Identificación, análisis y evaluación de la seguridad en las comunicaciones con tecnología ZigBee

Por Javier Areitio Bertolín

El Prof. Dr. Javier Areitio Bertolín es Catedrático de la Facultad de Ingeniería y Director del Grupo de Investigación Redes y Sistemas de la Universidad de Deusto.

En el presente artículo se analiza ZigBee una de las tecnologías relacionadas con redes WPAN/WBAN/HAN (Wireless Personal Area Network / Wireless Body Area Network / Home Area Network) desde la perspectiva de la seguridad y privacidad de la información. La seguridad-privacidad en dispositivos móviles es esencial para poder gestionar los entornos inteligentes. Los dispositivos móviles están evolucionando hasta convertirse en servidores (proveedores de servicios sensibles al contexto, a la localización, servicios sociales móviles, etc.) si no se protegen de forma profesional sus riesgos el resultado será desastroso.

La tecnología de los sistemas CPS (Cyber Physical Systems) integra la computación y las capacidades de comunicación con la monitorización y control de entidades en el mundo físico, a veces se percibe como sistemas embebidos en red. Actualmente es esencial tratar la seguridad de WSN (Wireless Sensor Networks) que constituye un elemento clave de la tecnología CPS, pensemos por ejemplo en infraestructuras críticas. ZigBee posibilita que los dispositivos establezcan interfaz del entorno físico con las aplicaciones del mundo real por tanto permiten el desarrollo de WSNs y por ende de CPSs. El abanico de aplicaciones de ZigBee se encuentra en expansión y crece de forma significativa cubre desde entornos industriales/SCADA/infraestructuras de sistemas críticos, gestión y eficiencia energética, servicios de telecomunicaciones, sanitarios, sociales, personales, automatización de edificios como control de acceso, detección de incendios, HVAC (Heating, Ventilation and Air Conditioning), AMI (Advanced Metering Infrastructure), AMR (Automatic Meter Reading), redes sociales dinámicas de vida limitada, transporte por carreteras, etc.

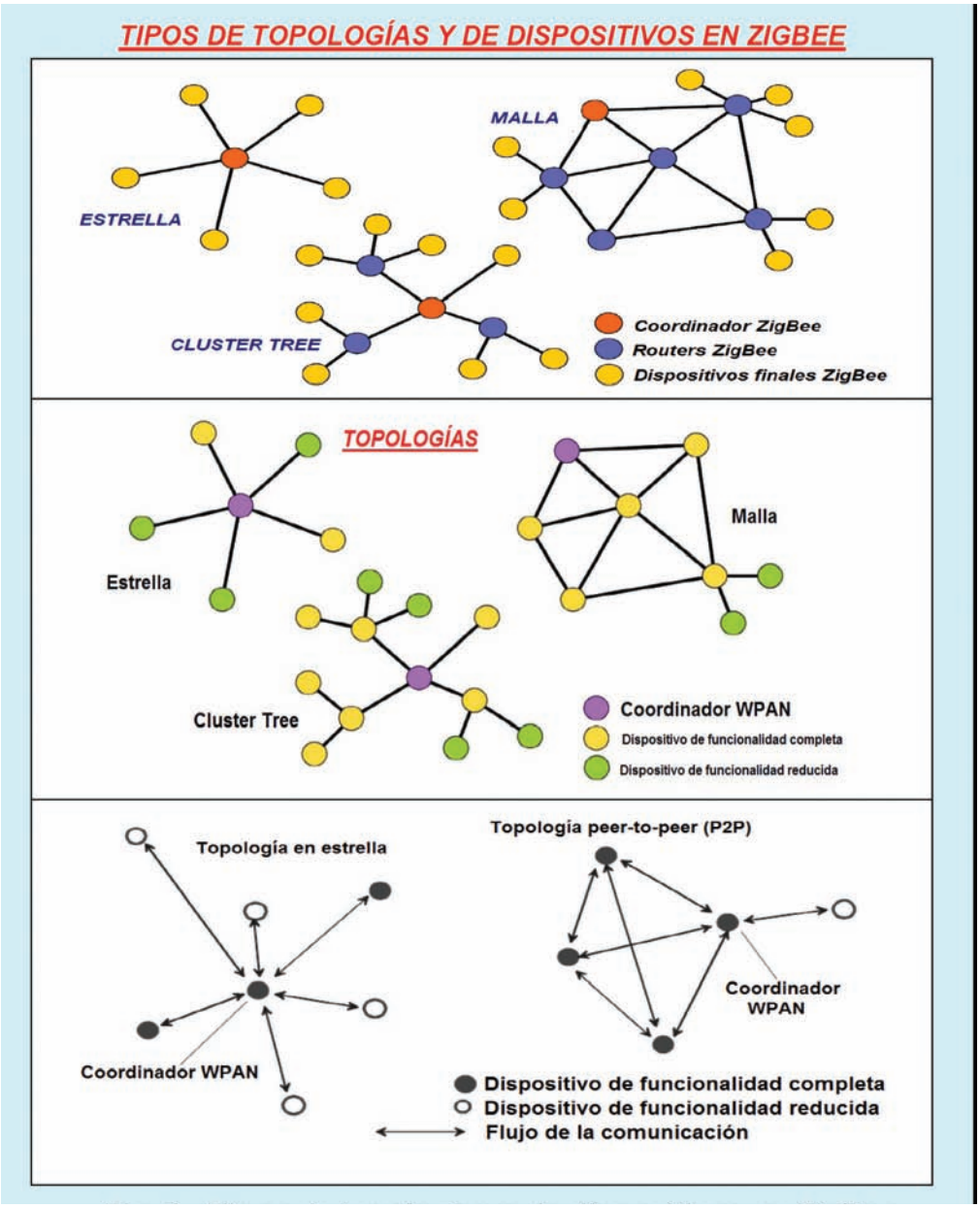


Figura 1.Tipos de topologías y de dispositivos en ZigBee

ZigBee y seguridad

ZigBee es una especificación inalámbrica, un estándar abierto y una tecnología que define un conjunto de protocolos y arquitectura para implantar redes-aplicaciones de control, sensores y monitorización que utiliza señales de radio. Esta basado en el estándar inalámbrico del IEEE 802.15.4 que caracteriza los niveles más bajos: físico/L1 (PHY) y MAC (Media Access Control)/L2. La Plataforma de la Alianza ZigBee define los niveles superiores de red/seguridad y framework de aplicación. Por encima, en lo más alto se encuentra el nivel de perfiles/aplicación definido por ZigBee o OEM. ZigBee esta diseñada para consumo de baja potencia, para aplicaciones de baja velocidad de datos. ZigBee es una red auto-organizada en malla de dispositivos tipo sensor diseñada para informar de las condiciones del entorno de una manera fiable, precisa y a tiempo. Con las ventajas de la alta disponibilidad, bajo precio, y

bajos requisitos de recursos, las redes ZigBee se presentan en principio ideales para aplicaciones industriales y comerciales como monitorización y control de procesos de fabricación, automatización de luces, calefacción, detectores de humo/fuego/intrusos y sensores y monitorización médica o aplicaciones residenciales como automatización en domótica y seguridad, etc. ZigBee es un estándar de red de sensores inalámbricos emergente con un gran potencial de utilizarse en áreas donde es crítica la seguridad, de modo que las redes ZigBee deberían poder ofrecer las garantías de seguridad deseadas. Actualmente ZigBee utiliza el algoritmo criptográfico simétrico o de secreto compartido AES-128 (Advanced Encryption Standard) con claves de 128 bits para el cifrado. Debido a que AES es un mecanismo simétrico no permite funcionalidades que ofrecen los mecanismos criptográficos asimétricos o de clave pública como son la firma digital y la distribución de la clave de sesión sin la intervención de un centro de distribución de claves criptográficas. Debido a los requisitos estrictos de seguridad de algunas aplicaciones de control y monitorización de misión crítica se requiere la capacidad para que la comunicación de dispositivos ZigBee se autentique por firma digital. En este caso se debería implantar criptografía asimétrica de poca exigencia de recursos como CPU, memoria y alimentación eléctrica como RSA basada en CRT y ECC. La seguridad de las redes de sensores inalámbricas como las basadas en ZigBee es muy importante y se deben gestionar adecuadamente los riesgos como son las vulnerabilidades teóricas (en base a la inyección y generación inteligente de PDUs (Protocol Data Units) y la captura de patrones-perfiles de flujo de tráfico), las escuchas clandestinas con sniffers, las interferencia de canal, el conflicto de la asignación de direcciones, el routing con inundación en la red, la escucha clandestina de claves, los defectos del cifrado simétrico sin protección de integridad/autenticación, la no certificación de identidad en los servicios de seguridad, etc. Posibles contramedidas son la autenticación basada en firma digital ECC o ECDSA o RSA con CRT, el intercambio de claves D-H (Diffie-Hellman) basado en ECC (Elliptic Curve Cryptography), establecimiento de canales standby, etc.

La especificación de ZigBee señala que las decisiones como actualizar/expirar las claves criptográficas, la saturación de contadores, la pérdida de sincronización, las condiciones de error que surgen de proteger tramas deben incluirse en el nivel de perfiles/aplicación de la arquitectura y deben ser abordadazos en las implementaciones reales. Sin embargo, el delegar cuestiones críticas a las implementaciones reales en vez de definirlas en la especificación crea azares de seguridad.

Según la base de datos de vulnerabilidades del NIST (Nacional Institute of Standards and Technology) una vulnerabilidad de ZigBee cuyo impacto es perturbación del servicio es la denominada CVE-2010-4301.

Seguridad comunicaciones inalámbricas

La seguridad en las comunicaciones inalámbricas se proporciona en relación a su utilización y topología de la red. Pueden identificarse tres tipos de conexiones: (i) Conexiones de corta vida. Por ejemplo, transferencias de ficheros, sacar datos por impresora, mensajería. (ii) Conexiones de vida media. Por ejemplo, llamadas, sesiones, etc. (iii) Conexiones de larga vida. Por ejemplo, redes inalámbricas de sensores. Las redes inalámbricas de sensores con dispositivos de baja potencia se utilizan tanto como infraestructura o como tecnología central para implementar entornos de computación ubicua. Actualmente

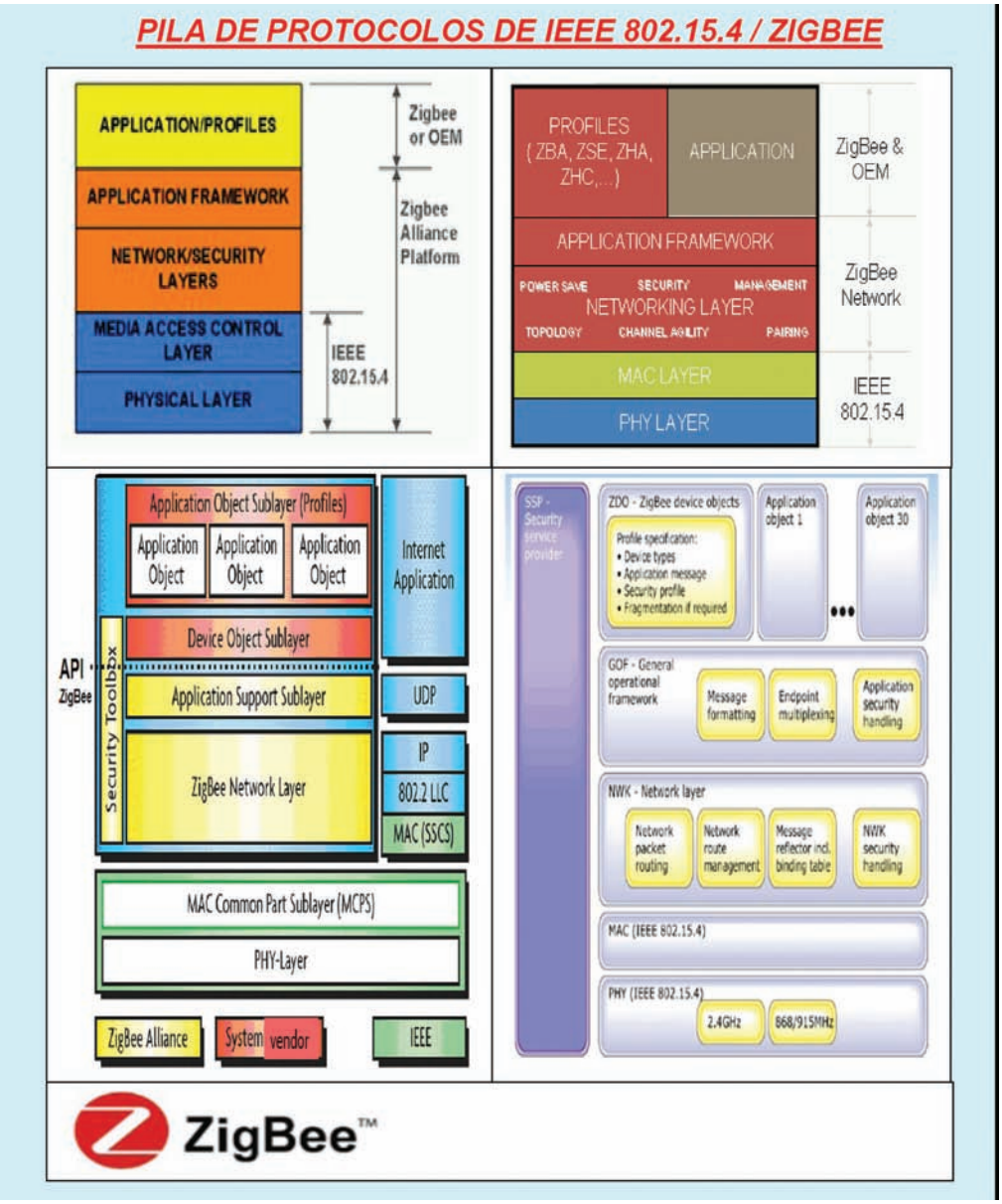


Figura 2. Pila de protocolos de IEEE 802.15.4/ZigBee

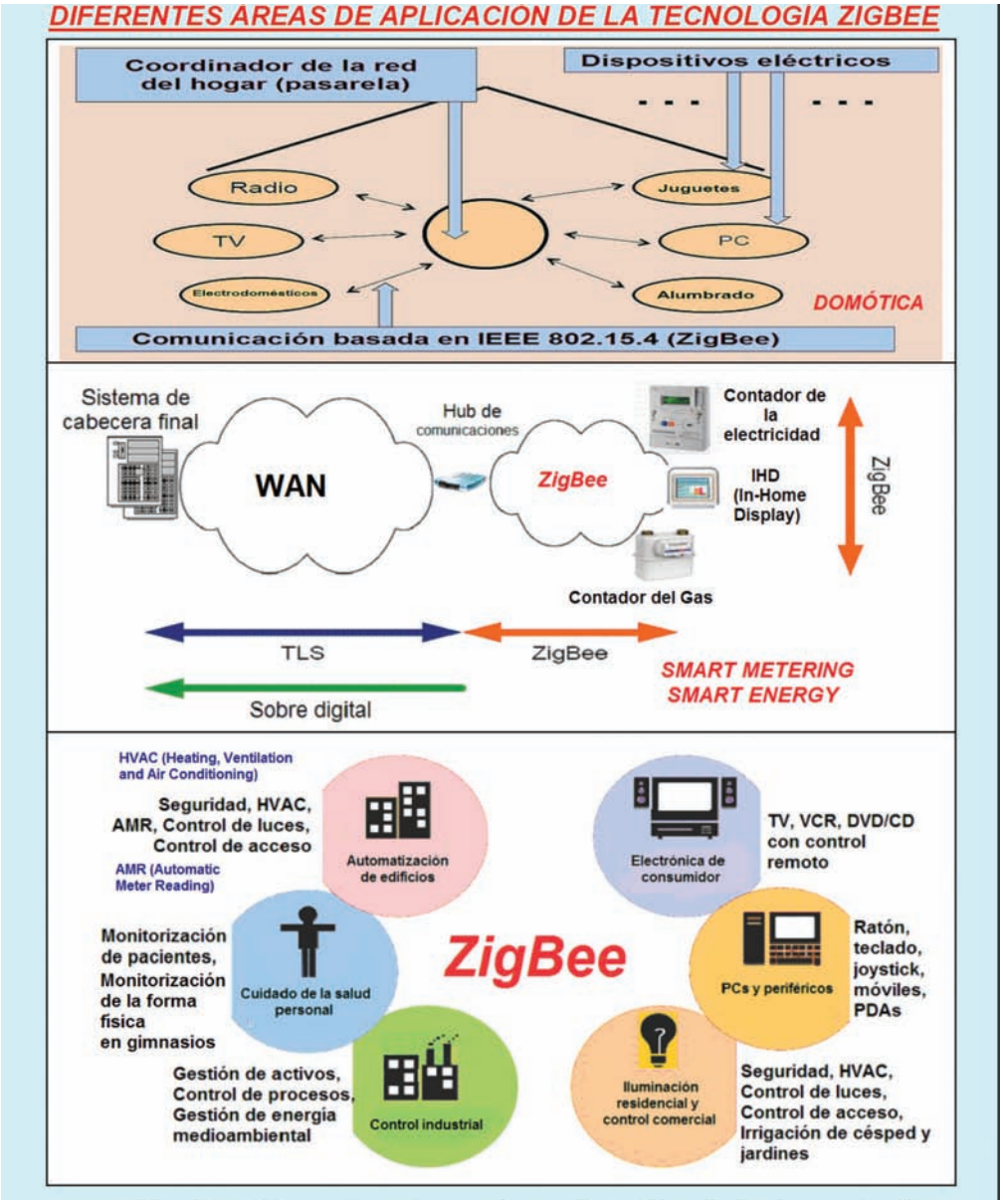


Figura 3. Diferentes áreas de aplicación de la tecnología ZigBee

existe un creciente número de aplicaciones con este tipo de redes para todo tipo de entornos de la sociedad, a nivel personal, de salud, ecológicos, lúdicos, de negocios, militares, etc. Estas aplicaciones incluyen información sensible-privada como salud de personas, de tipo financiero, confidencial de negocios, etc. Además las redes inalámbricas de sensores presentan una gran cantidad de vulnerabilidades debido a que constan de recursos limitados (poca memoria y vida de la batería) y poseen potencia de computación (CPU) baja. Las amenazas pueden clasificarse atendiendo a la capa de la arquitectura de protocolos: (i) A la capa física: como el jamming y perturbaciones (ataque a la disponibilidad y DoS). (ii) A la capa de enlace de datos: como las colisiones, la no equidad de acceso. (iii) A la capa de red: como la falsificación/alteración, la retransmisión de la información de routing, el reenvío selectivo. (iv) A la capa de transporte: como la inundación y la de-sincronización. (v) A las capas superiores: como malware/virus/gusanos, el seguimiento de la localización ya que la señal de radio permite su trazabilidad. Consecuentemente para poder proteger a los datos de los sensores que pueden ser críticos y de naturaleza sensible y a las amenazas de seguridad (como gusanos, virus, troyanos, etc.) son esenciales las capacidades de seguridad-privacidad (disponibilidad, autenticación, autorización, confidencialidad, integridad, no repudio, anonimato, control de acceso, registro-monitorización, etc.)

Tecnología ZigBee. Perfiles públicos ZigBee.

La tecnología ZigBee fue desarrollada por la Alianza ZigBee (consorcio industrial en crecimiento a nivel mundial y ecosistema global de compañías que integra los principales fabricantes de semiconductores, proveedores de tecnología, OEMs (Original Equipment Manufacturer) y usuarios finales) creada en octubre del 2002. Trabaja junto con el Grupo 802.15 del IEEE (para asegurar la interoperabilidad) con lo que también se denomina IEEE 802.15.4. ZigBee toma su nombre del camino-danza en zig-zag de las abejas de miel que guía a sus miembros del enjambre a las flores y que forman redes en forma de malla entre las flores; metafóricamente hablando los dispositivos ZigBee simples trabajan juntos para llevar a cabo tareas complejas. Desde su creación ha pasado por tres versiones o documentos de especificación: ZigBee v1.0 (diciembre 2004), 2006 y ZigBee 2007. El perfil de aplicación Smart Energy se denomina ZigBee-SE. Uno de los últimos perfiles de pila publicados es el ZigBee PRO que es un conjunto expandido de características de la especificación de protocolo ZigBee pero incompatible con ZigBee antiguos. Otros perfiles son ZigBee RF4CE, ZigBee PRO SEP1.x y ZigBee PRO SEP2.0 este es el más nuevo, incompatible con otras pilas ZigBee antiguas.

Permite crear redes de hasta 65.536 nodos o dispositivos (con batería no recargable), su alcance es de unos treinta metros, utilizan un interfaz de aire DSSS (Direct Sequence Spread Spectrum) donde la señal original se multiplica por una señal de ruido generada por una secuencia pseudo-aleatoria que oscila entre +1 y – 1. Posee una pila de protocolo con 4 a 30Kbyte de código ZigBee dependiendo del grado de funcionalidades que integre el dispositivo. Utiliza la banda de frecuencias de 2,4 GHz establecida por acuerdo internacional (no necesita licencias) para el uso de dispositivos ISM (Industrial, Scientific and Medical) [2,402 GHz , 2,480 GHz] espectro que lo divide en dieciséis canales. Latencia inferior a 15 milisegundos. Opera a velocidades de 20 a 250 Kbps y utiliza dos tipos

de direcciones: (i) Direcciones de 16 bits (direcciones cortas asignadas por padres de una topología en árbol o establecidos por aplicaciones). Tamaño de red de hasta 264 nodos. Permite dos modos de direccionamiento red más identificador de dispositivo (topología de estrella) e identificador de la fuente/destino para topología P2P (Peer-to-Peer). (ii) Direcciones IEEE de 64 bits (direcciones extendidas son direcciones únicas para un dispositivo ZigBee). Su objetivo global es satisfacer las necesidades de monitorización y control remoto así como aplicaciones de red de sensores. La tecnología ZigBee define los niveles más altos de la pila de protocolos basada en IEEE 802.15.4 (que cubre las dos primeras capas física y MAC) desde la capa de red a la capa de aplicación (define gestión de la topología, el routing, el protocolo de descubrimiento, etc.).

Los principales perfiles públicos ZigBee son: ZHA (ZigBee Home Automation), ZSE (ZigBee Smart Energy) como SCADA/AMI/medidas de gestión-eficiencia energética, ZRC (ZigBee Remote Control), ZHC (ZigBee Health Care), ZTS (ZigBee Telecom Services) como m-commerce/servicios de información/juegos/chat, ZID (ZigBee Input Device), ZRS (ZigBee Retail Services), Z3DS (ZigBee 3D Sync) y ZBA (ZigBee Building Automation).

Dispositivos y topologías ZigBee. Modos de seguridad ZigBee PRO.

El estándar de WPAN ZigBee/802.15.4 (soporta confidencialidad y autenticidad de datos y protección contra repeticiones), para redes inalámbricas que consta de dispositivos con requisitos de recursos muy bajos, define básicamente tres tipos de dispositivos-nodos que pueden clasificarse en dos categorías:

(1) Dispositivos con todas las funcionalidades: (i) Los coordinadores ZigBee (ZC). Son los únicos dispositivos capaces de iniciar una nueva formación de red. Son los dispositivos con mayor número de capacidades, permiten iniciar la red y hacer de puente a otras redes. Forman la raíz de una red y pueden hacer de puente a otras redes. Sólo existe uno de estos dispositivos en cada red, actúa como Centro de Confianza y repositorio de claves de seguridad. Transmite beacons es decir proporciona sincronización. (ii) Los routers ZigBee (ZR). Realiza funciones complejas, actúa como un router intermedio que pasa datos entre dispositivos. Retransmite datos y extiende la cobertura de la red.

(2) Dispositivos con funcionalidad reducida. Son los dispositivos finales ZigBee (ZED). Sólo pueden conversar con un dispositivo coordinador o con un router, realizan las funcionalidades básicas por ejemplo sensor, actuador, etc. Pueden estar dormidos durante una cantidad de tiempo significativa. Todos los dispositivos proporcionan las siguientes funcionalidades: juntarse a una red y abandonar una red. Los coordinadores y routers proporcionan las siguientes funcionalidades adicionales: participar en asignar direcciones lógicas de red y mantener una lista de dispositivos vecinos.

Posibilita despliegues de topologías variadas:

(1) Estrella centralizada. En el centro incluye un dispositivo coordinador y en los extremos se colocan routers o sensores.

(2) Arquitectura P2P basada en cluster-árbol. Consiste en una conexión de estrellas, donde uno de los centros es un dispositivo de coordinador y el resto de los centros de las estrellas son routers, los dispositivos extremos con sensores o routers.

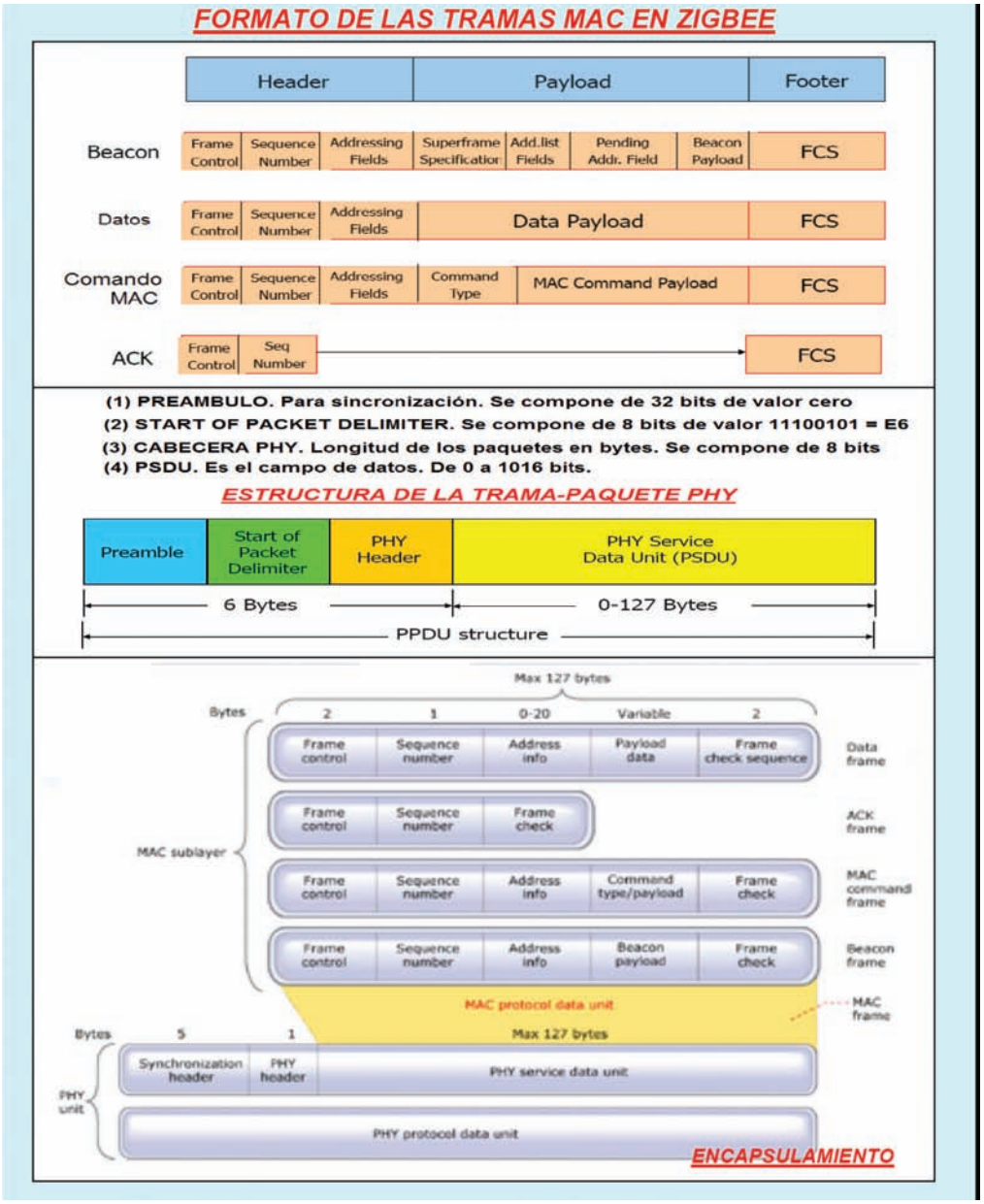
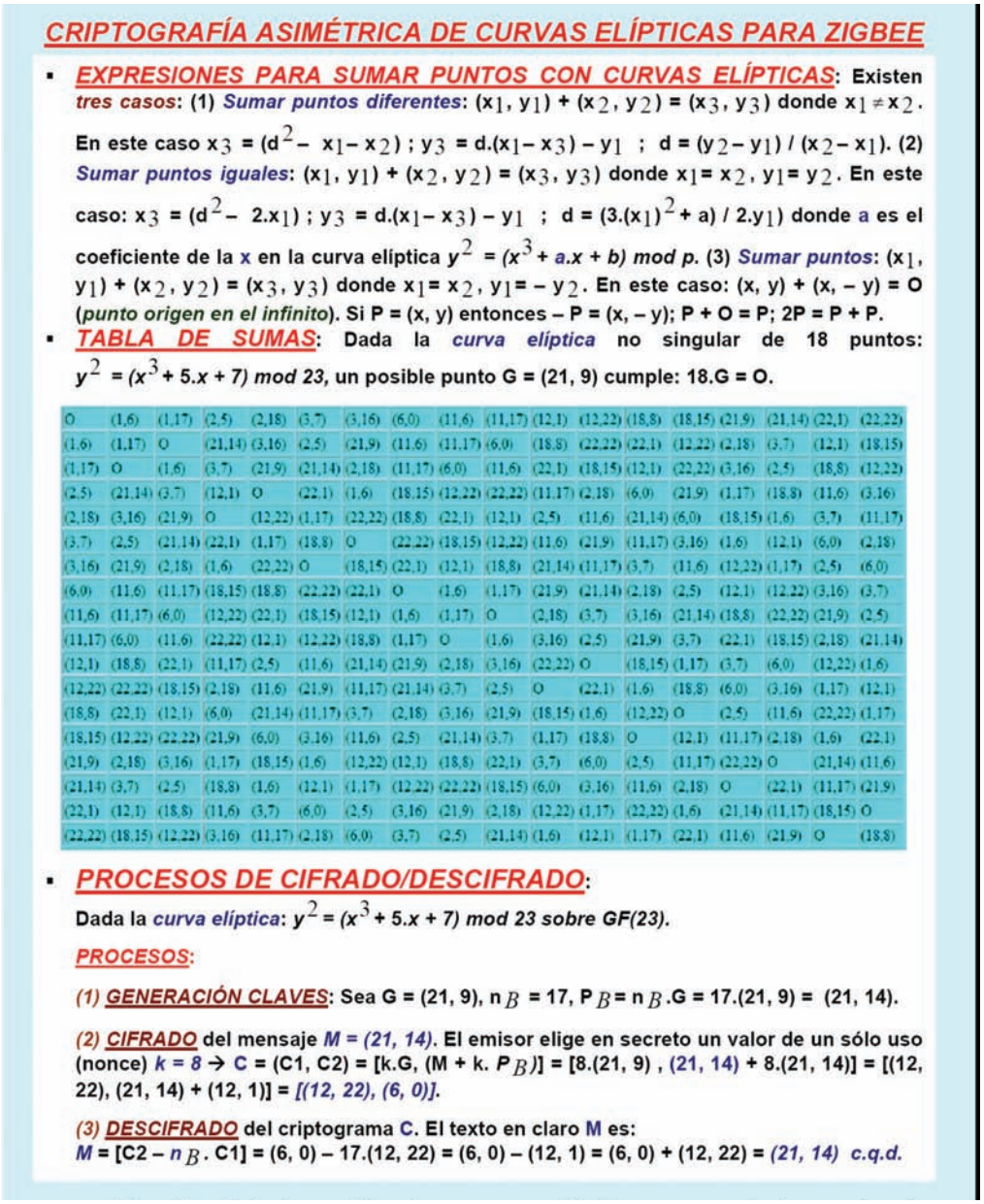


Figura 4. Formato de tramas MAC y PHY en la tecnología ZigBee



CRIPTOGRAFÍA ASIMÉTRICA DE CURVAS ELÍPTICAS PARA ZIGBEE

- **EXPRESIONES PARA SUMAR PUNTOS CON CURVAS ELÍPTICAS**: Existen *tres casos*: (1) *Sumar puntos diferentes*: $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ donde $x_1 \neq x_2$. En este caso $x_3 = (d^2 - x_1 - x_2)$; $y_3 = d.(x_1 - x_3) - y_1$; $d = (y_2 - y_1) / (x_2 - x_1)$. (2) *Sumar puntos iguales*: $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ donde $x_1 = x_2$, $y_1 = y_2$. En este caso: $x_3 = (d^2 - 2.x_1)$; $y_3 = d.(x_1 - x_3) - y_1$; $d = (3.(x_1)^2 + a) / 2.y_1)$ donde a es el coeficiente de la x en la curva elíptica $y^2 = (x^3 + a.x + b) \bmod p$. (3) *Sumar puntos*: $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ donde $x_1 = x_2$, $y_1 = -y_2$. En este caso: (x, y) + (x, – y) = O (*punto origen en el infinito*). Si P = (x, y) entonces – P = (x, – y); P + O = P; 2P = P + P.
- **TABLA DE SUMAS**: Dada la *curva elíptica* no singular de 18 puntos: $y^2 = (x^3 + 5.x + 7) \bmod 23$, un posible punto G = (21, 9) cumple: 18.G = O.

O	(1,6)	(1,17)	(2,5)	(2,18)	(3,7)	(3,16)	(6,0)	(11,6)	(11,17)	(12,1)	(12,22)	(18,8)	(18,15)	(21,9)	(21,14)	(22,1)	(22,22)
(1,6)	(1,17)	O	(21,14)	(3,16)	(2,5)	(21,9)	(11,6)	(11,17)	(6,0)	(18,8)	(22,22)	(22,1)	(12,22)	(2,18)	(3,7)	(12,1)	(18,15)
(1,17)	O	(1,6)	(3,7)	(21,9)	(21,14)	(2,18)	(11,17)	(6,0)	(11,6)	(22,1)	(18,15)	(12,1)	(22,22)	(3,16)	(2,5)	(18,8)	(12,22)
(2,5)	(21,14)	(3,7)	(12,1)	O	(22,1)	(1,6)	(18,15)	(12,22)	(22,22)	(11,17)	(2,18)	(6,0)	(21,9)	(1,17)	(18,8)	(11,6)	(3,16)
(2,18)	(3,16)	(21,9)	O	(12,22)	(1,17)	(22,22)	(18,8)	(22,1)	(12,1)	(2,5)	(11,6)	(21,14)	(6,0)	(18,15)	(1,6)	(3,7)	(11,17)
(3,7)	(2,5)	(21,14)	(22,1)	(1,17)	(18,8)	O	(22,22)	(18,15)	(12,22)	(11,6)	(21,9)	(11,17)	(3,16)	(1,6)	(12,1)	(6,0)	(2,18)
(3,16)	(21,9)	(2,18)	(1,6)	(22,22)	O	(18,15)	(22,1)	(12,1)	(18,8)	(21,14)	(11,17)	(3,7)	(11,6)	(12,22)	(1,17)	(2,5)	(6,0)
(6,0)	(11,6)	(11,17)	(18,15)	(18,8)	(22,22)	(22,1)	O	(1,6)	(1,17)	(21,9)	(21,14)	(2,18)	(2,5)	(12,1)	(12,22)	(3,16)	(3,7)
(11,6)	(11,17)	(6,0)	(12,22)	(22,1)	(18,15)	(12,1)	(1,6)	(1,17)	O	(2,18)	(3,7)	(3,16)	(21,14)	(18,8)	(22,22)	(21,9)	(2,5)
(11,17)	(6,0)	(11,6)	(22,22)	(12,1)	(12,22)	(18,8)	(1,17)	O	(1,6)	(3,16)	(2,5)	(21,9)	(3,7)	(22,1)	(18,15)	(2,18)	(21,14)
(12,1)	(18,8)	(22,1)	(11,17)	(2,5)	(11,6)	(21,14)	(21,9)	(2,18)	(3,16)	(22,22)	O	(18,15)	(1,17)	(3,7)	(6,0)	(12,22)	(1,6)
(12,22)	(22,22)	(18,15)	(2,18)	(11,6)	(21,9)	(11,17)	(21,14)	(3,7)	(2,5)	O	(22,1)	(1,6)	(18,8)	(6,0)	(3,16)	(1,17)	(12,1)
(18,8)	(22,1)	(12,1)	(6,0)	(21,14)	(11,17)	(3,7)	(2,18)	(3,16)	(21,9)	(18,15)	(1,6)	(12,22)	O	(2,5)	(11,6)	(22,22)	(1,17)
(18,15)	(12,22)	(22,22)	(21,9)	(6,0)	(3,16)	(11,6)	(2,5)	(21,14)	(3,7)	(1,17)	(18,8)	O	(12,1)	(11,17)	(2,18)	(1,6)	(22,1)
(21,9)	(2,18)	(3,16)	(1,17)	(18,15)	(1,6)	(12,22)	(12,1)	(18,8)	(22,1)	(3,7)	(6,0)	(2,5)	(11,17)	(22,22)	O	(21,14)	(11,6)
(21,14)	(3,7)	(2,5)	(18,8)	(1,6)	(12,1)	(1,17)	(12,22)	(22,22)	(18,15)	(6,0)	(3,16)	(11,6)	(2,18)	O	(22,1)	(11,17)	(21,9)
(22,1)	(12,1)	(18,8)	(11,6)	(3,7)	(6,0)	(2,5)	(3,16)	(21,9)	(2,18)	(12,22)	(1,17)	(22,22)	(1,6)	(21,14)	(11,17)	(18,15)	O
(22,22)	(18,15)	(12,22)	(3,16)	(11,17)	(2,18)	(6,0)	(3,7)	(2,5)	(21,14)	(1,6)	(12,1)	(1,17)	(22,1)	(11,6)	(21,9)	O	(18,8)

- **PROCESOS DE CIFRADO/DESCIFRADO**:

Dada la *curva elíptica*: $y^2 = (x^3 + 5.x + 7) \bmod 23$ *sobre GF(23).*

PROCESOS:

(1) **GENERACIÓN CLAVES**: Sea G = (21, 9), n_B = 17, $P_B = n_B.G = 17.(21, 9) = (21, 14)$.

(2) **CIFRADO** del mensaje *M = (21, 14)*. El emisor elige en secreto un valor de un sólo uso (nonce) *k = 8* → C = (C1, C2) = [k.G, (M + k. P_B)] = [8.(21, 9) , (21, 14) + 8.(21, 14)] = [(12, 22), (21, 14) + (12, 1)] = *[(12, 22), (6, 0)]*.

(3) **DESCIFRADO** del criptograma C. El texto en claro M es:
M = [C2 – n_B. C1] = (6, 0) – 17.(12, 22) = (6, 0) – (12, 1) = (6, 0) + (12, 22) = *(21, 14) c.q.d.*

Figura 5. Criptografía de curvas elípticas para la tecnología ZigBee

(3) Redes P2P en malla (normalmente son parcialmente interconectadas) o WMN (Wireless Mesh Network). Incluye un coordinador y routers para formar los contornos cerrados y el resto son sensores o routers. Las topologías en malla permiten crear redes ad-hoc.

ZigBee PRO define dos modos de seguridad diferentes: (1) Modo de seguridad estándar (denominado residencial en ZigBee 2006). La lista de dispositivos, las claves maestras, las claves de enlace y las claves de red pueden ser mantenidas bien por el Centro de Confianza o por los propios dispositivos. El Centro de Confianza es responsable de mantener la clave de red estándar y controla las políticas de admisión a la red. En este modo los requisitos de memoria para el Centro de Confianza son menores que para el modo de alta seguridad. (2) Modo de seguridad elevado. El Centro de Confianza mantiene la lista de dispositivos, las claves maestras, las claves de enlace y las claves de red que necesita para controlar y aplicar las políticas de actualización de claves de red y la admisión a la red. Conforme crece el número de dispositivos de la red así también crece la memoria requerida para el Centro de Confianza.

Seguridad ZigBee. Centro de confianza.

ZigBee utiliza un modelo de confianza abierto donde los niveles de la pila de protocolos confían entre sí, esto es posible ya que los dispositivos ZigBee normalmente son microcontroladores inalámbricos de único chip. La protección criptográfica sólo ocurre entre dispositivos y se utiliza el mismo nivel de la suite de seguridad para todos los servicios. El estándar define tres servicios de seguridad: establecimiento de clave, transporte de la clave, protección de trama y autorización de dispositivo. Para que funcione adecuadamente una red ZigBee con funcionalidad de seguridad debe incluir un único dispositivo denominado Centro de Confianza (este rol normalmente lo asume el Coordinador ZigBee) que controle el acceso y distribuya las claves cuyas principales funcionalidades son: (i) Mantener y distribuir las claves de red. (ii) Autenticar un dispositivo en la red. (iii) Permite seguridad extremo a extremo entre dispositivos. Se definen dos modos: (a) Modo residencial (baja seguridad). Permite que los dispositivos se junten a la red pero no establece claves. (b) Modo comercial (alta seguridad). Establece y mantiene las claves y contadores de no repetición de mensajes con cada dispositivo. El control y actualización de claves es centralizado. La seguridad de ZigBee se basa en claves simétricas de modo que ambas partes comparten la misma clave.

Se han definido tres métodos básicos para llevar a cabo este proceso relacionado con las claves: (1) Pre-instalación. Las claves se colocan en el dispositivo antes de desplegarlo o con métodos fuera de banda (si las comunicaciones no se protegen debidamente con cifrado HTTPS/SSL/TLS nos encontramos con un problema de seguridad). (2) Transporte. El Centro de Confianza envía la clave (de forma segura donde sea posible) al dispositivo. (3) Establecimiento. El dispositivo y el Centro de Confianza negocian la clave bien con "Establecimiento de clave simétrico" o con el "Establecimiento de clave basada en certificados".

Tipos de claves. Características de seguridad.

Se han definido tres tipos de claves: (a) Clave maestra. Diseñada para seguridad a largo plazo entre dos dispositivos, puede ser pre-instalada o transmitida por el aire (si se transmiten los mensajes en texto en claro, surge el riesgo de las escuchas clandestinas

MECANISMO D-H SOBRE CURVAS ELÍPTICAS PARA ZIGBEE

MECANISMO D-H (DIFFIE-HELLMAN) DE ACUERDO DE CLAVE SECRETA COMPARTIDA K BASADO EN CRIPTOGRAFÍA ASIMÉTRICA (DE CLAVE PÚBLICA) DE CURVAS ELÍPTICAS:

- Permite que dos entidades A y B (*dispositivos ZigBee*) acuerden un secreto compartido K (o clave criptográfica compartida).
- Se elige una *curva elíptica*, por ejemplo: $y^2 = (x^3 + 11.x + 7) \bmod 19$ sobre *GF(19)* de dieciocho puntos y un punto G tal que *18.G = O*, por ejemplo *G = (0, 8)* ambos públicos. Existen seis puntos G de orden 18.
- ***MECANISMO***:
- La *entidad A* selecciona su *clave privada* $n_A = 12$, y calcula su *clave pública* $P_A = n_A.G = 12.(0, 8) = (12, 10)$ que *se la envía a la entidad B*.
- La *entidad B* selecciona su *clave privada* $n_B = 17$ y calcula su *clave pública* $P_B = n_B.G = 17.(0, 8) = (0, 11)$ y *se la envía a la entidad A*.
- La *clave compartida* K que obtiene cada entidad es:

  (i) Cálculos en la entidad A: $K = n_A . P_B = 12.(0, 11) = (12, 9)$.

  (ii) Cálculos en la entidad B: $K = n_B . P_A = 17.(12, 10) = (12, 9)$.

O	(0,8)	(0,11)	(1,0)	(4,1)	(4,18)	(5,4)	(5,15)	(6,2)	(6,17)	(7,3)	(7,16)	(12,9)	(12,10)	(14,6)	(14,13)	(16,2)	(16,17)
(0,8)	(5,4)	O	(6,2)	(5,15)	(7,3)	(4,18)	(0,11)	(14,6)	(1,0)	(16,17)	(4,1)	(14,13)	(16,2)	(12,10)	(6,17)	(7,16)	(12,9)
(0,11)	O	(5,15)	(6,17)	(7,16)	(5,4)	(0,8)	(4,1)	(1,0)	(14,13)	(4,18)	(16,2)	(16,17)	(14,6)	(6,2)	(12,9)	(12,10)	(7,3)
(1,0)	(6,2)	(6,17)	O	(12,9)	(12,10)	(14,6)	(14,13)	(0,8)	(0,11)	(16,2)	(16,17)	(4,1)	(4,18)	(5,4)	(5,15)	(7,3)	(7,16)
(4,1)	(5,15)	(7,16)	(12,9)	(12,10)	O	(0,11)	(16,2)	(14,13)	(16,17)	(0,8)	(14,6)	(4,18)	(1,0)	(6,17)	(7,3)	(6,2)	(5,4)
(4,18)	(7,3)	(5,4)	(12,10)	O	(12,9)	(16,17)	(0,8)	(16,2)	(14,6)	(14,13)	(0,11)	(1,0)	(4,1)	(7,16)	(6,2)	(5,15)	(6,17)
(5,4)	(4,18)	(0,8)	(14,6)	(0,11)	(16,17)	(7,3)	O	(12,10)	(6,2)	(12,9)	(5,15)	(6,17)	(7,16)	(16,2)	(1,0)	(4,1)	(14,13)
(5,15)	(0,11)	(4,1)	(14,13)	(16,2)	(0,8)	O	(7,16)	(6,17)	(12,9)	(5,4)	(12,10)	(7,3)	(6,2)	(1,0)	(16,17)	(14,6)	(4,18)
(6,2)	(14,6)	(1,0)	(0,8)	(14,13)	(16,2)	(12,10)	(6,17)	(5,4)	O	(7,16)	(12,9)	(5,15)	(7,3)	(4,18)	(0,11)	(16,17)	(4,1)
(6,17)	(1,0)	(14,13)	(0,11)	(16,17)	(14,6)	(6,2)	(12,9)	O	(5,15)	(12,10)	(7,3)	(7,16)	(5,4)	(0,8)	(4,1)	(4,18)	(16,2)
(7,3)	(16,17)	(4,18)	(16,2)	(0,8)	(14,13)	(12,9)	(5,4)	(7,16)	(12,10)	(6,17)	O	(6,2)	(5,15)	(4,1)	(14,6)	(0,11)	(1,0)
(7,16)	(4,1)	(16,2)	(16,17)	(14,6)	(0,11)	(5,15)	(12,10)	(12,9)	(7,3)	O	(6,2)	(5,4)	(6,17)	(14,13)	(4,18)	(1,0)	(0,8)
(12,9)	(14,13)	(16,17)	(4,1)	(4,18)	(1,0)	(6,17)	(7,3)	(5,15)	(7,16)	(6,2)	(5,4)	(12,10)	O	(0,11)	(16,2)	(0,8)	(14,6)
(12,10)	(16,2)	(14,6)	(4,18)	(1,0)	(4,1)	(7,16)	(6,2)	(7,3)	(5,4)	(5,15)	(6,17)	O	(12,9)	(16,17)	(0,8)	(14,13)	(0,11)
(14,6)	(12,10)	(6,2)	(5,4)	(6,17)	(7,16)	(16,2)	(1,0)	(4,18)	(0,8)	(4,1)	(14,13)	(0,11)	(16,17)	(7,3)	O	(12,9)	(5,15)
(14,13)	(6,17)	(12,9)	(5,15)	(7,3)	(6,2)	(1,0)	(16,17)	(0,11)	(4,1)	(14,6)	(4,18)	(16,2)	(0,8)	O	(7,16)	(5,4)	(12,10)
(16,2)	(7,16)	(12,10)	(7,3)	(6,2)	(5,15)	(4,1)	(14,6)	(16,17)	(4,18)	(0,11)	(1,0)	(0,8)	(14,13)	(12,9)	(5,4)	(6,17)	O
(16,17)	(12,9)	(7,3)	(7,16)	(5,4)	(6,17)	(14,13)	(4,18)	(4,1)	(16,2)	(1,0)	(0,8)	(14,6)	(0,11)	(5,15)	(12,10)	O	(6,2)

Figura 6. Mecanismo D-H para tecnología ZigBee

por parte de adversarios). (b) Clave de enlace. Proporciona seguridad entre dos y sólo dos dispositivos, se calcula a partir de la clave maestra. Puede ser pre-instalada o distribuida por el Centro de Confianza. (c) Clave de red. Es una clave global utilizada por todos los dispositivos de la red. El Centro de Confianza guarda un conjunto de claves de red y la clave corriente se identifica por un número de secuencia.

ZigBee proporciona cuatro características de seguridad: (i) Mensaje nuevo/no repetido. Los dispositivos ZigBee mantienen contadores para generar marcas de tiempo de treinta y dos bits para entradas y salidas (aproximadamente se repite en 136 años con una tasa de una comunicación por segundo). (ii) Integridad de mensajes. Puede utilizar 0 (no utiliza), 32, 64 o 128 bits para comprobaciones de integridad; por defecto el valor es 64. (iii) Autenticación. A nivel de red se realiza a través de una clave de red común. A nivel de dispositivo se realiza utilizando una única clave de enlace. (iv) Cifrado. ZigBee utiliza el algoritmo de criptografía simétrica AES-128 bits para el cifrado (aunque el algoritmo es robusto, peligro si la implementación tiene bugs). Puede

FIRMA DIGITAL BASADA EN ECDSA PARA ZIGBEE

▪ ALGORITMO ECDSA (ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM):

(1) PROCESO DE GENERACIÓN DE LA FIRMA DIGITAL:

(i) Sea m el mensaje a firmar digitalmente con la *clave privada* de la entidad firmante. Se selecciona una curva elíptica sobre *GF(p)*, por ejemplo: $y^2 = (x^3 + x + 13) \bmod 23$ definida sobre *GF(23)*. Se selecciona un punto G de ella cuyo orden n sea el número de puntos de la curva. Aquí la curva tiene 16 puntos. En este caso: el punto G = (0, 6) cumple *16.G = O*. Por tanto n = 16.

(ii) Sea d la *clave privada* del firmante y Q la *clave pública* del firmante. En este caso: si d = 3 entonces Q = d.G = 3.(0, 6) = (21, 7).

(iii) Se calcula e = HASH(m) donde la función criptográfica HASH puede ser: *SHA-1, SHA-512*, etc. Por ejemplo e = HASH(m) = 2.

(iv) Se selecciona un número entero aleatorio k dentro del intervalo [1, n – 1] por ejemplo k = 3. Se calcula: *k.G = (x1, y1)* y se determina: *r = x1 mod n*. Si *r = 0* entonces se vuelve al punto (iv). En este caso k.G = 3.(0, 6) = (21, 7) = (x1, y1) se calcula r = x1 mod 16 = 5 que es distinto de cero.

(v) Se calcula: $s = k^{-1}.(e + d.r) \bmod n$. Si el resultado *s = 0* se vuelve al punto (iv). En este caso: $s = 3^{-1}.(2 + 3.5) \bmod 16 = 11.(17) \bmod 16 = 187 \bmod 16 = 11$. Como s es distinto de cero, es un valor válido. Por tanto, la *firma digital ECDSA* obtenida es el par de valores enteros: *(r, s) = (5, 11)*.

(2) PROCESO DE VERIFICACIÓN DE LA FIRMA DIGITAL:

(i) Para que el receptor pueda autenticar la firma (r, s) recibida junto al mensaje m del *emisor o firmante* necesita saber la *clave pública del firmante Q*. En este caso: *(r, s) = (5, 11) y Q = (21, 7)*.

(ii) Se verifica que r y s sean números enteros en el intervalo [1, n – 1]. En caso contrario la firma digital no es válida. En este caso es válida.

(iii) Se calcula: *e = HASH(m)*. En este caso: e = 2. Se obtiene: $w = s^{-1} \bmod n$. Aquí: $w = 11^{-1} \bmod 16 = 3$. Se determinan los valores: *u1 = e.w mod n* y *u2 = r.w mod n*. En este caso: u1 = 6, u2 = 15. Se halla: *u1.G + u2.Q = (x1, y1)*. En este caso: 6.(0, 6) + 15.(21, 7) = (21, 7) donde x1 = 21 mod 16 = 5.

(iv) La firma es válida si se cumple que: *x1 = r mod n*. En este caso: 5 = 5 mod 16 → Por tanto *la firma se ha verificado que es válida*.

O	(0,6)	(0,17)	(2,0)	(4,9)	(4,14)	(7,8)	(7,15)	(8,2)	(8,21)	(16,10)	(16,13)	(20,11)	(20,12)	(21,7)	(21,16)
(0,6)	(4,9)	O	(7,15)	(21,7)	(0,17)	(2,0)	(20,11)	(21,16)	(16,10)	(20,12)	(8,2)	(16,13)	(7,8)	(8,21)	(4,14)
(0,17)	O	(4,14)	(7,8)	(0,6)	(21,16)	(20,12)	(2,0)	(16,13)	(21,7)	(8,21)	(20,11)	(7,15)	(16,10)	(4,9)	(8,2)
(2,0)	(7,15)	(7,8)	O	(20,11)	(20,12)	(0,17)	(0,6)	(8,21)	(8,2)	(21,16)	(21,7)	(4,9)	(4,14)	(16,13)	(16,10)
(4,9)	(21,7)	(0,6)	(20,11)	(8,21)	O	(7,15)	(16,13)	(4,14)	(20,12)	(7,8)	(21,16)	(8,2)	(2,0)	(16,10)	(0,17)
(4,14)	(0,17)	(21,16)	(20,12)	O	(8,2)	(16,10)	(7,8)	(20,11)	(4,9)	(21,7)	(7,15)	(2,0)	(8,21)	(0,6)	(16,13)
(7,8)	(2,0)	(20,12)	(0,17)	(7,15)	(16,10)	(4,14)	O	(21,7)	(16,13)	(8,2)	(4,9)	(0,6)	(21,16)	(20,11)	(8,21)
(7,15)	(20,11)	(2,0)	(0,6)	(16,13)	(7,8)	O	(4,9)	(16,10)	(21,16)	(4,14)	(8,21)	(21,7)	(0,17)	(8,2)	(20,12)
(8,2)	(21,16)	(16,13)	(8,21)	(4,14)	(20,11)	(21,7)	(16,10)	(2,0)	O	(0,6)	(7,8)	(20,12)	(4,9)	(0,17)	(7,15)
(8,21)	(16,10)	(21,7)	(8,2)	(20,12)	(4,9)	(16,13)	(21,16)	O	(2,0)	(7,15)	(0,17)	(4,14)	(20,11)	(7,8)	(0,6)
(16,10)	(20,12)	(8,21)	(21,16)	(7,8)	(21,7)	(8,2)	(4,14)	(0,6)	(7,15)	(20,11)	O	(0,17)	(16,13)	(2,0)	(4,9)
(16,13)	(8,2)	(20,11)	(21,7)	(21,16)	(7,15)	(4,9)	(8,21)	(7,8)	(0,17)	O	(20,12)	(16,10)	(0,6)	(4,14)	(2,0)
(20,11)	(16,13)	(7,15)	(4,9)	(8,2)	(2,0)	(0,6)	(21,7)	(20,12)	(4,14)	(0,17)	(16,10)	(8,21)	O	(21,16)	(7,8)
(20,12)	(7,8)	(16,10)	(4,14)	(2,0)	(8,21)	(21,16)	(0,17)	(4,9)	(20,11)	(16,13)	(0,6)	O	(8,2)	(7,15)	(21,7)
(21,7)	(8,21)	(4,9)	(16,13)	(16,10)	(0,6)	(20,11)	(8,2)	(0,17)	(7,8)	(2,0)	(4,14)	(21,16)	(7,15)	(20,12)	O
(21,16)	(4,14)	(8,2)	(16,10)	(0,17)	(16,13)	(8,21)	(20,12)	(7,15)	(0,6)	(4,9)	(2,0)	(7,8)	(21,7)	O	(20,11)

Figura 7 Firma digital basada en ECDSA para ZigBee

hacerse a nivel de red (con clave de red) o a nivel de dispositivo (utilizando una clave de enlace). Existen dos cuestiones de seguridad relacionadas con la actualización de claves. Debido a que ZigBee utiliza dispositivos con recursos limitados, la actualización de la clave tiene que realizarse offline o por el aire, el problema es que en este caso tipo OTA (Over-The-Air) la clave puede transmitirse en texto en claro (las escuchas clandestinas estarán en su salsa). Así mismo la clave se almacena en cualquier dispositivo, por tanto la seguridad física de los dispositivos no puede garantizarse piénsese por ejemplo en las redes de sensores. Un atacante sólo necesita acceso a un dispositivo (incluso un dispositivo final ZigBee) y puede recuperar la clave hackeándolo. En este caso puede reinsertar el dispositivo hackeado en la red (ataque desde dentro) de modo que se gana acceso de forma inherente a la red. Como contramedida: el uso de la clave de enlace en vez de la clave de red puede limitar los ataques desde dentro a los sensores directamente conectados al dispositivo hackeado.

CRIPTOGRAFÍA ASIMÉTRICA RSA BASADA EN CRT PARA TECNOLOGÍA ZIGBEE

- *RSA* es un mecanismo criptográfico asimétrico con dos claves una pública e y otra privada d. Los procesos de *cifrado/descifrado/firma/verificación de firma digital* convencionales ($C = M^e \bmod n$; $M = C^d \bmod n$; $F = M^d \bmod n$; $V = F^e \bmod n$) requieren de *CPUs* de gran rendimiento. Para operar los dispositivos con tecnología ZigBee cuyas *CPUs* son poco potentes requieren reformular *RSA* basándose en el *CRT*.
- *PROCESO DE CREACIÓN DE CLAVES*:
  - Se sintetizan dos números secretos primos muy grandes p y q utilizando un PRNG. Se halla su producto n = (p . q) que se hace público. Donde la función *totem de Euler* es: $\varphi(n) = (p - 1).(q - 1)$.
  - Se sintetiza la *clave privada* que es un número d secreto con $1 < d < \varphi(n)$, donde *mcd (d, $\varphi(n)$) = 1* y se halla la *clave pública*: $e = 1/d \bmod \varphi(n)$. Se cumple que: $d = 1/e \bmod \varphi(n)$.
- *PROCESO DE CIFRADO*: De un mensaje *M* basado en el *CRT* (*Teorema del Resto Chino*) con la clave pública e del receptor. El resultado es un *criptograma o texto cifrado C*:
  - $C_p = (M \bmod p)^{e \bmod (p-1)} \bmod p$; $C_q = (M \bmod q)^{e \bmod (q-1)} \bmod q$
  - $C = [C_q + [(C_p - C_q).(q^{-1} \bmod p) \bmod p].q\,] \bmod n$
- *PROCESO DE DESCIFRADO*: De un texto cifrado C basado en el *CRT* (*Teorema del Resto Chino*) con la clave privada d del receptor. El resultado es un *mensaje o texto en claro M*:
  - $M_p = (C \bmod p)^{d \bmod (p-1)} \bmod p$; $M_q = (C \bmod q)^{d \bmod (q-1)} \bmod q$
  - $M = [M_q + [(M_p - M_q).(q^{-1} \bmod p) \bmod p].q\,] \bmod n$
- *PROCESO DE FIRMA DIGITAL*: De un *documento en claro o cifrado D* basado en el *CRT* (*Teorema del Resto Chino*) con la clave privada d del emisor. El resultado es la *firma digital F*:
  - $F_p = (D \bmod p)^{d \bmod (p-1)} \bmod p$; $F_q = (D \bmod q)^{d \bmod (q-1)} \bmod q$
  - $F = [D_q + [(D_p - D_q).(q^{-1} \bmod p) \bmod p].q\,] \bmod n$

CASO – 1: Cifrar el documento M = 688 si: p = 47, q = 71, e = 79, d = 1019, n = 3337, $\varphi(n) = 3220$. *Solución*: $C_p = (688 \bmod 47)^{79 \bmod 46} \bmod 47 = 688^{33} \bmod 47 = 19$; $C_q = (688 \bmod 71)^{79 \bmod 70} \bmod 71 = 688^{9} \bmod 71 = 8$; $C = [8 + [(11).(71^{-1} \bmod 47) \bmod 47].71\,] \bmod 3337 = [8 + [(11).(2) \bmod 47].71\,] \bmod 3337 = [8 + [1562]] \bmod 3337 = 1570$.

CASO – 2: Firmar el documento M = 2 si: p = 17, q = 31, d = 7, e = 343, n = 527, $\varphi(n) = 480$.

Solución: $F_p = (2 \bmod 17)^{7 \bmod 16} \bmod 17 = 128 \bmod 17 = 9$; $F_q = (2 \bmod 31)^{7 \bmod 30} \bmod 31 = 124 \bmod 31 = 4$; $F = [4 + [(9-4).(31^{-1} \bmod 17) \bmod 17].31\,] \bmod 527 = [4 + [(5).(11) \bmod 17].31\,] \bmod 527 = [4 + (4).(31)] \bmod 527 = 128 \bmod 527 = 128$.

CASO – 3: Descifrar el criptograma C = 106 si: p = 11, q = 13, e = 11, d = 11, n = 143, $\varphi(n) = 120$.

Solución: $M_p = (106 \bmod 11)^{11 \bmod 10} \bmod 11 = 7^1 \bmod 11 = 7$; $M_q = (106 \bmod 13)^{11 \bmod 12} \bmod 13 = 2^{11} \bmod 13 = 2048 \bmod 13 = 7$; $M = [7 + [(7-7).(13^{-1} \bmod 11) \bmod 11].13\,] \bmod 143 = 7 \bmod 143 = 7$.

Figura 8. RSA basada en CRTpar4a tecnología ZigBee

Consideraciones finales.

Nuestro grupo de investigación lleva trabajado más de cinco años en tecnología ZigBee, analizando-evaluando y sintetizando redes WSN (Wireless Sensor Networks) de sensores con tecnología ZigBee utilizadas para numerosas aplicaciones como son la construcción de redes WPAN/WBAN desde la perspectiva de la seguridad-privacidad. Se han sintetizado diferentes contramedidas de seguridad-privacidad.

Este artículo se enmarca en las actividades desarrolladas dentro de LEFIS-Thematic Network.

Bibliografia

-Areitio, J. "Seguridad de la Información: Redes, Informática y Sistemas de Información". Cengage Learning-Paraninfo. 2011.
-Areitio, J. "Identificación de la tecnología firewall para la protección de la seguridad de red". Revista Española de Electrónica. Nº 638. Enero 2008.
-Areitio, J. "Análisis en torno a las tecnologías de privacidad en redes. Anonimato en transmisión de datos". Revista Española de Electrónica. Nº 660. Noviembre 2009.
-Alianza ZigBee: http://www.zigbee.org/
-Pearson, B. "Wireless Network Security. A Beginners Guide". McGraw-Hill Osborne Media. 2011.
-Burmester, M. and Yasinsac, A, "Security Issues in Ad-Hoc Networks". Springer. 2006.
-Cayirci, E. and Rong, C. "Security in Wireless Ad-Hoc and Sensor Networks". Wiley. 2009.
-Holger, K. and Willing, A. "Protocols and Architectures for Wireless Sensor Networks". Wiley-Interscience. Chichester. UK. 2007.
-Nichols, R. and Lekkas, P. "Wireless Security". McGraw-Hill. New York. 2002.
-Goleniewski, L. "Telecommunications Essentials". Addison-Wesley. Boston. MA. 2007.