Seguretat en xarxes sense fils d'abast personal

Cristina Pérez Solà

PID_00191682

UOC
Universitat Oberta de Catalunya

Índex

Introducció

Les xarxes sense fils d'abast personal (també conegudes com a WPAN pel seu nom en anglès, *Wireless Personal Area Networks*) són xarxes formades per dispositius, possiblement heterogenis, que es troben a poca distància (normalment de l'ordre de pocs metres). La magnitud exacta de la distància a la qual es poden comunicar diversos dispositius i també les característiques específiques de la comunicació seran determinades per la tecnologia específica que s'utilitzi.

En aquest mòdul didàctic veurem quins són els problemes de seguretat que han d'afrontar les WPAN, i també les alternatives que es fan servir habitualment per a solucionar aquests problemes. Per a fer-ho, ens centrarem en tres de les tecnologies més populars per a crear aquest tipus de xarxes: RFID, Bluetooth i ZigBee.

En primer lloc, veurem una descripció de la tecnologia RFID i dels atacs que poden experimentar els dispositius que en fan ús. Seguidament, veurem què es pot fer per a aconseguir primitives criptogràfiques per a dispositius RFID, prestant especial atenció als recursos necessaris per a implementar-les, i detallarem alguns dels protocols que es fan servir per a oferir seguretat en aquests sistemes.

En segon lloc, descriurem l'estàndard Bluetooth i els mecanismes de seguretat que preveu. Repassarem els diferents modes de seguretat de Bluetooth, tot detallant alguns dels processos bàsics, com ara els que permeten autenticar dispositius.

Finalment, comentarem l'estàndard ZigBee i veurem també els mecanismes de seguretat que incorpora. Exposarem els diferents serveis de seguretat que ZigBee ofereix per a cada una de les capes, analitzant alguns dels protocols de l'estàndard, com el protocol d'establiment de claus o el protocol d'autenticació mútua.

Objectius

En els materials didàctics associats a aquest mòdul l'estudiant trobarà les eines i els continguts necessaris per a assolir els objectius següents:

1. Conèixer les tecnologies i estàndards bàsics per a xarxes sense fils d'abast personal (WPAN).
2. Identificar els problemes de seguretat que sorgeixen en entorns WPAN.
3. Comprendre les propietats que es volen garantir quan es parla del disseny de sistemes per a WPAN segurs.
4. Adquirir un coneixement genèric de les tècniques criptogràfiques que s'utilitzen per a afrontar els problemes de seguretat de les xarxes WPAN.
5. Entendre les limitacions de cada una de les tecnologies exposades i també el que aquestes limitacions impliquen a l'hora de dissenyar sistemes segurs.

1. RFID

Començarem l'estudi de les tecnologies per a xarxes WPAN analitzant RFID. En primer lloc, descriurem la tecnologia RFID i classificarem els diferents tipus de dispositius RFID segons la seva capacitat de còmput. Aquesta classificació ens serà útil, posteriorment, per a analitzar les solucions criptogràfiques que es presenten i la seva adaptabilitat als diferents dispositius.

Seguidament passarem a enumerar els atacs als quals són vulnerables els sistemes RFID per a proposar, després, solucions que permetin minimitzar o evitar completament els efectes d'aquests atacs. En aquest sentit, veurem com podem crear primitives criptogràfiques adients als dispositius RFID i estudiarem alguns dels protocols que permeten garantir certes propietats dels sistemes segurs.

1.1. Descripció de la tecnologia RFID

RFID* és una tecnologia que permet la comunicació sense fils a partir de l'emissió d'ones de radiofreqüència. Els components principals d'un sistema RFID són el lector i el transponedor (o etiqueta). La tecnologia RFID s'utilitza, avui en dia, en una gran varietat d'escenaris, des de passaports fins a sistemes de control d'accés, passant per sistemes de tiquets o mecanismes de protecció contra falsificació.

* De l'anglès, *Radio Frequency Identification.*

Els elements principals d'una etiqueta RFID són l'antena i el xip. L'antena és l'encarregada d'emetre i rebre les ones de radiofreqüència que fan possible la comunicació. Per la seva part, el xip incorpora un modulador i un desmodulador que processen els senyals i uns circuits que implementen la memòria i les eines de processament de la informació. Opcionalment, les etiquetes poden incorporar altres circuits amb tasques més específiques.

Amb el nom d'etiqueta RFID, s'hi engloben, en realitat, un gran ventall de dispositius amb característiques molt diferents. Mentre que algunes de les etiquetes RFID no disposen de bateria i fan servir el senyal que els arriba del lector per a induir un petit corrent elèctric suficient per a operar (etiquetes passives), altres etiquetes sí que disposen d'una font d'energia pròpia i poden funcionar de manera autònoma (etiquetes actives). A mig camí, hi trobem els dispositius semipassius, que disposen d'una bateria que es fa servir únicament per a computacions internes, però que necessiten energia externa per a fer possible la comunicació. La font d'energia no és l'única característica diferenciadora de les etiquetes RFID. Altres paràmetres, com ara la mida, també varien enor-

ment d'un tipus d'etiqueta a una altra. Atès que la mida de l'àrea del xip està condicionada per la tecnologia que s'utilitza, la mesura de la capacitat del xip no es fa directament amb l'àrea disponible sinó que es realitza en portes lògiques equivalents (o GE*).

* De l'anglès, *gate equivalent*.

Una **porta equivalent** o **GE** correspon a l'àrea del xip necessària per a implementar una porta NAND de dues entrades. Les GE permeten especificar la complexitat d'un circuit electrònic independentment de la tecnologia amb la qual aquest s'hagi creat.

La porta lògica NAND

Les portes NAND són especialment importants en el disseny de circuits lògics ja que qualsevol funció booleana pot ser implementada fent servir únicament una combinació de portes d'aquest tipus.

Així doncs, la capacitat de còmput d'una etiqueta RFID mesurada en GE és un dels paràmetres que pot variar molt depenent del tipus concret d'etiqueta. Aquestes diferències fan que les solucions de seguretat proposades per les etiquetes amb més recursos puguin no ser viables per a les més limitades i que, per tant, sigui necessari tenir molt clar amb quin tipus de dispositiu RFID es vol treballar abans de definir-ne els mecanismes de seguretat que s'hi volen implementar. En general, podem classificar les etiquetes RFID en tres categories:

- **Gamma baixa**. Etiquetes de baix cost amb menys de 5.000 GE. Mentre que algunes d'aquestes etiquetes no disposen de cap tipus de mecanisme de seguretat ni privacitat, altres incorporen funcionalitats de seguretat bàsiques com sumes de verificació (*checksums*), una comanda KILL protegida mitjançant contrasenya, una contrasenya d'accés o un generador de nombres pseudoaleatoris. Els RFID de gamma baixa són utilitzats, principalment, per a realitzar identificació automàtica.

  Per exemple, es troben dispositius de gamma baixa com a etiquetes antirobatori enganxades als productes en venda en una botiga. Les etiquetes *EPC* (*Electronic Product Code*) *Class 1 Gen 2* són un exemple comercial d'aquesta categoria.

La comanda KILL

La comanda KILL permet a un lector desactivar permanentment una etiqueta RFID.

- **Gamma mitjana**. Etiquetes de cost moderat amb transponedors que permeten fer tant operacions de lectura com d'escriptura. Disposen de memòria de dades no volàtil que pot variar des dels 100 bytes fins a més de 100 kB. Les etiquetes d'aquesta gamma implementen, habitualment, protocols d'autenticació mútua i control d'accés a la memòria del transponedor. Durant la comunicació entre l'etiqueta i el lector, s'estableixen claus de sessió que permeten enviar les dades xifrades i assegurar-ne la seva integritat.

  Trobem etiquetes de gamma mitjana en immobilitzadors d'automòbils (que eviten que el motor es posi en marxa sense la presència de la clau correcta), mecanismes de control d'accés a edificis o sistemes de tiquets. D'entre les etiquetes d'aquesta gamma, les més conegudes són les *MiFare Classic*.

- **Gamma alta**. Etiquetes de cost més elevat que contenen xips de targetes intel·ligents (*smartcards*) i que estan equipades amb sistemes operatius

específics per a aquestes targetes. Les etiquetes de gamma alta incorporen mecanismes de seguretat amb funcions criptogràfiques avançades, normalment específiques per a cada aplicació. Les etiquetes amb més prestacions d'aquesta gamma poden arribar a incorporar un coprocessador criptogràfic que permet fer operacions de criptografia de clau pública, com la creació de signatures digitals.

Amb les sigles NFC* s'engloben un conjunt d'estàndards basats en RFID que requereixen proximitats molt altes entre l'etiqueta i el lector, de l'ordre de pocs centímetres, per tal d'establir una comunicació entre ells. El fet de limitar la distància que hi pot haver entre dos dispositius perquè es puguin comunicar pot ser una limitació, però també una característica desitjable a l'hora de millorar la seguretat del sistema.

* De l'anglès, *Near Field Communication.*

Exemples d'NFC

Exemples d'aplicacions que fan servir NFC són dispositius de pagament per mitjà del telèfon mòbil, targetes de fidelització de línies aèries o tiquets de metro multiviatge.

Així doncs, les característiques dels diferents dispositius RFID es determinaran, en gran mesura, pel cost màxim que es pugui assumir a l'hora de produir-lo. La capacitat de còmput d'aquests dispositius en limitarà també el grau de seguretat que es pot assolir.

1.2. Seguretat en dispositius RFID

Hi ha tot un conjunt de propietats que es volen assolir quan s'intenten crear dispositius RFID segurs. Mentre que les propietats més bàsiques oferiran nivells de seguretat elementals, algunes de les més avançades garantiran nivells de seguretat més elevats. El conjunt específic de propietats a garantir es determinarà per les necessitats de l'aplicació que es vulgui donar al sistema:

- **Identificació**. La funció principal d'un lector RFID és, precisament, identificar un valor únic (una ID) que s'assigna a cada etiqueta RFID. La propietat d'identificació permet a un lector descobrir la identitat d'una etiqueta a partir de la sortida d'aquesta etiqueta. A grans trets, les etiquetes RFID reben un identificador únic quan estan en producció. Aquest identificador s'escriu a la ROM (memòria només de lectura) de l'etiqueta, de manera que és molt difícil de canviar posteriorment. Es pot aconseguir identificació sense fer servir cap mena de tècnica criptogràfica. La identificació, però, pot resultar en la fuga de dades secretes, la qual cosa pot permetre, per exemple, atacs de *tracking* com els que veurem posteriorment.

- **Autenticació**. Quan un lector llegeix dades d'una etiqueta, el lector no pot saber si les dades que està rebent són d'una etiqueta vàlida o no, tret que s'afegeixi un sistema de validació. El mateix escenari es presenta en la direcció oposada, quan una etiqueta rep dades d'un lector. Per tal d'assegurar-se que les comunicacions es fan entre dispositius vàlids, cal in-

corporar un mecanisme d'autenticació al sistema que permeti garantir que un lector (respectivament, una etiqueta), només acceptarà les dades d'una etiqueta (respectivament, un lector) si pot assegurar-ne la seva validesa. Els sistemes de control d'accés a edificis són un exemple de dispositius RFID que necessitaran implementar autenticació.

- **Privacitat**. El fet que la propietat d'identificació sigui la més bàsica d'un sistema RFID i que cada etiqueta contingui un identificador únic fa que apareguin problemes de privacitat associats a l'ús de dispositius RFID. Així, per exemple, es podrien seguir els moviments d'una persona o d'un objecte que porti una etiqueta RFID enganxada. Les necessitats específiques de privacitat dependran en gran mesura de l'aplicació concreta que s'estigui donant a les etiquetes RFID.

- **Indistingibilitat**. La indistingibilitat és una propietat molt relacionada amb la privacitat. Diem que una etiqueta té indistingibilitat si un atacant que realitza una escolta passiva no és capaç de distingir entre dues etiquetes diferents només observant-ne les sortides.

- **Seguretat cap endavant***. És una extensió de les propietats d'autenticitat i d'indistingibilitat que garanteix que aquestes propietats es mantenen per a transaccions passades quan un atacant és capaç de corrompre una etiqueta en un moment determinat. Per exemple, es fàcil imaginar un escenari on una etiqueta RFID que disposava de mecanismes per a garantir l'autenticitat i la indistingibilitat és llançada a les escombraries una vegada acabada la seva vida útil. Aleshores, un atacant pot recuperar aquesta etiqueta, manipular-la i obtenir-ne els valors secrets que conté. Si donada aquesta informació, l'atacant continua sense ser capaç de distingir entre les sortides de dues etiquetes que va enregistrar en el passat (una de les quals pertanyia a l'etiqueta compromesa), aleshores diem que té seguretat cap endavant per a la propietat d'indistingibilitat.

  *** En anglès, *forward security*.**

- **Delegació i restricció**. Aquestes propietats són necessàries en aplicacions on les etiquetes són reutilitzades per diversos propietaris. En aquestes aplicacions, es vol que el propietari original pugui delegar el dret de rastrejar una etiqueta a un nou propietari, assegurant que una vegada delegats els drets el propietari original perd la capacitat de rastrejar-la.

- **Prova d'existència**. La prova d'existència és una propietat que permet garantir l'existència d'una etiqueta particular en una localització concreta, en un temps determinat i amb un conjunt d'altres etiquetes particulars. Aquesta propietat és necessària, per exemple, en aplicacions on s'assignen etiquetes RFID als diferents components que formen part d'una cadena de subministrament, de manera que diversos lectors distribuïts al llarg de la cadena puguin controlar-ne el funcionament. En aquest cas, és interessant que el lector pugui detectar que un seguit de components es troben junts en un espai en un moment determinat (per exemple, si aquests components s'han de combinar per a formar una sola peça).

- **Límit de distància**. Per tal de dificultar els atacs de *relay* (que descriurem posteriorment), es pot intentar limitar la distància acceptable entre una etiqueta i un lector. Per fer-ho, es limita el temps d'anada i tornada (*round trip time*) dels intercanvis entre el lector i l'etiqueta.

- **Sincronització**. En protocols basats en màquines d'estats (on les diferents parts van canviant d'estat a mesura que avança el protocol), un atacant pot provocar que el protocol no es completi amb èxit pertorbant o retardant les comunicacions entre l'etiqueta i el lector, és a dir, provocant una desincronització. La propietat de sincronització permet a una etiqueta i un lector tornar-se a sincronitzar, una vegada s'han desincronitzat durant l'execució d'un protocol.

1.2.1. Atacs a sistemes RFID

Els sistemes RFID són vulnerables a diferents tipus d'atacs, alguns dels quals apareixen també en molts altres sistemes d'informació. Depenent del mètode que es faci servir per a atacar el sistema, podem classificar els atacs a dispositius RFID en diferents categories:

- **Lectura passiva**. El mètode de lectura passiva permet a un atacant escoltar els missatges transmesos entre el lector i l'etiqueta, normalment amb la intenció de descobrir informació secreta. Com que és un mètode passiu, l'atacant només té l'habilitat d'escoltar els missatges, sense poder-los manipular de cap manera. El següent és un atac que necessita realitzar una lectura passiva:

– Escoltes no autoritzades*. És l'atac de lectura passiva on l'atacant simplement escolta la comunicació entre una etiqueta i un lector. Atès que les comunicacions RFID són sense fils, és relativament fàcil per a un atacant interceptar aquestes comunicacions, sempre que es pugui situar a prop dels altres dispositius. Aquest tipus d'atacs poden ser difícils de detectar i poden comprometre la identificació, l'autenticació o la privacitat del sistema RFID.

*** En anglès, *eavesdropping*.**

- **Lectura activa**. El mètode de lectura activa consisteix a intentar llegir informació (o de l'etiqueta, del lector o del mateix canal sense fils) però ara tenint la capacitat de modificar els missatges que s'intercanvien l'etiqueta i el lector i d'interactuar amb les diferents parts. La intenció de l'atacant és la de descobrir informació secreta o la d'atacar el mecanisme d'autenticació. Es poden identificar diferents atacs que necessiten poder realitzar lectures actives per a perpetrar-se:

– Atacs de reinjecció**. En un atac de reinjecció, l'atacant enregistra la sortida d'una etiqueta i, posteriorment, envia aquesta sortida cap al lector. Normalment, el moment en què l'atacant enregistra la sortida i el mo-

**** En anglès, *replay attacks*.**

ment en el qual l'atacant reprodueix aquesta sortida es troben separats en el temps. Els atacs de reinjecció poden permetre trencar alguns sistemes d'autenticació.

– Atacs de retransmissió*. En un atac de retransmissió, l'atacant llegeix la sortida d'una etiqueta, transporta aquesta sortida a una altra localització i envia la sortida cap a un lector remot. Aquest tipus d'atacs també poden aconseguir trencar sistemes d'autenticació.

*** En anglès, *relay attacks*.**

– Atac de modificació del missatge. En atacs de modificació del missatge, l'atacant intercepta i modifica la comunicació entre una etiqueta i un lector. Per tal d'evitar aquest tipus d'atacs, s'afegeixen mecanismes de control d'integritat a les dades que s'envien. Els atacs d'aquest tipus poden trencar la identificació, l'autenticació o la privacitat d'un sistema RFID.

- **Reescriptura**. El mètode de reescriptura permet a un atacant reescriure la informació emmagatzemada a l'etiqueta per a obtenir informació secreta o bé amb l'objectiu d'enganyar el mecanisme d'autenticació. Alguns atacs que fan servir la reescriptura són els següents:

– Atac de reescriptura de l'etiqueta / del lector. En un atac de reescriptura de l'etiqueta, l'atacant reescriu els continguts de la memòria d'una etiqueta fent servir un lector fals. Aquest tipus d'atacs es poden prevenir exigint a les etiquetes que autentiquin els lectors abans de permetre reescriure contingut o bé desplegant mecanismes de bloqueig de memòria. De la mateixa manera, també es poden considerar atacs de reescriptura del lector, on una etiqueta falsa aconsegueix comprometre la memòria d'un lector. Els atacs d'aquest tipus poden trencar la identificació, l'autenticació o la privacitat d'un sistema RFID.

– Virus / programari maliciós. Els atacs de reescriptura poden permetre la transmissió de programari maliciós entre dispositius RFID. Per exemple, un lector pot llegir codi maliciós d'una etiqueta contaminada, executant aquest codi i passant a reescriure'l a altres etiquetes al seu abast, i escampar així el programari maliciós.

- **Clonació**. El mètode de clonació consisteix a crear una còpia (un clon) d'una etiqueta o d'un lector. Un atac de clonació és el següent:

– Atac de clonació d'una etiqueta / lector. En un atac de clonació l'atacant aconsegueix una còpia completa d'una altra etiqueta o lector. L'ús de mecanismes d'autenticació o la creació d'etiquetes i lectors a prova de manipulacions són mecanismes de defensa contra la clonació. Aquest tipus d'atacs poden trencar la identificació i l'autenticació d'un sistema RFID.

- **Destrucció / denegació de servei**. Aquest tipus d'atacs inhabiliten l'ús dels dispositius RFID, o destruint-los físicament, saturant-los creant més peticions de les que poden atendre o creant interferències al canal. Alguns atacs de denegació de servei són els següents:

– Denegació de servei i destrucció. En aquest atac l'adversari intenta destruir físicament una etiqueta, deixant-la inutilitzable o bé realitza un atac de denegació de servei que impedeix l'ús del sistema als usuaris legítims.

– Atacs de creació d'interferències*. En aquest tipus d'atacs l'adversari intenta bloquejar o interferir el canal de comunicació sense fils creat entre una etiqueta i un lector.

* En anglès, *jamming*.

- **Rastreig****. Aquest mètode d'atac consisteix a escanejar una etiqueta, o per a obtenir-ne informació o per a detectar-ne els seus moviments. Atacs de rastreig són els següents:

** En anglès, *tracking*.

– Atacs d'escaneig. En un atac d'escaneig l'atacant intenta obtenir informació sobre l'objecte que duu una etiqueta RFID.

– Atacs de rastreig. En un atac de rastreig l'atacant segueix una etiqueta (o la persona o objecte que duu aquesta etiqueta).

- **Canals laterals**. Aquest mètode consisteix a aprofitar informació lateral, com el consum energètic de les etiquetes o el temps de resposta, per a intentar obtenir informació secreta. El següent és un atac que fa servir el mètode de canals laterals:

– Atacs amb canals laterals***. Ateses les característiques tècniques i físiques dels RFID, un atacant pot observar la força del camp electromagnètic que es genera o analitzar els temps d'adquisició i processament de dades per tal d'obtenir informació secreta emmagatzemada en una etiqueta o un lector RFID.

*** En anglès, *side channel attacks*.

1.2.2. Solucions criptogràfiques per a sistemes RFID

Per tal de prevenir, detectar o mitigar els atacs a sistemes RFID que hem descrit anteriorment, es poden implementar solucions criptogràfiques als dispositius RFID. Com hem vist, els sistemes RFID disposen d'uns recursos limitats que es determinaran pel tipus d'etiquetes o lectors que es facin servir. La necessitat d'aconseguir dispositius de baix cost en limita, doncs, la complexitat dels algorismes que s'hi poden implementar i, per tant, les solucions criptogràfiques aplicables.

El conjunt de tècniques criptogràfiques dissenyades per a dispositius amb recursos limitats que intenten oferir un compromís entre rendiment, seguretat i cost es coneix com a **criptografia lleugera***.

* En anglès, *lightweight cryptography*.

Per tal d'aconseguir obtenir implementacions criptogràfiques utilitzables en dispositius RFID, se segueixen, normalment, quatre enfocaments diferents:

- Implementar de manera eficient sistemes de xifra ja existents.
- Fer servir sistemes de xifra ja existents amb paràmetres més petits.
- Dissenyar nous mecanismes de xifratge.
- Desenvolupar solucions totalment dedicades.

Als subapartats següents, repassarem algunes de les solucions de criptografia lleugera que s'utilitzen habitualment en dispositius RFID, tant si són adaptacions de sistemes que originalment necessitaven molts recursos com noves propostes que s'adapten als recursos disponibles en dispositius RFID. En primer lloc, veurem algunes de les primitives criptogràfiques més utilitzades i com es poden fer servir en dispositius RFID. Després, passarem a repassar alguns dels protocols que permeten oferir algunes garanties de seguretat en RFID.

Generadors de nombres pseudoaleatoris

Generadors pseudoaleatoris

Els generadors de nombres pseudoaleatoris es coneixen amb les sigles PRNG (de l'anglès, *Pseudorandom Number Generator*) o bé DRBG (de l'anglès, *Deterministic Random Bit Generator*).

Els generadors de nombres pseudoalteatoris són algorismes deterministes que permeten generar seqüències de nombres que semblen aleatòries. Aquests algorismes tenen com a paràmetre d'entrada un valor inicial o llavor que permet inicialitzar-los i ofereixen una sortida que té unes propietats similars a les que s'observen en seqüències aleatòries.

Un **generador pseudoaleatori** és una funció

$$G : \{0,1\}^s \rightarrow \{0,1\}^n$$

amb $n \gg s$. La funció G ha de ser computable de manera eficient per un algorisme determinista i la seva sortida ha de ser impredictible.

En l'àmbit criptogràfic, és important que les seqüències generades per un generador pseudoaleatori siguin impredictibles, és a dir, que donats els k primers bits d'una seqüència, un atacant no sigui capaç de predir el bit $k+1$ amb una probabilitat superior a $1/2 + \epsilon$, per un valor d'ϵ no negligible. Això implica que la seqüència de sortida del generador és indistingible d'una seqüència realment aleatòria.

Per tal de decidir si la sortida d'un generador pseudoaleatori s'assembla o no a una seqüència aleatòria, s'han creat tot un conjunt de tests que les seqüències aleatòries compleixen i que, per tant, s'espera que les pseudoaleatòries també satisfacin. Així, per exemple, un dels estàndards d'*EPCGlobal* exigeix a les implementacions de PRNG que generin seqüències seguint certes propietats,

com ara que la probabilitat que un nombre qualsevol de 16 bits aparegui a la propera sortida estigui entre $0,8 \cdot 2^{-16}$ i $1,25 \cdot 2^{-16}$, entre d'altres.

Un dels mètodes més populars per a generar PRNG és a partir de registres de desplaçament realimentats linealment o LFSR.

Un **LFSR** de longitud n és un dispositiu format per n cel·les de memòria (o registres).

A cada cicle de rellotge, l'estat de l'LFSR s'actualitza, de manera que el contingut de la cel·la s_i passa a ser el que hi havia a la cel·la s_{i-1}.

El nou bit d'entrada, S_{n+1} es calcula a partir de l'estat dels registres i del polinomi de connexions que defineix l'LFSR:

$$S_{n+1} = c_1 s_n + \cdots + c_n s_1$$

Tot i que els LFSR són molt fàcils d'implementar a nivell *hardware*, fets servir directament també són molt predictibles, limitant-ne el seu ús com a PRNG. Per tal de trencar la linealitat dels LFSR (i fer-los, per tant, menys predictibles) es fan servir diferents tècniques, com aplicar una funció de filtratge no lineal als bits que s'extreuen o combinar la sortida de diferents LFRS mitjançant una funció no lineal.

Hi ha altres maneres de crear PRNG que es basen en les propietats estadístiques que presenten els sistemes de xifra i les funcions *hash*. Així, per exemple, es poden construir PRNG fent crides a algunes funcions *hash* (com ara SHA-1, SHA-256, SHA-386 o SHA-512) amb els valors d'un comptador com a entrada, iterant funcions HMAC fent servir alguna de les funcions *hash* esmentades anteriorment o bé xifrant un comptador amb certs algorismes de xifra de bloc com ara l'AES o el triple-DES.

Xifres de bloc

Una xifra de bloc sobre l'alfabet binari és una projecció bijectiva $E_k : \{0,1\}^n \rightarrow \{0,1\}^n$ indexada per una clau k. Les xifres de bloc permeten xifrar dades de mida arbitrària dividint-les en blocs d'n bits, afegint *padding* si és necessari i aplicant la funció E_k. Per tal d'utilitzar xifres de bloc, es defineixen un conjunt de modes d'operació que expliciten com s'han de combinar els diferents blocs, a quins valors s'ha d'aplicar la funció E_k i com s'han d'incorporar vectors d'inicialització, *nonces* i comptadors als esquemes.

Entre els sistemes de xifra de bloc més coneguts hi ha l'AES i el DES. Com hem vist, una de les alternatives més directes per a obtenir eines criptogràfiques per dispositius amb recursos limitats és la implementació eficient de sistemes ja existents. En aquesta línia, es pot trobar una implementació de la versió serialitzada del DES que requereix només 2310 GE i que fa servir 144 cicles de rellotge per a xifrar un bloc d'entrada. Aquesta versió del DES, però, ja no es considera segura ja que, d'una banda, s'han trobat debilitats en l'àmbit teòric i, d'altra banda, s'han produït atacs distribuïts que han permès trencar claus DES (de 56 bits) en menys d'un dia.

Una de les variants de DES creades amb l'objectiu d'incrementar la complexitat d'un atac per força bruta és el triple-DES:

$$3DES_{k_1,k_2,k_3}(m) = E_{k_1}(E^{-1}_{k_2}(E_{k_3}(m))).$$

DES

El DES (*Data Encryption Standard*) és un algorisme de xifra inventat als anys 70. Les claus del DES estan formades per 64 bits, però només 56 d'aquests bits s'utilitzen efectivament en el procés de xifratge / desxifratge. Els altres 8 bits es fan servir únicament per a fer comprovacions de paritat.

Per la seva construcció, 3DES ofereix compatibilitat amb el DES: si les tres claus utilitzades són la mateixa, aleshores 3DES és equivalent a DES ($3DES_{k,k,k}(m) = E_k(E^{-1}_k(E_k(p))) = E_k(p)$. La longitud de la clau pot ser de fins a 168 bits ($56 * 3$). 3DES es pot implementar amb 4600 GE, requerint 62 cicles de rellotge per a l'operació de xifratge.

Una altra de les variants del DES que es va desenvolupar amb l'objectiu de millorar-ne la seguretat és el DESX:

$$DESX_{k_1,k_2,k_3}(m) = k_3 \oplus E_{k_1}(k_2 \oplus m).$$

Tot i que amb aquest esquema la longitud de la clau és de 184 bits (64+64+56), la longitud efectiva és bastant menor i està condicionada per la informació que és capaç d'obtenir l'atacant, en concret, pel nombre de parells de text en clar i text xifrat que aquest és capaç d'aconseguir.

La versió original del DES (i, en conseqüència, la del DESX) preveu la utilització de caixes *S* (caixes de substitució), la implementació de les quals necessita una quantitat substancial de memòria (normalment s'implementen com a taules de *lookup* estàtiques). Per tal d'obtenir una versió del DES amb menor requeriments d'espai que l'original, es va crear una versió optimitzada coneguda amb el nom de DESL que reemplaça les 8 caixes *S* originals per una única caixa *S* dissenyada de nou. De la combinació del DESL amb el DESX en va sorgir el sistema de xifra DESXL, que s'ha implementat amb només 2169 GE.

L'AES és un algorisme de xifra que ja va ser dissenyat amb l'eficiència com un dels requisits. L'AES (128 bits) en mode de només xifratge es pot implementar fent servir 3100 GE i necessita 1044 cicles de rellotge per a realitzar el xifratge d'un bloc de dades.

Xifres de flux

A diferència de les xifres de bloc, les xifres de flux generen una cadena de bits a partir de la clau i realitzen l'operació de xifratge fent una xor del text en clar amb la cadena obtinguda.

L'algorisme RC4 és una xifra de flux bastant popular. Tot i això, no és gens adequada per a sistemes amb recursos limitats ja que conté una permutació que necessita més de 12.000 portes per a ser implementada.

En el cas de les xifres de flux, l'alternativa de dissenyar nous sistemes que requereixin poques GE és la que ha tingut més acceptació. Així doncs, sistemes de xifra com ara Grain o Trivium es van dissenyar específicament per a dispositius amb recursos molt limitats.

El funcionament de Trivium està basat en 3 LFSR de 93, 84 i 11 bits de longitud. Per generar un bit de sortida, s'extreuen dos bit de cada un dels LFSR i es realitza una xor de tots ells. Trivium es pot implementar amb 3090 GE i necessita 176 cicles de rellotge per a xifrar 128 bits de dades.

Grain fa servir dos registres de desplaçament i una funció no lineal de sortida per tal d'operar. Grain pot ser ser implementat amb 3360 GE, i requereix 104 cicles de rellotge per a xifrar 128 bits. Una de les característiques addicionals d'aquest algorisme és que permet augmentar-ne la velocitat, pagant un preu a nivell de portes lògiques necessàries per a implementar-lo. Així doncs, la implementació més senzilla (i també la més lenta) requereix només 1450 GE. La mida de la clau és de 80 bits.

Funcions hash

Una funció *hash H* és una funció que fa correspondre a un missatge m de mida variable un valor $H(m)$ de mida fixada. Hi ha un conjunt de propietats que les funcions *hash* haurien de satisfer per a poder-se considerar segures:

1) per qualsevol valor y, és difícil trobar un valor m tal que $H(m) = y$;

2) donat un valor m_1, és difícil trobar un altre valor $m_2 \neq m_1$ tal que $H(m_1) = H(m_2)$;

3) és difícil trobar dos valors m_1, m_2 amb $m_1 \neq m_2$ tals que $H(m_1) = H(m_2)$.

Després que la popular funció de *hash* MD5 es considerés trencada, la família de funcions SHA n'ha pres el relleu. Existeixen implementacions de SHA-256 amb 10868 GE que requereixen 1128 cicles de rellotge per a calcular el *hash* d'un bloc de 512 bits. Per a SHA-1, les implementacions requereixen una mica menys d'espai (8120 GE). En tots dos casos, però, el nombre de GE necessàries és molt elevat per a ser usats en RFID de gamma mitjana-baixa.

Criptografia de clau pública

La criptografia de clau pública es basa en l'ús de parells de claus que tenen una relació matemàtica especial. Cada usuari disposa d'una clau pública que és coneguda per tothom i d'una clau privada que només ell coneix. Per a xifrar un missatge *m*, s'aplica una funció de xifratge *E* sobre *m* fent servir la clau pública de l'usuari al qual va destinat. Per tal de desxifrar el missatge, l'usuari destinatari haurà d'aplicar una funció de desxifratge *D* al text xifrat *c*, fent servir la seva clau privada.

La utilització de criptografia basada en corbes el·líptiques* per sistemes RFID és un camp en desenvolupament. S'estima que una implementació d'ECC de 192 bits necessitaria 23600 GE i més de 500.000 cicles de rellotge per a realitzar una operació de multiplicació de punts.

*** En anglès, *Eliptic Curve Cryptography* o *ECC*.**

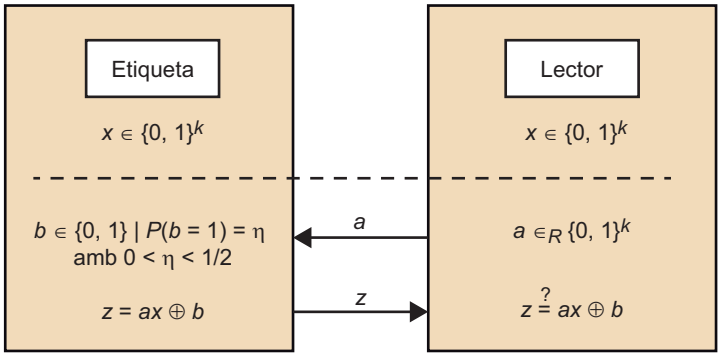
Protocols per autenticar

El protocol de Hopper i Blum (*HB*) és un esquema que ofereix autenticació sense oferir privacitat. El protocol original, que es coneix com a *protocol HB*, només és segur davant d'atacants passius que només escolten la comunicació, sense interferir-la ni modificar-la de cap manera. L'avantatge principal d'aquest protocol és la seva gran simplicitat, la qual cosa el fa més adequat per a dispositius RFID amb poques GE. Donat un lector i una etiqueta que comparteixen una tira de *k* bits secreta, *x*, el protocol permet al lector autenticar una etiqueta sense que un atacant que fa una escolta passiva pugui aprendre el valor secret *x*. La figura 1 descriu els passos que conformen el protocol HB.

Figura 1

El protocol requereix que l'etiqueta i el lector comparteixin un valor secret x de k bits. El lector (que fa de verificador), genera un repte aleatori a també de k bits i l'envia a l'etiqueta (el provador). Aleshores, l'etiqueta calcula el producte escalar entre el valor secret x i el repte aleatori a, i canvia el resultat de l'operació amb una probabilitat η (és a dir, selecciona un bit b aleatòriament de manera que aquest sigui 1 amb probabilitat η i fa una xor del resultat amb aquest bit b). El resultat d'aquesta operació, el valor z, s'envia al verificador, que comprovarà si és el mateix que el resultat de fer el producte escalar entre els vectors a i x. Atès que el provador canviarà el resultat amb una probabilitat $\eta < 1/2$, aquest valor serà igual amb una probabilitat superior a 1/2. El protocol es repeteix, per tant, un nombre de vegades determinat, i l'autenticació es dóna per vàlida si els valors obtinguts han estat iguals en un nombre mínim de repeticions.

Figura 1. Protocol HB



Com es pot observar, aquest protocol no és segur davant d'atacants actius que poden fer-se passar per verificadors i executar el protocol múltiples vegades, tenint sota el seu poder la decisió dels valors de repte *a* enviats en cada moment. Una altra versió d'aquest protocol, *HB+*, estèn la seva funcionalitat perquè sigui segur davant d'atacants actius que poden interactuar tant amb l'etiqueta com amb el lector, tot i que no de manera concurrent. Una tercera extensió d'aquest mateix protocol anomenada $HB^{\#}$ assegura l'autenticació correcta davant d'atacants actius amb accés concurrent a l'etiqueta i al lector.

Protocols per a garantir la seguretat cap endavant

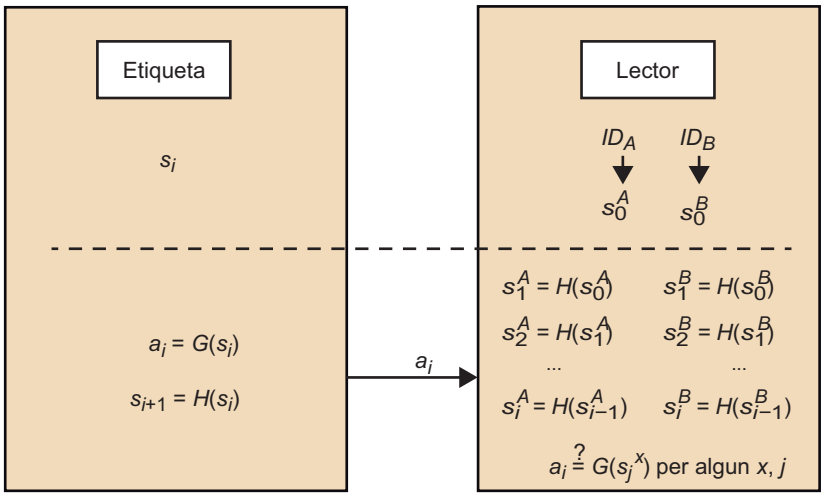
Com hem vist, una de les propietats de seguretat que pot ser interessant de garantir en sistemes RFID és la seguretat cap endavant, que permet evitar que un atacant pugui identificar transaccions passades que involucraven una etiqueta donada si aconsegueix descobrir-ne les dades secretes que conté en un instant de temps concret. Una de les alternatives proposades per a aconseguir garantir aquesta propietat és l'ús de cadenes de funcions *hash*.

L'esquema proposat per Ohkubo, Suzuki i Kinoshita fa servir dues funcions de *hash* H i G. Cada etiqueta té un valor secret s_i on i és un comptador de transaccions, de manera que el valor secret canvia a cada nova transacció. Per tal d'identificar-se, una etiqueta enviarà al lector el valor $a_i = G(s_i)$, que és el resultat d'aplicar la funció *hash* G al valor secret que té en aquell moment. Aleshores, l'etiqueta renova el seu valor secret fent servir la funció *hash* H, de manera que $s_{i+1} = H(s_i)$, i seguidament esborra el valor secret s_i. El lector manté una base de dades amb les correspondències entre cada identificador d'etiqueta i la informació secreta inicial s_0 associada a aquella etiqueta. Quan el lector rep un valor a_i, comprova si aquest valor correspon a algun valor $G(H^i(s_0))$ per algun s_0 de les etiquetes que coneix, i recupera així l'identificador de l'etiqueta. Mentre que el nombre d'operacions a realitzar per l'etiqueta és baix, el lector ha de calcular sortides de la funció hash per cada un dels valors i i per cada una de les etiquetes que té a la base de dades, la qual cosa pot suposar un cost elevat en escenaris determinats.

Exemple d'autenticació amb cadenes *hash*

En el cas que es mostra a la figura 2, el lector només té dues etiquetes a la seva base de dades. Quan rep un valor a_i, el lector pot comprovar a quina etiqueta pertany calculant tots els valors de la cadena *hash*, fent servir com a valor inicial de la cadena el secret inicial s_i de cada una de les etiquetes que reconeix.

Figura 2. Autenticació amb cadenes de *hash*



2. Bluetooth

En aquest apartat descriurem l'estàndard Bluetooth i els mecanismes de seguretat que preveu. En primer lloc, veurem quines classes de dispositius Bluetooth existeixen i quina és l'estructura de les xarxes de dispositius Bluetooth.

Després, repassarem els diferents modes de seguretat de Bluetooth, tot detallant alguns dels processos bàsics, com els que permeten autenticar dispositius, i veurem les diferents claus que permeten oferir seguretat als dispositius Bluetooth.

2.1. Descripció de l'especificació Bluetooth

Bluetooth és un estàndard industrial per a comunicacions sense fils barates de curt abast. Té com a objectiu principal substituir els cables de teclats, ratolins i perifèrics en general, i també permetre comunicacions entre dispositius portables. L'estàndard de Bluetooth es desenvolupa per mitjà del Bluetooth Special Interest Group, al qual pertanyen companyies del sector de les telecomunicacions, les xarxes i l'electrònica de consum.

L'origen del nom Bluetooth

El nom de Bluetooth deriva del nom del rei danès i noruec Harald Blåtand. La traducció directa a l'anglès del nom d'aquest rei és Harold Bluetooth. Aquest rei és conegut per ser un bon comunicador i per unificar les tribus daneses, noruegues i sueques.

Els dispositius Bluetooth es classifiquen en 3 classes, depenent de la seva potència i del seu abast de comunicació. La taula 1 mostra les classes disponibles.

Taula 1. Dispositius Bluetooth

Classe	Potència màxima	Rang aproximat
1	100 mW	100 m
2	2,5 mW	10 m
3	1 mW	1 m

L'estàndard Bluetooth està enfocat cap a dispositius que disposen de bateria. Així doncs, tant el rendiment de les aplicacions que s'hi executin com la seguretat dels dispositius Bluetooth estaran limitats, d'una banda, pel consum energètic i, d'altra banda, pel seu cost.

Les xarxes Bluetooth es creen seguint una topologia d'estrella amb 8 membres com a màxim, un dels quals actua com a mestre. La resta de membres adopten el paper d'esclaus. Cadascuna d'aquestes xarxes es coneix amb el nom de *piconet*. Atesa la topologia de les *piconets*, les comunicacions amb Bluetooth sempre impliquen un dispositiu mestre, la qual cosa permet que hi hagi comunicació tant des d'un mestre cap a un esclau com des d'un esclau cap a un mestre. Si dos dispositius esclaus es volen comunicar entre ells, necessiten que

un dispositiu mestre actuï com a intermediari. Per tal d'optimitzar aquesta comunicació, un dels dispositius esclaus implicats pot decidir crear una nova *piconet* i convertir-se en mestre d'aquella xarxa, i així pot comunicar-se directament amb l'altre dispositiu. Un dispositiu pot pertànyer a més d'una *piconet* alhora, però només pot ser-ne mestre d'una com a màxim.

2.2. Seguretat en dispositius Bluetooth

L'arquitectura de seguretat del Bluetooth permet obtenir les propietats de confidencialitat, integritat i autenticació. El fet que els sistemes de xifratge que s'utilitzen siguin de clau simètrica implica que no es pot aconseguir la propietat de no-repudi.

Els dispositius Bluetooth poden operar en tres modes de seguretat:

- **Mode de seguretat 1**. Aquest és el mode més insegur ja que no incorpora cap mecanisme de seguretat. Així permet la connexió entre qualsevol dispositiu o aplicació.

- **Mode de seguretat 2** (nivell de servei). Aquest és el mode de seguretat que actua a nivell de servei. El dispositiu deixa realitzar connexions però després aplica la seguretat i restringeix l'ús de les aplicacions. En aquest cas, la política de seguretat s'aplica amb posterioritat a la connexió.

- **Mode de seguretat 3** (nivell d'enllaç). Aquest és el mode de seguretat que actua directament a nivell d'enllaç. Per tant, la política de seguretat s'aplica ja abans de fer la connexió.

Poca seguretat

De fet, el mode de seguretat 1 no s'hauria de considerar de seguretat, però les especificacions de l'arquitectura així ho indiquen.

A continuació passarem a detallar els diferents modes de seguretat de l'arquitectura Bluetooth. Ens centrarem només en els modes de seguretat 2 i 3, és a dir, el que opera a nivell de servei i el que ho fa a nivell d'enllaç, ja que el mode de seguretat 1 no té cap interès perquè no ofereix cap tipus de seguretat.

2.2.1. Mode de seguretat 2: nivell de servei

El mode de seguretat que actua a nivell de servei té una seguretat més feble que el mode de seguretat 3. Això es deu al fet que les restriccions s'apliquen un cop la comunicació entre els dispositius ja ha estat efectuada. La justificació per la utilització d'aquest nivell de seguretat, en comptes del nivell 3, recau en el fet que si es restringeixen les connexions a nivell d'enllaç no es possible dissenyar aplicacions més obertes com podrien ser l'intercanvi de targetes de negoci o la consulta dels serveis oferts per un dispositiu.

El component clau que implementa la política de seguretat és el **gestor de seguretat***.

* En anglès *security manager*.

El **gestor de seguretat** s'encarrega, entre altres tasques, de:

- Emmagatzemar informació de seguretat dels serveis.
- Emmagatzemar informació de seguretat dels dispositius.
- Acceptar o refusar les peticions d'accés generades pels protocols o les aplicacions.
- Forçar autenticació o xifratge abans de connectar amb l'aplicació.
- Demanar el PIN a l'usuari o a l'aplicació corresponent.

El PIN

Els dispositius Bluetooth disposen d'un PIN per a autenticar els usuaris. Aquest PIN té una longitud d'entre 1 i 16 bytes (normalment quatre dígits) i l'usuari pot canviar el seu valor quan vulgui.

La política de seguretat que interpreta el gestor de seguretat es basa en la informació emmagatzemada en dues bases de dades: la base de dades dels dispositius i la base de dades dels serveis.

La base de dades dels dispositius manté informació dels requisits de seguretat dels dispositius en funció de la confiança que es té sobre aquests dispositius. Així s'especifiquen dos nivells de confiança:

- **Dispositius de confiança**. Són aquells que han estat prèviament autenticats, hi ha una clau d'enllaç emmagatzemada i en la base de dades estan marcats com a dispositius de confiança.
- **Dispositius *untrusted***. Són aquells que han estat prèviament autenticats, hi ha una clau d'enllaç emmagatzemada i en la base de dades no estan marcats com a dispositius de confiança. Normalment, s'aplica aquest nivell de seguretat als dispositius amb els quals no es té una relació permanent.

La base de dades dels dispositius pot estar especificada per a qualsevol servei o es pot mantenir separada per a cada servei o per a un conjunt d'aquests.

La base de dades dels serveis especifica les necessitats de seguretat dels diferents serveis. Així, els serveis es divideixen en:

- **Serveis oberts**: en els quals no es restringeix l'accés i pels quals no es requereix cap tipus d'informació.
- **Serveis amb autenticació**: aquells en els quals els diferents dispositius cal que s'autentiquin per a poder-hi tenir accés.
- **Serveis amb autenticació i autorització**: que són els serveis més restringits que hi ha i que requereixen tant un procés d'autenticació com un procés d'autorització. És a dir, no n'hi ha prou amb el fet de dir qui ets sinó que a més a més has d'estar autoritzat.

Exemple

En molts webs simplement es requereix registrar-se per a obtenir un servei. Aquest seria el cas de servei amb autenticació. En canvi, en altres webs, com per exemple els de les entitats bancàries, a part d'identificar-te has de tenir autorització per a poder operar-hi.

La base de dades de serveis també especifica si un servei necessita que les dades que s'intercanviïn siguin xifrades o estiguin en clar.

El gestor de seguretat, situat des d'un punt de vista conceptual entre el nivell d'enllaç i en nivell d'aplicació, implementa la política de seguretat per la via de peticions i respostes dels dos nivells i sobre la base de les informacions incloses en les dues bases de dades mencionades anteriorment. A més, el gestor de seguretat s'encarregarà també de la petició i comprovació del PIN de l'usuari per a realitzar els processos d'autenticació.

2.2.2. Mode de seguretat 3: nivell d'enllaç

El mode de seguretat a nivell d'enllaç és el sistema més segur especificat en l'arquitectura Bluetooth ja que les restriccions de seguretat s'apliquen amb anterioritat a la connexió entre els dispositius i, d'aquesta manera, es pot minimitzar el risc d'atacs de dispositius ja connectats. Aquest mode de seguretat permet obtenir les propietats d'autenticació, confidencialitat i integritat.

Per tal d'obtenir aquestes propietats, l'arquitectura Bluetooth disposa de les entitats següents:

- **Adreça del dispositiu Bluetooth (BD_ADDR)**. Cada dispositiu Bluetooth té una adreça única de 48 bits. Aquesta adreça és equivalent a les adreces MAC de les targetes de xarxa.
- **Clau d'enllaç*** (K_e). Per tal de dur a terme el procés d'autenticació dels dispositius, l'arquitectura Bluetooth utilitza una clau de 128 bits.

*** En anglès, *link key*.**

- **Clau de xifratge** (K_x). La confidencialitat en la transmissió de les dades s'obté per mitjà d'una clau de xifratge, diferent de la clau d'enllaç, que pot tenir una longitud d'entre 8 i 128 bits. Aquesta clau també s'utilitza per a obtenir la propietat d'integritat.
- **Nombre aleatori (RAND)**. Els dispositius Bluetooth disposen d'un generador pseudoaleatori que els permet obtenir, quan cal, diferents valors pseudoaleatoris de 128 bits.

Basant-se en les entitats que acabem de descriure, el procés d'autenticació d'un dispositiu amb el mode de seguretat 3 es descriu en la figura 3.

El procés d'autenticació segueix el model repte-resposta. Els passos que se segueixen en l'esquema de la figura 3 són els següents:

Nomenclatura

Anomenarem el dispositiu que vol autenticar-se *provador*, mentre que el dispositiu que valida l'autenticació serà el *verificador*.

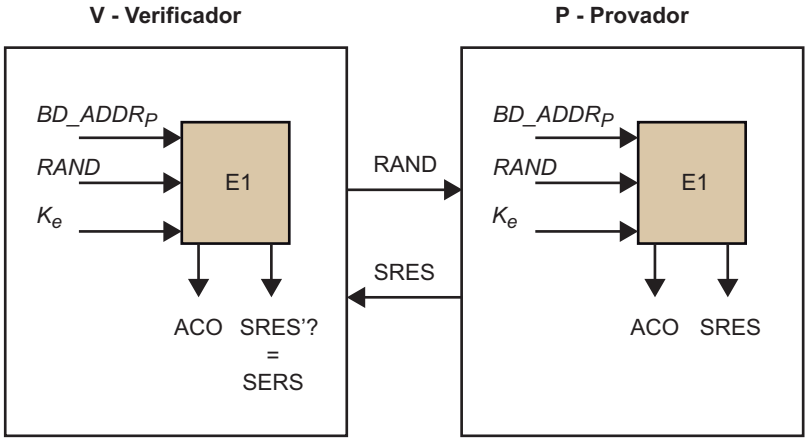
1) El verificador envia al provador un repte en forma de valor aleatori RAND. Utilitzant la funció E1 amb les entrades RAND, l'adreça de P, BD_ADDRP i la clau d'enllaç K_e, el verificador obté SRES'. A més, també obté un valor ACO* que s'utilitza posteriorment per a obtenir la clau de xifratge.

*** De l'anglès, *Authenticated Ciphering Offset*.**

2) El provador, amb el valor RAND i la resta de valors, calcula una resposta SRES, alhora que també obté el mateix valor ACO que el verificador.

3) El provador envia la resposta al verificador que comprova que SRES' = SRES i, per tant, valida la identitat del provador.

Figura 3. Procés d'autenticació

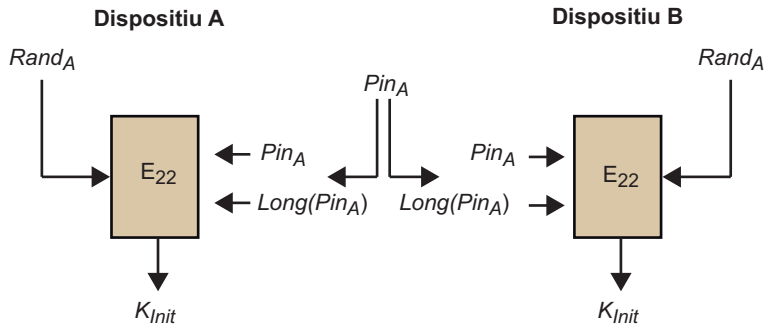


Per tal d'obtenir autenticació mútua, es repeteix el procés intercanviant el rol que representen les dues parts en el protocol anterior.

Com ja hem mencionat anteriorment, un procés d'autenticació repte-resposta com el descrit requereix que els dos interlocutors coneguin un valor amb anterioritat al procés d'autenticació, en aquest cas la clau d'enllaç, K_e. L'arquitectura Bluetooth descriu diferents tipus de clau d'enllaç que es poden utilitzar en funció de diferents supòsits. En concret es descriuen quatre tipus de claus d'enllaç:

1) Clau d'inicialització K_{Init}. Es fa servir per a obtenir posteriorment la clau d'enllaç en cas que els dos dispositius no s'hagin comunicat prèviament i, per tant, no disposin de cap valor intercanviat. Aquesta clau es genera (figura 4) a partir del PIN del dispositiu que es vol autenticar, i un valor aleatori generat pel mateix dispositiu que inicia el procés d'autenticació.

Figura 4. Generació de la clau d'inicialització



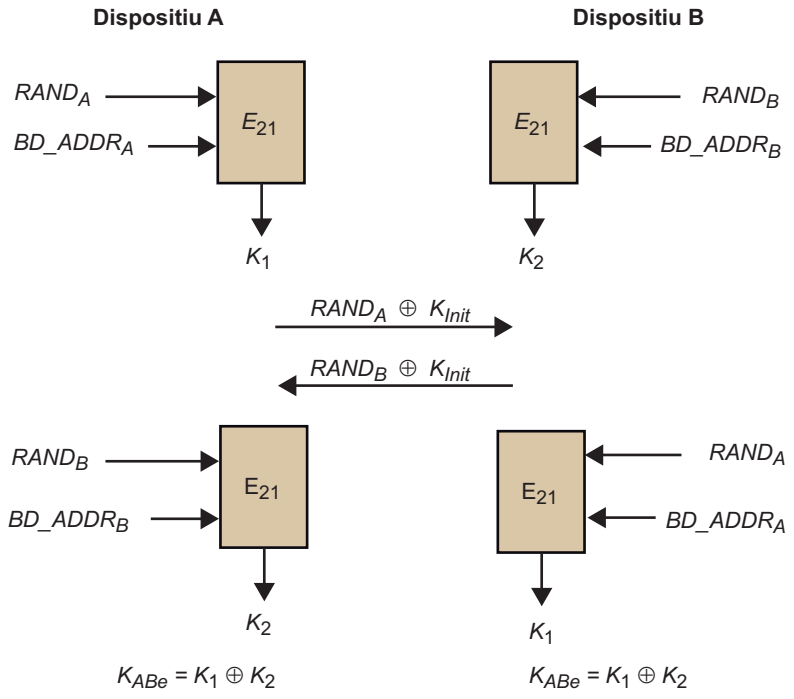
Tal com mostra el gràfic, s'utilitza l'algorisme E_2 en mode 2 (denotat per E_{22}) per a generar la clau d'inicialització a partir d'un valor aleatori, del PIN del dispositiu A (PIN_A) i de la longitud d'aquest PIN. Fixem-nos que el valor aleatori RAND l'aporta el dispositiu que es vol autenticar (i l'envia en clar a l'altre

dispositiu) i és necessari que l'usuari del dispositiu que s'autentica introdueixi també el seu PIN en l'altre dispositiu al qual es vol connectar. D'aquesta manera, al final del procés tots dos dispositius disposen d'una clau compartida K_{Init}. En principi, aquesta clau no s'utilitza com a clau d'enllaç sinó que serveix per a protegir la informació que els dos dispositius s'intercanviaran per a fixar la clau d'enllaç.

2) Clau de dispositiu K_D. La clau de dispositiu es genera amb la instal·lació del dispositiu Bluetooth a partir de l'adreça del dispositiu BD_ADDR i un valor aleatori fent servir l'algorisme E_2 en mode 1 (denotat per E_{21}). Aquesta clau no s'acostuma a canviar mai i es guarda en memòria no volàtil. A diferència de la clau d'inicialització, la clau de dispositiu sí que es pot fer servir com a clau d'enllaç. Això s'utilitza quan les restriccions de memòria d'algun dels dispositius són molt grans i no es té més espai per a emmagatzemar una altra clau d'enllaç diferent de la clau de dispositiu. En aquest cas, si el dispositiu A és el que té restriccions d'espai, A enviarà la seva clau de dispositiu K_A al dispositiu B. Perquè la transmissió de la clau no pugui ser interceptada A enviarà a B el valor $K_A \oplus K_{Init}$. Quan B obté aquest valor li tornarà a sumar K_{Init} que ja coneix i obtindrà el valor K_A.

3) Clau combinació K_{AB}. La clau combinació és una clau d'enllaç que s'obté a partir de la informació aportada pels dos dispositius, A i B, a diferència de la clau de dispositiu que quan s'utilitza com a clau d'enllaç només depèn d'un dels dispositius. Atès que es crea a partir dels dos dispositius aquest tipus de claus es generen per cada parell de dispositius i ofereixen molta més seguretat que l'ús de la clau de dispositiu com a clau d'enllaç. En la figura 5 podem veure el procés de generació de la clau combinació.

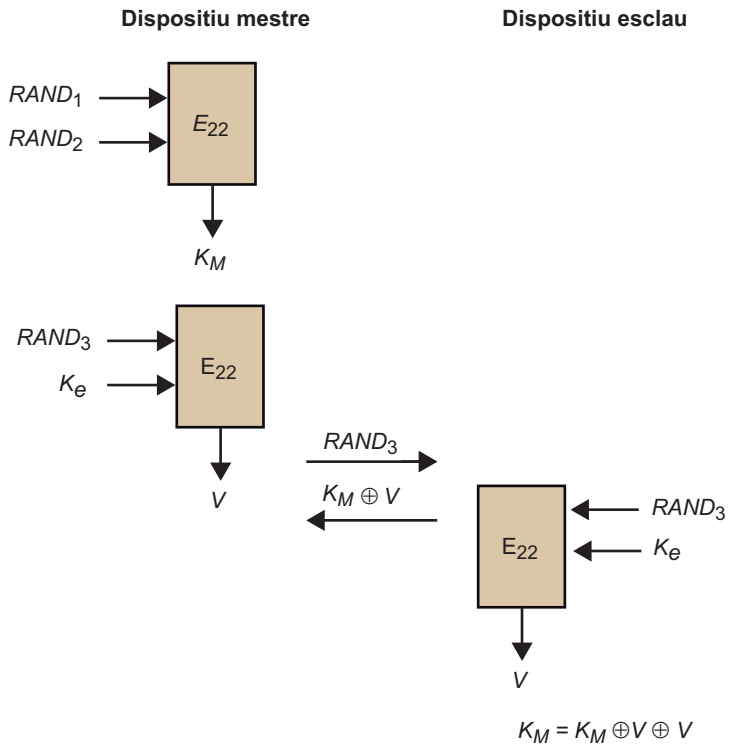
Figura 5. Generació de la clau combinació K_{AB}



A partir d'un valor aleatori, $RAND_A$ i la seva adreça BD_ADDR_A, el dispositiu A utilitza l'algorisme E_2 en mode 1 (denotat per E_{21}) per generar el valor K_1. El dispositiu B realitza el mateix procés per a obtenir K_2. Tots dos dispositius s'intercanvien els valors aleatoris $RAND_A$ i $RAND_B$ protegits per la clau d'inicialització K_{Init}. En aquest punt, cada dispositiu està en condicions de poder generar el valor K_i de l'altre dispositiu. D'aquesta manera, els dos dispositius poden establir una clau d'enllaç compartida que serà el valor $K_1 \oplus K_2$.

4) Clau mestra K_M. La clau mestra és una clau temporal que s'utilitza en una xarxa Bluetooth amb més de dos dispositius connectats quan el dispositiu mestre vol transmetre simultàniament als altres dispositius. Aquesta clau mestra substitueix cada una de les claus d'enllaç K_e que el mestre compartia amb cada un dels dispositius. El procés de generació d'aquesta clau mestra es descriu en la figura 6.

Figura 6. Generació de la clau mestra K_M



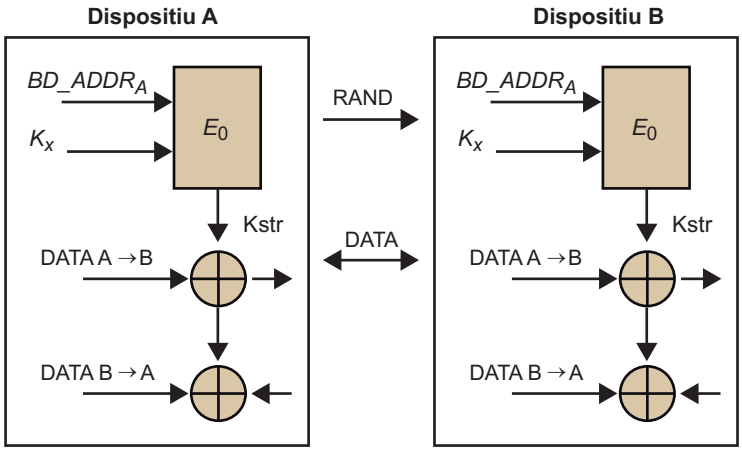
El dispositiu mestre utilitza dos valors aleatoris i l'algorisme E_2 en mode 2 (denotat per E_{22}) per a generar la clau mestra. A més, utilitza un altre valor aleatori i la clau d'enllaç per a l'obtenció d'un valor V que servirà per a protegir la transmissió de la clau mestra K_M. El dispositiu mestre envia $RAND_3$ i $K_M \oplus V$ al dispositiu esclau. Aquest, per mitjà del valor $RAND_3$ i la clau d'enllaç, que compartia amb el dispositiu mestre, pot generar el valor V que li permetrà obtenir el valor de la clau K_M.

Fins a aquest punt hem descrit el procés d'autenticació que es realitza a partir de la clau d'enllaç, que com hem vist pot ser de diferents tipus. Passem a veure com el mode de seguretat 3 de l'arquitectura Bluetooth ens ofereix la propietat de confidencialitat.

Per tal de tenir confidencialitat en la comunicació entre dos dispositius és necessari xifrar les dades. Per fer-ho, Bluetooth utilitza un criptosistema de xifratge en flux anomenat E_0.

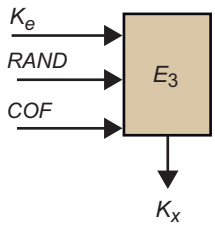
Tal com es mostra en la figura 7, a partir de l'adreça d'A, BD_ADDR_A, i la clau de xifratge, K_x, el criptosistema genera una seqüència aleatòria, denotada en la figura per Kstr, que s'utilitza per a xifrar o per a desxifrar la informació que circula entre els dos dispositius. D'aquesta manera per les dades que s'envien xifrades s'obté la propietat de confidencialitat.

Figura 7. Generació de la clau de xifratge K_x



Com veiem, la clau de xifratge és l'únic element secret que els dos dispositius comparteixen. Aquest valor es genera a partir d'un valor aleatori, la clau d'enllaç, i un tercer valor anomenat *Ciphering OFfset number* (COF). Tal com es mostra en la figura 8.

Figura 8. Generació del COF



El valor COF és, en general, el valor ACO intercanviat durant el procés d'autenticació. La longitud de la clau de xifratge obtinguda varia d'entre 8 i 128 bits i en cada cas es fixa per mitjà d'una negociació entre els dos dispositius. En cada dispositiu hi ha un paràmetre que defineix el màxim de longitud de clau permès. També cada aplicació té un mínim acceptable de longitud de clau.

3. ZigBee

En aquest apartat descriurem algunes de les funcionalitats que ofereix l'estàndard ZigBee. En primer lloc, exposarem les característiques principals de les xarxes ZigBee i la seva arquitectura. Seguidament, farem un repàs als dispositius que l'especificació de ZigBee reconeix i a les possibles configuracions que permeten agrupar-los.

Després de la descripció de l'especificació de ZigBee, ens centrarem en els aspectes de seguretat que preveu: analitzarem els diferents modes de seguretat, estudiarem les diferents claus que utilitzen els dispositius ZigBee i la seva funció, i detallarem els diferents serveis de seguretat que ZigBee especifica per cada una de les capes.

L'origen del nom ZigBee

Es diu que el nom de ZigBee ve d'un paral·lelisme amb la manera en què es comuniquen les abelles, realitzant una mena de dansa per a comunicar informació important a altres membres del rusc. Aquesta dansa és la que els dissenyadors de ZigBee intenten emular amb aquest protocol, permetent a un conjunt de dispositius senzills comunicar-se i treballar plegats per a aconseguir fer tasques complexes.

3.1. Descripció de l'especificació ZigBee

ZigBee és el nom amb el qual es coneix l'especificació d'un conjunt de protocols per a xarxes WPAN basades en l'estàndard IEEE 802. ZigBee està dissenyat per a ser utilitzat en dispositius de radiofreqüència de curt abast que disposen de baixa potència i que requereixen una taxa de transmissió de dades baixa. ZigBee es diferencia així d'altres protocols per WPAN, com ara Bluetooth, que permeten assolir taxes de transmissió de dades molt més elevades però que tenen un consum energètic també molt més elevat.

Les característiques principals de ZigBee són:

- **Baix consum**. Els dispositius ZigBee poden estar funcionant durant anys amb un mateix parell de bateries AA. Això és possible perquè els dispositius d'una xarxa ZigBee no cal que estiguin constantment enviant missatges (poden estar adormits).

- **Estàndard obert**. L'especificació de ZigBee és un estàndard obert, la qual cosa permet, d'una banda, assegurar la interoperabilitat de dispositius i, d'altra banda, l'accés lliure a l'especificació. Tot i així, la llicència de ZigBee permet utilitzar l'estàndard lliurement només per a aplicacions no comercials, la qual cosa suposa conflictes amb certes llicències com ara la GPL.

- **Seguretat**. ZigBee permet afegir seguretat a les comunicacions mitjançant una sèrie de serveis que permeten la gestió de claus criptogràfiques, el xifratge dels missatges transmesos i l'autenticació dels dispositius, entre d'altres característiques que veurem al llarg d'aquest apartat.

- **Baix cost d'implementació**. Mantenint l'especificació senzilla, ZigBee intenta minimitzar el cost de crear noves aplicacions que en facin ús.

- **Baixa velocitat de transmissió**. Per tal de poder oferir dispositius de baix consum i de baix cost, ZigBee no permet assolir velocitats de transmissió de dades elevades, i limita el seu ús a aplicacions poc exigents en aquest àmbit.

ZigBee opera a les bandes de freqüència de 868 MHz (a Europa), 915 MHz (a Amèrica) i 2,4 GHz (en l'àmbit global). La taxa de transmissió de dades màxima que pot assolir és de 250 kb/s quan opera a 2,4 GHz (16 canals), 40 kb/s a 915 MHz (10 canals) i 20 kb/s a 868 MHz (1 canal). La distància màxima a la qual dos dispositius ZigBee poden comunicar-se és molt variable i depèn de la potència de sortida i de les condicions ambientals, podent variar des de 10 fins a 1.600 metres.

L'especificació de ZigBee està desenvolupada per la ZigBee Alliance, una associació d'empreses, universitats i governs, fundada el 2002 amb l'objectiu de desenvolupar tant estàndards com productes per a xarxes sense fils de baix consum. La ZigBee Alliance s'encarrega tant de mantenir i actualitzar l'especificació de ZigBee com de promocionar i fomentar-ne l'ús.

Atès que ZigBee és una especificació de protocols d'alt nivell, es pot fer servir en multitud d'escenaris diferents. Així, per exemple, podem trobar dispositius ZigBee utilitzats en domòtica i automatització, en aplicacions comercials, en dispositius de *fitness* o en electrònica de consum, per posar alguns exemples.

Evolució de l'especificació ZigBee

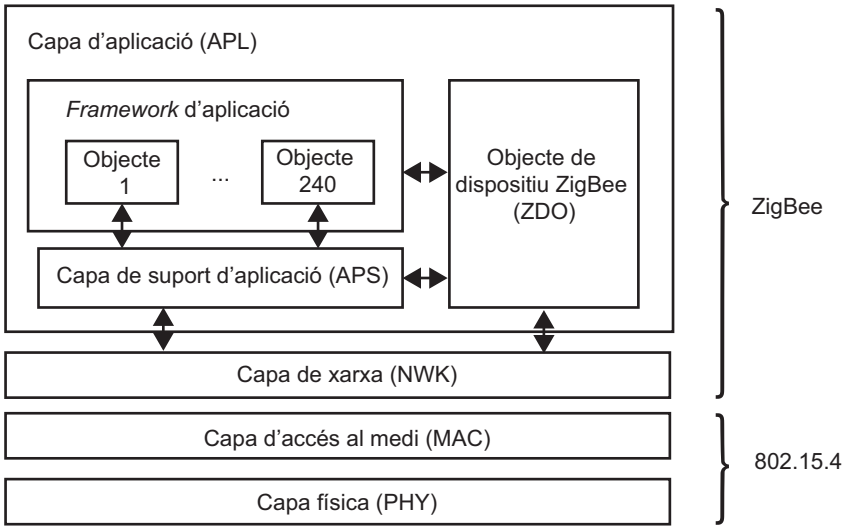
L'especificació de ZigBee ha anat canviant amb el temps, implementant millores a cada nova versió. La primera versió de l'especificació de ZigBee va ser aprovada el desembre de 2004. Aquesta primera versió es coneix com a ZigBee v1.0 o bé com a ZigBee 2004 i actualment es considera obsoleta. Dos anys després, el desembre de 2006, una nova versió va ser publicada (ZigBee 2006). L'octubre de 2007, una altra revisió va ser anunciada. Aquesta última especificació conté dos perfils de pila diferents ZigBee 2007 i Pro, que presenten algunes diferències en relació amb les característiques disponibles i, conseqüentment, en la memòria necessària per a executar-les.

3.1.1. Arquitectura

ZigBee adopta l'especificació de la capa física i de la subcapa de control d'accés al medi (MAC) de l'estàndard IEEE 802.15.4. D'aquesta manera, ZigBee proporciona una especificació per a la capa de xarxa (NWK) i proveeix d'un *framework* per a la capa d'aplicació (APL), i delega a l'estàndard IEEE 802.15.4 tota l'especificació de baix nivell.

Com es pot apreciar a la figura 9, a nivell d'aplicació (APL) ZigBee ofereix, una subcapa de suport a les aplicacions (APS), uns objectes de dispositiu ZigBee (ZDO) i un *framework* d'aplicació.

Figura 9. Model de capes ZigBee



La subcapa APS és una interfície entre la capa de xarxa (NWK) i la capa d'aplicació (APL) que ofereix tot de serveis disponibles tant per a les aplicacions com per al ZDO. Aquests serveis inclouen, entre d'altres, sistemes d'aparellament de dispositius, fragmentació de missatges, generació de PDU d'aplicació i serveis de seguretat.

Vegeu també

Els serveis de seguretat els veurem amb més detall al subapartat 3.2.3.

Els objectes ZDO proveeixen d'una interfície entre els objectes d'aplicació, el perfil del dispositiu i la subcapa APS. El ZDO és l'encarregat d'inicialitzar la subcapa d'aplicació (APS) i la capa de xarxa (NWK). A més, també ofereix serveis de gestió de la xarxa com ara el descobriment d'altres dispositius o el descobriment de serveis.

PDU

PDU, o *Protocol Data Unit*, és el nom que rep el conjunt de la informació de control del protocol i de les dades d'usuari en una capa concreta.

El *framework* d'aplicació pot contenir fins a 240 objectes d'aplicació, és a dir, de mòduls definits per l'usuari que formen part de l'aplicació ZigBee.

3.1.2. Tipus de dispositius i topologies

Com hem vist, ZigBee adopta l'especificació de l'IEEE 802.15.4 per a la capa de control d'accés al medi. Aquesta especificació defineix dos tipus de dispositius:

- **Dispositius amb funcionalitat completa**. Poden realitzar qualsevol paper dins de la xarxa, és a dir, poden funcionar com a coordinadors, encaminadors o dispositius finals. A més, poden comunicar-se amb qualsevol altre dispositiu de la xarxa.

- **Dispositius amb funcionalitat reduïda**. Només poden actuar com a dispositius finals i només poden interaccionar amb un únic dispositiu FFD.

FFD i RFD

En anglès, anomenem *Full-function devices* o *FFD* els dispositius de funcionalitat completa i *Reduced-function devices* o *RFD* els dispositius de funcionalitat reduïda.

ZigBee identifica, a nivell de xarxa, tres tipus de dispositius diferents:

- **Dispositiu final**. És el dispositiu més senzill, normalment connectat a sensors, que correspon o bé a un RFD o bé a un FFD actuant com a dispositiu simple.
- **Encaminador**. És un FFD amb capacitats d'encaminament de xarxa.
- **Coordinador ZigBee**. És un FFD que coordina tota la xarxa.

ZE, ZR i ZC

En anglès, anomenem *ZigBee End Device* o *ZE* el dispositiu final, *ZigBee Router* o *ZR* el dispositiu encaminador i *ZigBee Coordinator* o *ZC* el dispositiu coordinador.

Tenint en compte els papers de cada dispositiu a la xarxa i les seves interconnexions, ZigBee permet estructurar els nodes desplegats en tres topologies diferents:

- **Estrella**. És la topologia més senzilla, formada per un únic dispositiu coordinador connectat a múltiples dispositius finals. Amb aquesta topologia, els dispositius finals no poden comunicar-se directament. El coordinador és el responsable de gestionar totes les comunicacions, i també d'inicialitzar i mantenir tots els dispositius de la xarxa.

- **Arbre**. És una topologia jeràrquica on cada dispositiu té un únic pare (excepte el node arrel, que no en té cap). El node arrel és el dispositiu coordinador, que s'encarrega de la inicialització de la xarxa. La xarxa es pot estendre amb l'addició de dispositius encaminadors, que s'encarreguen de transportar les dades i els missatges de control fent servir una estratègia jeràrquica.

- **Malla**. És una topologia no jeràrquica, on cada dispositiu pot intentar comunicar-se amb qualsevol altre dispositiu de la xarxa, o directament o per mitjà d'algun dispositiu encaminador. Les rutes entre nodes es creen sota demanda i poden ser modificades dinàmicament, la qual cosa permet a aquesta topologia adaptar-se als canvis de la xarxa.

3.2. Seguretat en dispositius ZigBee

La seguretat de ZigBee es basa en un model de confiança oberta on les diferents aplicacions que corren en un mateix dispositiu, així com les diferents capes de la pila de comunicacions, confien les unes en les altres. Aquest model de confiança permet que tant les diferents aplicacions com les diferents capes comparteixin les claus, la qual cosa suposa un estalvi de recursos, normalment escassos en xarxes de sensors. L'ús d'aquest model implica que només existeix protecció a nivell criptogràfic entre diferents dispositius de la xarxa.

Altres decisions de disseny de l'arquitectura de ZigBee també afecten la seguretat, com ara el principi que cada capa és responsable de la seguretat dels missatges que s'originen en aquella capa.

L'especificació de ZigBee proveeix d'eines per a garantir l'autenticació, la confidencialitat i la integritat de les dades transmeses. A més, també ofereix eines per a garantir la frescor*, és a dir, per a assegurar que un atacant no podrà reutilitzar paquets capturats durant una comunicació vàlida.

* En anglès, *freshness*.

L'especificació de ZigBee defineix l'existència d'un dispositiu especial a cada xarxa anomenat Centre de Confiança**, que gaudeix de la confiança de tots els dispositius d'aquella xarxa.

** En anglès, *Trust Center*.

El Centre de Confiança pot ser utilitzat per a la distribució de claus i pot operar en dos modes diferents:

- **Mode d'alta seguretat**. Aquest mode està dissenyat per a aplicacions comercials que necessitin un alt nivell de seguretat. Quan el Centre de Confiança es troba configurat en aquest mode, ha de mantenir una llista amb tots els dispositius i totes les claus necessàries per a assegurar que es compleixen les polítiques de renovació de claus i d'admissió a la xarxa. A més, quan s'està operant en aquest mode, es verifica la frescor de totes les trames entrants, i s'assegura així que no són trames duplicades.

- **Mode de seguretat estàndard**. Aquest mode està dissenyat per a aplicacions residencials que necessitin un nivell de seguretat baix. Quan el Centre de Confiança es troba configurat en aquest mode, no és necessari que mantingui totes les claus (només la clau de xarxa, que descriurem més endavant) tot i que sí que cal que controli les polítiques d'admissió de la xarxa. D'aquesta manera, s'aconsegueix que la memòria necessària per a operar el Centre de Confiança no creixi amb el nombre de dispositius de la xarxa, com passava en el mode d'alta seguretat.

3.2.1. Claus

ZigBee utilitza claus simètriques per tal d'establir comunicacions segures. La seguretat de les comunicacions depèn de la correcta inicialització i instal·lació d'aquestes claus. L'arquitectura de seguretat fa ús de tres claus diferents per a oferir seguretat:

- **Clau d'enllaç**. És una clau de 128 bits compartida únicament entre 2 dispositius que s'utilitza per a assegurar la comunicació *unicast* entre dues entitats APL. Un dispositiu pot adquirir una clau d'enllaç utilitzant els serveis de la subcapa APS de transport de clau o d'establiment de clau, o bé mitjançant la preinstal·lació de la clau (per exemple, a la fàbrica). La clau d'enllaç és també utilitzada per a generar claus derivades per a diferents

serveis de la xarxa fent servir funcions d'un sol sentit. D'aquesta manera, s'aconsegueix fer servir claus independents per a executar diferents protocols de seguretat, i s'eviten interaccions no desitjades.

- **Clau mestra**. La clau mestra es fa servir en el protocol d'establiment de claus simètriques (per exemple, per a generar claus d'enllaç). Un dispositiu pot adquirir la clau mestra per mitjà del servei de transport de clau, mitjançat preinstal·lació o bé a partir d'alguna informació que proporciona l'usuari (com ara per exemple, una contrasenya).

- **Clau de xarxa**. És una clau de 128 bits compartida entre tots els dispositius de la xarxa que s'utilitza tant per a enviar missatges de *broadcast* des de la subcapa d'aplicació (APS) com per a enviar missatges des de la capa de xarxa (NWK). Un dispositiu ha d'adquirir una clau de xarxa o bé mitjançant el servei de transport de la clau o bé mitjançant preinstal·lació.

Els diferents mètodes que permeten obtenir cadascuna de les claus són serveis oferts per la capa d'aplicació de ZigBee i, per tant, es troben descrits al subapartat 3.2.3.

La clau d'enllaç i la clau mestra només són accessibles des de la subcapa APS, mentre que la clau de xarxa es troba disponible tant des de la capa APL com des de la capa NTW.

3.2.2. Seguretat a la capa de xarxa

Els missatges ZigBee es protegeixen criptogràficament a la capa de xarxa quan s'originen en aquesta capa (segons el principi que cada capa és responsable de la seguretat dels missatges que s'originen a aquesta capa) o bé quan s'originen en una capa superior i s'especifica explícitament que s'han de protegir a nivell de xarxa.

La taula 2 mostra els camps que conté una trama ZigBee de la capa de xarxa. Com es pot apreciar, a part de les capçaleres pròpies de cada capa, la capa de xarxa afegeix una capçalera auxiliar i un camp d'integritat, que permeten incloure la informació necessària per a gestionar la seguretat del contingut.

Taula 2. Trama de xarxa

SYNC	PHY HDR	MAC HDR	NWK HDR	Auxiliary	ENC NWK Payload	MIC

La capçalera auxiliar conté:

- **Camp de control de seguretat**:

– Nivell de seguretat. Indica els paràmetres de seguretat que s'han fet servir en aquella trama. La taula 3 mostra tots els nivells de seguretat oferts i també les característiques de cadascun d'ells.

Taula 3. Nivells de seguretat disponibles a les capes de xarxa i aplicació

Identificador nivell	Seguretat	Xifratge	Integritat
0	Cap	No	No
1	MIC-32	No	Sí
2	MIC-64	No	Sí
3	MIC-128	No	Sí
4	ENC	Sí	No
5	ENC-MIC-32	Sí	Sí
6	ENC-MIC-64	Sí	Sí
7	ENC-MIC-128	Sí	Sí

Taula 3

Noteu que els nivells 0 i 4 no asseguren de cap manera la integritat dels missatges enviats i que els nivells de 0 a 3 no proporcionen confidencialitat.

– Identificador de la clau. Conté dos bits que identifiquen quin tipus de clau s'ha fet servir.

– *Nonce* estesa. Un bit que indica si s'inclou el camp d'adreça d'origen o si s'omet.

- **Comptador de trames**. Permet, d'una banda, assegurar la frescor de la trama i, d'altra banda, evitar que es processin trames per duplicat.

- **Adreça d'origen**. Si s'ha especificat anteriorment que s'inclouria l'adreça d'origen (al camp *extended nonce*), aleshores conté l'adreça del dispositiu responsable d'afegir seguretat a la trama.

- **Número de seqüència de la clau**. Si s'ha especificat una clau de xarxa (al camp identificador de la clau), conté el número de seqüència de la clau de xarxa.

L'especificació de ZigBee exigeix l'ús de l'AES (*Advanced Encryption Standard*) com a algorisme de xifratge. Atès que l'AES és un algorisme de xifratge en bloc, l'especificació també fixa com s'ha d'utilitzar l'AES per a protegir els missatges, és a dir el mode d'operació. ZigBee utilitza AES en mode CCM* (*Counter with Cipher Block Chaining Message Authentication Code*), un mode que combina tant xifratge com autenticació, de manera que tant el missatge xifrat com el valor del camp d'integritat són el resultat d'aplicar AES-CCM* sobre la càrrega de la trama de xarxa. El mode CCM* també permet operar en mode només xifratge (sense autenticació) o en mode només autenticació (sense xifratge).

AES

El NIST va aprovar l'algorisme de xifratge Rijndael com a AES el 26 de maig de 2002. El Rijndael va ser creat per dos criptòlegs, Joan Daemen i Vincent Rijmen.

El mode CCM*

El mode CCM* coincideix amb l'especificació de CCM per missatges que requereixen autenticació i possiblement xifratge. CCM* afegeix l'alternativa de permetre només xifrar, sense garantir l'autenticitat del missatge.

Si el nivell de seguretat exigeix xifratge, la càrrega de la trama es xifra amb AES en CCM*. D'aquesta manera, si un atacant observa el trànsit entre dispositius, no serà capaç de llegir-ne el contingut, i es garantirà la confidencialitat de la informació transmesa.

Si el nivell de seguretat exigeix integritat, el camp MIC* conté una etiqueta calculada a partir de la càrrega de la trama i de la clau, d'una manera coneguda tant per l'emissor com pel receptor. Quan el receptor rep la trama, calcularà també el valor MIC a partir del contingut rebut i de la clau que comparteix

*** De l'anglès, *Message Integrity Code.***

amb l'emissor. Si durant el transport del missatge el contingut de la trama ha estat alterat, aleshores el MIC calculat pel receptor serà diferent del MIC contingut a la trama, i pot així detectar que hi ha hagut una modificació del missatge. Atès que és necessari conèixer la clau per a calcular el MIC, l'atacant que modifiqui el missatge no podrà modificar tampoc el MIC adequadament, ja que desconeix la clau feta servir. El nivell de seguretat marca la longitud del camp de MIC (0, 32, 64 o 128 bits), que determina la probabilitat que un valor triat a l'atzar coincideixi amb el valor correcte de MIC.

MIC

El MIC també es coneix amb el nom de MAC (*Message Authentication Code*). En l'especificació de ZigBee, s'utilitza MIC en comptes de MAC per a evitar la confusió que podria provocar en interpretar MAC com a *Medium Access Control*, una subcapa de la capa d'enllaç especificada pel model OSI.

A part de les dades i de la clau, el mode CCM* requereix l'ús d'un valor de *nonce* per a operar. Donada una mateixa clau, el valor de *nonce* serà únic per cada missatge que s'enviï. El valor de *nonce* que es fa servir a CCM* es construeix concatenant els valors dels camp de control de seguretat, el comptador de trama i l'adreça d'origen. Noteu que el valor del *nonce* canvia per cada nou missatge mentre es fa servir una mateixa clau ja que el comptador de trames es va incrementant. D'aquesta manera, si un atacant captura un paquet i l'intenta tornar a utilitzar passat un temps, el receptor serà capaç de detectar-ho, i així garantirà la frescor dels missatges. Si l'atacant no modifica el comptador de la trama, aleshores el receptor detectarà que és una trama antiga. Si per contra, l'atacant modifica el comptador de la trama, aleshores la verificació del MIC no serà correcta, i detectarà també l'atac. L'ús d'un *nonce* també assegura que missatges amb exactament el mateix contingut en clar siguin xifrats com a textos diferents.

***Nonce* deriva de l'expressió en anglès *Number used ONCE*.**

Comptador de trama

ZigBee utilitza comptadors de 32 bits: dos dispositius intercanviant 1 missatge cada segon no generaran un comptador de trama duplicat fins al cap de més de 136 anys d'interacció.

3.2.3. Seguretat a la capa d'aplicació

La subcapa APS s'encarrega de la seguretat dels missatges originats a la capa d'aplicació, fent servir o bé la clau d'enllaç (per a missatges *unicast*) o bé la clau de xarxa (per a missatges *broadcast*).

La taula 4 mostra els camps que conté una trama ZigBee de la capa d'aplicació. Com es pot apreciar, a part de les capçaleres pròpies de cada capa, la capa d'aplicació afegeix una capçalera auxiliar i un camp d'integritat, que permeten incloure la informació necessària per a gestionar la seguretat del contigut. La creació de la capçalera auxiliar, del camp d'integritat, i de la càrrega xifrada (si s'escau), segueixen el mateix format que l'especificat per a la capa de xarxa al subapartat 3.2.2. En aquest cas, però, el valor del camp de *nonce* estesa sempre serà 0. La capa d'aplicació també fa ús de l'AES en mode CCM* per a xifrar i oferir integritat i autenticitat als missatges.

Taula 4. Trama de la capa d'aplicació

SYNC	PHY HDR	MAC HDR	NWK HDR	APS HDR	Aux HDR	ENC APS Payload	MIC

La subcapa APS de la capa d'aplicació també és la responsable d'oferir serveis de seguretat a les aplicacions i el ZDO. En els subapartats següents, veurem

quins serveis de seguretat ofereix la subcapa APS i com funcionen aquests serveis.

Gestió de claus

La subcapa APS ofereix quatre serveis bàsics de gestió de claus: l'establiment de clau, el transport de clau, la petició d'una clau i el canvi de clau.

El servei d'**establiment de clau** permet que dos dispositius ZigBee puguin derivar una clau secreta compartida (una clau d'enllaç) a partir d'una informació secreta compartida prèviament (la clau mestra). El protocol d'establiment de claus es duu a terme entre dos dispositius, un que inicia el protocol i un altre que respon a la petició d'establiment de claus. Prèviament, els dos dispositius han de compartir algun secret, que pot ser obtingut per mitjà del Centre de Confiança. Així doncs, per tal d'establir una clau se segueixen els passos següents:

1) Establir una relació de confiança.

2) Intercanviar dades efímeres.

3) Utilitzar les dades efímeres per a derivar una clau d'enllaç.

4) Confirmar que les claus s'han calculat correctament.

Una altra alternativa per a obtenir una clau és l'enviament d'aquesta clau per mitjà d'un canal, preferiblement segur. El servei de **transport de clau** de l'APS permet que un dispositiu enviï una clau a altres dispositius. El servei pot operar de manera segura, protegint criptogràficament les claus enviades, o bé de manera no segura, sense oferir cap mena de protecció sobre el contingut enviat. En aquest últim cas, s'entén que la seguretat del transport de la clau es garantirà per algun altre mitjà (no criptogràfic).

Quan el transport de clau es fa en mode segur, aleshores s'utilitzen claus específiques per a xifrar els missatges que transporten les claus. Si la clau que es transporta és una clau mestra, es fa servir la clau de càrrega de clau (*key-load key*), mentre que per a qualsevol altra clau, es fa servir la clau de transport de clau (*key-transport key*). Tant la clau de càrrega com la de transport de claus són claus derivades de la clau d'enllaç fent servir HMAC (*Hash-based Message Authentication Code*, vegeu la figura 10) amb la funció de *hash* Matyas-Meyer-Oseas.

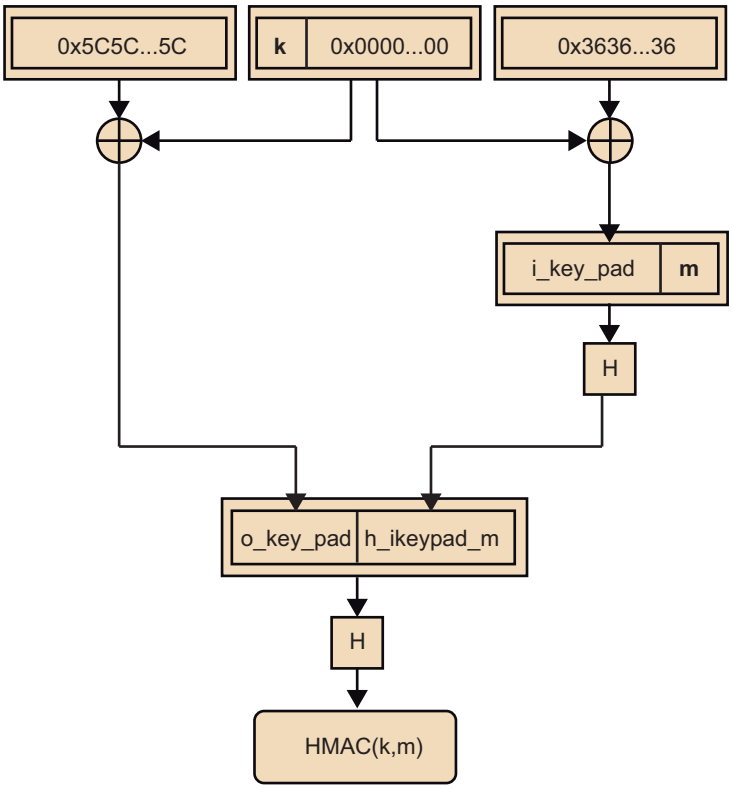
Clau de transport i clau de càrrega

La clau de transport de claus s'obté fent servir com a entrada el valor 0x00 i com a clau la clau d'enllaç. En canvi, la clau de càrrega de clau fa servir com a entrada el valor 0x02 (i utilitza també la clau d'enllaç com a clau).

Figura 10

Donada una funció de *hash* criptogràfica H, una clau k i un missatge m, l'esquema de la figura mostra com calcular-ne el codi d'autenticació HMAC. Com es pot apreciar, HMAC fa servir dues cadenes constants (0x5C ... 5C i 0x36 ... 36) juntament amb l'aplicació d'una funció *hash* intermèdia per a emmascarar els valors d'entrada de la funció *hash* que retorna el valor HMAC.

Figura 10. Esquema HMAC



La subcapa APS també proporciona als dispositius de serveis per a sol·licitar una clau o bé per a informar un altre dispositiu que hauria de canviar de clau. El servei de **sol·licitud de clau** permet a un dispositiu demanar una clau (o bé la clau de xarxa activa o bé una clau mestra) a un altre dispositiu de manera segura. El servei de **canvi de clau** permet a un dispositiu informar un altre dispositiu que hauria de canviar a una clau de xarxa activa diferent de manera segura.

Modificació de la xarxa

La capa APL també disposa de serveis per a eliminar un dispositiu de la xarxa de manera segura i per a informar d'aquests canvis, i també de qualsevol altre canvi d'estat, a altres dispositius de la xarxa.

El servei per a eliminar un dispositiu permet a un dispositiu com el Centre de Confiança informar un altre dispositiu, per exemple, l'encaminador, que un dels seus fills hauria de ser eliminat de la xarxa. Aquest servei pot ser útil, per exemple, si es vol eliminar de la xarxa un dispositiu que no compleix els requisits de seguretat que el Centre de Confiança estableix.

El servei d'actualització permet a un dispositiu informar un segon dispositiu que un tercer dispositiu ha tingut un canvi d'estat. D'aquesta manera, el Centre de Confiança pot mantenir una llista actualitzada dels dispositius actius a la xarxa.

Autenticació

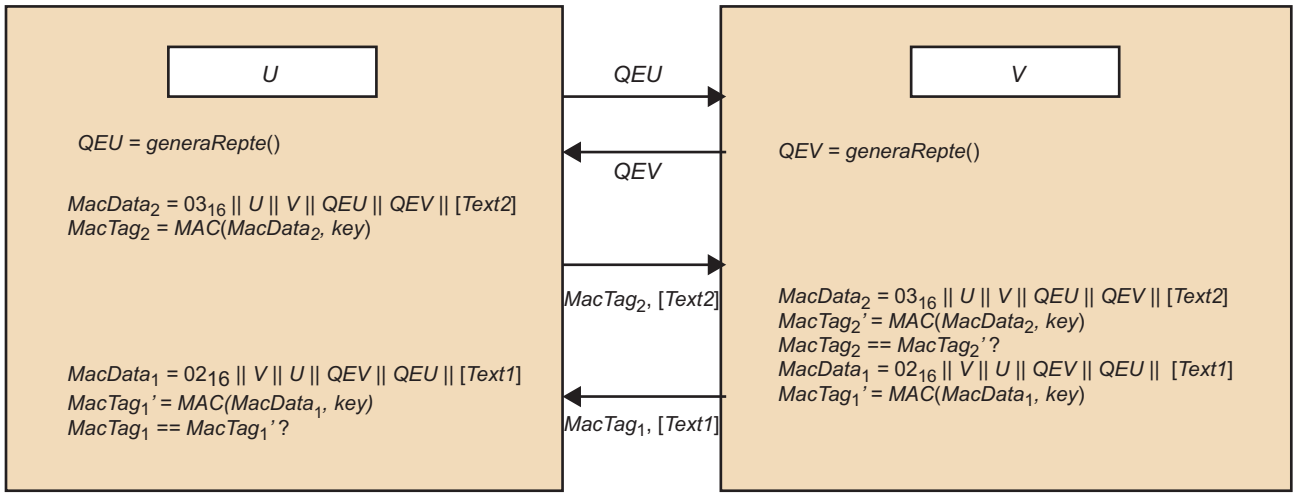
La subcapa de suport d'aplicació també ofereix el servei d'autenticació d'entitats, la qual cosa permet als dispositius sincronitzar informació alhora que assegurar l'autenticitat dels dispositius implicats. Opcionalment, també permet autenticar no només els dispositius sinó també les dades que s'estan transmetent. L'autenticació es duu a terme a partir d'un secret compartit prèviament, en aquest cas, una clau compartida entre els dispositius.

La figura 11 descriu el funcionament del protocol d'autenticació mútua d'entitats. Una vegada finalitzat el protocol, els dos dispositius saben que s'estan comunicant amb el dispositiu amb el qual compartien prèviament la clau utilitzada durant el protocol. El protocol assegura que una escolta passiva no permet a un atacant descobrir la clau que comparteixen els dispositius.

Figura 11

L'esquema s'inicia amb un intercanvi de reptes: el dispositiu que inicia el protocol, *U*, envia un repte al dispositiu *V* i *V* respon amb un altre repte. El dispositiu iniciador calcula aleshores el valor MacTag2 aplicant una funció MAC a una cadena que conté un valor fix 03_{16}, els dos reptes intercanviats, els identificadors dels dispositius i, opcionalment, un text a transmetre. Per a calcular aquesta MAC, *U* fa servir la clau *key* que els dos dispositius, *U* i *V* compartien prèviament. *U* envia el valor calculat a *V*. Per tal de comprovar que s'està comunicant amb el dispositiu amb el qual compartia la clau, *V* calcularà també el mateix valor MacTag2 i el compararà amb el valor rebut. Si són iguals, aleshores *V* sap que efectivament s'està comunicant amb *U*, dispositiu amb el qual comparteix la clau *key*. El protocol segueix ara en sentit contrari, i permet a *U* comprovar l'autenticitat de *V*.

Figura 11. Protocol d'Autenticació Mútua



4. Comparativa i discussió de la seguretat

Com hem vist, la tecnologia RFID es fa servir en dispositius molt diversos, des d'etiquetes passives que no disposen de cap tipus de bateria per a operar de manera autònoma i amb uns recursos de còmput molt limitats, fins a dispositius actius, que disposen de bateria i d'una capacitat de còmput molt més elevada. Tota aquesta gamma de dispositius RFID respon a diferents exigències del mercat, on el cost de cada etiqueta n'és un factor clau. L'àrea de l'etiqueta, mesurada en portes lògiques equivalents, determinarà les capacitats de còmput del dispositiu i, per tant, en limitarà els mecanismes de seguretat que s'hi puguin desplegar. Així doncs, el nivell de seguretat que es pugui aconseguir depèn en gran mesura del dispositiu RFID concret que s'estigui utilitzant.

Com hem vist, s'està treballant a desenvolupar protocols i primitives criptogràfiques que requereixin pocs recursos de càlcul per a ser implementats. D'aquesta manera es pot dotar fins i tot els dispositius més senzills d'algun nivell de seguretat. Tot i així, les necessitats de recursos de certs mecanismes, com ara la criptografia de clau pública, encara estan molt lluny dels que es troben disponibles en la majoria de dispositius RFID.

Els dispositius Bluetooth no es troben tan limitats pels recursos disponibles. A diferència de l'RFID, Bluetooth té una especificació de seguretat que en descriu els seus modes d'ús i els mecanismes de seguretat que s'han d'utilitzar amb cada configuració. Tot i això, hi ha punts del disseny de la seguretat que fan disminuir-ne la robustesa.

Des del punt de vista del xifratge, el criptosistema de flux E_0 no és suficientment robust ja que s'ha provat que es pot trencar sota certes circumstàncies.

La problemàtica més important, però, prové dels mecanismes d'autenticació. Com hem vist, la clau d'enllaç és molt important i se'n descriuen diferents tipus. En el cas de no existir una connexió prèvia entre els dispositius, la clau d'enllaç s'obté per mitjà de la clau d'inicialització. Aquesta clau es genera, bàsicament, a partir del PIN, ja que el valor aleatori és transmès en clar d'un dispositiu a l'altre. Tenint en compte que els PIN estan formats per 4 dígits, el nombre de possibilitats és força baix. D'altra banda, un cas pitjor es produeix quan s'utilitza la clau de dispositiu com a clau d'enllaç. Ja hem comentat que la clau de dispositiu es genera en inicialitzar-lo i rarament es canvia. Aquest fet fa que una vegada un dispositiu A ha utilitzat la seva clau de dispositiu com a clau d'enllaç per a autenticar-se davant de B, el següent procés d'autenticació d'A davant un tercer dispositiu amb la seva clau de dispositiu com a clau d'enllaç no pot ser fiable, ja que el dispositiu B podria fer-se passar per A (atès que coneix la seva clau de dispositiu).

Finalment, cal fer notar que els esquemes de seguretat que incorpora l'arquitectura Bluetooth autentiquen dispositius però no usuaris. Aquest fet, juntament amb la poca longitud del PIN, fa que no sigui adequat en certes aplicacions.

De la mateixa manera que amb Bluetooth, ZigBee és una especificació d'un conjunt de protocols de comunicacions. L'especificació de seguretat de ZigBee també preveu l'ús de diferents modes de seguretat que permeten ajustar les necessitats de seguretat depenent de l'aplicació. Com hem vist, la seguretat de ZigBee es basa en l'ús de dues claus de 128 bits: la clau d'enllaç i la clau de xarxa. La clau de xarxa, compartida entre tots els dispositius d'una mateixa xarxa, és un dels punts pels quals es pot atacar fàcilment una xarxa ZigBee. Un atacant pot obtenir-la, per exemple, interceptant-ne la seva transmissió pel canal fora de banda o aconseguint accedir a un dels dispositius de la xarxa i extraient-ne la informació. Coneixent aquesta clau, un atacant pot desxifrar totes les comunicacions *broadcast* de la xarxa.

ZigBee també proposa l'ús d'un Centre de Confiança en el qual confien tots els nodes de la xarxa. El Centre de Confiança és responsable del control d'admissió dels nodes i de la distribució de claus. Mentre que disposar d'un Centre de Confiança permet mantenir un control centralitzat sobre la seguretat de la xarxa, també suposa un punt únic de fallada que un atacant pot aprofitar.

Més enllà dels mecanismes de seguretat que implementen, ZigBee i Bluetooth presenten algunes similituds, però també força diferències. Mentre que una xarxa ZigBee pot tenir fins a 65.535 nodes (en subxarxes de 255), una *piconet* Bluetooth només en pot tenir 8. El consum dels dispositius també és un punt diferenciador: mentre que els dispositius ZigBee consumeixen menys d'1 mW, els dispositius Bluetooth poden consumir fins a 100 mW. En relació amb la velocitat de transmissió, Bluetooth ofereix fins a 3 Mb/s (velocitat nominal a la versió 2.2), mentre que amb ZigBee només s'arriba als 250 kb/s. Aquestes diferències fan que Bluetooth s'utilitzi normalment en telèfons mòbils o dispositius portàtils, mentre que l'ús de ZigBee es trobi més estès en altres àmbits com la domòtica.

Resum

En aquest mòdul didàctic hem vist els problemes de seguretat que afronten les xarxes sense fils d'abast personal i hem donat algunes pinzellades als esquemes que diferents tecnologies posen en joc per a afrontar aquests problemes.

La tecnologia RFID es troba altament limitada pel cost que es pot assumir en la producció de cada dispositiu. Hem vist que aquestes limitacions afecten el nivell de seguretat que es pot arribar a implementar en aquests dispositius. Per tal de poder implementar algorismes criptogràfics en dispositius RFID, hem observat com s'han d'adaptar per a reduir-ne la complexitat, o mitjançant el redisseny dels sistemes o per mitjà de la reducció de la mida dels paràmetres que fan servir. A part d'adaptar algorismes existents a les capacitats dels RFID, una altra alternativa és dissenyar esquemes nous tot tenint en compte des del primer moment els recursos disponibles.

La tecnologia Bluetooth pot treballar en diferents modes de seguretat i n'hem destacat els dos més importants: el mode de seguretat en l'àmbit d'enllaç i el mode de seguretat en l'àmbit de servei. En el primer, la política de seguretat s'aplica amb anterioritat a la connexió, mentre que en el segon, s'aplica en l'àmbit d'aplicació (un cop la connexió entre els dispositius ja s'ha fet). Els problemes bàsics dels mecanismes de seguretat es desprenen de la gestió de les claus d'enllaç i la seva reutilització en diferents processos d'autenticació.

L'especificació de ZigBee també preveu l'ús de diferents modes de seguretat per a les seves xarxes. Durant l'apartat, hem repassat diferents aspectes de la seguretat en sistemes ZigBee, des de la gestió de claus fins als mecanismes de seguretat que es poden aplicar a les diferents capes.

Finalment, hem revisat els aspectes de seguretat comentats per les tres tecnologies des d'un punt de vista més crític i n'hem elaborat una petita comparativa que resumeix les diferències essencials entre els dispositius RFID, Bluetooth i ZigBee.

Activitats

1. Busqueu informació sobre aplicacions reals on es faci servir RFID i intenteu trobar quins mecanismes de seguretat implementen.

2. Per tal de decidir si una seqüència pseudoaleatòria s'assembla o no a una seqüència vertaderament aleatòria es fan servir un conjunt de tests estadístics. Busqueu informació sobre quins són aquests tests.

3. Els termes *Bluejacking*, *Bluesnarfing* i *Bluebugging* s'utilitzen per a definir atacs a dispositius mòbils fent servir el seu mòdul Bluetooth. Busqueu informació sobre aquests atacs.

4. ZigBee descriu un conjunt de perfils d'alt nivell per a afavorir la interoperabilitat entre dispositius. Busqueu informació sobre els perfils permesos i la seva utilització.

5. UWB és una altra especificació per a comunicacions sense fils. Busqueu informació sobre la seguretat que implementa UWB.

Exercicis d'autoavaluació

1. Hem dit que el protocol HB només és segur davant d'un atacant passiu. Què podria fer un atacant actiu, amb capacitat per a interactuar amb l'etiqueta, per a descobrir el valor secret x?

2. Quines limitacions presenta el model d'autenticació repte-resposta i l'ús de la criptografia de clau compartida en les comunicacions sense fils?

3. Per què es descriu un mode de seguretat 2 en l'estàndard Bluetooth si el mode de seguretat 3 incorpora un nivell més elevat de seguretat?

4. Per què es descriu un mode de seguretat estàndard en ZigBee si el mode d'alta seguretat incorpora un nivell més elevat de seguretat?

Solucionari

1. Un atacant actiu té la capacitat d'executar el protocol amb l'etiqueta tantes vegades com vulgui, i té l'habilitat de triar el valor *a* a cada execució del protocol. Per tant, en primer lloc l'atacant pot executar diverses vegades el protocol amb un mateix valor *a*, de manera que pot eliminar el soroll introduït pel bit *b*. Una vegada assumim que l'atacant coneix el resultat de *ax*, només ha de recollir els valors *ax* per diferents *a* i construir un sistema d'equacions lineal.

2. La limitació principal que presenta el model d'autenticació repte-resposta i l'ús de la criptografia de clau compartida és que en tots dos casos les parts que es comuniquen han de compartir certa informació. Segons l'entorn (per exemple, en la telefonia mòbil), aquest fet no presenta cap problema, però per a aplicacions obertes, l'intercanvi d'aquesta informació pot esdevenir un problema difícil de gestionar.

3. El mode de seguretat 3 és molt més restrictiu que el mode 2 ja que el control es fa directament en l'àmbit d'enllaç, mentre que en el mode 2 es fa a nivell d'aplicació. L'avantatge de disposar d'un nivell de seguretat 2 és que permet la connexió de qualsevol dispositiu, cosa que facilita l'existència d'aplicacions més obertes, com per exemple la consulta dels serveis disponibles d'un dispositiu.

4. De la mateixa manera que amb Bluetooth, els modes de seguretat més elevats són més restrictius, i limiten l'accés a la xarxa a nodes que compleixen tots els requisits de seguretat fixats. A més, en mode de seguretat alta, els recursos necessaris per a mantenir el Centre de Confiança són molt més elevats i creixen a mesura que la xarxa es fa més gran.

Glossari

AES *m advanced encryption standard*

autenticitat *f* Propietat de trobar-se, en relació amb la informació, en el mateix estat en què va ser produïda, sense modificacions no autoritzades.
en *authenticity*

clau *f* Paràmetre, normalment secret, que controla els processos de xifratge o de desxifratge.

clau combinació *f* Clau generada conjuntament per dos dispositius Bluetooth i utilitzada com a clau d'enllaç.

clau de dispositiu *f* Clau específica de cada dispositiu Bluetooth sovint utilitzada com a clau d'enllaç.

clau d'enllaç *Bluetooth: f* Clau utilitzada en la tecnologia Bluetooth per a dur a terme el procés d'autenticació entre dispositius. *ZigBee: f* Clau que comparteixen dos dispositius ZigBee utilitzada en la comunicació *unicast*.

clau d'inicialització *f* Clau utilitzada en la tecnologia Bluetooth per a protegir l'intercanvi de la clau d'enllaç.

clau mestra *Bluetooth: f* Clau temporal que s'utilitza en una xarxa Bluetooth amb més de dos dispositius connectats quan el dispositiu mestre vol transmetre simultàniament als altres dispositius. *ZigBee: f* Clau que comparteixen dispositius ZigBee que serveix com a secret compartit inicial per a derivar noves claus.

clau de xarxa *f* Clau que comparteixen tots els dispositius ZigBee dins d'una mateixa xarxa. S'utilitza per a la comunicació *broadcast* a nivell d'aplicació o per a la comunicació a nivell de xarxa.

centre de confiança *m* En una xarxa ZigBee, dispositiu especial que gaudeix de la confiança de tots els altres dispositius de la xarxa.
en *Trust Center*

confidencialitat *f* Propietat que assegura que només els que hi estan autoritzats tindran accés a la informació.
en *Secrecy*

criptografia *f* Ciència que estudia les tècniques matemàtiques utilitzades per a la protecció de la informació.

criptografia de clau compartida *f* Grup de criptosistemes que basen la seva seguretat en una sola clau, que emissor i receptor fan servir tant per a xifrar com per a desxifrar.

criptografia lleugera *f* Conjunt de tècniques criptogràfiques dissenyades per a dispositius amb recursos limitats que intenten oferir un compromís entre rendiment, seguretat i cost.
en *Lightweight cryptography*

criptosistema *m* Mètode que permet xifrar un text en clar per a obtenir-ne un text xifrat inintel·ligible.
sin. Xifra

criptosistema de flux *m* Criptosistema que basa el seu funcionament en un generador pseudoaleatori que per mitjà d'una clau com a valor d'entrada genera una seqüència de xifratge.

denegació de servei *f* Atac que consisteix a aconseguir que el servei no estigui disponible per als usuaris legítims o bé que el servei que es doni es retardi o s'interrompi.
en *denial of service*
sigla DoS

denial of service *m* Vegeu denegació de servei.

DES *data encryption standard*

deterministic random bit generator *m* Vegeu generador pseudoaleatori.
sigla DRBG

dispositius amb funcionalitats completes *m* En l'especificació ZigBee, dispositius que poden realitzar qualsevol paper dins de la xarxa.
en *full-function devices*

dispositius amb funcionalitats reduïdes *m* En l'especificació ZigBee, dispositius que només poden actuar com a dispositius finals i que només poden interaccionar amb un sol dispositiu amb funcionalitats completes.
en *reduced-function devices*

DoS *m* Vegeu denegació de servei.

DRBG *deterministic random bit generator m* Vegeu generador pseudoaleatori.

forward security *f* Vegeu seguretat cap endavant.

FFD *full-function devices m* Vegeu dispositius amb funcionalitats completes.

full-function devices *m* Vegeu dispositius amb funcionalitats completes.
sigla FFD

gate equivalents *f* Portes equivalents a una NAND de dues entrades.
sigla GE

GE *f* Vegeu *gate equivalents*.

generador pseudoaleatori *m* Procés determinista capaç de generar una seqüència pseudoaleatòria.

gestor de seguretat *m* Entitat de la tecnologia Bluetooth que implementa la política de seguretat especificada en el mode de seguretat 2.

indistingibilitat RFID: *f* propietat que evita a un adversari distingir, és a dir diferenciar, entre dues etiquetes diferents només observant-ne les sortides.

integritat *f* Propietat que assegura la no-alteració de la informació.

jamming *m* Atac que consisteix a atenuar el senyal de ràdio per a provocar interferències en el servei.

LFSR *m* Vegeu registre de desplaçament realimentat linealment.

lightweight cryptography *f* Vegeu criptografia lleugera.

NLFSR *m* Registre de desplaçament realimentat no linealment.

Nonce *m* Vegeu *number used once*.

number used once *m* Nombre arbitrari que es fa servir una única vegada i que permet, per exemple, evitar atacs de *replay*.

privacitat *f* Vegeu confidencialitat.

PRNG *pseudorandom number generator m* Vegeu generador pseudoaleatori.

pseudorandom number generator *m* Vegeu generador pseudoaleatori.
sigla PRNG

reduced-function devices *m* Vegeu dispositius amb funcionalitats reduïdes.
sigla RFD

registre de desplaçament realimentat linealment *m* Dispositiu físic o lògic format per *n* cel·les de memòria i una funció d'alimentació lineal.
sigla LFSR

repte-resposta *m* Sistema d'autenticació pel qual dues parts es poden autenticar remotament. Aquest sistema d'autenticació requereix que totes dues parts s'hagin intercanviat certa informació anteriorment al procés d'autenticació.

RFD *reduced-function devices m* Vegeu dispositius amb funcionalitats reduïdes.

RFID *f* Identificació mitjançant radiofreqüència.

seguretat cap endavant *f* Extensió de les propietats d'autenticitat i d'indistingibilitat que garanteix que aquestes propietats es mantenen per a transaccions passades quan un atacant és capaç de corrompre una etiqueta en un moment determinat.
en *forward security*

trust center *m* Vegeu centre de confiança.

xifra *f* Vegeu criptosistema.

Bibliografia

Baronti, P.; Pillai, P.; Chook, V.; Chessa, S.; Gotta, A.; Hu, Y. (2007). *Wireless Sensor Networks: a Survey on the State of the Art and the 802.15.4 and ZigBee Standards*. Amsterdam: Elsevier Science Publishers B. V.

Domingo, J.; Herrera, J. (1999). *Criptografia*. Barcelona: UOC.

Farahani, S. (2008). *ZigBee Wireless Networks and Transceivers*. Newton, MA, EUA: Newnes.

Finkenzeller, K. (2003). *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*. John Wiley & Sons.

Gehrmann, C.; Persson, J; Smeets, B. (2001). *Bluetooth security*. Artech House Publishers.

Gislason, D. (2008). *ZigBee Wireless Networking*. Newton, MA, USA: Newnes.

Jakobsson, M.; Wetzel, S. (2001). "Security weaknesses in Bluetooth". A: *Proceedings of RSA 2001* (LNCS 2020, pàg. 176-191). Springer Verlag.

Knospe1, H.; Lemke-Rust, K. (2010). *Towards Secure and Privacy-Enhanced RFID Systems* capítol 16 de RFID Systems - Research Trends and Challenges: John Wiley & Sons.

Lee, J. S.; Su, Y-W.; Shen, Chung-Chou (2007). *A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi*. Taiwan: Proceedings of the 33rd Annual Conference of the IEEE Industrial Electronics Society.

Maimut, D.; Ouafi, K. (2012). *Lightweight Cryptography for RFID Tags*. IEEE Security and Privacy: IEEE Computer Society.

Menezes, A.; Oorschot, P.; Vanstone, S. A. (2001). *Handbook of Applied Cryptography (5a ed.)*. CRC-Press.

Vainio, J. T. (2000). "Bluetooth security". A: *Proceedings of Helsinki University of Technology, Telecommunications Software and Multimedia Laboratory*. Hèlsinki.

ZigBee Alliance (2007). *ZigBee Specification*. ZigBee Document 053474r17.