quan es fa servir amb 6LoWPAN (RFC4944), qualsevol missatge hauria de cabre idealment en una única trama 802.15.4 per tal d'evitar la fragmentació.

A la figura de sota es mostra una representació gràfica del format de missatge CoAP:

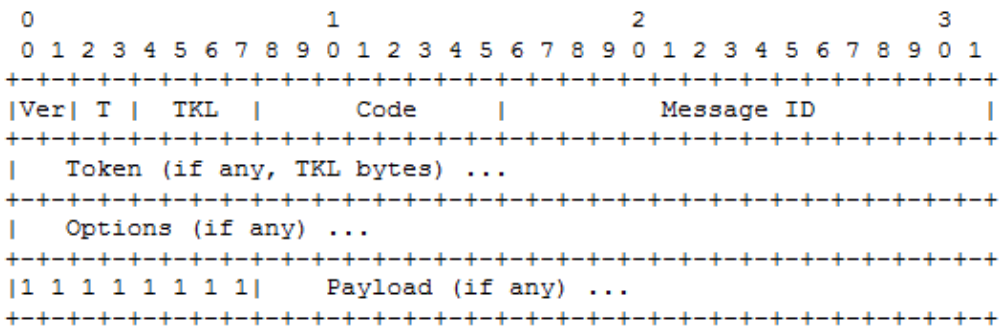


Figura 69. Format d'un missatge CoAP.

De manera similar a HTTP, CoAP suporta negociació de contingut, la qual cosa significa que els clients fan servir opcions de tipus *Accept* per expressar als servidors la representació preferida d'un recurs; llavors, els servidors contesten anb una opció *Content-Type* per comunicar als clients el que rebran. Això permet als clients i servidors evolucionar independentment, afegint noves representacions sense affectar a cap altra, igual que passava amb HTTP. Una particularitat de CoAP és que permet que les peticions facin servir cadenes de consulta del tipus `?a=b&c=d`; d'aquesta manera, es pot proporcionar als clients de funcionalitats de cerca i paginació, entre d'altres. CoAP, a més, extèn el model de petició HTTP amb l'habilitat de poder "observar" un recurs: quan un *flag* de tipus *Observe* s'activa en una petició GET, llavors el servidor pot continuar responent un cop s'ha transferit el document inicial, permetent als servidors enviar els canvis d'estat als clients tan bon punt ocorreixen, podent cancel·lar l'observació qualsevol de les dues parts.

Pel que fa a la qualitat del servei, tant els missatges de petició i resposta en CoAP poden ser marcats com *Confirmable* (CON) o *NonConfirmable* (NON): els primers fan necessari una confirmació (ACK) per part del receptor mentre que els segons no ho necessiten, per la qual cosa aquests darrers també es poden anomenar *fire & forget* (dispara i oblida). Quan un node no pot processar en absolut un missatge *Confirmable* (és a dir, ni tan sols proporcionar una resposta d'error adequada) llavors aquest contesta amb un missatge *Reset* (RST).

Pel que fa a la seguretat, com que CoAP fa servir UDP en comptes de TCP, no es pot fer servir SSL/TLS per autenticació/encriptació. En canvi, es fa servir DTLS (*Datagram Transport Layer Security* – RFC6347), que proporciona el mateix nivell d'assegurança que TLS però per a transferència sobre UDP. A més, els dispositius CoAP amb DTLS típicament també suporta RSA/AES o ECC/AES.

Pel que fa al descobriment de recursos, CoAP defineix un mecanisme estàndard per a aquesta finalitat: els servidors proporcionen un llistat dels seus recursos (juntament amb metadades sobre ells) en l'adreça URL `/.well-known/core`. D'aquesta manera, es permet als clients descobrir els recursos proporcionats pels seviros i quin tipus de "mèdia" són.

Pel que fa a l'encaminament de missatges, amb CoAP tenim que un node sensor és normalment un servidor, no un client (encara que els nodes poden tenir els dos rols). Això és així perquè el sensor/actuador proporciona recursos que poden ser accedits pels clients, tant en mode lectura com escritura, en el darrer cas per alterar l'estat del sensor (un exemple seria quan un usuari o ordinador remot vol accedir a un sensor per llegir els valors de temperatura o humitat i, en funció de quins siguin aquests, activar una sèrie d'actuadors per tal de canviar les condicions ambientals). Donat que les motes actuen com a servidors, això significa que han de poder rebre paquets entrants quan sigui necessari, no únicament enviar paquets sortints de manera periòdica. Llavors, per funcionar correctament darrere d'un dispositiu que faci NAT (una pasarel·la entre la xarxa interna i Internet), el node ha d'enviar primer una petició cap al servidor, igual com es fa per exemple amb altres estàndars com LWM2M (*Lightweight M2M*); d'aquesta manera, l'encaminador o pasarel·la pot associar client i servidor.

Per altra banda, tot i que l'ús de IPv6 no és obligatori amb CoAP, sí que és recomanable utilitzar-ho com per a l'adreçament de tots els dispositius de la xarxa, ja que és la manera més fàcil, en entorns IP, de fer els nodes directament encaminables (*routables*) cap a l'exterior.

Actualment hi ha diverses implementacions de CoAP, tant a nivell servidor com client. Entre les que implementen els dos components tenim: libcoap, nCoap, jCoAP, CoAPOthon, txThings, TinyOS CoapBlip, Erbium for Contiji, Californium, Copper, ETRI CoAP, etc. La major part d'elles estan escrites en C/C++ o Java/Javascript encara que algunes poques ho estan en Phyton. El 99% d'elles segueixen l'RFC7252 encara que algunes poques tant sols implement l'esborrany anterior a l'estàndard (coap-13).

Annex XXXVIII. Microcontroladors per a aplicacions IoT.

Atmel

Atmel és un fabricant de circuits integrats i microcontroladors [52]. Pel que fa als segons, es disposa de tres grans famílies: AVR, SAM i 8051.

- AVR: es tracta d'una família d'MCUs de 8 o 32 bits, de baix consum, destinats a aplicacions de propòsit general. Per exemple, la subfamília/sèrie AVR AC3 són MCUs de 32 bits, amb una memòria Flash que pot anar de 16 a 512 KB, una freqüència de treball de fins a 66 MHz i una taxa de fins a 1.5 MIPS (Milions d'Instruccions per Segon) per MHz.

  Per altre cantó, la subfamília/sèrie XMEGA està formada per MCUs de 8 bit, amb memòria Flash de 16 a 384 KB, una freqüència de fins a 32 MHz i un rendiment de 1.0 MIPS/MHz. Per últim, també existeixen les sèries megaAVR (4-256 KB Flash, fins a 20 MHz, 1.0 MIPS/MHz) i tinyAVR (0.5-6 KB memòria Flash, fins a 20 MHz, 1.0 MIPS/MHz). Aquestes dues darreres serien les més indicades per a xarxes de sensors de baix consum i baixa potència i on l'espai físic a la placa és limitat.

- SAM: és una família de microcontroladors de 32 bits, basada en processadors ARM (ARM és un tipus d'arquitectura RISC –*Reduced Instruction Set Computing*, desenvolupada per l'empresa ARM Holdings) [58]. En concret, els processadors poden ser ARM Cortex-M4, Cortex-M3, Cortex-M0+, ARM926EJ-S i ARM7TDMI. Aquests MCUs tenen una memòria Flash de 8 KB fins a 2 MB i una SRAM –*Static RAM*- de 4 KB fins a 160 KB. També hi ha un altre conjunt, basat en MPUs –microprocessadors- en comptes d'MCU, basats en els processadors ARM Cortex-A5 i ARM926EJ-S.

  Tot i que tots els MCUs anteriors són de baix consum, segons el web del fabricant, els models més adients per a xarxes de sensors i IoT són els de la subfamília SAM G (16-512 KB memòria Flash, fins 96 MHz, consum de corrent mínim de 100 µA/MHz en mode actiu) i els de la subfamília SAM4L (128-256 KB Flash, 48 MHz). També hi ha altres subfamílies més adients per a aplicacions M2M, com ara la SAMA5, la SAM4N, la SAM4S, la SAM3X i la SAM9X. En realitat, totes les subfamílies són molt semblants entre sí i el que canvia entre una i l'altra és bàsicament les quantitats mínima i màxima de memòria Flash i la màxima freqüència de treball (en xarxes LLNs hauria d'haver-hi prou amb els models inferiors, amb menys memòria i velocitat més baixa, ja que normalment seran el més econòmics i els que consumiran menys, a bada de ser més petits).

  A la figura de sota tenim un gràfic amb algunes de les sèries SAM d'Atmel, on es veu el processador que incorpora cadascuna així com els rangs de memòria Flash de cadascuna.

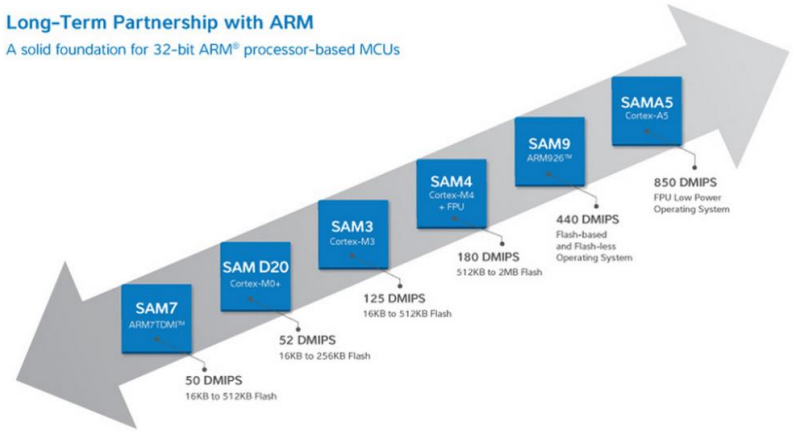


Figura 70. Sèries de la família de MCUs SAM d'Atmel.

- 8051: per últim, tenim aquesta sèrie de MCUs, de 8 bits, basada en el joc d'instruccions del microcontrolador d'Intel 8051, un µC bastant senzill i molt popular, desenvolupat a la dècada del 1980. Aquesta família pot incorporar de 2 fins a 64 KB de memòria Flash i es pot aconseguir fins a 30 MIPS fent servir MCUs AT89LP (de tipus *low power, single cycle*), que també són de tipus 8051 però aconsegueixen un rendiment fins a 12 vegades superiors a aquests darrers. Alguns SoC (sistemes en un xip) implementen aquest µC es poden fer servir per a aplicacions M2M/ioT senzilles.

Texas Instruments

Texas Instruments (TI) és una coneguda companyia nord-americana que desenvolupa i comercialitza semiconductors i altres tecnologies per a computadores. Pel que fa ls seus MCUs, tenen per un cantó aquells orientats a baix consum (*low-power*) i per altre cantó aquells destinats a rendiment (*performance*).

Centrant-nos en el primer grup –que és el que ens interessa per a LLNs- tenim les famílies MSP430Fx (MSP430F1x, MSP430F2x/4x, MSP430FRxx RAM, MSP430G2x/i2x, MSP430L09x *Low Voltage*) i MSP430F5x/6x. Els primers estan orientats a ultra baix consum mentre que els darrers combinen baix consum i rendiment. Pel que fa als MCUs amb més rendiment, hi ha les famílies Piccolo, Delfino, C24x i Hercules, entre d'altres.

Les característiques bàsiques de la família MSP430 és que són microcontroladors de 16 bits, basats en RISC, orientats a baix o ultra baix consum. El consum pot arribar a ser inferior a 100 µA per MHz, fent que la vida de les bateries pugui arribar als 20 anys o més. El sistema de rellotje d'aquest MCU és que té l'habilitat d'habilitat i deshabilitat diversos rellotges i oscil·ladors, que permeten al dispositiu entrar en diversos modes de baix consum (LPMs – *Low Power Modes*).

A la taula següent es poden apreciar les característiques i diferències entre cada subfamília MSP430. Bàsicament el que canvia entre models és la màxima velocitat/freqüència de treball (de 4 fins a 24 MHz), la quantitat màxima de memòria no volàtil (de 0 fins a 512 KB) i SRAM (de 2 fins a 67 KB), el nombre de pins d'entrada/sortida –GPIO- i els tipus d'interfícies de comunicació suportats (UART, I^2C, SPI, etc.). També veiem que hi ha dos models o subfamílies, l'RF-430 i el CC430, que incorporen, a més, un transceptor RF a 13.56 GHz (freqüència RFID) o bé Sub-1GHz.

Series	Ultra-Low Power					Low Power + Performance	Security + Communications	
Part Number	L09x Low Voltage	G2x/I2x	F1x	F2x/F4x	FRxx FRAM	F5x/6x	RF-430	CC430
Max speed (MHz)	4	16	16	16	24	25	4	20
NVM (max KB)	0	56	120	120	128	512	ROM Fixed Function	32
SRAM (max KB)	2	4	10	8	2	67	4	4
GPIO	11	4–32	10–48	14–80	17–40	29–90	Up to 8	30–44
Comparator	●	●	●	●	●	●	●	●
Timer	●	●	●	●	●	●	●	●
ADC	●	●	●	●	●	●	On select	●
DAC	●		●	●		●		
UART		●	●	●	●	●	●	●
I^2C		●	●	●	●	●	●	●
SPI		●	●	●	●	●	●	●
Capacitive touch		●			●			
Multiplier		●	●	●	●	●		●
DMA			●	●	●	●		●
Op amps			●	●				
LCD				●	●	●		●
RTC				●	●	●		●
PMM					●	●	●	●
1.8-V I/O						●		
CRC					●	●	●	●
High-resolution timer						●		
USB						●		
Hardware encryption (AES)					●	●		●
FRAM					●		On select	
RF							13.56 MHz (ISO 15693 or ISO 14443B interface)	Sub-1GHz

Taula 15. Sèries de MCUs de la família MSP430 de TI.

NXP

NXP és un altre conegut fabricant de tot tipus de components i dispositius electrònics. Pel que fa als seus MCUs, es divideixen en quatre grans famílies: de 8/16 bit, de 32 bits *entry-level* (més econòmics), de 32 bits amb alt rendiment i específics d'aplicació.

- MCUs de 8/16 bit: tenim la subfamília LPC700, la LPC900 i l'OTP/ROM (*One-Time Programmable*, *ROMless*). Tots ells es basen en el 80C51 ja vist abans (com el 8051 però fabricat amb tecnologia CMOS en comptes d'NMOS i per tant amb un consum més baix). Aquests MCUs llencen un rendiment fins a sis vegades superior al 8051 original. La versió OTP únicament . Es pot veure que també tenen una versió programable un sol cop i/o sense ROM.

- 32 bits nivell d'entrada: hi ha les sèries LPC800, LPC1100 i LPC1200.

- 32 bits d'alt rendiment: tenim les sèries LPC1300, LPC1500, LPC1700, LPC1800, LPC2100/200/300/400, LPC2900, LPC3100/200, LPC400, LPC54100, LH7 I LH7A.

A les gràfiques de sota es pot veure les diferències en nombre de potes (*pins*) i quantitat de memòria Flash de cada sèrie de MCUs:

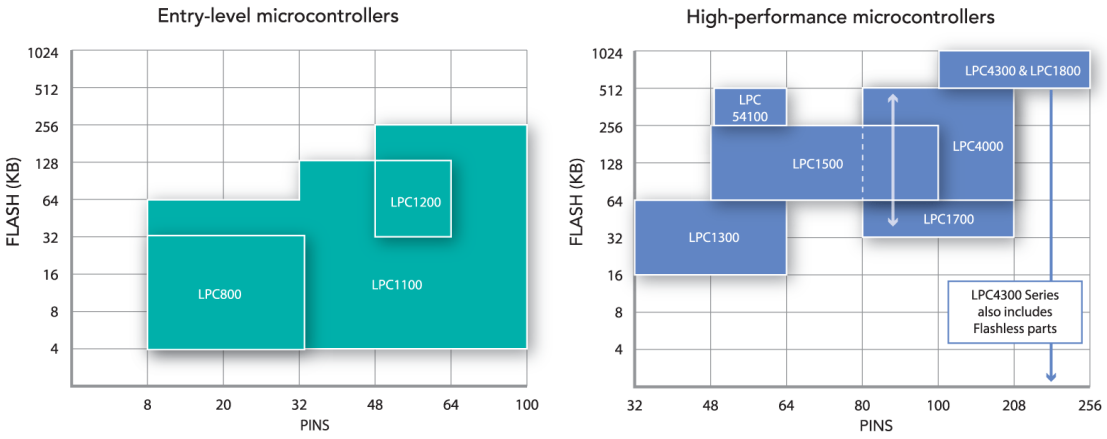


Figura 71. Nombre de *pins* i memòria Flash de cada sèrie de MCUs XNP de 32 bits.

Pel que fa als processadors de cada sèrie, tenim des del bàsic ARM Cortex-M0+ a 30 MHz de la sèrie LPC800, fins al potent ARM Cortex-M4F *Dual-Core* a 100 MHz o ARM Cortex-M4 a 200 MHz de les sèries LPC4300 i LPC54100, respectivament. Qualsevol d'ells es pot fer servir en aplicacions M2M/IoT tot i que, òbviament, els que consumeixen menys són els de la sèrie LPC800, ja que tenen menys potes, ocupen menys espai físic i funcionen a menys freqüència. Aquesta sèrie seria adient, per tant, per a aplicacions bàsiques de sensorització.

- Específics d'aplicació: hi ha la sèrie EM783 i JN516x. La primera sèrie està orientada a aplicacions d'*smart metering* i MPPT (*Maximum Power Point Tracking*) mentre que la segona es composa bàsicament d'un microcontrolador RISC de 32 bit (amb una quantitat de RAM, Flash i velocitat de CPU que depenen del model concret) més un transceptor RF de 2.4 GHz incorporat, adient per a xarxes ZigBree PRO o RF4CE.

  A la figura següent podem veure l'esquema de blocs dels MCUs de la sèrie JN516x.

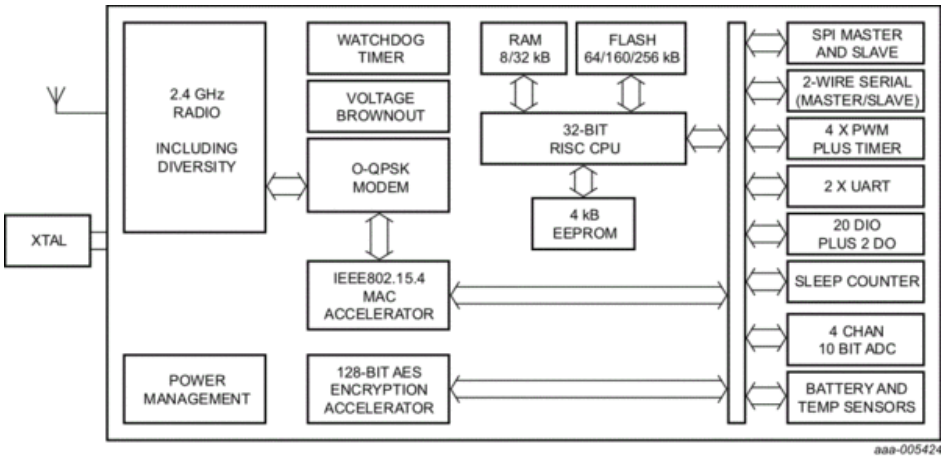


Figura 72. Diagrama de blocs de l'MCU NXP JN516x [44].

Al igual que la resta de fabricants, les diferències entre cada sèrie/model venen determinades per la velocitat màxima de rellotge, la quantitat de mèmoria Flash, RAM o EEPROM, les capacitats de comunicació (ports Ethernet, USB, UART, SPI, I^2C, etc.), el nombre de bits del DAC (conversor digital-analògic), els bits dels temporitzadors (*timers*) o el tipus d'empaquetament (*package*).

Freescale

Freescale és un fabricant de microcontroladors, processadors i sensors, entre d'altres. Pel que fa als MCUs, tenen tant de 8, 16 com 32 bits (aquests darrers són majoria). Les seves famílies són: Kinetis (baix consum), Qorivva (destinats a automoció, confiabilitat a llarg termini), MAC57Dxxx (destinats a targetes gràfiques) i Coldfire/Coldfire+ (combinació entre potència i consum). Si ens centren en la família Kinetis, les seves sèries són les que es mostren en la figura de sota:

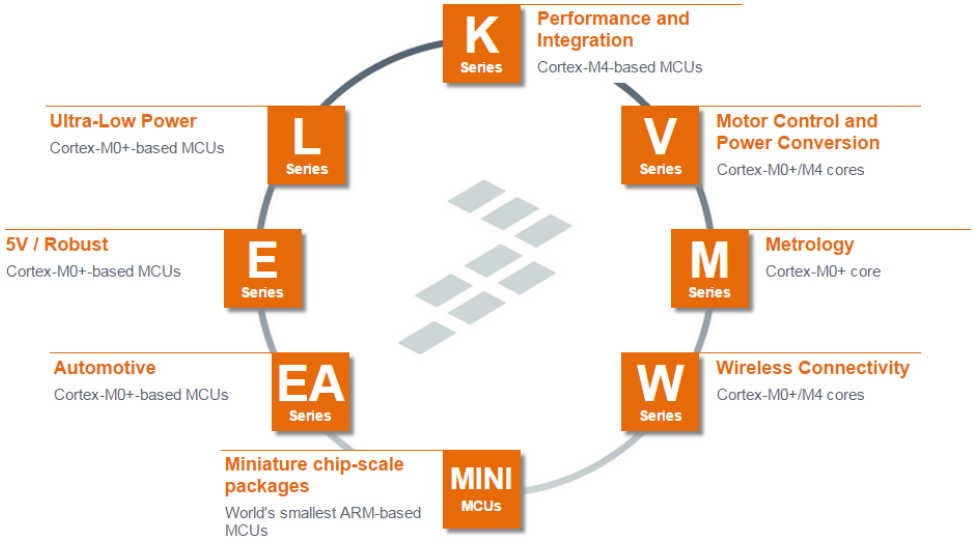


Figura 73. Sèries de la família d'MCUs Kinetis de Freescale.

Podem veure que totes les sèries es basen en els processadors de 32 bits ARM Cortex-M0+ i Cortex-M4. Les dues sèries més adients per a WSNs serien, per un cantó, la sèrie W (connectivitat sense fils) i, per altre cantó, la sèrie L (*ultra-low power*):

- Sèrie W: incorpora, a més del processador Cortex-M0+/M4, un transceptor RF (bé Sub-1 GHz o bé 2.4 GHz) per a aplicacions 802.15.4. La velocitat de rellotge és de 48-50 MHz, 128-512 KB de memòria Flash i 64 KB d'SRAM. Aquesta sèrie està optimitzada per a solucions sense fils encastades.

- Sèrie L: a més d'un processador Cortex-M0+ a 48 MHz, incorpora 8-256 KB de memòria Flash i fins a 32 KB de SRAM. Aquesta sèrie és la més adient per a temporitzadors de baix consum i perifèrics intel·ligents.

  A la taula de sota es poden apreciar les característiques de cada model concret de la sèrie L (quantitat de Flash, SRAM, nombre de potes, ports E/S, nombre de bits del DAC, etc.).

Common Features

System
ARM® Cortex®-M0+ Core, 48 MHz
Multi-Low-Power Modes and Peripherals, Low-Power Boot, Clock Gating
1.71–3.6 V, –40° C to +105° C [1]
Memory
90 nm TFS Flash, SRAM
Internal Memory Security/Protection
Analog Peripherals
12-/16-bit ADC, 12-bit DAC
High-Speed Comparator
Serial Interfaces
UART (including 1 LPUART)
SPI, I²C
Timers
Real-Time Clock [2]
16-bit Low-Power TPMs (SP Timer/PWM)
Low-Power Timers
32-bit Periodic Interrupt Timer

[1] Feature not available on CSP packages
[2] For KL02, use software to support

Feature Options

Family	Flash	SRAM	Pin Count	Key Features										
				USB	SLCD	DMA	RTC	ADC	DAC	I2S	TSI	Boot ROM	VREF	FLEXIO
KL46	128–256 KB	16–32 KB	64–121	OTG	√	√	√	16-bit	12-bit	√	√			
KL43	128–256 KB	16–32 KB	64	Slave	√	√	√	16-bit	12-bit	√		√	√	√
KL36	64–256 KB	8–32 KB	64–121		√	√	√	16-bit	12-bit	√	√			
KL34	64 KB	8 KB	64–100		√	√	√	12-bit						
KL33	128–256 KB	16–32 KB	64		√	√	√	16-bit	12-bit	√		√	√	√
KL27	128–256 KB	32 KB	32–64	Slave		√	√	16-bit	12-bit	√		√	√	√
KL26	32-256 KB	4–32 KB	32-121	OTG		√	√	16-bit	12-bit	√	√			
KL25	32–128 KB	4–16 KB	32–80	OTG		√	√	16-bit	12-bit		√			
KL24	32–64 KB	4–8 KB	32–80	OTG		√	√	12-bit						
KL17	128–256 KB	32 KB	32-64			√	√	16-bit	12-bit	√		√	√	√
KL16	32–256 KB	4-32 KB	32-64			√	√	16-bit	12-bit	√	√			
KL15	32–128 KB	4–16 KB	32–80			√	√	16-bit	12-bit		√			
KL14	32–64 KB	4–8 KB	32–80			√	√	12-bit						
KL05	8–32 KB	1–4 KB	24–48			√	√	12-bit	12-bit		√			
KL04	8–32 KB	1–4 KB	24–48			√	√	12-bit						
KL03	8–32 KB	2 KB	16–24				√	12-bit				√	√	
KL02	8–32 KB	1–4 KB	16–32					12-bit						

Taula 16. Models de la sèrie L (ultra baix consum) de la família Kitenis de Freescale.

Silicon Labs

Silicon Labs és una companyia que fabrica tot tipus de components electrònics: rellotges, oscil·ladors, sensors, transceptors RF, receptors de satèl·lit, demoduladors de TV digital, etc [81]. Pel que fa als seus MCUs, bàsicament es divideixen en tres grans tipus:

- De 8 bits: basats en l'MCU C8051, de manera similar als fabricants que ja s'han vist abans. L'arquitectura 8051 representa gairebé un 25% de la quota de mercat de microcontroladors en l'actualitat. Aquests MCUs tenen de 32 a 64 KB de memòria Flash, 4.25 KB d'SRAM i s'aconsegueix un rendiment de fins a 25 MIPS. Són MCUs que ocupen molt poc i gasten molt poc i es fan servir per aplicacions que no requereixen gran potència de procés (per exemple sensoritzat de temperatura)

- De 32 bits: basats en els processadors Cortex M-0+/M3/M4. Les famílies disponibles dintre d'aquest grup són: Zero, Tiny, Gecko, Leopoard, Giant, Wonder, SIM3L1xx, SIM3U1xx i SIM3c1xx, essent la primera família –Zero- la menys potent i amb menys memòria (24 MHz, 4-32 KB Flash, 2-4 KB RAM) i la darrera –SIM3C1xx- la més potent i amb més memòria (80 MHz, 32-256 KB Flash, 8-32 KB RAM).

- Sense fils/RF: són plaques amb MCU i transceptor RF sub-GHz incorporat. Hi ha tres famílies disponibles (de menys a més potència): Si106x (25 MHz, 64 KB Flash, 4 KB RAM), Si108x (25 MHz, 16 KB Flash, 0.75 KB RAM), EM35x (24 MHz, 192 KB Flash, 12 KB RAM).

Silicon Labs també disposa de plataformes de desenvolupament (sistemes en un xip), com per exemple Ember, basada en la família d'MCUs EM35x i destinada a xarxes ZigBee i ZigBee PRO.

Microchip Technology

Microchip Technology és l'empresa creadora de la famosa família de microcontroladors PIC (que actualment no és un acrònim però que originàriament significava *Peripheral Interface Controller*). El primer model va ser creat fa gairebé 40 anys, l'any 1975 (era un µC de 8 bits). Aquests MCUs fan servir arquitectura RISC i actualment hi ha quatre grans tipus: de 8 bits, de 16 bits (tipus PIC), de 16 bits (tipus dsPIC –com PIC però amb processador digital de senyal incorporat) i de 32 bit.

- 8 bits: tenim les famílies PIC10, PIC12, PIC16 i PIC18. Són els microcontroladors més econòmics (el seu preu unitari orientatiu quan es compra per volum –més de 5.000 unitats- pot arribar, com a mínim, als 0.31 USD). La memòria per a programes pot anar de 384 bytes fins a 512 KB, RAM de 16 byte a 4 KB, velocitat de CPU de 4 a 64 MHz, rendiment fins als 100 DMIPS (*Dhrystone MIPS*) i xips de 6 a 144 potes.

- 16 bits PIC: les famílies disponibles són PIC24F, PIC24H i PIC24E. El seu preu unitari en compra per volum pot arribar fins als 0.80 USD mínims. La CPU pot anar de 16 a 70 MHz, la memòria per a programes fins a 512 KB, la RAM fins a 96 KB, i poden tenir de 18 a 144 potes, depenen del model.

- 16 bit dsPIC: les famílies disponibles són dsPIC30F, dsPIC33F i dsPIC33E. El preu unitari mínim en compra per volum pot arribar als 1.57 USD com a mínim. La CPU pot arribar a 70 MHz, la memòrial per a programes fins a 512 KB, la RAM fins a a 52 KB i poden tenir de 12 a 122 pins, entre d'altres característiques.

- 32 bits: l'única família disponible és la PIC32 (però amb molts models dins de la mateixa). El preu unitari mínim arriba als 1.51 USD. La CPU pot arribar als 200 MHz, la memòria Flash a 2 KB i la RAM a 512 KB.

Pel que fa a MCUs de molt baix consum, la companyia té una sèrie de famílies basades en una tecnologia anomenada nanoWatt XLP (*eXtreme Low Power*), que es poden alimentar amb tensions de 1.8, 2.0 o 3.0V i que disposen de modes *sleep* que llencen consums molt baixos. Les famílies de microcontroladors disponibles són: PIC16F1503, PIC16F1823, PIC16F1827, PIC18F14K22, PIC18F46J50, PIC24F16KA102, PIC24FJ128GB204, PIC24FJ128GA310 i PIC24FJ128GC010. A mode d'exemple, a l'Annex IL es pot veure un full amb les característiques tècniques del PIC24FJ128GA310, que té un consum en mode adormit d'únicament 10 nA. Altres famílies incorporen característiques com ara encriptació i port USB [73].

Annex XXXIX. Sistemes en un Xip per a aplicacions IoT.

Broadcom BCM20736

La companyia Broadcom disposa del BMC20736, un que SoC pertany a la família de productes WICED (*Wireless Internet Connectivity for Embedded Devices – WiFi and Bluetooh Smart*) de la companyia.

Es composa d'una MCU ARM Cortex-M3, un transceptor RF de 2.4 GHz i piles Wi-Fi (802.11) i Bluetooh Smart, en un mateix xip. S'alimenta amb una pila de botó d'únicament 1.2V i inclou interfície SPI (*Serial Peripheral Interface*). La mida és d'únicament 6.5 x 6.5mm i està enfocat a la seva inclusió en *wearables* (roba, rellotges, etc).

Texas Instrument

La companyia Texas Instruments disposa de diversos SoC en el mercat, en funció de la tecnologia sense fils que es vulgui fer servir a la xarxa:

- Wi-Fi: es disposa del model CC3200 que, segons la companyia, es tracta d'un *wireless* MCU (microcontrolador sense fils). Segont TI, no es tracta d'un veritable SoC sinó d'un MCU amb connectivitat Wi-Fi 802.11 b/g/n integrada. Es basa en: processador ARM Cortex-M4 a 80 MHz; fins a 256 KB de RAM; interfícies UART, SPI i I^2C; *Cryto Engine* suportant AES, DES, 3DES, SHA2, MD5, CRC i Checksum; 27 potes GPIO; consum en hibernació de 4µA i en mode *deep sleep* 120 µA; ADC 12 bits.

- Bluetooth/BLE: es disposa dels SoCs CC2540 i CC2541, que es basen en: MCU de 8 bits 8051; 8 KB RAM; 128 o 256 KB memòria Flash; 21 potes GPIO; consum mínim de 0.4 µA (*stand-by*) o 0.9 µA (temporitzador *sleep* activat); alimentació de 2 a 3.6V; ADC 12 bits.

- Sub-1 GHz: es disposa, per un cantó, de la família CC430, que són SoCs que es basen en: MCU de 16 bits MSP430, fins a 32 KB memòria Flash; fins a 4 KB RAM; ADC 10 bits; alimentació d'1.8 a 3.6V; consum en mode *stand-by* 2.0 µA; bandes de freqüència 300-348 MHz, 389-464 MHz i 779-928 MHz. Per altre cantó, també hi ha els SoCs CC1110/CC1111, que es basen en: MCU de 8 bits 8051; fins a 32 KB Flash; fins a 4 KB RAM; consun mínim de 0.3 µA; mateixes bandes que el CC430.

- IEEE 802.15.4-2006, ZigBee, 6LoWPAN: es disposa, per un cantó, del SoC CC2538, que es basa en: processador ARM Cortex-M3 a 32 MHz; ràdio IEEE 802.15.4 a 2.4 GHz; fins a 512 KB memòria Flash; fins a 32 KB RAM; consum mínim de 0.4 µA; alimentació de 2 a 3.6V; suport per a AES, SHA2, RSA i ECC. Per altre cantó, el SoC CC2530, que és un model inferior, basat en l'MCU 8051 i que únicament admet fins a 256 KB de Flash i fins a 8 KB de RAM. Segons el fabriacant, tots dos models serveixen per a LLNs tot i que únicament el CC2538 està preparant per a entorns IoT.

A la figura següent es pot veure el diagrama funcional del TI CC2538, que és un dels més emprats per les empreses per implementar les seves plataformes de desenvolupament IoT. Es poden veure, entre d'altres, els blocs referents a memòria Flash, SRAM, EEPROM, oscil·ladors de 32 MHJz, temporitzadors, ADC de 12 bits, ràdio 802.15.4, seguretat, interfícies de comunicació i MCU ARM.

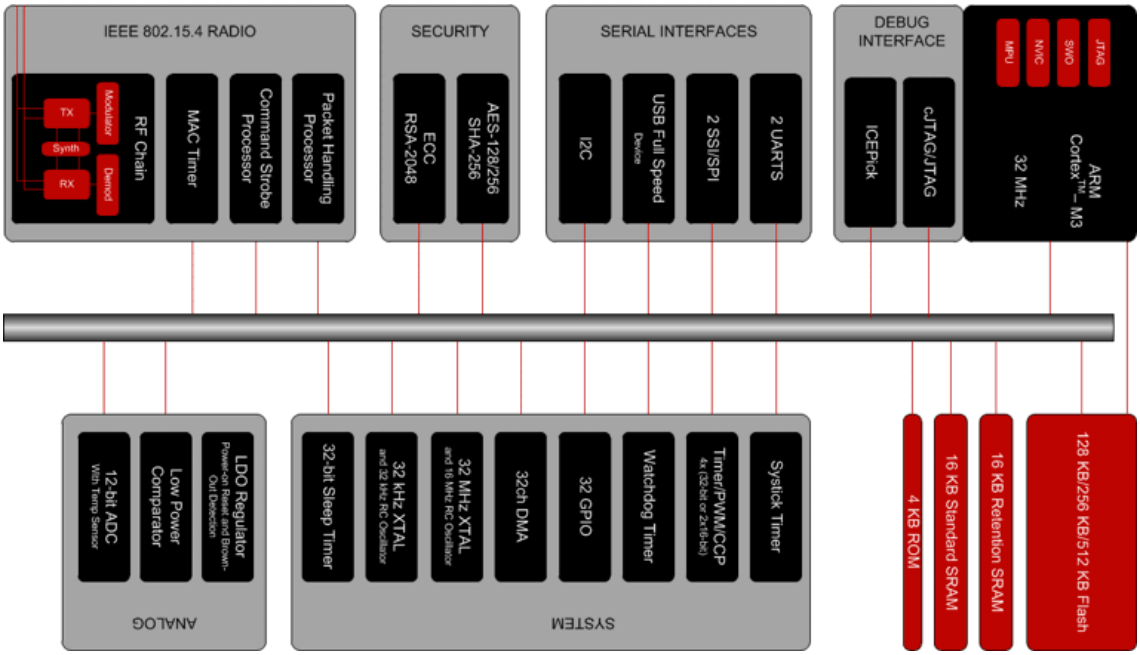


Figura 74. Diagrama de blocs del SoC TI CC2538.

Marvell

Al igual que abans, aquesta companyia també disposa dels seus propis SoCs de baix consum, preparats per IP, amb connectivitat Bluetooh, Wi-Fi o ZigBee, destinats a LLNs i aplicacions com ara *smart grid*.

- Bluetooth: tenim el 88MB300, SoC que es basa en: processador Cortex M-3 a 128 MHz, transceptor RF Bluettoth 4.1 + LE; 200 KB de memòria d'usuari; interfícies UART i I^2C; 32 potes GPIO. Està orientat a aplicacions de control d'enllumentat, automatització d'edificis i llars, *wearables*, cura de la salut, automoció, etc.

- ZigBee: tenim el 88MZ100, SoC basat en: Cortex-M3 a 32 o 64 MHz; transceptor ZigBee; alimentació de 2 a 3.6V; 31 potes GPIO; 512 KB memòria Flash. Està orientat a control d'enlllumenat, *smart metering*, automatització de llargs i edificions, cura de la salut, etc.

- Wi-Fi: tenim, per un cantó, el 88W8688, SoC basat en: CPU Marvell Feroceon a 106 MHz; ràdio 802.11a/b/g i Bluetooth 3.0 + HS; interfícies de comunicació SPI i UART; RAM i ROM (quantitats no especificades al web del fabricant); oscil·lador (font de rellotge) de fins a 52 MHz. Per altre cantó, també existeix el 88W8786 i l'Avastar 88W8782, que són semblants a l'anterior però tenen una CPU a 128 MHz i admeten

802.11n (300 Mbps màxims teòrics). Aquets SoCs estan orientats a plataformes de jocs, dispositius electrònics de consumidor (televisors, reproductos de Blu-Ray, etc.), impressores, càmeres fotogràfiques*, e-books*, etc.

Silicon Labs

Aquesta companyia disposa dels SoCs EM35x/EM358x/EM359x (tots ells de la sèrie Ember) que es basen en: processador ARM Cortex-M3 a 6, 12 o 24 MHz; transceptor RF IEEE 802.15.4 de 2.4 GHz (ZigBee); memòria Flash de 128 a 512 KB; RAM de 12 a 64 KB; oscil·lador a 24 MHz (opcional extern a 32 MHz); consum mínim de 0.4 µA. Les seves aplicacions principals són: *smart energy*, automatització de llargs i edificis, control d'enllumenat, automatització industrial i monitoratge i automatització de la seguretat.

Intel

La companyia Intel també disposa de la seva pròpia família de SoCs de baix consum: Quark i Tangier.

- Per un cantó, tenim l'Intel Quark, amb únic model disponible fins ara, l'X1000. Es tracta d'un Sistema en un Xip de 32 bits, que incorpora un processador Pentium (P54C/i586) a 400 MHz, 512 KB de RAM de tipus DDR3-800 (pot arribar fins a 2 GB); interfícies PCIe, UART, I^2C, Fast Ethernet i USB 2.0; mida de 15 x 15mm i preu unitari de 9.62 USD. Per si mateix, aquest SoC no incorpora cap transceptor ràdio, encara que es pot fer servir amb dispositius que incorporin ràdio Wi-Fi, Bluetooth o 3G (UMTS) entre d'altres.

- Per altra banda, tenim l'Intel Tangier, un altre SoC, que incorpora tant una CPU Atom *dual-core* a 500 MHz (una versió retallada de la CPU Atom Z34XX per a tabletes i *smartphones*) comn, al mateix temps, el SoC Quark fent de microcontroladora però "retallat" i funcionant únicament a 100 MHz. Aquest darrer es trobarà inactiu inicialment però es preveu que executi el sistema operatiu en temps real (RTOS) ViperOS.

Cap dels dos SoC incopora transceptor RF per sí mateix, encara que les plataformes –plaques- de desenvolupament que els incorporen –veure propers apartats- sí que disposen de mòduls de comunicació sense fils, per exemple ràdio a 2.4 GHz (Wi-Fi, BLE).

Ambdós SoCs estan destinats a aplicacions IoT molt específiques, principalment *wearables* i aplicacions personals/a la llar. Es tracta, però, d'alternatives més costoses i que consumeixen més que les d'altres fabricants, com ara els SoCs de Texas Instruments.

No s'ha de confondre Intel Quark -que és un SoC, amb CPU Pentium- amb Intel Tangier –un altre SoC, amb CPU Atom i que també incorpora, eventualment, un SoC Quark però retallat. Tampoc s'ha de confondre cap dels dos amb Intel Galileo -una plataforma de desenvolupament certificada per Arduino i que incopora el SoC Intel Quark- ni amb Intel Edison –inicialment un mini-ordinador de la mida d'una targeta de memòria SD i actualment una altra plataforma de desenvolupament, que incorpora el SoC Intel Tangier.

Annex XL. Plataformes de desenvolupament per a IoT.

Intel

Com ja s'ha dit a a l'apartat anterior, Intel disposa actualment de dues plataformes/plaques de desenvolupament basades en SoCs seus, totes dues pensades per a prototipatge d'aplicacions:

- Galileo: actualment Galileo GEN2, es tracta d'una placa que incorpora el SoC Quark X1000, a més de ranura PCIe, port FE a 100 Mbps, ranura microSD (accepta targetes de màxim 32 GB) i port client USB. Es tracta d'una plataforma certificada per Arduino i dissenyada específicament per a creadors, desenvolupadors, educadors i entusiastes de l'ectrònica. A nivell de sistema operatiu, és compatible amb Windows, MAC OS i Linux. S'alimenta amb 12V. Es pot afegir una ràdio a través dels seus ports de comunicació (per exemple a través d'un *dongle* USB o tarjeta PCI).

- Edison: en aquest cas, aquesta placa incorpora el SoC Tangier, que es basa en una CPU Intel Atom de doble nucli a 500 MHz i tecnologia de fabricació de 22 nm, així com el SoC Quark fent les funcions de microcontroladora i "capat" a 100 MHz. Inicialment, el projecte Edison estava destinat a ser un mini-ordinador de molt baix consum i de la mida d'una targeta de memòria SD però la segona versió del projecte va mostrar Edison com una plataforma de desenvolupament en comptes de com un ordinador *standalone*. La placa Intel Edison incoropora, entre d'altres, una ràdio Broadcom 43340 de banda dal (2.4 i 5 GHz), compatible amb Wi-Fi 802.11 a/b/b/n i Bluetooh 4.0. El consum de la placa sense la rádio activada és de 13 mW i l'alimentació de la placa és de 3.3 a 4.5 V.

Una de les principals diferències entre Galileo i Edison és que la primera no incorpora ràdio de sèrie mentre que la segona sí que incorpora un mòdul Wi-Fi/BLE per defecte. D'aquesta manera, Edison es troba molt més orientada a aplicacions IoT que no pas Galileo [42]. A més, el consum i necessitats d'alimentació d'Edison també són menors.

A la figura de sota es poden veure les dues plaques de desenvolupament en la seva darrera versió (Desembre 2014):

Figura 75. Plaques de desenvolupament Intel Galileo GEN2 i Intel Edison [60]

Per la seva banda, la figura de sota mostra l'interior del mòdul Intel Edison, que és el veritable "cor" de la placa anterior. A la figura es pot veure, gairebé al centre, el mòdul Wi-Fi/BLE, així com l'antena interna i el connector coaxial per si es vol una antena externa:

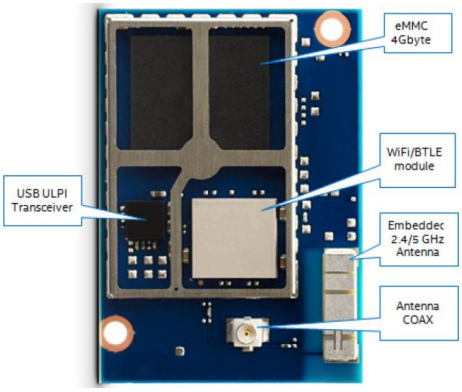


Figura 76.Módul Intel Edison [46]

Arduino

Arduino és una plataforma de maquinari lliure, basada en una placa amb un MCU i un entorn de desenvolupament, dissenyada per facilitar l'ús de l'electrònica en entorns multidisciplinars. Originalment el HW consisteix en una MCU Atmel AVR de 8 bits (per exemple Atmega168, Atmega328 o Atmega1280) encara que avui dia també es fan servir MCUs ARM Cortex-M3 de 32 bits. Fins i tot i, tal i com s'ha vist a l'apartat anterior, també existeixen plataformes Arduino basades en el SoC Quark d'Intel. En funció de l'MCU que es faci servir, l'alimentació serà de 3.3 o 5V.

Avui dia hi ha molts models de placa Arduino en el mercat: Uno, Leonardo, DUE, Yún, Tre, Zero, Micro, Esplora, Mini, Nano, etc, en funció de les característiques de MCU, memòria i ports que aquesten incorporen. Per exemple, si ens centren en aplicacions IoT, algunes de les plataformes Arduino més adients són les següents:

- TinyDuino: basada en l'MCU Atmega328P, 32 KB de memòria Flash, 2 KB de RAM i 1 KB d'EEPROM, amb connectivitat RF via mòdul extern (Wi-Fi o BLE). Bàsicament, té la potència de l'Arduino Uno però amb una quarta part de la seva mida.

- Arduino Uno: basada en l'MCU Atmega328, amb 32K de Flash.

- XinoRF: és tracta d'una plaaca Arduino UNO R3 amb un mòdul ràdio Ciseco SRF. Té les mateixes quantaits de memòria que les plaques anteriors.

- Pinoccio: es basa en l'MCU ATmega256FR2 a 16 MHz però incorpora, a més, una ràdio a 2.4 GHz (802.15.4 i Wi-Fi) i una bateria LiPo. La seva mida és tan sols una miqueta més gran que un llapis de memòria USB. Els nodes poden funcionar com a *field scout* (es reenvien dades entre ells) o *lead scout* (pasarel·la que connecta a Internet).

A la figura següent es mostra l'aspecte d'una mota placa Arduino Pinoccio (*field scout*).

Figura 77.Arduino Pinoccio (*field scout*).

El preu d'aquest darrer és d'uns 59 USD (mota) o 138 USD (pasarel·la Wi-Fi).

Raspberry Pi

A diferència d'una placa Arduino (destinada a desenvolupament i prototipatge), una placa Raspberry Pi esdevé una computadora/ordinador complet per sí mateixa. La principal diferència és que una Raspberry ja incorpora sortida de vídeo (port HDMI) però també hi ha altres diferències, com ara que la Raspberry també incorpora de sèrie un port Ethernet JR-45 i que la velocitat de rellotge també és molt més elevada. També incorpora quatre ports USB, així com un port especial CSI per connectar una càmera, un port DSI per connectar una pantalla tàctil i un jack 3.5mm per a sortida d'àudio.

Una Raspberry Pi es basa en un SoC Broadcom BCM2835 a 700 MHz que, al seu voltant, es basa en un processador ARM1176JZFS i una GPU VideoCore IV; a més disposa de 512 MB de RAM, compartida entre CPU i GPU (Raspberry Pi model B). A nivell de CPU, el rendiment d'una Raspberry és similar al d'un Pentium II a 300 MHz, mentre que a nivell gràfic, la potència és equivalent a la d'una consola XBox de primera generació. Per altra banda, una altra particularitat és que el SoC es troba apilat sota el xip de RAM, per la qual cosa gairebé no és visible. El preu unitari del model B+ és d'uns 35 USD. L'alimentació de la placa ha de ser de 5V (a través de port MicroUSB) i el consum és d'uns 600 mA (3.0 W) per al model B+.

Donat l'alt consum d'aquesta placa, sembla clar que no és un component idoni per a LLNs, tot i que es pot fer servir en xarxes que es puguin connectar al corrent elèctric o a fons d'energia alternatives (per exemple mitjançant plaques solars).

A la figura de sota es mostra l'aspecte d'una Raspberry Pi model B+:

Figura 78.Raspberry Pi B+.

BeagleBone Black

Aquesta placa és similar a una Raspberry Pi. Es basa en un processador TI AM 335x (ARM Cortex A-8) amb velocitats que poden anar de 300 a 1000 MHz, 4 GB de memòria Flash, 512 MB de RAM DDR3, acceleradora gràfica 3D i ports Ethernet RJ-45, USB i HDMI. També existeix el model BeagleBone original (sense el "Black"), que únicament disposa de 256 MB de RAM i no té port HDMI (aquest model s'assemblaria més a un Arduino), així com models BeagleBoard i BeagleBoard-xM, que incorporen acceleració 3D adicional i reproducció de vídeo HD. En tots els casos l'alimentació és de 5V DC. El preu aproximat de la versió Black és d'uns 60 USD.

Al igual que passa amb Arduino i Raspberry Pi, degut al seu consum promig, entre 210-460 mA a 5V (molt alt comparat amb altres alternatives *ultra-low power*), fan aquesta opció adient per a entorns de desenvolupament i proves però potser no per a entorns de producció, on els motes han de tenir uns requeriments d'energia el més petits possibles. Un aventatge de la placa és que pot funcionar tant en mode "dispositiu final" (motes que es reenvien dades entre elles) com en mode "pasarel·la" (connexió amb xarxa externa).

A la figura de sota es motra l'aspecte extern d'una BeagleBone Black:

Figura 79. Placa BeagleBone Black.

Libelium Waspmote

Aquesta placa, de l'empresa Libelium, es basa en un MCU ATmega1281 a 14 MHz, 8 KB SRAM, 4 KB EEPROM i 128 KB de memòria Flash. Té una ranura per a targetes SD de fins a 2 GB. El consum en mode *sleep* es d'uns 55 µA i en mode hibernació de tant sols 0.7 µA (hi ha una versió PRO de la placa, que únicament consumeix 0.06 µA en hibernació), mentre que en mode actiu és de 15 mA. El voltatge de la bateria va de 3.3 a 4.2V; aquesta es pot carregar via port USB o bé mitjançant panell solar. S'incorpora un endoll (*socket*) per a sensors bàsics, com ara temperatura, humitat i llum, encara que en realitat es poden connectar fins a 70 tipus de sensors diferents, a través de plaques adicionals (gasos, videocàmera, radiació, mesurament d'aigua, aparcament intel·ligent, etc). Opcionalment, també se li pot acoplar un mòdul GPS. El pes de la placa és de 20 grams.

Un dels grans avantatges d'aquesta placa, a més de la gran quantitat de sensors que es poden connectar, és la gran diversitat de tecnologies ràdio –interfícies sense fils- que admet, tant de gran abast (GPRS, UMTS, LoRA, 868-900 MHz), de mig abast (802.15.4, ZigBee/PRO, Wi-Fi, 6LoWPAN) i de curt abast (RFID, NFC, BLE), a través de mòduls adicionals.

Altres avantatges és que es pot programar per l'aire (OTA – *Over The Air*), incorpora llibreries d'encriptació AES i RSA i soporta protocols industrials (RS-232, RS-485, Modbus, CAN BUS i 4-20 mA).

A la figura de sota [83] es mostra l'aspecte de la placa per tots dos costats:

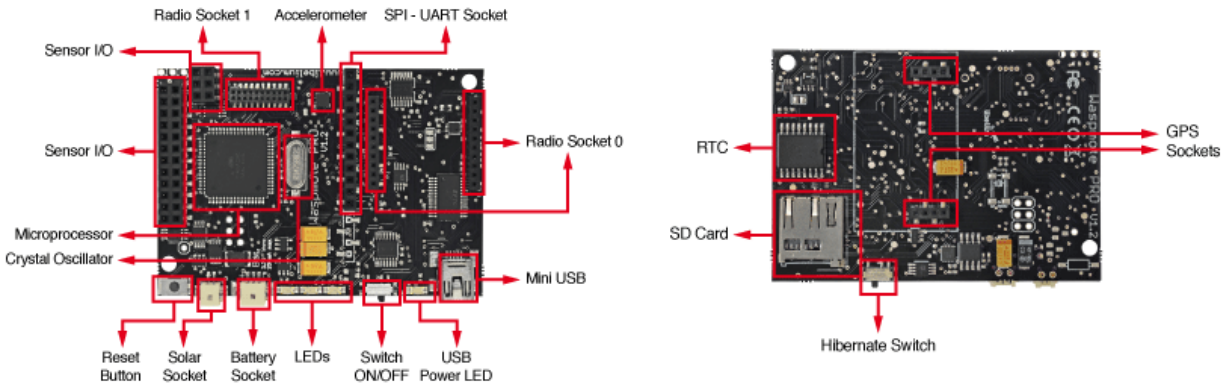


Figura 80. Placa Libelium Waspmote.

Per la seva banda, la figura de sota mostra la placa amb un mòdul ràdio connectat, concretament el de 6LoWPAN, amb antena externa mitjançant connector coaxial.

Figura 81. Waspmote amb mòdul ràdio 6LoWPAN a 868 MHz.

La primera figura mostra un dispositiu final (end node) o mota corrent, mentre que la segona mostra un dispositiu de tipus *gateway* (que connecta amb una xarxa IPv4 i/o amb Internet, mitjançant un port Fast Ethernet RJ-45). A aquest darrer port se li podria connectar, en cas de necessitat, un adaptador Wi-Fi, com ara el de la figura següent:

Figura 82. *Dongle* Wi-Fi amb connector RJ-45.

L'empresa ven, juntament amb IBM, un *pack* anomenat *WaspMote Mote Runner Networking Kit,* especialment enfocat per al desenvolupament i experimentació d'aplicacions IoT amb IPv6 i que inclou cinc nodes de tipus *End Device* i un node de tipus *Gateway*, per un preu total de 1.425 EUR, per la qual cosa cada mota tindria un cost unitari aproximat d'uns 230-240 EUR (tanmateix, en les motes que es venen individualment, en funció del tipus de ràdio i la ganància de l'antena escollides, el preu pot reduir-se fins als 150-160 EUR per mota). Tots els nodes del *kit* incorporen mòduls ràdio 6LoWPAN (bé a 868 MHz o a 2.4 GHz, a escollir) i es poden programar mitjançant llenguatges C# o Java i a través de l'aire. També s'inclouen bateries de 2300 mAh per a cada node, així com sis antenes externes i sis adaptadors de corrent 220V USB.

La figura de sota mostra el contingut complet d'aquest *kit*:

Figura 83. Contingut del paquet WaspMote Mote Runner Networking Kit.

El seu baix consum en mode adormit (sobretot en la versió PRO de la placa); la possibilitat de connectar tot tipus de ràdios –fins i tot 6LoWPAN; el fet que admeti entre 60-70 tipus de sensors diferents ja provats; que pugui fer-se servir com a dispositiu final o pasarel·la; i, per últim, que el *Time to Market* de la solució sigui molt reduït (en tractar-se d'una plataforma propietària, que bàsicament és *Plug & Play* si no es vol desenvolupar amb ella sinó simplement recol·lectar dades tal i com es capten dels sensors) fan que aquesta alternativa sigui una de les més adients per a desenvolupament i implementació de solucions IoT/LLNs.

TelosB

TelosB és una mota dissenyada per la comunitat de desenvolupament de la Universitat de California, Berkeley. Es basa en un MCU de 16 bits TI MSP430 a 8 MHz, amb 10 KB RAM, EEPROM per a dades de configuració de 16 KB, 48 KB de memòria Flash interna i 1 MB de Flash externa (per a emmagatzematge de logs) [100]. Inclou un CDA i un CAD de 12 bits, així com un transceptor ràdio IEEE 802.15.4 (TI CC2420) a 2.4 GHz amb antena interna integrada, tot plegat aconseguint taxes de dades màximes de 250 Kbps. Inclou un connector USB per a la seva programació, així com sensors integrats de llum, temperatura i humitat relativa. El consum de corrent en mode *idle* (en espera) és de 23 µA, mentre que en mode *sleep* és de tant sols 1 µA, S'alimenta amb dues bateries de tipus AA. El sistema operatiu que fa servir és TinyOS 1.1.11 o una versió superior (encara que també pot córrer d'altres, com ara Contiki). El pes de la placa és de tant sols 23 grams.

A la figura de sota es pot veure el diagrama de blocs de la mota, així com el seu aspecte extern:

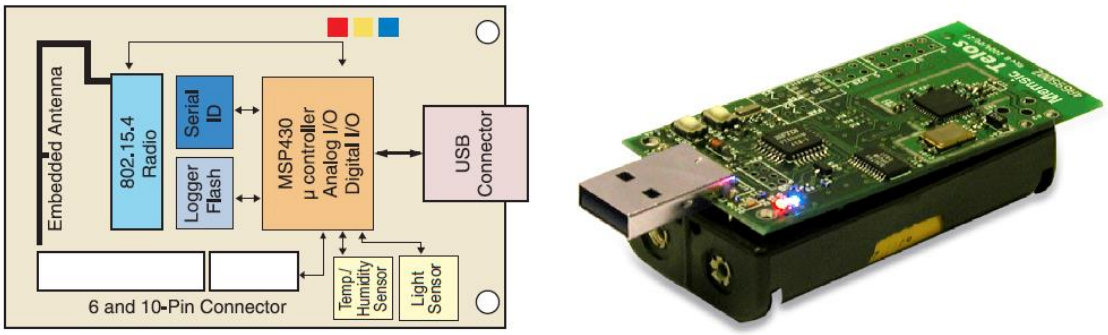


Figura 84. Diagrama de blocs i aspecte extern de mota TelosB.

Com que es tracta d'una plataforma oberta, hi ha moltes empreses que comercialitzen motes basades en TelosB, com per exemple AdvanticSys (MTM-CM5000-MSP), Memsic (TPR2420) o Epsssilon Networks (EPS-5000 i XM-1000).

Donat el seu baix preu unitari -uns 69 USD- es tracta d'una opció molt adient per a plataformes de recerca i desenvolupament (R+D), ja que permet creat LLNs de baix cost on, a més, si es vol monitorar llum, humitat o temperatura, els sensors ja venen integrats a la pròpia mota. El principal problema d'aquesta placa és que no es pot expandir amb mòduls adicionals, per la qual cosa, entre d'altres, únicament pot actuar com a *end device* però no com a pasarel·la, ja que no incorpora cap port (per exemple port USB o FE RJ-45) que permeti afegir un mòdul Wi-Fi, GPRS o similar per a comunicació amb una xarxa exterior (per exemple amb Internet).

GINA

GINA són les sigles de *Guidance and Inertial Navigation Assistant* (Assistent de Navegació Inercial i Guia). Es tracta d'una placa desenvolupada a través del projecte WARPwING (*Wireless Autonomous Robot Platform with Inertial Navigation and Guidance*), per part de l'UC Berkeley. GINA 2.2 –darrera versió disponible- és una mota "tradicional", basada en un MCU TI MSP430 i una ràdio de baix consum Atmel AT86RD231 (transceptor RF a 2.4 GHz, compatible amb IEEE 802.15.4, ZigBee, RF4CE, SP-100, WirelessHART i aplicacions ISM). A més, inclou una antena interna (Rainsun AN3215-245), així com conector per antena externa. La placa s'alimenta amb una bateria externa (per exemple, una bateria de 130 mAh LiPo (polímer de Liti) a 3.7V.

La particularitat d'aquesta mota és que incorpora un sensor de temperatura (TI TMP20AIDRLT), així com acceleròmetre de sensitivitat (STMElectronics LIS344ALHTR), acceleròmetre de llarg abast (Kionix KXDS9-1026), giroscopi (Invensense ITG3200) i magnetòmetre (Honeywell HMC5843).

A la figura de sota es pot observar l'aspecte de la placa per tots dos costats:

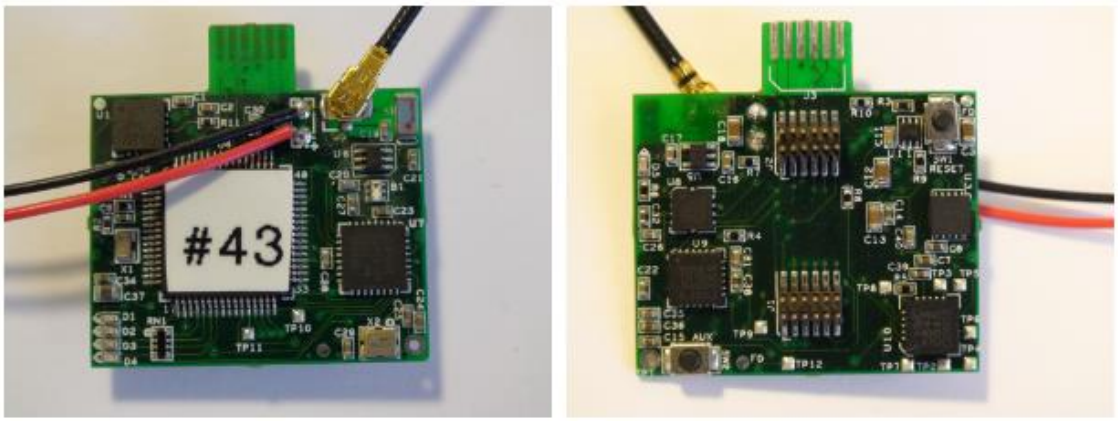


Figura 85. Aspecte extern mota GINA.

També existeix una altra configuració de la placa, anomenada GINA-*basestation*, que es tracta d'una versió retallada de l'original, que no inclou cap capacitat de mesura ni sensor). Per la seva part, també existeix la GINA-*breakout*, que és una targeta que permet connectar sensors externs a la placa GINA.

OpenMote-CC2528

En aquesta ocasió, ens trobem amb una mota fabricada per l'*startup* catalana OpenMote Technologies. Es tracta d'una placa basada en el SoC CC2538 de TI que, al seu voltant, consta d'un MCU ARM Cortex-M3 de 32 bit a 32 MHz i un transceptor TI CC2520, compatible IEEE 802.15.4-2006. L'MCU inclou 32 KB de RAM i 512 KB de memòria Flash, així com la resta d'elements necessaris en aquests casos (GPIOs, ADC, temporitzadors, etc).

La placa també inclou, per altre cantó, un convertidor DC/DC reductor TI TPS62730, que permet o bé deixar passar la tensió d'entrada de 3V inalterada cap al circuit –mode *bypass*- o bé abaixar-la fins a 2.1V –mode regulat- permetent millorar l'eficiència del sistema, tant quan la mota es troba emetent/rebent, com quan es troba en mode *sleep*; un cristall Abracon ABM8G a 32 MHz (valotat a 30 ppm) que fa de rellotge del MCU i la ràdio; un altre ccristal Abracon ABS07 a 32.768 MHz (valorat a 10 ppm) que fa de rellotge del RTC (*Real Time Clock*) de l'MCU; quatre LEDs (vermell, verd, groc i taronja) per a depuració; dos butons (per a fer un reset i per despertar l'MCU del mode *sleep* a través d'una interrupció) i un connector per a antena externa.

Una particularitat d'aquesta mota és que té un factor de forma (*form factor*) que compleix amb XBee, la qual cosa significa que pot comunicar-se amb una computadora fent servir un *dongle* USB, concretament l'*XBee Explorer Dongle*, de l'empresa SparkFun Electronics. D'aquesta manera, el *dongle* es connecta a l'ordinador i fa de pasarel·la entre aquest darrer i la mota, fent possible la programació de la mateixa. El preu d'aquest dongle és d'uns 25 USD.

A la figura de sota es pot veure l'OpenMote-CC2538 (a la dreta, part superior) amb una antena externa connectada a través del connector micro-coaxial adient. La mota es troba connectada, al seu voltant, a l'*XBee Explorer Dongle* (part dreta, pla inferior) que fa de *gateway* amb un ordinador a través del seu port USB. Finalment, el *dongle* es connecta a una Raspberry Pi (part esquerra) que fa les vegades de computadora, per a la programació de la mota.

Figura 86. OpenMote-CC2538 connectat a *dongle* USB i aquest a Raspberry Pi.

A més de la pròpia mota, l'empresa també comercialitza els següents dos complements de maquinari:

- OpenBattery: una placa que es connecta a la mota a través dels connectors XBee (*Xbee header*) i que incorpora un receptacle per a dues bateries de tipus AAA, un commutador per encendre i apagar la placa i tres sensors digitals (temperatura/humitat, acceleració i llum), que es comuniquen amb la mota a través del bus I^2C.

- OpenBase: una placa interfície amb la mota que es connecta amb aquesta darrera, igual que en el cas de la bateria, fent servir els pins XBee. La finalitat de la placa és triple: programar i depurar codi, fent servir una sonda amb un connector estàndard ARM JTAG de 10 potes; permetre la comunicació amb una computadora a través de port Sèrie o USB per programar i depurar la mota; habilitar la comunicació amb una xarxa Ethernet 10/100 Mbps, permetent per tant connectar-se a la mota remòtament, sense necessitat de connexió directa a un ordinador.

A la figura de sota podem veure, a l'esquerra, l'aspecte de l'OpenBattery i, a la dreta, el de l'OpenBase:

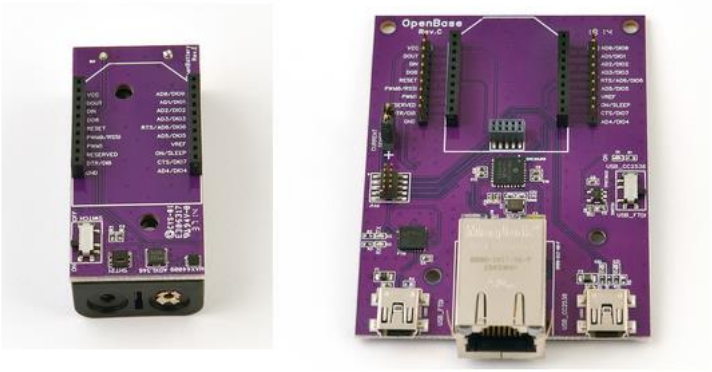


Figura 87. Mòduls OpenBattery i OpenBase per a OpenMote [30].

Actualment, les motes poden córrer el sistemes operatius Contiki, OpenWSN, FreeRTOS o RIOT.

El preu unitari d'una mota OpenMote-CC2528 és de 90 EUR, mentre que el de la placa OpenBase és de 60 EUR i el de l'OpenBattery és de 30 EUR. També es venen *kits* formats per dues, cinc o deu motes, anomenats Bronze, Silver i Gold i amb preus de 250 EUR, 500 EUR i 1.000 EUR, respectivament. Per exemple, el kit Gold inclou deu motes, nou OpenBattery i un OpenBase. Això significa que nou motes poden funcionar com a *end devices* (també anomenats *remote nodes*) mentre que l'altra mota restant, que es connectarà a una computadora a través de l'OpenBase, farà de pasarel·la o *gateway* (també anomenat *sink node*) amb una xarxa exterior.

Com es pot veure, aquesta mota representa una alternativa més econòmica a altres ja vistes, com ara Waspmote (preu unitari per mota de 90-100 EUR en el cas d'OpenMote-CC2528 Vs 150-240 EUR en el cas de Libelium Waspmote). A més, el processador d'OpenMote (ARM Cortex-M3, 32 bit, 32 MHz) és molt més potent que el de Libelium (ATmega1281, 8 bit, 14 MHz). L'OpenMote també inclou quatre vegades més d'SRAM (32 KB Vs 8 KB) i de Flash (512 KB Vs 128 KB). Per altra banda, els avantatges de la mota de Libelium és que incorpora una ranura per a targeta SD de fins a 2 GB, que es poden connectar més de 60 plaques de sensors específiques per a la plataforma i que es pot incorporar tot tipus de ràdios (UMTS, GSM, GPRS, Wi-Fi, BLE, etc.)

Altres plataformes

A banda de les plataformes de R+D per a LLNs i solucions IoT que s'han vist fins ara, existeixen moltíssimes més, com ara: Arago Systems WiSMote Dev, Arago Systems WiSMote Mini, COOKIEs, BEAN, BTnode, COTS, Dot, EPIC mote, GWnode, IMote, SenseNode, Tmote Sky, Zolertia Z1, Firefly, WiSense, BitSense, Ubimote 1 i 2; etc.

Seria massa extens comentar-les totes, ja que n'apareixen de noves gairebé cada setmana. A més, totes elles són molt semblants, ja que es basen sempre en els mateixos SoCs i MCUs i totes acostumen a incorporar ràdios de 2.4 GHz que compleixen l'estàndard IEEE 802.15.4. Les diferències entre plataformes radiquen bàsicament en: la potència de l'MCU o processador de cadascuna; la quantitat de RAM i Flash que incorporen; la possibilitat d'afegir sensors externs, antena externa i bateria externa; *slot* per targetes de memòria externa; etc. Un punt important també és el consum de les motes, tant en mode actiu, com en mode *idle* (espera) i en mode *sleep*, tot i que en la majoria dels casos acostuma a ser de l'ordre de molt pocs µA en mode adormit.

Per exemple, tenim el cas de Tmote Sky, que no és més que una evolució/reemplaçment d'una mota Telos. De fet, la mota TelosB –vista en apartats anteriors- també es ven amb el nom de MoteIV Tmote Sky.

Annex XLI. Sistemes operatius per a aplicacions IoT.

OpenWSN

OpenWSN no es tracta d'un sistema operatiu en sí mateix, sinó d'una implementació de codi obert d'una pila de protocols completa, basada en els estàndars de l'Internet de les Coses i, per tant, en IPv6/6LoWPAN i 802.15.4e a nivell MAC, destinada a la creació de WNs en entorns limitats [2]. Aquest programari està desenvolupat per l'UC Berkeley, la darrera versió disponible és la 1.8.0 i es divideix en dos parts: *firmware* i *software*. La primera, és la part de codi que s'ha de compilar i executar en les motes, mentre que la segona és la part que es compila i s'executa en les computadores (per exemple les que fan de *gateway* o aquelles que volen comunicar-se amb les motes). El *code footprint* –mida del codi- de la pila completa OpenWSN és de tant sols 30 KB en memòria Flash i d'uns 3.5 KB en RAM [38].

OpenWSN implementa els següents protocols de l'IoT:

- A nivell d'Aplicació: CoAP i HTTP
- A nivell de Transport: TCP i UDP
- A nivell de xarxa i encaminament: IETF RPL
- A nivell de capa d'adaptació: IETF 6LoWPAN
- A nivell d'accés al medi (MAC): IEEE 802.15.4e
- A nivell de capa física (PHY): IEEE 802.15.4-2006

Pel que fa al maquinari –motes- suportades, són aquestes actualment:

- TelosB
- GINA
- WSN430
- Z1
- OpenMoteCC2538
- OpenMoteSTM
- SAM R21 Xplained Pro
- USP Mote MC13213
- USP Mote CC2538
- IoT-LAB_M3
- AgileFox
- A nivell experimental
    - OpenMoteHack
    - K20hack
    - USP/SC Motes
    - eZ430-RF2500
    - Current Monitor
    - XpressoHack

En realitat i, en línies generals, qualsevol maquinari del llistat següent hauria d'estar suportat per OpenWSN:

- SoCs: Ember EM357, STMicroelectronics STM32W, Freescale MC13224V, Jennic JN5148, TI CC2531.

- MCUs: ARM7TDMI, ARM920T, MSP430f2274, MSP430f1611, ATmega128A.

- Ràdios IEEE802.15.4: AT86RF230, AT86RF231, TI CC2420, TI CC2520.

- Motes: deUSB2400, RAVEN, EPIC, TelosB, IRIS, MICAz, CC2531EMK.

Per altra banda, pel que fa a la part que ha de córrer en una computadora, existeixen *ports* –versions- tant per al sistema operatiu Linux com per a Windows.

A banda del programari anterior, OpenWSN també posa a disposició dels usuaris els següents elements de *software*:

- OpenSim: programa que permet simular una xarxa OpenWSN sense necessitat de dispositius –nodes- físics. Es necessita el compilador `gcc` instal·lat a la computadora, així com un mòdul d'extensió Python, ja que el *firmware* de cada mota es compila a la pròpia computadora com un mòdul Python. El programa pot córrer tant en Linux com en Windows. Bàsicament, es tracta de crear "motes virtuals" a la computadora, de manera similar a com es crearia una màquina virtual fent servir algun programari de tipus VMWare, VirtualBox, Xen o similar. Les motes virtuals, un cop configurades, poden comunicar-se entre ells o bé amb motes físiques i a la inversa.

- OpenVisualizer: és l'eina principal per poder connectar una xarxa OpenWSN a Internet (IPv4), fent servir una interfície virtual. Pot executar-se en Linux i Windows. Suporta tant nodes físics com nodes emulats amb OpenSim (per a OpenVisualizer, el fet de tractar-se de motes físiques o virtuals és completament transparent).

- Llirería Python per a CoAP: com el seu propi indica, són les llibreries que permeten suportar CoAP, tant a nivell de client com de servidor, així com les següents característiques: missatges confirmables i no confirmables, *timeouts* i reintents, peticions concurrents. En canvi, la implementació del protocol encara no suporta funcionalitats com ara el *caching*, el *proxying*, la seguretat DTLS o el *multicast*, entre d'altres.

- Endpoint: es tracta d'un programa en Phyton que, bàisicament, s'instal·la en una computadora destinació i que fa el següent: escolta els paquets entrants –típicament UDP; posa un segell temporal –*timestamp*- a cada paquet que arriba i els passa a un *parser*; passa els paquets 'parsejats' a un llistat de publicadors; finalment, cada publicador publica les dades que necessita. Una publicació pot ser des d'una impressió a la pantalla a un fitxer de *log*, passant per una piulada (Twitter), un SMS, etc.

Contiki

De manera similar a OpenWSN, Contiki també suporta i implementa tots els estàndars relatius a LLNs: 6LoWPAN, RPL i CoAP. També suporta els clàssics HTTP, UDP i TCP, entre d'altres [101]. La diferència principal radica en que Contiki sí que és un sistema operatiu en sí mateix i segueix un apropament modular, similar al concepte de capes. Altra característica diferenciadora és que requereix molt poca quantitat de memòria per executar-se (el que en anglès es denomina *small footprint*): en concret, únicament es necessiten menys 10 KB de RAM i 30 KB de ROM per a poder implementar IPv6 amb encaminadors –nodes que reenvien paquets a altres nodes- adormits i encaminament RPL.

Contiki por executar-se en el següent maquinari (SoCs/MCUs i ràdios):

- RL 78 – ADF7023
- TI CC2538 – Ràdio integrada
- TI MSP430x – TI CC2420 o TI CC2520
- Atmel AVR – Atmel RF230 o TI CC2420
- Freescame MC1322x – Ràdio integrada
- ST STM32w – Ràdio i ntegrada
- TI MSP430 – TI CC2420, TI CC1020 o RFM TR1001
- Atmel Atmega 128 RFA – Ràdio integrada
- Microchip PIC32MX795F512I – Microchip MRF24J40
- TI CC2530 – Ràdio integrada
- 6502

De manera semblant a OpenWSN, Contiki també disposa d'un programari per simular una xarxa de motes virtuals. En aquest cas, l'aplicació s'anomena Cooja i la manera més fàcil d'instalar-la és descarregant-se, des de la pròpia web de Contiki, una màquina virtual VMWare anomenada *Instant Contiki* (la darrera versió disponible és la 2.7) que ocupa uns 2.2 GB i que inclou un SO Linux Ubuntu amb el programari Cooja ja instal·lat [41]. Fent servir qualsevol aplicació que permeti executar màquinas virtuals, com ara VMWare Player, es pot executar la VM –*Virtual Machine*- i, un cop arrencat l'SO, executar Cooja i configurar una nova simulació. A la figura de sota es pot veure un exemple de l'aspecte del programa, un cop s'ha creat una xarxa i s'ha està simulant l'enviament de paquets entre motes:

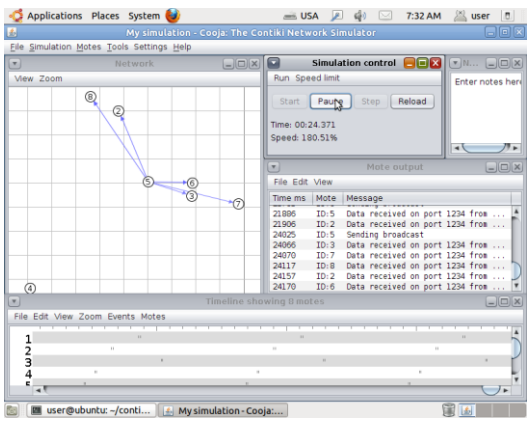


Figura 88. Programari Instant Contiki sota Ubuntu

En cas de xarxes amb motes físiques i, igual que passava amb OpenWSN, hi ha una part de SW que s'ha de pujar i compilar en les motes, per tal de suportar els protocols descrits anteriorment.

Un tret diferenciador de Contiki és que fa servir, com a mètode de *duty cycling* per defecte, ContikiMAC, un mecanisme per determinar el cicle de treball de la ràdio [29]. Bàsicament, ContikiMAC es basa en l'ús de *wake-ups* (despertaments) periódics per tal de poder escoltar transmissions de paquets dels nodes veïns. Si es detecta una transmissió durant un *wake-up*, llavors la ràdio del receptor es queda activa (*on*) per poder rebre el paquet; quan aquest s'ha rebut, el receptor envia un ACK de capa d'enllaç a l'emisssor. Això es així ja que, per enviar un paquet, un emissor ha d'enviar-lo repetidament fins que rep un ACK d'enllaç per part del receptor. En canvi, això no aplica a paquets de *broadcast* ja que, en aquest cas, l'emissor envia el paquet durant tot el seu interval de *wake-up* per tractar d'assegurar-se que tots els veïns l'han rebut, encara que no ho pot confirmar. Fent servir aquest mecanisme de *duty cycling*, s'aconsegueix un ús més eficient de la ràdio de les motes, ja que es defineixen unes restriccions de temps durant el qual aquestes han d'estar apagades, aconseguint que, en general, ho estiguin al voltant d'un 99% del temps (o, el que és el mateix, que el cicle de treball estigui per sota de l'1%), fins i tot en nodes que fan de *router* (que reenvien dades a altres nodes per poder cobrir distàncies més llargues)

- ContikiMAC també inclou una optimització d'una tècnica anomenada *fast sleep* (adormiment ràpid): si no es detecta un període de silenci abans d'un temps t_l predefinit, llavors el receptor es posa en *sleep*; igualment, si el període de silenci és superior a un altre temps t_i, llavors el receptor també es posa a dormir; per últim, si no es rep cap paquet després d'un període de silenci, el receptor es posa a dormir, fins i tot si es detecta activitat de ràdio.

- Per últim, ContikiMAC també inclou una tècnica anomenada *Transmission Phase-Lock*: després d'una transmissió satisfactòria d'un emissor a un receptor, l'emissor haurà après quina és la fase/període de *wake-up* del receptor i, per tant, a partir d'aquell moment, necessitarà enviar menys transmissions i, al seu voltant, disminuir el seu cicle de treball.

Contiki incorpora, a més, la pila de comunicació Rime (*Rime communication stack*) que no és més que un conjunt de primitives de comunicació lleugeres, destinades específicament a LLNs i que van des de difusió d'àrea local *best-effort* anònima fins a inundacions de xarxa conmfiables. Per altra banda, com a sistema de fitxers, Contiki fa servir Coffee, un *filesystem* molt petit i fàcil d'utilitzar que s'assembla a l'accés a fitxers que es fa en llenguatge C.

Per últim, pel que fa a la pila IPv6, Contiki fa servir uIPv6 (micro IPv6), que és una versió de codi obert de la pila capaç d'executar-se en microcontroladors de 8 i 16 bits. Aquesta versió implementa IP, TCP, UDP i ICMP i, segons Atmel, Cisco i SICS –empreses publicadores- es tracta de la pila IPv6 de codi obert més petita –que ocupa menys- que hi ha en l'actualitat (ocupa 11.5 KB en ROM i 1.8 KB en RAM), tot i que altres alternatives com NanoStack ocupen fins i tot encara menys. Per la seva banda, es suporta multisalt entre nodes fent servir el protocol AODV.

FreeRTOS

FreeRTOS és un sistema operatiu en temps real (RTOS – *Real Time Operating System*) desenvolupat i mantingut per la companyia Real Time Engineers Ltd durant els darrers 12 anys. Es considera l'estàndard *de facto* per a MCUs. Els seus objectius principals són: ser fàcil d'utilitzar (ser simple), tenir una emprempta petita (*small footprint*) i ser robust. De fet, el *kernel* de l'SO consisteix únicament en tres o quatre fitxers en C (`task.c`, `list.c`, `queue.c`). Altres característiques clau són que afegeix una baixa sobrecàrrega (*low overhead*) i que permet una execució molt ràpida. FreeRTOS proporciona mètodes que permeten fils i tasques múltiples, semàfors, temporitzadors *software*, entre d'altres. En resum la missió d'aquest SO, segons els propis desenvolupadors, és "proporcionar un producte liure que sobrepassi la qualitat i servei demanats pels usuaris d'alternatives comercials".

FreeRTOS fa servir una implementació d'un temporitzador *software* molt eficient, que no fa servir cap "temps de CPU" a menys que cap temporitzador realment necessiti atendre les seves necessitats (els temporitzadors per programari no contenen variables que necessiten ser comptades fins a zero). Per altra banda, FreeRTOS no realitza mai cap operació no determinista –com per exemple caminar per una llista enllaçada- des de dintre d'una secció crítica o interrupció.

FreeRTOS suporta fins a 35 arquitectures, des de petits MCUs de 8 bits fins a potents processadors de 32 bits (ARM7, ARM9, MSP430, AVR, PIC, 8051, etc.); concretament, es suportan MCUs i processadors dels següents fabricants:

- Altera
- Atmel
- Cortus
- Cypress
- Energy Micro
- Freescale
- Infineon
- Luminary Micro
- Microchip
- NEC
- Microsemi (formally Actel)
- NXP
- Renesas
- Silicon Labs
- Spansion (ex Fujitsu)
- ST Microelectronics
- Texas Instruments
- Xilinx
- x86 (mode real)
- x86 / Windows (simulador)

Pel que fa al simulador x86, es tracta d'un programari per a SO Windows i, més concretament, per a Visual Studio o Eclipse i MingW (gcc). El simulador permet l'execució de projectes de demostració –operacions simulades- tot i que no es pot aconseguir un comportament en veritable temps real, tal i com passaria quan FreeRTOS corre en maquinari físic.

Pel que fa a la seva emprempta, és molt petita: únicament ocupa de 6 a 10 KB en ROM; de fet, aquesta és altra de les seves característiques clau, el ser *ROMable* (es pot carregar enterament en ROM).

Pel que fa a l'ús d'aquest sistema operatiu en entorns IoT, la principal particularitat és que es pot fer servir juntament amb un programari anomenat Nabto. Aquest SW permet, quan s'instal·la en una mota, que aquesta pugui ser accedida i controlada remòtament, a través d'una interfície web (fent servir un PC, *smartphone* o *tableta* amb navegador web i un *plug-in* especial), a través d'una aplicació específica per a *smartphones* (iOS o Android) o fent servir un sistema d'adquisició de dades intel·ligent (DAS). Amb Nabto, cada dispositiu disposa d'una URL única, accesible des d'Internet de manera segura (amb autenticació + encriptació de dades), fent servir una comunicació P2P que requereix molt baix ample de banda i amb accesibilitat assegurada fins i tot si la mota es troba al darrere d'un tallafocs. Els nodes també poden ser accedits des de la pròpia xarxa local, òbviament. Per dir-ho d'alguna manera, Nabto és com una mena de servidor web que s'instal·la a la mota i permet controlar-la gràficament. El servidor Nabto, un cop compilat, ocupa menys de 10 KB (fent servir `gcc`), sumant en total menys de 23 KB, comptant el propi FreeRTOS i la pila UDP/IP. La tecnologia no requereix que la mota tingui cap sistema de fitxers ni tampoc exigeix l'ús de TCP.

A la figura de sota es mostra un esquema a alt nivell del funcionament del programari:

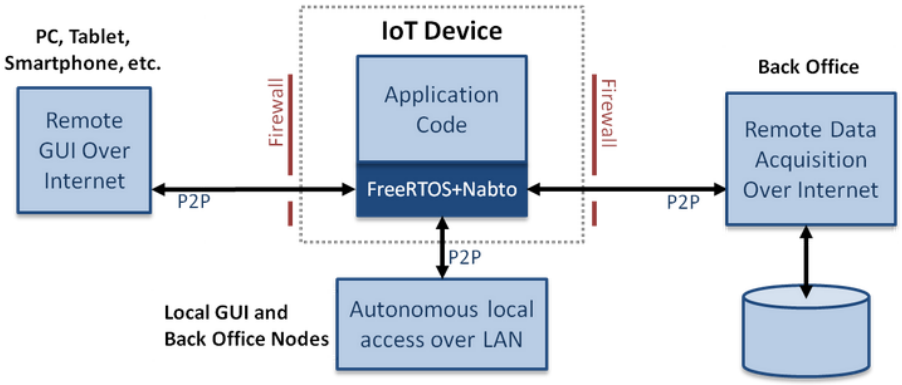


Figura 89. Accés remot a mota fent servir FreeRTOS + Nabto.

Per últim, pel que fa al suport d'IPv6, FreeRTOS implementa NanoStack, una pila de protocol 6LowPAN amb una implementació completa de l'IEEE 802.15.4, que inclou suport per a IPv6 i UDP, ICMP, la capa MAC de l'IEEE 802.15.4 i el protocol de sensors SSI (*Simple Sensor Interface*). No s'ha de confondre Nanostack v1.x (solució *open source*) amb Nanostack v2.x (solució propietària de la companyia Sensinode). El *footprint* de la versió de codi obert és de 10 KB de ROM i 2 KB de RAM. Es suporta multisalt entre nodes fent servir l'algorisme NanoMesh.

RIOT

Al igual que els SOs anteriors, RIOT és un sistema operatiu de codi obert per a l'Internet de les Coses. Té llicència GNU de tipus LGPL (*Lesser General Public License*) i va ser inicialment desenvolupat per la *Free University of Berlin*, l'*Institut National de Recherche en Informatique et en Automatique* (INRIA) i la *Hamburg University of Applied Sciences* (HAW).

RIOT es basa en una arquitectura de *microkernel*; en concret, el seu *kernel* està heretat de FireKernel, un altre *kernel* que va ser creat originàriament per a xarxes de sensors. El *footprint* de RIOT és similar al d'altres sistemes operatius per a IoT (1.5 KB RAM i 5 KB ROM mínims) però compta amb suport complert per a multi-fil i temps real, al contrari que altres alternatives com per exemple Contiki o Tiny OS, que únicament incorporen suport parcial per a *multi-threading* i temps real. L'SO es pot programar fent servir C/C++.

Els principals objectius de disseny de RIOT són: eficiència energètica, confiabilitat, capacitats de temps real, emprenta de memòria petita, modularitat, accés a APIs uniforme (independent de la plataforma de maquinari). De fet, existeixen diverses llibreries –com ara Wiselib- per a RIOT, que inclouen algorismes d'encaminament, clusterització, sincronització de temps, etc.

RIOT pot ser i nstal·lat tant en dispositius encastats –motes- com en ordinadors personals. Les arquitectures que es suporten són:

- MSP430
- ARM7
- Cortex-M0
- Cortex-M3
- Cortex-M4
- X86

Per altra banda, les plaques suportades són:

- Arduino Due
- UDOO Board (Cortex-M3 part)
- Nordic nrf51822 (DevKit)
- mbed NXP LPC1768
- TelosB
- Zolertia Z1
- Texas Instruments EZ430-Chronos
- STM32F4DISCOVERY
- STM32F3DISCOVERY
- STM32F0DISCOVERY
- WSN 430 (v1.3b and v1.4)
- HiKoB FOX
- ScatterWeb MSB-A2
- ScatterWeb MSB-430H

Per últim, les ràdios que es suporten actualment (per a les quals hi ha controladors SW) són:

- CC2420,
- CC1100,
- CC1101,
- CC1111,
- AT86RF231.

Per altra banda, el grau d'implementació de protocols i tecnologies IoT és el següent:

- Nivell físic: transmissió de ràdio,
- Nivell MAC: IEEE 802.15.4,
- Nivell d'integració: 6LoWPAN (compleix amb RFC6282 i RFC6775) i ICMP,
- Capa d'encaminament: RPL (compleix amb RFC6550 i RFC6719; implementació parcial)
- Capa de transport: UDP,
- Capa d'aplicació: CoAP.

RIOT suporta virtualització de xarxa (placa i CPU de les motes) a través del programari `desvirt`, que permet a RIOT córrer dins d'un procés UNIX (Linux o Mac OS), fent servir ràdios virtuals de tipus Nativenet, on es poden crear topologies configurables i fins i tot fer sevir eines de monitoratge de paquets com ara Wireshark.

Per últim, també existeix el programari RIOT-TV, una eina distribuida per a la visualització gràfica d'WSNs que facin servir RIOT com a sistema operatiu.

TinyOS

TinyOS és un sistema operatiu de codi obert, dissenyat per l'UC Berkeley en col·laboració amb Intel, escrit en nesC (un "dialecte" del llenguatge C, optimitzat per a xarxes de sensors amb limitacions de memòria) dirigit a xarxes sense fils formades per dispositius de baix consum (WSNs/LLNs), PANs, *smart metering*, etc. [20]. Es basa en un disseny de *kernel* monolític (arquitectura de sistema operatiu on tot l'SO al complet treballa en espai de *kernel* i està sol, en mode supervisor). La major part de llibreries associades a l'SO estan escrites en C, encara que existeixen diverses eienes complementàries escrites en altres llenguatges, majoritàriament en Java o Bash. Per la seva banda, el *footprint* de TinyOS és molt reduït, de menys de 400 bytes per al *core* de l'SO (sense comptar suport per a 6LoWPAN, entre d'altres) [39].

El maquinari suportat per TinyOS és:

- A nivell d'MCUs: MSP430, Atmega128, Atmega128L, Atmega 1281, Intel px27ax, Cortex M3 (treball encara en progrés).

- A nivell de xips ràdio: CC1000, CC2420, TDA5220, RF212, RF230, XE1204, CC1100, CC2500.

- A nivell de xips de memòria Flash: AT45DB, STM25P.

TinyOS pot córrer en Linux (paquets RPM i Debian), Windows (instal·lant primerament Cygwin i fent servir paquets RPM) o Mac OS. També existeixen màquines virtuals amb suport TinyOS ja pre-instal·lat (per exemple Jetos, VM basada en Debian amb suport per a MSP420 i AVR), que únicament s'han de descarregar i executar. Per altra banda, mitjançant l'eina de visualització Graphviz –que genera documents HTML- es poden veure les relacions existents entre components TinyOS d'una mateixa xarxa.

TinyOS suporta xarxes miltusalt, sincronització de temps en tota la xarxa per sota del milisegon fent servir el protocol FTSP (*Flooding Time Synchronization Protocol*), recol·lecció de dades cap a un node arrel designat o pasarel·la, fent servir el protocol CTP (*Collection Tree Protocol*), disseminació de dades a la xarxa fent servir l'algorisme Trickle, així com instal·lació de nous binaris remòtament, a través de la xarxa sense fils, fent servir l'aplicació Deluge.

Per últim, les implementacions d'IPv6/6LoWPAN per a TinyOS s'anomenen 6lowpancli (ja obsoleta) i BLIP (*Berkeley Low-Power IP Stack*). La versió 2.0 d'aquesta darrera suporta els següents protocols i tècniques:

- Encaminament: modes *Mesh Under* –capa d'accés al medi- i *Route Over* -nivell de xarxa,
- Descobriment de veïns (*Neighbour Discovery*),
- TCP (únicament suport experimental),
- UDP,
- ICMPv6,
- RPL (la versió 2.0 de BLIP integra el projecte TinyRPL, que abans anava per separat); el protocol d'encaminament abans de la versió 2.0 era HYDRO)
- CoAP (també integrat a BLIP a partir de la darrera versió).

El gran punt feble de BLIP es que les ràdios oficialment suportades són únicament dues: CC2420 (en plaques Epic, TelosB i Micaz –en aquesta darrera amb limitacions de *buffering*) i AT86RF230 (en placa Iris), encara que no oficialment també es suporten d'altres, com ara AT86RF212.

El *footprint* de BLIP 2.0 és d'uns 7.3 KB RAM i 23 KB ROM per a les motes i d'uns 6.3 KB RAM i uns 38.5 KB ROM per a un servidor d'aplicació.

Per últim, comentar que aquest SO també disposa del seu propi simulador de xarxes/motes TinyOS, anomenat TOSSIM. Aquest programari es complementa amb TinyViz, una eina personalitzable per a la visualització de dades i actuació. En la figura següent es pot veure una captura de pantalla d'aquesta darrera eina, treballant conjuntament amb TOSSIM:

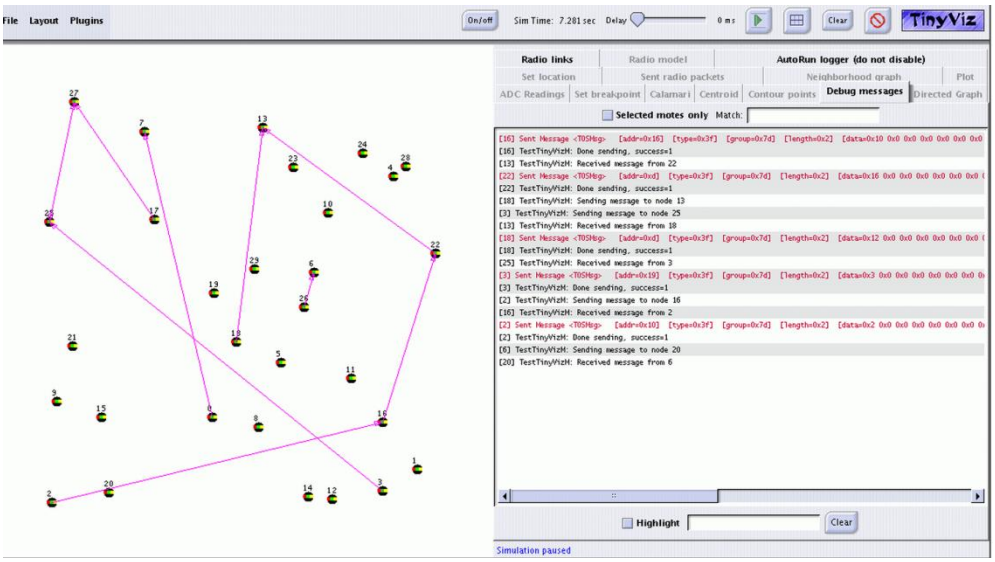


Figura 90. Eina TinyViz per a visualització de xarxes TinyOS [54].

Annex XLII. Especificacions tècniques de sensor TSWASTE.

TSWASTE

TST

SENSOR VOLUMÉTRICO PARA CONTENEDORES DE BASURA

A través de su sensor volumétrico TSwasTe, TST ofrece una solución de sensado inalámbrica de muy bajo coste y alta fiabilidad adaptable a cualquier tipo de contenedor urbano.

Fabricado en polietireno de alta densidad, su diseño está ideado para aguantar las inclemencias climatológicas, los golpes provocados por recogidas y las limpiezas y posibles daños por químicos de lavado.

El interfaz de sensado está basado en ultrasonidos y dispone de un sistema de detección de apertura de tapa de contenedor para evitar falsas medidas.

Su interfaz de radio a 868 MHz de muy bajo consumo garantiza una vida de hasta 7 años* con alcances de medio kilómetro hasta el sistema de repetidores TSmarT compatibles con interfaces celulares (2G/3G), WiFi, Ethernet o ZigBee, solución muy fácilmente integrable con redes existentes.

* Vida de batería estimada para 8 medidas por día y condiciones de cobertura media

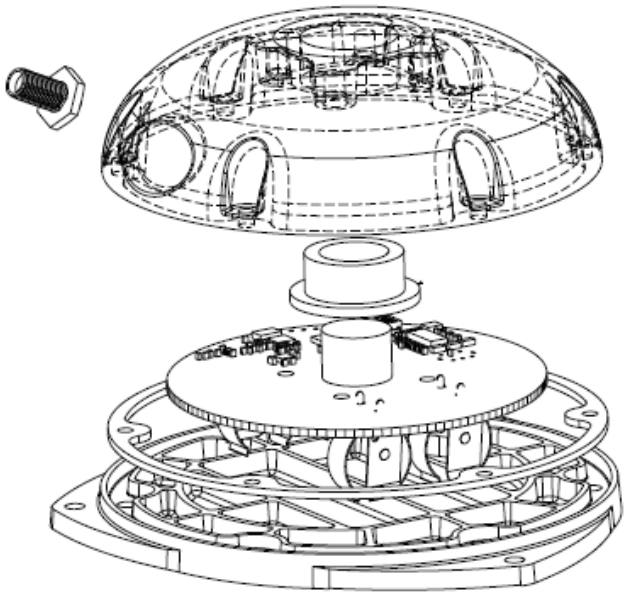
CARACTERÍSTICAS PRINCIPALES

Solución de sensado de contenedores urbanos de bajo coste

Ultra bajo consumo y vida estimada de 7 años*

Sensórica de ultrasonidos con detección de tapa abierta

Caja de polietireno de alta densidad resistente a golpes



ELÉCTRICO	
Alimentación	2 baterías AAA 1,5 VDC (Reemplazables)
Duración de batería	5 a 7 años* dependiendo uso

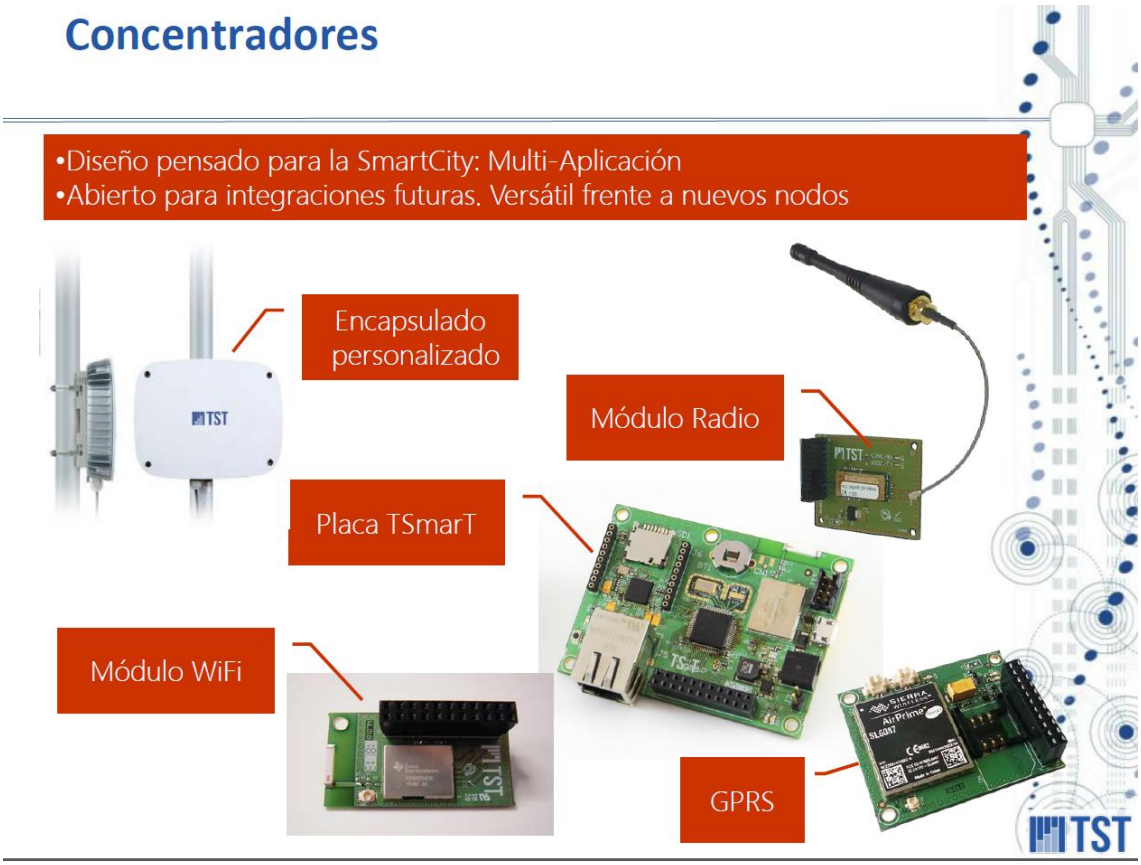
MECÁNICO	
Dimensiones	32 mm de alto / 100 mm de diámetro
Conectores	Conector SMA antena (opcional)

PARÁMETROS RADIO	
Banda de frecuencia sensor	868 MHz
Estándares soportados sensor	Propietario
Estándares soportados repetidor	GPRS, UMTS, WiFi, Ethernet, ZigBee, IEEE 802.15.4, Modbus
Cobertura sensor	500m LOS

TST

TECNOLOGÍAS, SERVICIOS TELEMÁTICOS Y SISTEMAS S.A.
39011 Santander (Spain)
www.tst-sistemas.es / @tstsistemas / info@tst-sistemas.es
Tel: (+34) 942 760 540 /Fax: (+34) 942 760 541

Figura 91. Característiques tècniques sensor TWASTE [45].



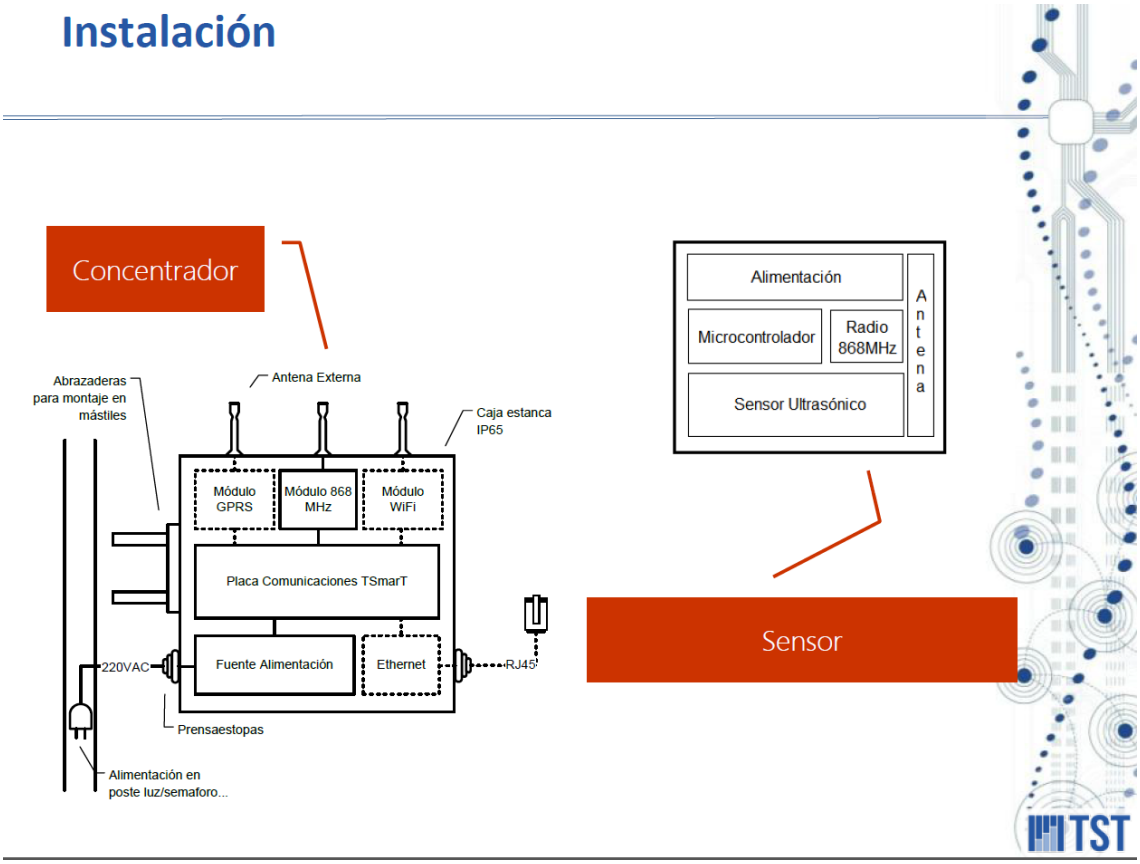


Figura 92. Diagrama de blocs del mòdul concentrador (*gateway*) i del sensor TWASTE.

Annex XLIII. Plataforma IoT 'Thinking Things' de Telefonica.

The Thinking Things Platform

Thinking Things allows you, not only to control your things and your sites, but to create new ideas.
You can check in the map where is parked your car. You can tweet if your room temperature is perfect. And you can make more astounding services if you want to code.

Modular Hardware | Easy-to-Use interface | Global Connectivity | REST API

Modular Hardware

The Thinking Things are different plastic cubes that you can put together like Lego pieces. Each block has a different function. A set of connected blocks is called a stack. You can put as many blocks in the same stack.

Connectivity modules

Communication

Every stack needs a connectivity module or "core". The connectivity module sends data from the other modules to the web page periodically. You can control this periodicity from the web page controls. It uses the mobile network, so it runs wherever your mobile phone runs. In case you are wondering, yes, it has a SIM inside. Just with the core module you get an approximate position of the stack (1Km in urban zones, 5Km or more in rural areas).
Available now

Sensor modules

Sensor modules get data from the environment and send this data to the web page where you can see them.

Ambient

The ambient module measures the air temperature, air humidity and ambient light.
Available now

Presence

The presence sensor detects movement of persons in front of it.
Available: September 2014

GPS

The GPS sensor gives an accurate position based in GPS satellites.
Available: September 2014

Actuator modules

Actuator modules will give you the possibility to act from the web page in the device.

Notifications

The future Notifications module has a changing-color light and can buzz.
Available: November 2014

Smart Plug

Switches electrical devices on or off, offers dimmer functionality and measures energy consumption.
Available: Early 2015

Energy modules

Battery

The Energy module is the battery of the stack. It can run and charge connected to a microUSB adaptor or even to a PC. It has a battery that can feed the stack independently. Its life depends on mobile coverage and time between connections. Present batteries can feed a stack, connecting every hour, for one month. You can put more than one module for longer life.
Available now

Figura 93. Descripció de la plataforma 'Thinkings Things' de Telefonica per a IoT [72].

Annex XLIV. Evolució nombre de transistors - Llei de Moore.

Figura 94. Evolució en el nombre de transistors de les CPUs en les darreres dècades.

Annex XLV. Bandes freqüencials ISM.

Frequency range		Bandwidth	Center frequency	Availability
6.765 MHz	6.795 MHz	30 kHz	6.780 MHz	Subject to local acceptance
13.553 MHz	13.567 MHz	14 kHz	13.560 MHz	Worldwide
26.957 MHz	27.283 MHz	326 kHz	27.120 MHz	Worldwide
40.660 MHz	40.700 MHz	40 kHz	40.680 MHz	Worldwide
433.050 MHz	434.790 MHz	1.74 MHz	433.920 MHz	Region 1 only and subject to local acceptance (within the amateur radio 70 cm band)
902.000 MHz	928.000 MHz	26 MHz	915.000 MHz	Region 2 only (with some exceptions)
2.400 GHz	2.500 GHz	100 MHz	2.450 GHz	Worldwide
5.725 GHz	5.875 GHz	150 MHz	5.800 GHz	Worldwide
24.000 GHz	24.250 GHz	250 MHz	24.125 GHz	Worldwide
61.000 GHz	61.500 GHz	500 MHz	61.250 GHz	Subject to local acceptance
122.000 GHz	123.000 GHz	1 GHz	122.500 GHz	Subject to local acceptance
244.000 GHz	246.000 GHz	2 GHz	245.000 GHz	Subject to local acceptance

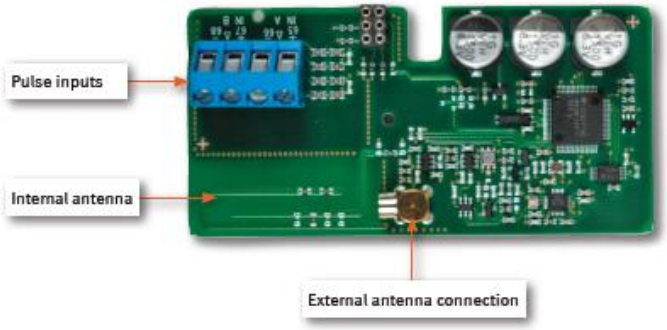
Taula 17. Taula amb les diferentes bandes de freqüència ISM [18].

Annex XLVI. Mòdul wM-Bus, mode C.

Wireless M-Bus, C mode

Module for MULTICAL® 602/62 and SVM S6 DATA SHEET

Module



Technical data

Frequency	868.95 MHz (EU licence-free area 868-870 MHz)
Communication	Wireless M-Bus, C mode, one-way communication
Standard	EN13757-4
Transmission interval	16 seconds
Transmission strength	10 mW
Battery lifetime	13 years
Range – internal antenna – external antenna	 Up to 200 meters Up to 500 meters
Update interval (data)	Every 2 minutes

Mechanical data

Dimensions (L X W x D)	90 x 44 x 16 mm
Temperature range	-40°C...+ 70°C

Markings

R&TTE	EN300 220 – class 2 EN301 489
CE marked	

Kamstrup 2 58101075_C1_GB_02.2014

Figura 95. *Datasheet* d'un mòdul wM-Bus [109].

Annex XLVII. Endoll amb commutador controlat per Z-Wave.

Enchufe controlado (on/off) Z-Wave Plus (GEN5) con medición de consumos - AEON LABS

Disponibilidad: En Existencia
Código Producto: es-51-AEO_ZW075-ZWEU
Marca: Aeon Labs

Sin Impuesto: € 53.68

€ 64.95

Sin valorar
Escribir Opinión

Cantidad: 1 COMPRAR

Lista de Regalos Comparar

DESCRIPCIÓN | COMENTARIOS (0)

El zócalo del módulo enchufe ontrolado Gen5 de Aeotec es un interruptor que le permite controlar la iluminación u otros equipos a través de los controles de Z-Wave. Está diseñado para funcionar con cualquier tipo de carga máxima 3500W de potencia. Puede ser controlado por un mando a distancia, software de PC, o cualquier controlador Z-Wave en tu red.

Además de la función de conmutación, este módulo también puede medir el consumo de potencia de la carga conectada. Los valores de potencia instantánea (en W) y el consumo total de energía (kWh) se pueden consultar.

Utilizando la tecnología de conmutación y monitorización poder comprobado laboratorios Aeon Smart Switch Gen5 es 50% más pequeño que el Smart Switch originales.

Y debido a que el Smart Switch es parte de la gama Aeotec Gen5 Gen5, que supera todo lo que existía antes. Se basa en el último chip Z-Wave de la serie 500, que proporciona un aumento de la cobertura de radio del 50% y una velocidad de comunicación 250% más rápido que en el anterior Z-Wave.

El módulo Z-Wave también funciona como un repetidor inalámbrico con otros módulos para asegurar una cobertura completa de su casa. Se requiere controlador Z-Wave (dongle remoto ...) para integrar este módulo en su red si usted ya tiene una red existente.

Características:

- Pida una lámpara o dispositivo de forma remota
- Módulo tomada integrar directamente con un enchufe eléctrico y la carga a ser controlado
- Función ON / OFF para controlar luces o aparatos (sin cambios)
- Medición del consumo instantáneo y acumulativo
- Control de carga a nivel local a través del botón incorporado
- Estado LED integrado en el botón
- 50% más pequeño que el Smart Switch originales Aeon laboratorios
- Protección contra la sobrecarga
- Parte de la gama de laboratorios Aeon Gen5
- Comunicación por radio de seguridad a través de AES-128
- Viruta integra Z-Wave de la serie 500
- Comunicación más rápida 250% en comparación con los dispositivos estándar Z-Wave
- Soporta exploración marcos Z-Wave
- Transmisión de apoyo
- Actualizaciones de Firmware Over The Air (OTA)
- Mensajes repetidor Z-Wave
- Optimización de la antena, 150 metros de alcance
- Facilidad de uso e instalación

ESPECIFICACIONES:

- Tipo de módulo: receptor Z-Wave
- Fuente de alimentación: 240VAC, 50/60 Hz
- Consumo: 1W
- Carga máxima: 3500W / 16A

Figura 96. Descripció de producte (endoll commutador) amb tecnologia Z-Wave [113].

Annex XLVIII. Pseudocodi de l'algorisme Bellman-Ford.

```
BELLMAN-FORD(G, w, s)
1  INITIALIZE-SINGLE-SOURCE(G, s)
2  for i ← 1 to |V[G]| − 1
3       do for each edge (u, v) ∈ E[G]
4            do RELAX(u, v, w)
5  for each edge (u, v) ∈ E[G]
6       do if d[v] > d[u] + w(u, v)
7            then return FALSE
8  return TRUE
```

Annex IL. Característiques tècniques del PIC24FJ128GA310.

PIC24FJ128GA310 Data Sheet (03/14/2014)

PIC24F 16-bit Microcontroller featuring nanoWatt XLP for eXtreme Low Power consumption. The device includes advanced low power features including a Low Voltage Sleep mode that maintains the device state and RAM with a typical current of 340 nA, and a Vbat pin that automatically transitions to the RTCC to a battery supply when Vdd is removed. The family is also includes a 480 segment LCD Driver with 60 segment x 8 common drive capability. The combination of feature make the part ideally suited to a number of battery powered and general purpose applications.

Features

Featuring LCD Drive and nanoWatt XLP Technology ideal for low power and batteryapplications

Typical nanoWatt XLP specifications include

- 10 nA Deep Sleep mode
- 400 nA RTCC in Vbat mode
- 330 nA Low Voltage Sleep mode (RAM retention)
- 400 nA Real Time Clock & Calendar operation in Sleep modes
- 270 nA Watch Dog Timer operation in Deep Sleep modes

Other Low Power Specifications include

- 150 uA/MHz Run mode
- Power Modes: Run, Doze, Idle, Sleep, Low Voltage Sleep, Deep Sleep, Vbat
- Multiple, Switchable Clock Modes for Optimum Performance and Power Management
- System Supervisors: Low Power BOR, WDT, INT0 and RTCC

CPU

- Up to 16 MIPS performance
- Single Cycle Instruction Execution
- 16 x 16 Hardware Multiply, & 32-bit x 16-bit Hardware Divider
- C Compiler Optimized Instruction Set System

Select Peripherals

- 10/12-bit Differential ADC, 24 channels, 200/500 Ksps with Threshold Detect
- Peripheral Pin Select allows I/O remapping of many peripherals in real time
- Charge Time Measurement Unit (CTMU) enabling 24 channels of Capacitive Touch
- Three Analog rail-to-rail comparators Peripherals
- Hardware RTCC, Real-Time Clock Calendar with Alarms

System

- Internal oscillators support - 31 kHz to 8 MHz, up to 32 MHz with 4X PLL
- Fail-Safe Clock Monitor - allows safe shutdown if clock fails
- Watchdog Timer with separate RC oscillator
- System Supervisors: Low Power BOR, WDT, INT0 and RTCC
- JTAG Boundary Scan

Parameter Name	Value
Architecture	16-bit
CPU Speed (MIPS)	16
Memory Type	Flash
Program Memory (KB)	128
RAM Bytes	8,192
Temperature Range C	-40 to 85
Operating Voltage Range (V)	2 to 3.6
I/O Pins	85
Pin Count	100
System Management Features	BOR, LVD
POR	Yes
WDT	Yes
Internal Oscillator	8 MHz, 32 kHz
nanoWatt Features	Low Sleep/Fast Wake/Fast Control
Digital Communication Peripherals	4-UART 2-SPI 2-I2C
Analog Peripherals	1-A/D 24x12-bit @ 200(ksps)
Comparators	3
Capture/Compare/PWM Peripherals	7/7
PWM Resolution bits	16
Timers	19 x 16-bit 9 x 32-bit
Parallel Port	EPMP
DMA	6
XLP	Yes
Cap Touch Channels	24

Figura 97. *Datasheet* del microcontrolador de 16 bits PIC24FJ128GA310.