Estudi de Xarxes WPAN 802.15.4

Sergi Gomis Gascó

Universitat Oberta de Catalunya
19 d'Abril del 2012

Abstract - Aquest projecte proposa l'estudi en profunditat de les xarxes WPAN 802.15.4, veure com formen els paquets d'informació per a poder atacar aquestes xarxes mitjançant sniffers per a escoltar la informació que transmeten els nodes i fins i tot intentar injectar paquets maliciosos en la xarxa o denegar el servei a partir de l'enviament de paquets formats especialment per a saturar aquest tipus de xarxes. Ens centrarem en l'estudi de les característiques de les xarxes 802.15.4 i de les xarxes ZigBee.

1. Introducció

S'ha estudiat molt sobre seguretat en xarxes wireless més comunes; les wifi (802.11), les xarxes bluetooth (802.15.1), etc. però existeixen pocs estudis sobre les xarxes industrials Wireless Personal Area Network (WPAN) de dedicació més industrial, com les 802.15.4, que s'utilitzen pel control de semàfors, de control i actuació en parcs verds a la ciutat, en aeroports, o en instal·lacions domòtiques.
Les xarxes WPAN es componen d'un gran nombre de nodes wireless que s'interconnecten entre ells, formant configuracions d'arbre en les quals els missatges que s'envien d'un node a un altre van passant a través d'alguns nodes que retransmeten els missatges que no van dirigits ells de manera intel·ligent, envien els paquets d'informació cap al node que més a prop està del node final.
D'aquesta manera és senzill ampliar la malla de nodes, ja que es van agregant a aquesta a partir d'altres nodes propers. Amb la limitació única de la configuració màxima de nodes i subnivells de l'arbre que es defineix en l'inici de la configuració de la xarxa.
Dins d'aquest tipus de xarxes, es poden trobar les xarxes ZigBee, que a partir de l'estàndard 802.15.4, implementa un protocol específic per a interconnectar els sensors d'aquest tipus de xarxes industrials.

2. Que és el ZigBee ?

ZigBee és el nom que rep les especificacions d'un conjunt de protocols d'alt nivell de comunicacions inalàmbriques per a ser utilitzat en radiodifusió digital de molt baix consum, basades en l'estàndard IEEE 802.15.4 de xarxes de àrea personal (WPAN).
El seu objectiu són les aplicacions que requereixen comunicacions segures amb baixa taxa de transferència de dades i maximitzar la vida útil de les bateries.
Permet transmetre dades a 250kbps fins a 75 metres.
Cada dispositiu Zigbee te un identificador únic que permet fer xarxes complexes de dispositiu

3. La norma IEEE 802.15.4

La normativa IEEE 802.15.4 [2] apareix l'any 2003 després de molts anys d'esforç. Aquest estàndard va significar un gran salt i definia la capa RF i la capa física d'uns nous dispositius capaços de transmetre dades a una velocitat de 250kbps i donant la possibilitat de poder transmetre en un rang de 27 canals sense cap tipus de llicencia en una freqüència segons la zona geogràfica de 868MHz, 915MHz i 2'4GHz. Actualment, la freqüència més utilitzada per no dir la única, és la de 2'4GHz. Zigbee utilitza la freqüència de 2'4GHZ amb 16 canals i una velocitat de transmissió de 250kbps amb una modulació QPSK en la banda ISM. No obstant això, la majora de xarxes sense fils actuals, operen a 2'4GHZ en banda ISM, com ara el Bluetooth i el Wifi (802,15,11b), a més de telèfons sense fils i forns microones, que fa que aquesta banda de freqüència estigui molt plena i sorollosa [1].

La modulació utilitzada en la norma IEEE 802.15.4, està basada en la PSK (phase shift key) perquè és bastant immune al soroll. La modulació PSK, ha estat utilitzada per la NASA durant molts anys per a comunicacions en missions espacials.

El Zigbee te la capacitat de treballar amb xarxes de gran densitat, aquest característica, ajuda a augmentar la confiabilitat de les comunicacions, ja que com més nodes existeixin dintre d'una xarxa, major és el nombre de rutes alternatives existents per garantir que un paquet arribi al seu destí.

Cada xarxa Zigbee, disposa d'un identificador de xarxa únic, lo que permet coexistir diferent xarxes en un mateix canal de comunicació sense ningun problema. Teòricament podrien existir fins a 16000 xarxes diferents en un mateix canal i cada xarxa pot estar formada per fins a 65000 nodes.

Utilitza un protocol de comunicacions multi salt, que pot establir comunicacions entre diferents nodes tot i que es trobin fora del rang de transmissió entre ells, sempre que existeixin nodes intermitjos entre ells que els interconectin. D'aquesta manera, s'incrementa l'àrea de cobertura de la xarxa.

La figura 1 mostra l'arquitectura general del dispositiu, amb el canal RF representat com el medi físic, el PHY controlar les característiques del canal de RF, i la MAC el control de la PHY. Com que és un protocol 802, s'incorpora el control de vincle de la capa 802,2, un nivell de tots els protocols 802. Igual que la majoria d'altres protocols 802, no especifica ni descriure les capes superiors de la pila OSI / ISO.

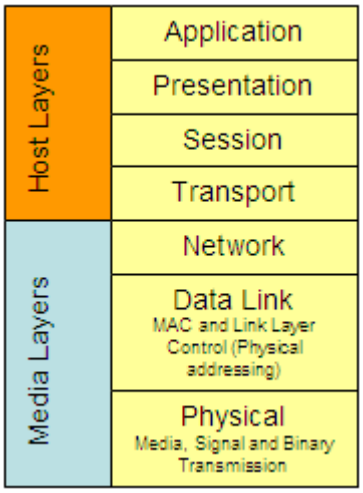

Figura 1. Model OSI /ISO

De fet, comparant les Figures 1 i 2, és evident que 802.15.4 ni tan sols representa un conjunt complet dels mitjans de comunicació que s'especifiquen en el model OSI.

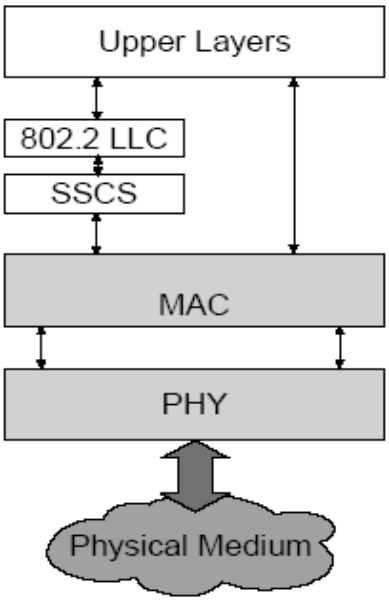

Figura 2. Arquitectura dispositiu 802.15.4

Existeixen 4 tipus diferents de formats de paquets: Paquets de dades, paquets d'Acknolegement, paquets de comandes MAC i finalment paquets de senyalitzacions.
Aquests paquets, contenen una seqüència de sincronització, una capçalera ambl a longitud del missatge, l'adreça dels dispositiu emissor i finalment un CRC per validar que les dades que s'han enviat i les que s'han rebut no han sofert errors de transmissió.

A la figura 3, podem veure una representació de la estructura dels paquets.

4. Tipus de Xarxes ZigBee

Existeixen tres tipus de dispositius fonamentalment [3]: El coordinador (PAN), el dispositiu router i els dispositius finals. El coordinador és l'element o dispositiu més important, ja que és l'encarregat de crear les xarxes i saber quins dispositius te a la seva xarxa. La funció dels dispositius "routers" és de retransmetre els paquets enviats desde un dispositiu a un altre.

A la figura 4, podem veure els tipus de xarxa que es poden formar amb els diferent dispositius.

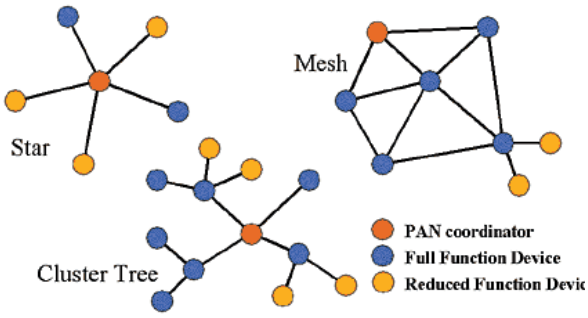

Figura 4. Tipus de xarxa ZigBee

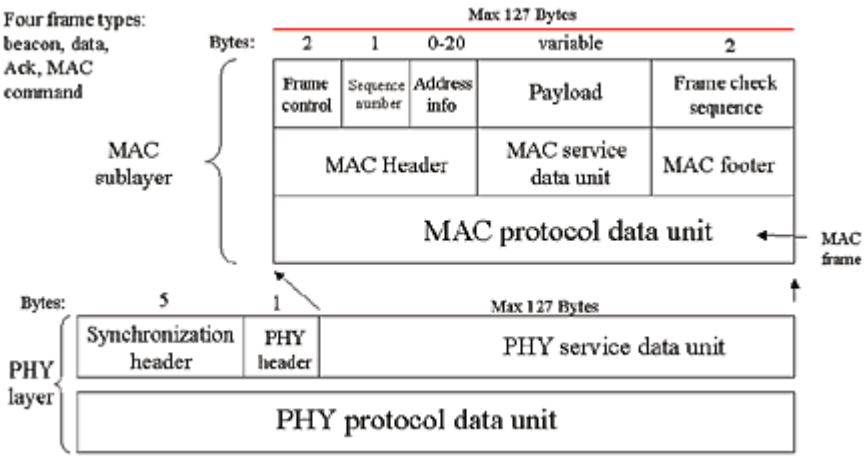

Figura 3. Estructura del paquets ZigBee

La capa de xarxa ZigBee, disposa de tres tipus de xarxa: La xarxa en estrella, la xarxa en arbre i la xarxa en malla. En la topologia d'estrella, la xarxa és controlada per un coordinador, que és el responsable d'iniciar i mantenir els dispositius de la xarxa. Els dispositius finals, es comuniquen directament amb el coordinador.
En la xarxa de malla o xarxa d'arbre, el coordinador és l'encarregat d'inicair la xarxa i d'escollir la clau, però la xarxa també es pot estendre a traves de l'ús de routers Zigbee, mentre que les rutes són establertes per mitja d'un protocol d'enrutament similar al Ad-Hoc.
A les xarxes d'arbre, els routers mouen les dades i els missatges de control a traves de la xarxa mitjançant un sistema d'enrutament jeràrquic.

5. Mètodes de Seguretat

Existeixen quatre serveis de seguretat en la norma IEEE 802.15.4. En el control d'accés, aquest proveeix una llista de dispositius segurs. Aquest mecanisme preveu la recepció de paquets de dispositius no autoritzats. Un altre dels serveis disponibles és la encriptació o xifratge dels paquets transmesos mitjançant algoritmes d'encriptació amb claus. Un altre dels serveis que es disposa en el tema de la seguretat, és la comprovació de la integritat de les dades rebudes, per evitar i prevenir la manipulació de les dades entre el dispositiu emissor i el dispositiu receptor per intrusió. Finalment, també es disposa de refresc seqüencial per evitar que es re-enviïn paquets.

En quan a la encriptació, existeixen 8 modes d'encriptació possible.
El primer mode, és el mode sense encriptació.
El segon mode, és mitjançant la codificació AES-CRT que permet tenir un control d'accés, encriptació de dades i control de seqüència.
El tercer, quart i cinquè, són els més complerts i utilitzen la codificació AES-CCM-128, AES-CCM-64 i AES-CCM-32 respectivament, tos ells amb control d'accés, encriptació de dades, control de seqüència i control d'integritat dels paquets.
Els últims tres modes, són els que utilitzen la codificació AES-CBCMAC-128, AES-CBCMAC-64 i AES-CBC-MAC-32. Aquest tres modes només disposen de control d'accés i de control d'integritat dels paquets.

La seguretat en la arquitectura ZigBee inclou també dos tipus de mecanismes en el stack del protocol. Una en la capa de xarxa (NWK) i l'altre en la sub-capa de aplicació (APS).

ZigBee adopta algoritmes d'encriptació CCM a més d'utilitzar tres tipus de claus per controlar la seguretat: Master, Netwrok i Link.
La clau mestre be fixada durant la fabricació dels dispositiu per un centre de confiança. La clau mestre no s'utilitza per encriptar la informació, però si que es utilitzada en el moment de realitzar l'emparellament dels diferents dispositius que formen la xarxa.
La clau de xarxa, és la clau que protegeix la xarxa en si. Tots els dispositius de la xarxa comparteixen aquesta clau.
La clau Link, només s'utilitza per la comunicació entre dos dispositius en missatges unicast. Aquest clau, està basada en la clau mestre.
Les claus Link i de xarxa, es poden anar actualitzant cada cert període de temps, tot i que aquest fet vulnera la seguretat de la xarxa perquè es comparteixen les claus entre els dispositius.

Existeixen diferents algoritmes d'encriptació i des-encriptació mitjançant el patró CMM3 [4].

6. Estructura dels paquets ZigBee

A.- Estructura de les trames MAC
El format general de les trames MAC es va dissenyar ser ser molt flexible i que s'ajusten a les necessitats de les diferents aplicacions amb diverses topologies de xarxa, al mateix temps que es mantenia un protocol simple. Els diferents tipus de trames que existeixen són:

Data Frame:
Utilitzat per totes les transferències de dades

Acknowledgment Frame:
Utilitzada per la confirmació de la recepció exitosa de les trames.

MAC Command Frame:
Utilitzades per al control de totes les entitats MAC.

Beacon Frame:
Utilitzada per un coordinador per transmetre "beacons"

B- Estructura de la trama de dades (Date Frame).
La trama general MAC es la denominada PPDU (Phy Protocol Data Uni), Capa física de la unitat de dades del protocol MAC. La trama comença per una capçalera de sincronització (SHR, Synchronization Header), seguida de una capçalera de la capa física per indicar la longitud del paquet (PHR, Phy Header) i seguidament la capa física amb les dades (PSDU, Phy service Data Unit).

El format general de la trama és mostra en la figura 5.

El preàmbul, de 32 bits, esta dissenyat per la adquisició de símbols i per els temps de xip i en alguns casos s'utilitza per ajustus de freqüència. No es requereix una equalització en el canal de la capa física degut a la combinació de petites áreas de cobertura amb rangs de transmisións baixos.

Dintre de la capçalera de la capa física, s'utilitzen 7 bits per especificar la longitud de la carrega de dades (en bytes). La longitud del paquet (que va de 0 a 127 bytes). El tamany típic dels paquets per la majoria d'aplicacions domòtiques, tal com la monitorització i control de dispositius de seguretat, il·luminació, aires condicionats i altres aplicacions van entre els 30 i 60 bytes, mentres que les aplicacions de jocs interactius i perifèrics de PC, requereixen paquets més llargs. La durada màxima dels paquets és de 4.25mS per la banda de 2.4GHz, de 26.6ms per la banda de 915MHz i de 53.2ms per la banda de 868MHz.

La trama de la unitat de dades del protocol MAC (MPDU, MAC Protocol Data Unit), es composa de la capçalera MAC (MHR MAC Header), Unitat de servei de dades MAC (MSDU MAC Service Data Unit) i acaba amb la comprovació de la trama (MFR (MAC Footer). El primer camp de la trama de capçalera MHR és el camp de control, denominat Frame Control.

Frame Control: Indica el tipus de trama MAC que es vols transmetre, especifica el format, el cap de direcció i controla els missatges d'Ack. La trama de control especifica com és la resta de trames de dades i que és el que conté.

Data Sequence Number: Verifica la integritat de la trama MAC. És una seqüència de números, al igual que les trames FCS. La seqüència de números en la capçalera enllaça les trames de ACK amb les transmissions anteriors. Una transmissió es considera exitosa quan la trama ACK conté la mateixa seqüència de números que la seqüència anterior. Les trames FCS ajuden a verificar la integritat de les trames MAC.

Address Information: El tamany de les adreces pot variar entre 0 i 20 bytes. Per exemple, una trama de dades pot contenir informació de la font i dels destinatari, metres que la trama ACK no conté ninguna informació de ninguna adreça. Per altre banda, una trama de guia només conté informació de la adreça de la fons. Aquesta flexibilitat en la estructura ajuda a incrementar la eficiència del protocol al mantenir els paquets el mes reduïts possible.

Payload: És de longitud variable. Tot i així, la trama MAC, no pot excedir els 127 bytes d'informació. Les dades que porta el Payload, depenen del tipus de trama. L'estàndard IEEE 802.15.4, te quatre tipus diferents de trames MAC: trama de guia, trama de dades, trama d'Ack i trama de comandes. Només les trames de dades i guia contenen informació que prové de capes superiors. Les trames de missatges ACK i de las de comandes MAC originades en la MAC són utilitzades per les comunicacions MAC Peer-to-Peer.

FCS (Frame Check Sequency): És una trama de comprovació de 16 bits CRC (Cyclic Redundancy Check).

C- Estructura de les trama ACK (Acknoledgment Frame)

LA trama ACK proporciona el intercanvi d'informació desde el receptor al emisor de que el paquet ha sigut rebut sense error. Aquest curt paquet aprofita el temps de silenci (quiet time), especificat ala norma, immediatament després de la transmissió del paquet de dades.

A la figura 6 es mostra com esta composada l'estructura de la trama d'ACK.

D- Estructura de les trames de comandes MAC (MAC Commnad Frame)

La trama de comandes MAC, són un mecanisme per al control o configuració a distancia del dispositius nodes. Permet que el coordinador de la xarxa centralitzada, pugui configurar els dispositius individualment sense importar lo gran que sigui la xarxa.

La trama de comandes MAC, es mostra al a figura 7.

E- Estructura de les trames "Beacon" (Beacon Frame)

La trama Beacon, afegeix un nou nivell de funcionalitat a la xarxa. Els dispositius dels nodes poden despertar-se només quan es transmesa una senyal de guia o "beacon", escolta la seva direcció i si no la escolta, torna al estat de dormit, amb el conseqüent estalvi d'energia. Les trames Beacon són importants en les xarxes de tipus "mesh" i "cluster tree" per mantenir tots el nodes sincronitzats sense requerir que els nodes consumeixin energia de la bateria, escoltant llargs períodes de temps.

Aquesta estructura de la trama Beacon conté els denominats "SuperFrames". Algunes aplicacions requereixen un ample de banda dedicat per aconseguir grans estats de latència, però un molt baix consum d'energia. Per aconseguir aquests estats latent, el IEEE 802.15.4, pot operat amb aquest mode.

A la figura 8, es pot veure l'estructura de les trames "Beacon".

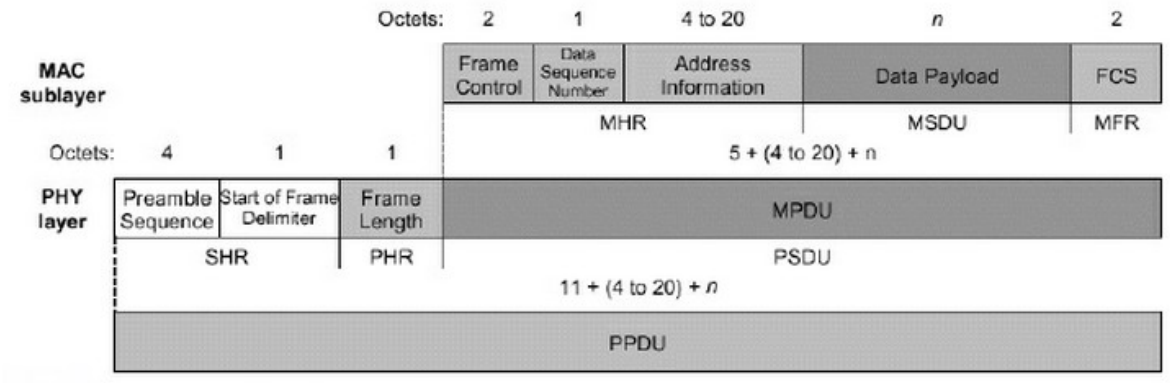

Figura 5.- Format general de la trama MAC

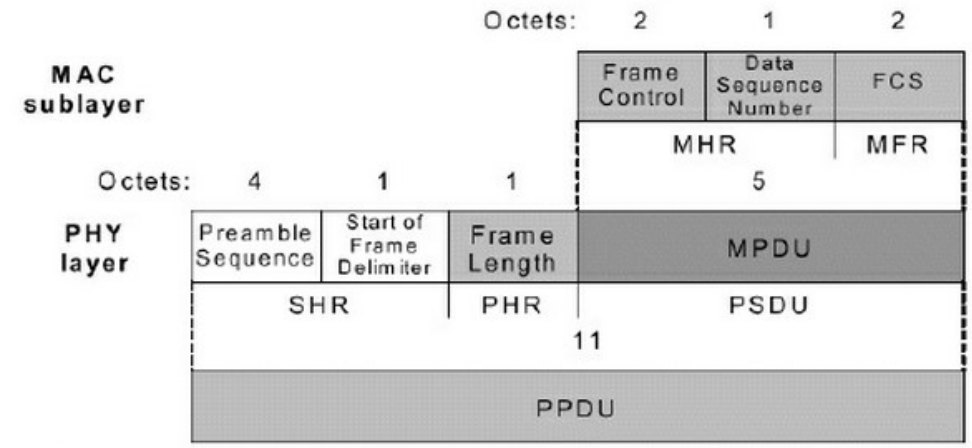

Figura 6.- Format de la trama ACK

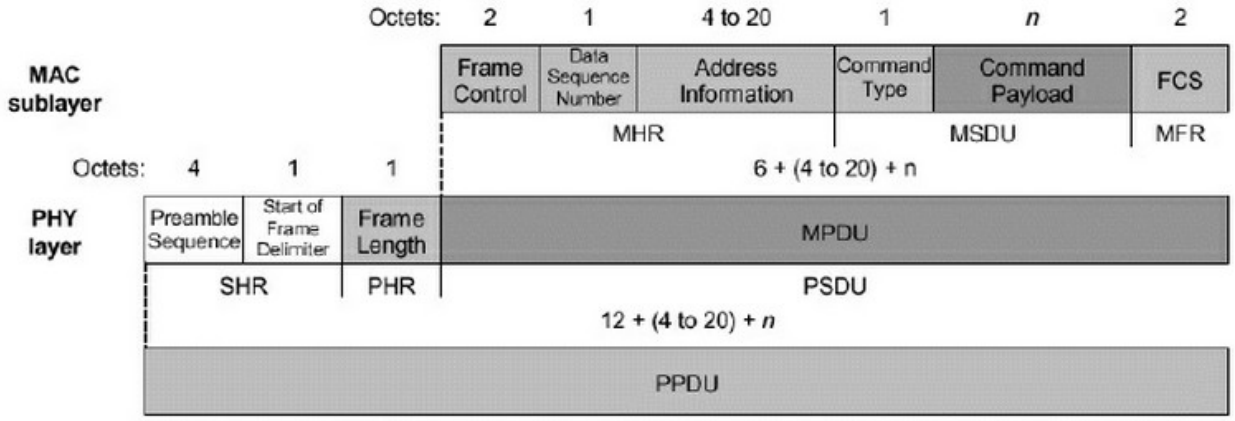

Figura 7.- Format de la trama "MAC Command"

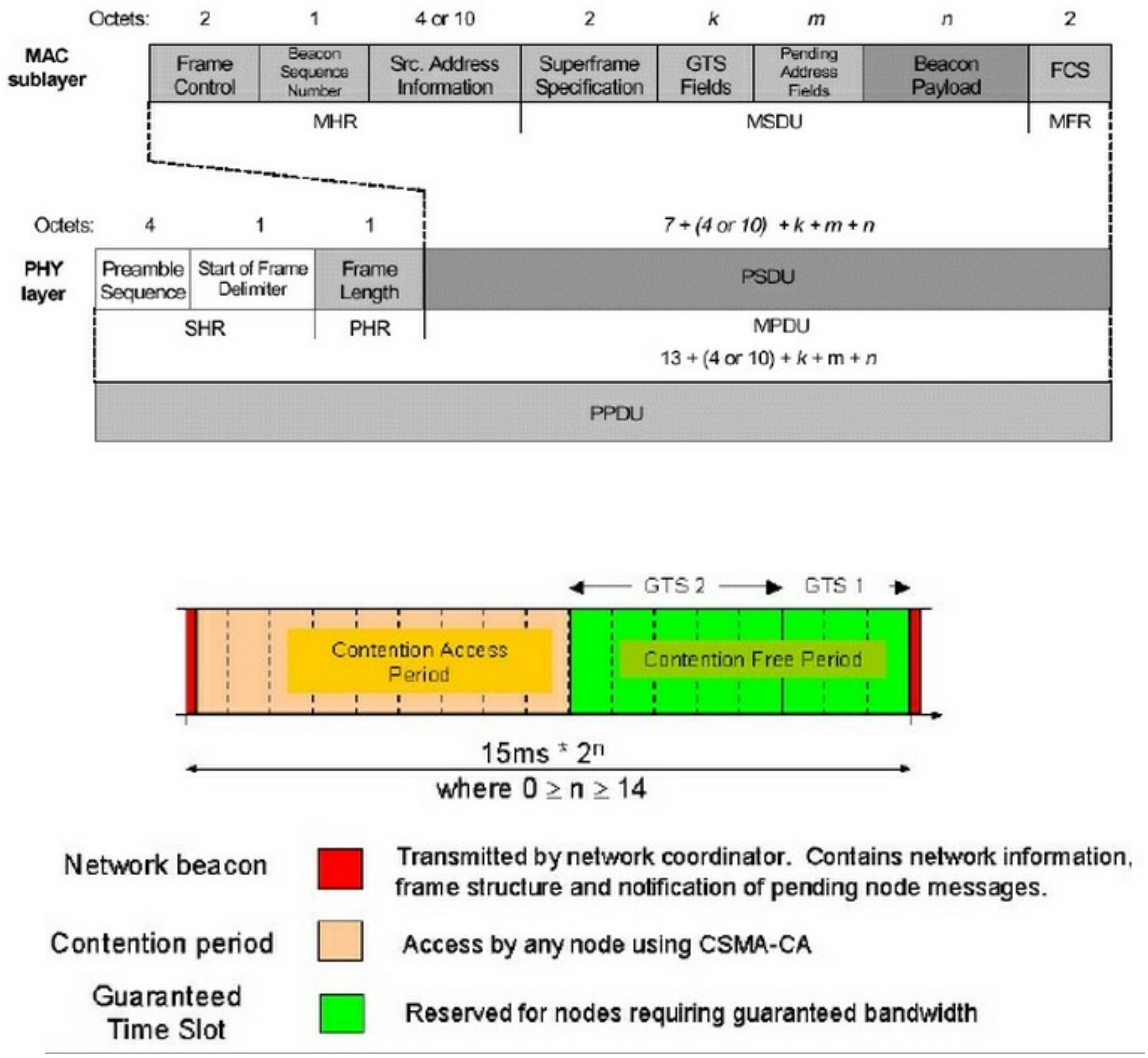

Figura 8. Format de la trama "Beacon"

7.- Exemples de paquets capturats

A continuació es mostren diferents tipus de paquets capturats mitjançant un sniffer de ZigBee, més concretament mitjançant el VW4RZUSBTICK del fabricant ATMEL i la suit de aplicacions KillerBee [9].

Posteriorment, analitzem les captures amb el programa WireShark,

A la següent figura, podem observar la captura d'una trama, més concretament la trama d'una comanda.

```
▶ Frame 1: 50 bytes on wire (400 bits), 50 bytes captured (400 bits)
▼ IEEE 802.15.4 Data, Dst: Broadcast, Src: 0x0000
  ▼ Frame Control Field: Data (0x8841)
      .... .... .... .001 = Frame Type: Data (0x0001)
      .... .... .... 0... = Security Enabled: False
      .... .... ...0 .... = Frame Pending: False
      .... .... ..0. .... = Acknowledge Request: False
      .... .... .1.. .... = Intra-PAN: True
      .... 10.. .... .... = Destination Addressing Mode: Short/16-bit (0x0002)
      ..00 .... .... .... = Frame Version: 0
      10.. .... .... .... = Source Addressing Mode: Short/16-bit (0x0002)
    Sequence Number: 14
    Destination PAN: 0x3359
    Destination: 0xffff
    Source: 0x0000
    [Extended Source: Control4_00:00:1f:02:22 (00:0f:ff:00:00:1f:02:22)]
    [Origin: 1]
    FCS: 0x11f6 (Correct)
▼ ZigBee Network Layer Command, Dst: Broadcast, Src: 0x0000
  ▶ Frame Control Field: Command (0x1209)
    Destination: 0xfffc
    Source: 0x0000
    Radius: 1
    Sequence Number: 192
    Extended Source: Control4_00:00:1f:02:22 (00:0f:ff:00:00:1f:02:22)
  ▶ ZigBee Security Header
  ▼ Data (5 bytes)
      Data: 658df37b6a
      [Length: 5]

0000  41 88 0e 59 33 ff ff 00  00 09 12 fc ff 00 00 01   A..Y3... ........
0010  c0 22 02 1f 00 00 ff 0f  00 28 ba 22 01 00 22 02   ."...... .(."..".
0020  1f 00 00 ff 0f 00 00 65  8d f3 7b 6a f6 97 6d a6   .......e ..{j..m.
0030  f6 11                                              ..
```

Figura 9.- Captura d'una comanda

Com es pot veure, els dos primers bytes, corresponent al "Frame Control", on ens indica per exemple si la trama esta codificada, si espera rebre un ACK...
El següent byte és el número de seqüència.
Seguidament, podem observar la adreça de destí, que en aquest cas és un broadcast (0xFFFF).
La adreça del originador (0x0000).
El "Frame Control Field", ens indica que es tracta d'un paquet de comanda.

A continuació es mostra una captura d'un missatge ACK.

```
▶ Frame 4: 5 bytes on wire (40 bits), 5 bytes captured (40 bits)
▼ IEEE 802.15.4 Ack, Sequence Number: 128
  ▼ Frame Control Field: Ack (0x0002)
      .... .... .... .010 = Frame Type: Ack (0x0002)
      .... .... .... 0... = Security Enabled: False
      .... .... ...0 .... = Frame Pending: False
      .... .... ..0. .... = Acknowledge Request: False
      .... .... .0.. .... = Intra-PAN: False
      .... 00.. .... .... = Destination Addressing Mode: None (0x0000)
      ..00 .... .... .... = Frame Version: 0
      00.. .... .... .... = Source Addressing Mode: None (0x0000)
    Sequence Number: 128
    FCS: 0x31b0 (Correct)

0000  02 00 80 b0 31                                     ....1
```

Figura 10.- Captura d'un ACK

Podem observar que aquest missatge ACK, es composa d'un "Frame Control" seguit del número de seqüència i el FCS.

També podem veure a la següent captura, una trama de Beacon.

```
▶ Frame 140: 28 bytes on wire (224 bits), 28 bytes captured (224 bits)
▼ IEEE 802.15.4 Beacon, Src: 0x0000
  ▼ Frame Control Field: Beacon (0x8000)
      .... .... .... .000 = Frame Type: Beacon (0x0000)
      .... .... .... 0... = Security Enabled: False
      .... .... ...0 .... = Frame Pending: False
      .... .... ..0. .... = Acknowledge Request: False
      .... .... .0.. .... = Intra-PAN: False
      .... 00.. .... .... = Destination Addressing Mode: None (0x0000)
      ..00 .... .... .... = Frame Version: 0
      10.. .... .... .... = Source Addressing Mode: Short/16-bit (0x0002)
    Sequence Number: 197
    Source PAN: 0x3359
    Source: 0x0000
  ▼ Superframe Specification
      .... .... .... 1111 = Beacon Interval: 15
      .... .... 1111 .... = Superframe Interval: 15
      .... 1111 .... .... = Final CAP Slot: 15
      ...0 .... .... .... = Battery Extension: False
      .1.. .... .... .... = PAN Coordinator: True
      1... .... .... .... = Association Permit: True
  ▶ GTS
    Pending Addresses: 0 Short and 0 Long
    FCS: 0x38e0 (Correct)
▶ ZigBee Beacon

0000  00 80 c5 59 33 00 00 ff  cf 00 00 00 22 84 06 b0   ...Y3... ....."...
0010  90 d1 c6 77 f9 8e ff ff  ff 00 e0 38               ...w.... ...8
```

Figura 11.- Captura d'un paquet de Beacon

Podem observar com la trama incorpora els bytes del "Super Frame"

8. Atac a una Xarxa ZigBee

Un atac a una xarxa Zigbee, pot obtenir la clau de xarxa a través de diferents mètodes com ara un atac a distancia o un atac físic.
En el primer cas, aquest es pot aconseguir mitjançant la intercepció de la clau durant la transmissió fora de banda o mitjançant la captura de text en el tràfic d'un coordinador ZigBee.
En el segon tipus, es roba desde el dispositiu físic, extraient la informació directament desde el seu hardware.

Els atacs a distància es basen en la intercepció de missatges i l'explotació dels mecanismes d'intercanvi de claus, que poden ser executades a través d'un atac d'enginyeria social. Per tant un atac físic és molt més complex que un atac a distancia.

Els atacs físics són factibles si es te accés al microcontrolador dels dispositius utilitzats. Els xips ZigBee són vulnerables a l'extracció de claus locals. Actualment, no hi ha protecció contra l'accés extern, que intenten robar claus amb memòries de dades sense protecció i l'explotació de la memòria flash.

És possible atacar un microcontrolador i la seva ràdio ZigBee, explotant el seu generador de número pseudo aleatori (PRNG). Aquest atac es diu "de canal lateral" Aquest número aleatori pot ser llegit perla CPU i s'utilitza per generar les claus aleatòries del xifrat.

En ZigBee, un missatge broadcast, és encriptat amb la clau de xarxa, que es comparteix entre tots els dispositius de la xarxa. Des-afortunadament, només cal posar en perill un sol dispositiu a la xarxa per ser capaç de posar en perill tota la xarxa. En utilitzar aquest clau, que l'atacant ha capturat en el contingut d'un missatge, és una de les vulnerabilitats més importants en la tecnologia ZigBee. Un adversari, pot obtenir les claus de xifratge remotament.

En contrast, les comunicacions unicast, estan assegurades per una clau d'enllaç única compartida entre dos dispositius a la xarxa. Això significa que si un dispositiu de la xarxa es veu compromès per agressió física, un atacant és capaç de capturar el contingut de tota la comunicació directa del dispositiu.
Per tal d'abordar aquest problema, s'hauria d'utilitzar un mecanisme d'intercanvi de claus per protegir-se. [5]

Un altre tipus d'atac possible, que es basa en la vulnerabilitat anterior en que tots els missatges de difusió són xifrats amb la mateixa clau. Això permet als atacants suplantar l identitat de qualsevol node de la difusió ja que no existeix cap comprovació d'autentificació. Aquest vulnerabilitat només s'aplica als missatges de difusió, per tant tot depèn de la quantitat d'emissions de cada aplicació.
Per resoldre aquest problema, s'utilitza un mecanisme per part de l'aplicació en un certificat d'autenticitat, utilitzant una signatura d'un sol sentit.

Els atacs que no requereixen d'un atacant per accedir a les claus criptogràfiques emmagatzemades als dispositius ZigBee, són una gran preocupació, ja que es pot realitzar de forma remota. No cal una manipulació física dels dispositius. Els dos atacs principals existents són els atacs de repetició i la denegació de servei.

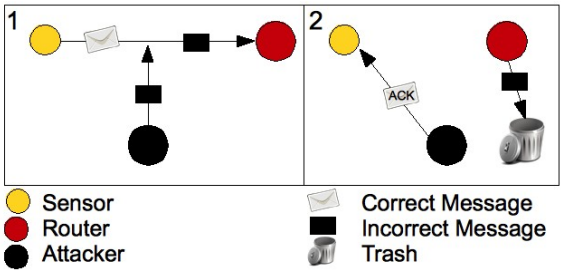

Figura 12. Mètode d'atac per suplantació

A. Atacs de Replay.
Els atacs de repetició (Replay), es poden aplicara a moltes aplicacions. La tecnologia Zigbee proporciona un mecanisme per evitar la recepció de paquets anomenada "comptador de quadres", que s'ha afegit a la capçalera de la trama en la capa de xarxa. Esta composat per un comptador en cada transmissió i que detecta les dades replicades. No obstant això, un atac de repetició ha estat executat amb èxit per Joshua Wright [10], un sènior de seguretat de "InGuardia"

Actualment, Joshua Wright està treballant en "KillerBee", un conjunt d'eines de codi obert en phyton, destinat a provar la seguretat de les xarxes ZigBee. Aquest és l'eina que en utilitat per realitzar captures i anàlisis de paquets.

B. Atacs DoS
L'altre tipus d'atac és el de denegació de servei (DoS). S0ha fet un gran esforç per part de la Aliança ZigBee per a poder realitzar una autentificació i proporcionar la confidencialitat de les dades transmeses. No obstant, cap dels esforços ha evitat la denegació de servei. Aquest atac es pot dur a terme en diferents capes i depèn de si el atacant s'ha unit a la xarxa, sent part d'ella o desde fora.
Si l'atacant te accés a dintre de la xarxa, l'atac DoS per ser canalitzat a les capes PHY, MAC, NWK o APS, mentre que si és un atac extern, l'atac només pot ser fet a les capes PHY o MAC.
La possibilitat de realitzar atacs DoS en diverses capes, és important perquè els atacs més complexis seran més difícils de detectar, perquè la intenció d'un atacant es ser invisible.

A la capa d'aplicació, el DoS es realitza mitjançant l'enviament d'una gran quantitat de missatges al dispositiu per interrompre el processament. A més, aquesta acció esgota els recursos del dispositiu com ara la bateria. Aquest atac pot ser fàcilment detectat, ja que tots els missatges s'envien des d'un únic dispositiu específic.

Si l'atacant es col·loca dintre de la xarxa, es pot aturar l'enviament de missatges entre els nodes.
Afortunadament, aquest atac DoS pot ser directament detectat i evitat per protocol d'enrutament per defecte. El dispositiu, pot començar a enviar missatges a través d'un altre enrutador si es possible [5].

REFERÈNCIES

[1] Jon T. Adams , "An introduction to IEEE STD 802,15,4"

[2] ZigBee Alliance. http://www.zigbee.org/Specifications/ZigBee/Overview.aspx

[3] http://www.specifications.nl/zigbee/zigbee_UK.php

[4] Li Chunqing, Zhang Jiancheng . "Research of ZigBee's data security and protection".

[5] Pedram Radmand . "ZigBee/ZigBee PRO security assessment based on compromised cryptographic keys "

[6] http://ww1.microchip.com/downloads/en/AppNotes/00965c.pdf

[7] http://www.scribd.com/doc/91786190/83/The-Auxiliary-Frame-Header-Format

[8] http://www.scribd.com/doc/52470242/128/ZigBee-security

[9] http://code.google.com/p/killerbee/

[10] http://www.willhackforsushi.com/