Ciberseguridad en las comunicaciones inalámbricas en entornos industriales

GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMÍA Y EMPRESA

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

incibe cert_

Marzo 2019

INCIBE_GUIA_SCI_003_ComunicacionesInalambricas_2017_v2

La presente publicación pertenece a INCIBE (Instituto Nacional de Ciberseguridad) y está bajo una licencia Reconocimiento-No comercial 3.0 España de Creative Commons. Por esta razón está permitido copiar, distribuir y comunicar públicamente esta obra bajo las condiciones siguientes:

- Reconocimiento. El contenido de este informe se puede reproducir total o parcialmente por terceros, citando su procedencia y haciendo referencia expresa tanto a INCIBE o INCIBE-CERT como a su sitio web: https://www.incibe.es/. Dicho reconocimiento no podrá en ningún caso sugerir que INCIBE presta apoyo a dicho tercero o apoya el uso que hace de su obra.

- Uso No Comercial. El material original y los trabajos derivados pueden ser distribuidos, copiados y exhibidos mientras su uso no tenga fines comerciales.

Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso de INCIBE-CERT como titular de los derechos de autor. Texto completo de la licencia: https://creativecommons.org/licenses/by-nc-sa/3.0/es/.

Índice

1. Introducción 6
2. Tecnologías inalámbricas más habituales 7
2.1. WiFi 8
2.1.1. Descripción 8
2.1.2. Características de seguridad 9
2.1.3. Uso en sistemas de control industrial 9
2.1.4. Buenas prácticas 9
2.2. Trusted Wireless 10
2.2.1. Descripción 10
2.2.2. Características de seguridad 11
2.2.3. Uso en sistemas de control industrial 11
2.2.4. Buenas prácticas 11
2.3. Bluetooth 11
2.3.1. Descripción 12
2.3.2. Características de seguridad 13
2.3.3. Uso en sistemas de control industrial 13
2.3.4. Buenas prácticas 14
2.4. Zigbee 14
2.4.1. Descripción 15
2.4.2. Características de seguridad 16
2.4.3. Uso en sistemas de control industrial 18
2.4.4. Buenas prácticas 18
2.5. WirelessHART 19
2.5.1. Descripción 19
2.5.2. Características de seguridad 21
2.5.3. Uso en sistemas de control industrial 21
2.5.4. Buenas prácticas 21
2.6. Resumen 22
3. Otras tecnologías inalámbricas 23
3.1. WiMax 23
3.1.1. Descripción 23
3.1.2. Características de seguridad 24
3.1.3. Uso en sistemas de control industrial 25
3.1.4. Buenas prácticas 25
3.2. Redes móviles 26
3.2.1. Descripción 26

3.2.2. Características de seguridad ... 28
3.2.3. Uso en sistemas de control industrial ... 28
3.2.4. Buenas prácticas ... 28
3.3. Radiocomunicaciones ... 29
3.3.1. Descripción ... 29
3.3.2. Características de seguridad ... 30
3.3.3. Uso en sistemas de control industrial ... 30
3.3.4. Buenas prácticas ... 30
3.4. RFID ... 30
3.4.1. Descripción ... 30
3.4.2. Características de seguridad ... 33
3.4.3. Uso en sistemas de control industrial ... 36
3.4.4. Buenas prácticas ... 36
3.5. ISA 100.11a o ISA100 Wireless ... 36
3.5.1. Descripción ... 36
3.5.2. Características de seguridad ... 38
3.5.3. Uso en sistemas de control industrial ... 39
3.5.4. Riesgos y buenas prácticas ... 39
4. Comparación entre las redes inalámbricas industriales y domésticas .. 40
4.1. Uso ... 40
4.2. Componentes ... 41
4.3. Seguridad ... 41
5. Análisis de seguridad en laboratorio ... 43
5.1. WiFi ... 43
5.2. Bluetooth ... 43
5.2.1. Conexión Bluetooth ... 43
5.2.2. Lectura de datos ... 45
5.3. Zigbee ... 47
5.3.1. Escuchas en la red ... 47
5.3.2. Reenvío de paquetes ... 48
5.3.3. Tramas de datos ... 49
5.3.4. Denegación de servicio ... 49
5.3.5. Suplantación vía spoofing ... 51
5.4. WirelessHART ... 52
5.4.1. Captura de información ... 52
5.4.2. Comunicación con el resto de la red ... 52
5.4.3. Denegación de servicio ... 53
Bibliografía ... 54

Índice de figuras

Figura 1: Comparación de aprovechamiento del espectro de frecuencias de varias tecnologías inalámbricas 8
Figura 2: Topologías. Fuente: Industrial Wireless. Transmisión inalámbrica desde el sensor hasta la red. Phoenix Contact 10
Figura 3: Infraestructura de red con sensores de comunicación Bluetooth. Fuente: Industrial Wireless. Transmisión inalámbrica desde el sensor hasta la red. Phoenix Contact 12
Figura 4: Uso de ZigBee en entornos industriales. Fuente: http://www.zigbee.org 15
Figura 5: Infraestructura con dispositivos HART y WirelessHART. Fuente: Industrial Wireless. Transmisión inalámbrica desde el sensor hasta la red. Phoenix Contact 19
Figura 6: Disposición de dispositivos en una red WirelessHART 20
Figura 7: Comparación de características de diferentes tecnologías 22
Figura 8: Red de acceso WiMAX. Fuente: Planificación mediante Atoll de red WiMAX móvil para los centros de la Universidad de Sevilla. 23
Figura 9: Evolución de las redes móviles 26
Figura 10: Uso de tecnologías móviles en los sistemas de control. Fuente: Industrial Wireless. Transmisión inalámbrica desde el sensor hasta la red. Phoenix Contact 27
Figura 11: Cálculo de la altura de la antena según la distancia y la frecuencia de una radiocomunicación 29
Figura 12.- Funcionamiento RFID 31
Figura 13.- Arquitectura ISA100 37
Figura 14: Router WiFi doméstico (izquierda) y router WiFi industrial (derecha). Fuente: http://www.visionsystems.de 41
Figura 15: Establecimiento de la conexión maestro/esclavo 44
Figura 16: Tramas de un proceso de pairing 45
Figura 17: Captura de tramas enviados sin cifrar 46
Figura 18: Captura de tramas enviados con cifrado 46
Figura 19: Red Zigbee del laboratorio. Coordinador (C), Routers (R) y dispositivos finales (E) 47
Figura 20: Replay de trama capturada 48
Figura 21: Petición del parámetro ID con datos sin cifrar 49
Figura 22: Ejemplo de denegación de servicio sobre un nodo en una red ZigBee 50
Figura 23: Router suplantado por un atacante 51
Figura 24: Red WirelessHART del laboratorio 52

Índice de tablas

Tabla 1: Comparación de diferentes tecnologías inalámbricas 7
Tabla 2: Niveles de seguridad ZigBee 18
Tabla 3: Resumen de características del estándar WiMAX 24
Tabla 4: Valores de altura de la antena según la distancia y la frecuencia de una radiocomunicación 30
Tabla 5.- Especificaciones RFID 32
Tabla 6.- Mecanismos de seguridad de RFID 35
Tabla 7.- Suites de cifrado ISA100 38
Tabla 8: Comparativa de uso de tecnologías inalámbricas 40

1. INTRODUCCIÓN

Hoy en día, en un mundo cada vez más interconectado, las tecnologías inalámbricas empiezan a cobrar protagonismo respecto al uso del cable gracias a las ventajas y comodidades que proporcionan. En lo que a entornos industriales se refiere, conceptos como Industria 4.0 y el Internet de las Cosas aplicado a la industria (IIoT) tienen mucho que ver en esta evolución, siendo cada vez mayor la cantidad de dispositivos inalámbricos y la sofisticación de los mismos.

La proliferación de dispositivos móviles como tabletas, PDA o smartphones y su influencia en entornos industriales es una muestra de la evolución que está sufriendo este sector en relación al acceso a la información del proceso industrial. Hoy en día resulta común que esta información esté disponible online en servidores con acceso restringido. El acceso será habitualmente como consulta para verificar valores, pero igualmente, en ocasiones existirá la posibilidad de modificar dichos valores de manera remota y rápida, gracias a las comunicaciones entre máquinas cada vez más inteligentes y a la interconexión de redes de sensores para la obtención de datos.

El uso de tecnologías como ZigBee, WirelessHART o Trusted Wireless entre otros, ya implantados en alguna industria, empieza a consolidarse como soporte para estas nuevas prestaciones.

El objetivo de este estudio es dar a conocer diferentes tecnologías inalámbricas utilizadas en muchas aplicaciones del entorno doméstico pero que se están abriendo paso en los entornos industriales. Además de las características y peculiaridades de cada tecnología, este estudio pretende comprobar la seguridad aplicada en cada uno y proponer contramedidas de tal forma que las comunicaciones se realicen de una manera segura a la vez que se aprovechan las características de seguridad disponibles en los propios protocolos utilizados.

2. TECNOLOGÍAS INALÁMBRICAS MÁS HABITUALES

Las comunicaciones inalámbricas se implantan tanto en la empresa como en la industria por varios motivos, aunque principalmente las razones son la sencillez del despliegue y la reducción de costes. Estos factores hacen que su uso sea cada vez más extendido y que aparezcan modernos protocolos inalámbricos que ofrecen las mismas funcionalidades que las comunicaciones cableadas o incluso superiores.

Los sistemas de control industrial demandan ciertas características de seguridad y robustez tanto físicas como lógicas que las comunicaciones inalámbricas deben satisfacer para contemplar su uso. Las principales son:

- Comunicación fiable y robusta.
- Funciones avanzadas de seguridad.
- Configuración y funcionamiento similares a las herramientas de automatización de uso común.
- Comportamiento en tiempo real y determinista.
- Gran rango de temperatura.
- Convivencia con las tecnologías inalámbricas existentes (sin interferencias).
- Bajo consumo de energía, para ciertas áreas de aplicación.

En la siguiente tabla se describen las características de tecnologías inalámbricas utilizados con frecuencia en entornos industriales y que son deseables:

COMUNICACIONES INALÁMBRICAS EN ENTORNOS INDUSTRIALES

	Bluetooth clásico	Wifi	ZigBee	Bluetooth de baja energía
RENDIMIENTO	Medio	Alto	Malo	Malo
ROBUSTEZ	Alta	Media	Media	Muy buena
RANGO	10-1000 m	50-300 m	10-200 m	10-250 m
DENSIDAD DEL SISTEMA LOCAL	Muy buena	Mala	Buena	Muy buena
ITINERANCIA	Buena	Alta	N/D	N/D
REDES DE GRAN ESCALA	Baja	Media	Muy buena	Buena
BAJA LATENCIA	Excelente	Media	Buena	Muy buena
CREACIÓN DE ARQUITECTURA	Lenta	Media	Muy rápida	Muy rápida
CONSUMO	Bueno	Malo	Muy bueno	Excelente
COSTE	Bajo	Alto	Bajo	Muy bajo

Tabla 1: Comparación de diferentes tecnologías inalámbricas

Por otro lado las bandas de frecuencia empleadas en cada tecnología también es un punto a tener en cuenta cuando se trata de adoptar un medio de comunicación inalámbrico en un sistema industrial que puede ser sensible a interferencias.

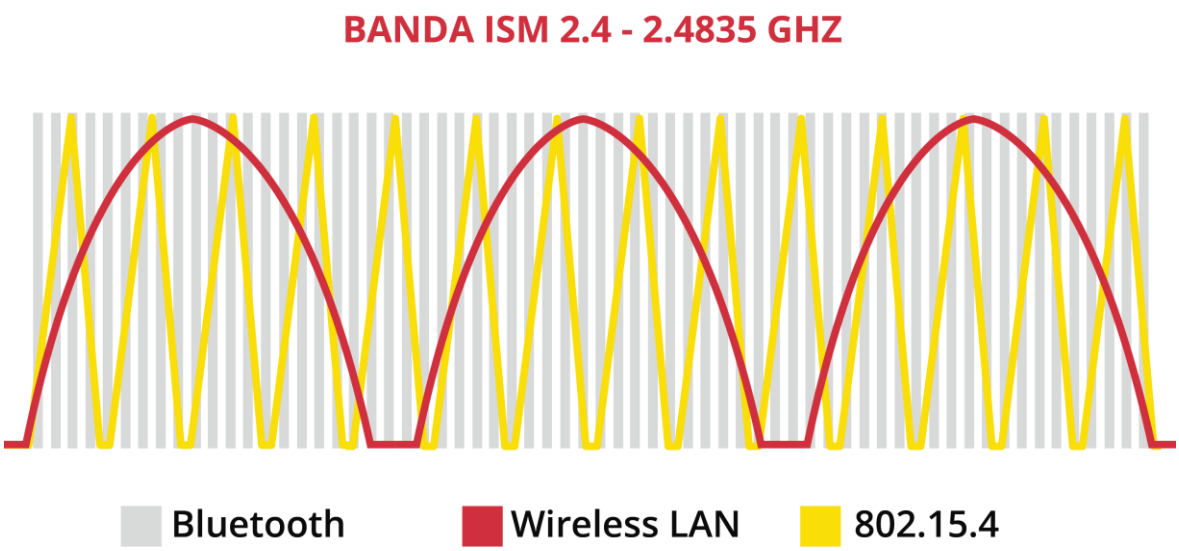

Figura 1: Comparación de aprovechamiento del espectro de frecuencias de varias tecnologías inalámbricas

Todas las tecnologías inalámbricas adecuadas cumplen con los requisitos exigidos por los sistemas de control. Adicionalmente, algunas funcionalidades generales que intrínsecamente aportan los sistemas inalámbricos y que resultan interesantes desde el punto de vista industrial son:

- Mayor movilidad y posibilidad de conectar otros dispositivos como tabletas y teléfonos inteligentes.
- Eliminación de caros y pesados medios de transmisión, como cables de cobre y soportes.
- Comunicación a grandes distancias y donde los cables físicos no pueden utilizarse.
- Flexibilidad para modificar la instalación.
- Escalabilidad.
- Aumento de la seguridad de las personas al no necesitar estar cerca del dispositivo durante la configuración o el mantenimiento.

Una vez expuestas las razones básicas de uso de comunicaciones aéreas en la industria es interesante analizar las características específicas y la seguridad de las principales tecnologías que pueden considerarse aplicables en entornos industriales.

2.1. WiFi

Las redes WiFi son las más utilizadas para el intercambio de datos de todas las redes inalámbricas existentes, tanto en el sector industrial como en el sector corporativo.

2.1.1. Descripción

La tecnología WiFi o WLAN (Wireless Local Access Network) está regulada por el estándar IEEE 802.11 en sus versiones a/b/g/n/ac. Las principales características son:

- Frecuencia de uso en banda libre, situada en 2,4 GHz o 5 GHz.
- Altas velocidades, dependiendo del estándar, que pueden llegar a 300 Mbits/s.

- Rápida itinerancia.
- Proporciona movilidad en redes de gran superficie.
- Alta fiabilidad, mediante el uso de tecnología MiMo (Multiple-input Multiple-output, Múltiple entrada múltiple salida).
- Rango de actuación de 50 metros (5 GHz) a 200 (2,4 GHz), aunque se puede incrementar si es en línea recta visible.
- 23 canales para frecuencia de 5 GHz y 13 canales para 2,4 GHz.
- Alta disponibilidad de productos.

2.1.2. Características de seguridad

La tecnología WiFi permite el cifrado de las comunicaciones. Para ello se han utilizado diversos métodos, que han ido evolucionando para subsanar las debilidades que iban apareciendo en el tiempo. La seguridad de las comunicaciones WiFi puede establecerse:

- **Sin cifrado:** no se establece una contraseña de cifrado en la conexión, por lo que cualquier dispositivo puede unirse y comunicarse. Habitualmente las conexiones WiFi sin conexión se conocen como libres o abiertas.
- **WEP (Wired Equivalent Privacy):** primer mecanismo de cifrado, incluido en el primer estándar IEEE 802.11. Está basado en el algoritmo de encriptación RC4, utilizando una clave secreta de 40 o 104 bits combinada con un Vector de Inicialización (IV) de 24bits; lo que hace un total de 64 o 128 bits. Este método de cifrado está totalmente desaconsejado debido a las vulnerabilidades que presenta y muchos dispositivos ya no permiten su uso por considerarlo vulnerable.
- **WPA (Wi-Fi Protected Access):** desarrollado para solucionar los problemas que presentaba el cifrado WEP, presentaba como característica principal su utilización de un servidor de autenticación (Tipo RADIUS[1] o similar) (WPA-Enterprise) mediante el protocolo EAP. También es posible su uso con claves precompartidas (PSK, Pre-Shared Keys) (WPA-Personal), aunque desciende su seguridad. Incorpora el Protocolo de Integridad de Clave Temporal[2] que se encarga del cambio dinámico de la clave. Opcionalmente es posible utilizar cifrado AES.
- **WPA2 (Wi-Fi Protected Access 2):** es una mejora de WPA que corrige ciertas deficiencias de su predecesor. Utiliza por defecto cifrado AES. En principio es el protocolo de seguridad más seguro para WiFi en este momento.

2.1.3. Uso en sistemas de control industrial

Dentro de las instalaciones industriales es común el uso de WiFi en los centros de control para adquisición, monitorización y configuración; pero también es posible encontrarlo a nivel de campo para control de acciones críticas en tiempo. En ocasiones es necesario utilizar soluciones particulares (software propietario) o realizar un estudio de frecuencias antes de llevar a cabo el despliegue.

2.1.4. Buenas prácticas

Al tratarse de una tecnología bastante conocida, más ligada al mundo de TI que al de TO y del que se han escrito muchos documentos sobre cómo aplicar medidas de seguridad,

[1] https://tools.ietf.org/html/rfc2865

[2] TKIP - Temporal Key Integrity Protocol

no se va a entrar en detalle en este estudio, para, de esta forma, centrarse en otras tecnologías inalámbricas más utilizadas en la industria.

2.2. Trusted Wireless

Trusted Wireless es una tecnología desarrollada específicamente para ser usada en sistemas de control industrial.

2.2.1. Descripción

La versión actual (2.0) presenta las siguientes características:

- Alcance de hasta varios km dependiendo de la frecuencia utilizada.
- Velocidad de datos ajustable (desde 16 hasta 500 kbps).
- Redes malladas con un máximo de 250 nodos.
- Comunicaciones robustas mediante espectro ensanchado por salto de frecuencia3.
- Utiliza la banda de 900 Hz (banda libre en América) o 2,4 GHz (banda libre mundial).

Admite diversas topologías en la arquitectura de su implementación:

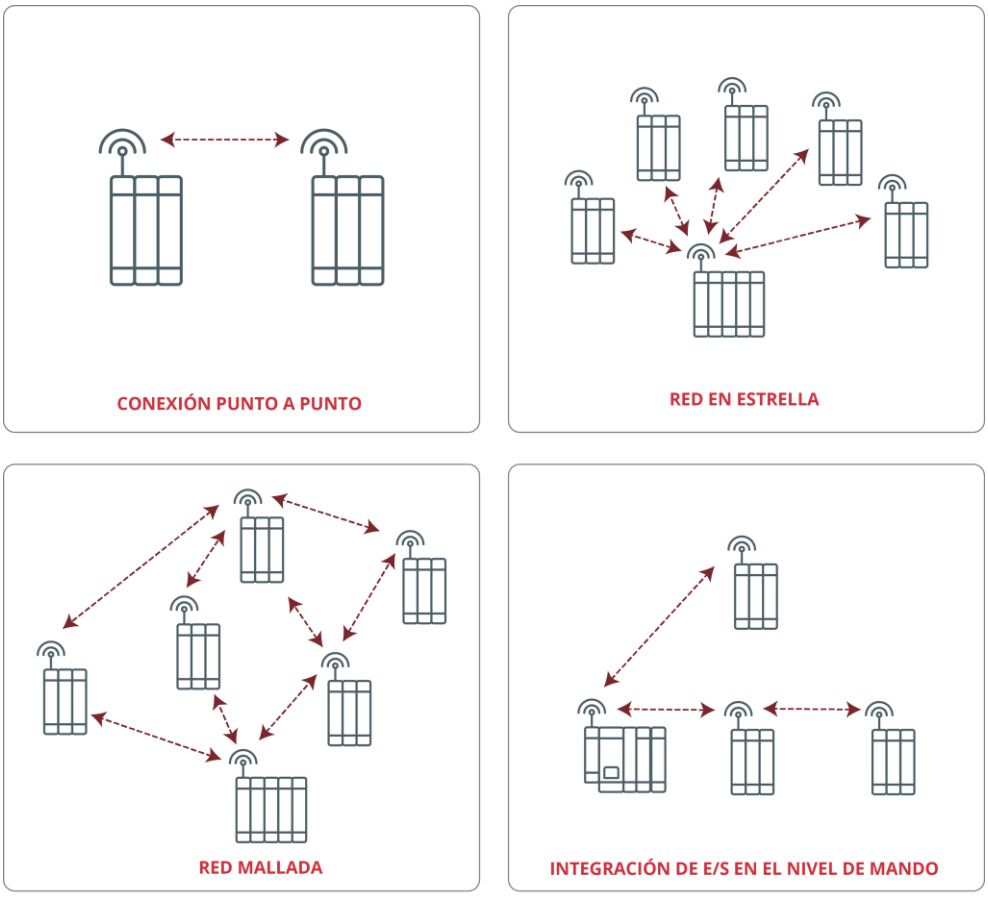

Figura 2: Topologías. Fuente: Industrial Wireless. Transmisión inalámbrica desde el sensor hasta la red. Phoenix Contact

[3] FHSS - Frequency Hopping Spread Spectrum

2.2.2. Características de seguridad

La seguridad de Trusted Wireless se basa en los componentes propietarios y en el salto de frecuencia. No obstante, añade dos características muy importantes:

- Autenticación, de acuerdo a RFC 36104.
- Cifrado AES de 128 bits (Pre Shared Keys).

2.2.3. Uso en sistemas de control industrial

Trusted Wireless se utiliza para transmitir datos y señales a través de grandes distancias dentro del sector industrial. Su uso se centra en:

- Wireless de E/S: señales de E/S analógicas y digitales capturadas por los dispositivos.
- Wireless Serial: envío de datos serie, RS232, RS485, provenientes de otros equipos, mediante la conversión de los mismos a Trusted Wireless.

Trusted Wireless ofrece un alto grado de fiabilidad, robustez, seguridad y flexibilidad.

2.2.4. Buenas prácticas

En el caso de Trusted Wireless, se trata de una tecnología robusta en su diseño que usa saltos en canales de frecuencia y permite el cifrado de las comunicaciones mediante AES de 128 bits.

Hay que tener en cuenta que esta tecnología se basa en una especificación privada, algo que era bastante frecuente hace años en el campo de los sistemas de control industrial, lo que hace que no esté sometido al mismo nivel de pruebas por parte de la comunidad como otros tecnologías con especificaciones públicas.

2.3. Bluetooth

Bluetooth es una tecnología que comenzó a desarrollarse en el año 1994 por Ericsson como sustituto del cable. Para su comunicación utiliza la FHSS.

[4] CBC-MAC (CCM) - Cipher Block Chaining - Message Authentication Code (Counter with CBC-MAC)

2.3.1. Descripción

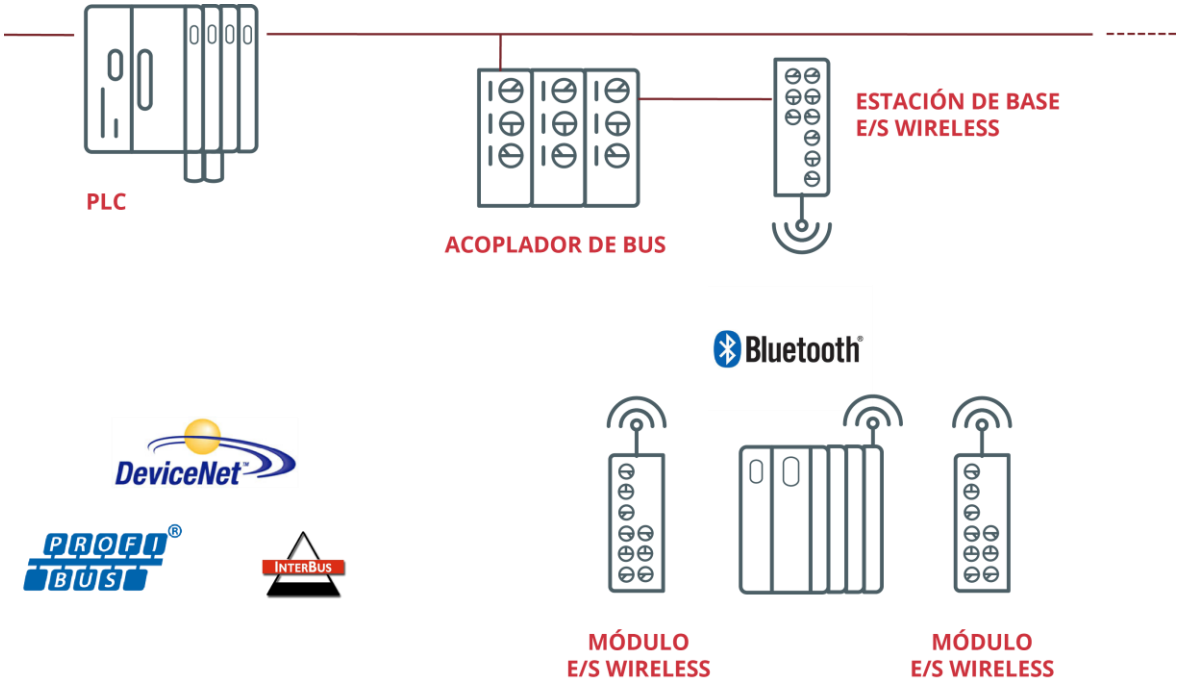

Figura 3: Infraestructura de red con sensores de comunicación Bluetooth. Fuente: Industrial Wireless. Transmisión inalámbrica desde el sensor hasta la red. Phoenix Contact

La tecnología Bluetooth se rige por la norma IEEE 802.15.1. Existen dos especificaciones de la tecnología:

- Bluetooth clásico: es una tecnología específica para dispositivos con alta demanda de pequeñas transmisiones, bajo consumo de energía y que sean rentables.
- Bluetooth de baja energía: esta tecnología es ideal para aplicaciones que requieren la comunicación de pequeñas cantidades de datos de forma puntual o periódica.

La tecnología Bluetooth destaca por las siguientes características:

- Distancia de comunicación de hasta 1 km (en línea recta sin obstáculos).
- Uso de frecuencia libre de 2,4 GHz.
- Transmisión de alta fiabilidad mediante canales de transmisión redundantes.
- Tiempo de retardo reducido (5-10 ms).
- Capacidad para funcionar en entornos con gran cantidad de dispositivos debido a su aprovechamiento de la frecuencia.

Centrándonos en las dos tecnologías de Bluetooth, las características más importantes de cada una de ellas son:

- Bluetooth clásico:
    - Transmisión rápida y cíclica de pequeños paquetes de datos.
    - Transmisiones de hasta 780 kbit/s.
    - Gran cantidad de dispositivos conectados en el mismo entorno de radio funcionando sin interferencias.
    - Alta disponibilidad en productos de consumo.

- Bluetooth de baja energía:
  - Permite un gran número de nodos de comunicación con requisitos de latencia limitados.
  - Muy bajo consumo de energía.
  - Robustez igual a la tecnología Bluetooth clásica.
  - Poca latencia, si el número de nodos conectados no es elevado.
  - Tiempo muy breve para despertar o reconectar.

2.3.2. Características de seguridad

Las características de seguridad que incorpora Bluetooth son similares a las de otras tecnologías inalámbricas. Se destacan:

- Cifrado de 128 bits.
- Robustez, dada mediante:
  - Salto de frecuencia adaptable (AFH)[5].
  - Corrección de errores hacia adelante (FEC), que permite al receptor corregir errores en la trasmisión sin necesidad de reenvíos.
  - Canales con frecuencia estrechas, lo que implica menos interferencias de otros dispositivos.
  - Baja sensibilidad a las reflexiones o múltiples rutas.

La seguridad de Bluetooth puede tiene varios modos de funcionamiento:

- ***Sin seguridad.*** Todos los mecanismos de seguridad (autenticación y cifrado) están deshabilitados. Los dispositivos permiten que todos los demás dispositivos se puedan comunicar con ellos.

- ***Seguridad en el nivel de servicios.*** La seguridad es inicializada después de establecerse un canal entre el nivel LM (Link Manager) y el de L2CAP. Las políticas de seguridad y los niveles de confianza se aplican de forma independiente, permitiendo accesos de aplicaciones con diferentes requerimientos.

- ***Seguridad en el nivel de enlace.*** Todas las rutinas están dentro del chip Bluetooth y nada es transmitido en claro. La seguridad es inicializada antes de establecerse un canal y todas las comunicaciones son cifradas. Además del cifrado de comunicaciones, utiliza una clave de enlace secreta compartida (PIN) entre los dos dispositivos de la comunicación y seguridad a nivel de MAC. Esta metodología consiste en compartir una clave de enlace (Link Key) secreta entre un par de dispositivos, cada vez que se comunican por primera vez.

2.3.3. Uso en sistemas de control industrial

El uso de la tecnología Bluetooth en sistemas de control industrial se centra en el intercambio de datos tanto a bajo nivel como a alto nivel. Así lo podemos encontrar en:

- E/S Wireless: señales de E/S analógicas y digitales.
- Wireless Serial: datos serie RS-232 y RS-422/485.

[5] Utiliza el mismo sistema que FHSS

- Wireless Ethernet: intercambio de datos Ethernet.

La tecnología de Bluetooth clásica está más orientada hacia la integración dispositivos de automatización en redes serie y de campo, sin embargo la tecnología de baja energía está pensada para sensores, actuadores o pequeños dispositivos que requieren capacidades de consumo realmente pequeñas.

2.3.4. Buenas prácticas

Tras las pruebas realizadas, se concluyen las siguientes prácticas de seguridad a la hora de utilizar la tecnología Bluetooth en cualquier dispositivo:

- Uso de cifrado en las comunicaciones en cuanto sea posible. El uso de LTK[6] permite una transmisión de comunicaciones cifrada entre el maestro y el esclavo desde el primer momento. Todos los dispositivos de una red de control que utilicen este protocolo deberían hacer uso de LTK.
- No aceptar conexiones de dispositivos desconocidos. Activar en el maestro la opción de listas blancas y requerir de un emparejamiento con clave de al menos 5 caracteres, evitando así que dispositivos maliciosos puedan conectarse sin permiso previo.
- Revisar periódicamente la lista de dispositivos de confianza registrados para evitar la incorporación de dispositivos maliciosos.
- Asignar un nombre a los dispositivos que no refleje información extra como puede ser la marca y el modelo del dispositivo, o la ubicación y servicio del mismo. Con esta práctica se evitará que posibles atacantes se aprovechen de vulnerabilidades conocidas asociadas a ciertos dispositivos para perpetrar ataques dirigidos.
- Mantener la configuración del dispositivo en modo invisible para no ser detectado por otros dispositivos de forma fácil.

Con estos consejos, se dificultan ataques como:

- Descubrimiento de dispositivos ocultos.
- Interceptación de comunicaciones.
- Inyección de tramas.
- Explotación de vulnerabilidades conocidas.
- Asociación de dispositivos maliciosos a la red.

2.4. Zigbee

ZigBee es una tecnología desarrollada por la ZigBee Alliance7 que adopta el estándar IEEE 802.15.4 para las capas bajas del modelo OSI, es decir, la capa física (PHY) y la subcapa de acceso al medio (MAC); y agrega la capa de red y de aplicación.

---

[6] http://www.fte.com/webhelp/sodera/Content/Documentation/Sodera/Help/ConfigurationSettings/IOConfigurationSettings/DatasourceLEEncryption.htm

[7] http://www.zigbee.org/

2.4.1. Descripción

La principal característica de ZigBee es su bajo consumo de energía, que hace que sea muy adecuado para dispositivos cuyo funcionamiento no dispone de suministro eléctrico continuo y requiere del uso de baterías externas. Estos dispositivos pueden funcionar hasta más de 2 años mediante pilas.

Las características adquiridas por ZigBee al adoptar el estándar IEEE 802.15.4 son las siguientes:

- Tasa de transmisión desde 20 kbit/s hasta 250 kbit/s dependiendo de la frecuencia.
- Uso de frecuencias en banda libre: 2.4 GHz (al igual que WiFi), 915MHz y 868 MHz.
- Dispone de 1, 10 o 16 canales de 5 MHz dependiendo de su frecuencia.
- Corto alcance, excluyendo la funcionalidad de malla entre 10 y 200 metros.

Figura 4: Uso de ZigBee en entornos industriales. Fuente: http://www.zigbee.org

En una red ZigBee se distinguen tres tipos diferentes de comportamientos para los dispositivos:

- **Dispositivo final:** responde a las peticiones de descubrimiento de dispositivos enviando su propia dirección IEEE o la dirección NWK (depende de la petición) y no posee la capacidad de enrutar paquetes. Este tipo de dispositivos deben actuar siempre a través de su nodo padre, ya sea este un coordinador o un router. Normalmente estos dispositivos van alimentados a baterías.
- **Router:** responde a peticiones enviando su dirección IEEE o NWK y las direcciones IEEE o NWK de todos los dispositivos que tiene asociados como router ZigBee (dependiendo de la petición) manteniendo información sobre la red para determinar la mejor ruta para transmitir un paquete de información. Este componente ha de

poder unirse a una red Zigbee antes de poder actuar como retransmisor de paquetes de otros routers o dispositivos finales.

- **Coordinador:** es el nodo de la red que tiene la única función de formar parte de una red responsabilizándose de establecer el canal de comunicaciones y el identificador de red (PAN ID) para toda la red. Responde a la petición enviando su dirección IEEE o NWK y las direcciones IEEE o NWK que tiene asociadas como coordinador ZigBee (dependiendo del tipo de petición). Una vez creada la red el Coordinador hace las funciones de router participando en el enrutado de paquetes. El coordinador también interviene en funciones relacionadas con la gestión de la seguridad de las comunicaciones actuando como Centro de Confianza (Trust Center).

2.4.2. Características de seguridad

La seguridad de las transmisiones y de los datos son puntos clave en la tecnología ZigBee. Por ello ZigBee utiliza el modelo de seguridad de la subcapa MAC IEEE 802.15.4, la cual especifica 4 servicios de seguridad:

- Uso de cifrado AES 128bits: ZigBee usa criptografía de clave simétrica y además permite la rotación de claves de red, lo que aporta un nivel extra de seguridad en el intercambio de información evitando así que dispositivos ajenos a la red puedan unirse a ella.
- Control de accesos de los dispositivos, mantiene una lista de los dispositivos 'comprobados' en la red.
- Integración de tramas para proteger los datos de ser modificados por otros.
- Secuencias de refresco, para comprobar que las tramas no han sido reemplazadas por otras. El controlador de red comprueba estas tramas de refresco y su valor, para ver si son las esperadas.

En ZigBee, las claves son la base de la arquitectura de seguridad y por ello, la protección de las mismas es fundamental. Para entender un poco más esta arquitectura, a continuación se describen brevemente las claves de 128 bits utilizadas en la misma:

- **Clave maestra (master key):** clave desde la cual se generan las diferentes claves de enlace. La seguridad de toda la red depende de ella ya que los distintos servicios utilizarán variaciones unidireccionales de la clave de enlace para evitar riesgos de seguridad. Dada la importancia de esta clave, la clave maestra inicial ha de obtenerse por medios seguros ya sea por transporte o por preinstalación.
- **Clave de enlace (link key):** dotan de seguridad las comunicaciones punto a punto a nivel de aplicación. Es una clave sólo conocida por los elementos que participan en una comunicación concreta.
- **Clave de red (network key):** clave utilizada a nivel de red y conocida por todos los elementos pertenecientes a ésta.

Las claves se pueden obtener de 3 métodos diferentes:

- **Preinstalación:** el fabricante incluye la clave en el propio dispositivo. En algunos casos el usuario puede seleccionar alguna de las claves instaladas mediante un conjunto de jumpers en el dispositivo en aquellos en los que se haya preinstalado más de una, pero sólo una estará activa en cada momento. Este método sólo es utilizado para la incorporación de claves maestras.

- **Transporte de clave:** el dispositivo hace una petición a un centro de confianza (Trust Center) para que le envíe una clave. El centro de confianza representa para el resto de dispositivos el origen de confianza encargado de realizar la distribución de las claves de seguridad. El centro de confianza tiene 2 modos de operación:
  - *Modo comercial:* el propio centro de confianza mantiene una lista de dispositivos, claves maestras, claves de enlaces y claves de red. En este modo, el espacio de memoria que se requiere en el centro de confianza, aumenta con la cantidad de dispositivos asociados a la red.
  - *Modo residencial:* la clave de red es la única que es obligatoria mantener en el Centro de Confianza. La memoria requerida para el almacenamiento de claves es independiente del tamaño de la red.
- **Establecimiento de clave:** es un método para generar claves al azar para dos dispositivos sin necesidad de comunicarlos. Este servicio ZigBee se basa en el protocolo SKKE (Symmetric-Key Key Establishment). Los dispositivos destino de la clave deben disponer de una clave común, llamada clave maestra, que pudo haber sido asignada de acuerdo al método de preinstalación o transporte de clave.

Con las características de seguridad ofrecidas, ZigBee proporciona dos niveles de seguridad para su infraestructura:

- **Seguridad standard (standard security mode):** destinado a instalaciones residenciales en las cuales no existe criticidad de la información. Los dispositivos se comunican entre sí y con el Centro de Confianza empleando la clave de red, que puede estar pre-instalada u obtenerse mediante transporte, en este caso sin seguridad adicional.
- **Alta seguridad (high security mode):** destinado a aplicaciones comerciales. Los dispositivos pueden comunicarse mediante clave de red o clave de enlace, de modo que el Centro de Seguridad debe mantener una lista de todas estas claves y realizar las operaciones de transporte y establecimiento. La clave de red puede ser cambiada periódicamente, de forma automática, por el Centro de Confianza. La clave de enlace con el Centro de Confianza puede estar pre-instalada u obtenerse mediante establecimiento a través de la clave maestra, que a su vez puede estar re-instalada u obtenerse mediante transporte, en este caso sin seguridad adicional.

La especificación aclara que el modo de alta de seguridad debe cumplir con todas las características que lo definen, mientras el modo standard puede implementar algunas características del modo superior.
Dependiendo del hardware ZigBee puede haber limitaciones respecto a la aplicación de modos de seguridad, permitiendo el modo sin seguridad o el modo estándar en hardware normal; mientas que el hardware denominado PRO permite aplicar cualquier modo de seguridad o utilizar el modo sin seguridad.

Nivel	Nombre	Cifrado	Integridad
0	None		
1	MIC-32		X
2	MIC-64		X
3	MIC-128		X
4	ENC	X	
5	ENC-MIC-32	X	X
6	ENC-MIC-64	X	X
7	ENC-MIC-128	X	X

Tabla 2: Niveles de seguridad ZigBee

La integridad del mensaje se verifica mediante un MIC (Message Integrity Code, código de integridad del mensaje).

2.4.3. Uso en sistemas de control industrial

Esta tecnología se utiliza principalmente en aplicaciones como la monitorización del consumo energético, recopilación de datos de procesos y automatización de edificios. Habitualmente son los pequeños sensores los que trabajan con esta tecnología, haciendo de coordinador de la infraestructura un dispositivo como una RTU o un PLC, que serán los encargados de procesar la información.

2.4.4. Buenas prácticas

A lo largo de las pruebas desarrolladas dentro del estudio se ha podido comprobar la robustez de ZigBee gracias a la configuración y uso de buenas prácticas como las que se comentan a continuación:

- Uso de listas blancas para el acceso de los dispositivos a la red ZigBee evitando así ataques como DoS, DDoS, suplantación de dispositivos, etc.
- Utilización de un cifrado AES 128 bits (el más robusto de los definidos en el estándar IEEE 802.15.4) usando criptografía de clave simétrica que además permite la rotación periódica de claves de red, lo que aporta un nivel extra de seguridad en el intercambio de información y evita así que dispositivos ajenos a la red puedan unirse a ella.
- Uso de la característica de integridad que posee el protocolo ZigBee para la comprobación de tramas como contramedida al reemplazo de las mismas por un posible atacante.

2.5. WirelessHART

WirelessHART se basa, al igual que ZigBee, en el estándar IEEE 802.15.4 y se utiliza para la conexión inalámbrica de dispositivos de campo HART en la industria.

2.5.1. Descripción

La tecnología WirelessHART se desarrolló entre 2004 y 2007 y su función es la de proporcionar comunicaciones inalámbricas a dispositivos que utilizan el protocolo HART. En el año 2010 fue aprobado como estándar IEC 62591.

Las características que definen a esta comunicación son:

- Transmisión confidencial y a prueba de manipulación.
- Alta fiabilidad gracias al enrutamiento Full-Mesh.
- Consumo energético muy bajo gracias a la comunicación sincronizada.
- 2,4 GHz.
- 15 canales de emisión.

Dentro de las características operativas de la tecnología, también se distinguen las siguientes ventajas frente a medios cableados:

- Menos autorizaciones y retrasos.
- Utilización de las mismas herramientas de mantenimiento y diagnóstico que con los dispositivos HART tradicionales cableados.
- No requiere una amplia planificación o estudio de las emisiones de radio.

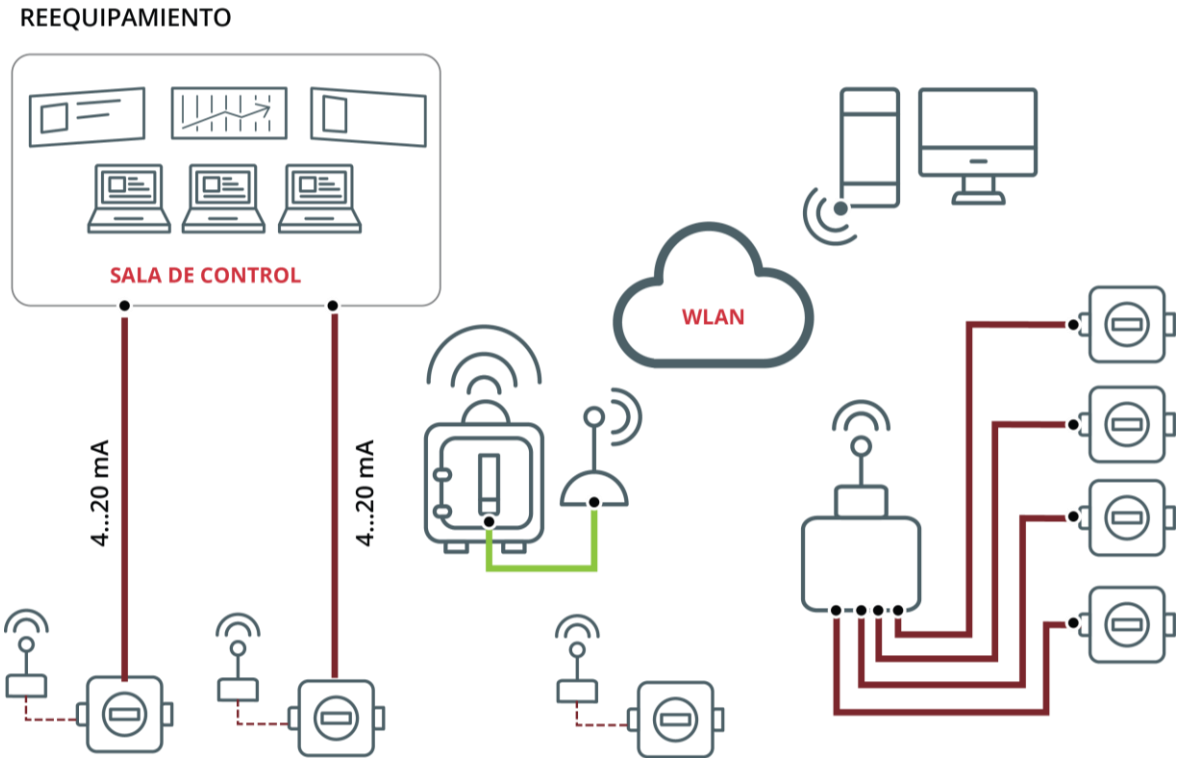

Figura 5: Infraestructura con dispositivos HART y WirelessHART. Fuente: Industrial Wireless. Transmisión inalámbrica desde el sensor hasta la red. Phoenix Contact

La especificación de WirelessHART define los siguientes dispositivos:

- **Dispositivos de red**:
  - **Dispositivos de campo**: sensores y actuadores comunicados mediante WirelessHART. Tienen capacidades para enrutar paquetes de otros dispositivos.
  - **Dispositivos de** mano: dispositivos para interactuar en el Sistema. Utilizados por los operadores.
- **Routers o repetidores**: dispositivo encargado únicamente de redirigir paquetes. En general estos equipos no son necesarios puesto que cualquier dispositivo de campo puede realizar esta función.
- **Adaptadores**: permite unir dispositivos HART a la red WirelessHART. Dispone de una interfaz cableada y una interfaz inalámbrica. Debe de ser capaz de interpretar el material de seguridad para equipamientos anteriores a la especificación HART 7.
- **Gateway**: encargado de conectar la red WirelessHART con otras redes. Es el punto único de conexión con la red WirelessHART.
- **Punto de acceso**: es el encargado de proporcionar la red inalámbrica. Se comunica directamente con el Gateway. Varios puntos de acceso pueden comunicarse con el Gateway.
- **Gestor de red** (Network Manager): mantiene y actualiza las rutas, contiene el listado de dispositivos y gestiona el ancho de banda.
- **Gestor de seguridad** (Security Manager): es el encargado de la creación y gestión de las claves utilizadas por la red para cifrar la comunicación.

No todos los dispositivos son obligatorios y deben estar presentes en todas las redes, sino que se utilizarán según sean las necesidades. Los dispositivos Gateway, punto de acceso, gestor de red y gestor de seguridad pueden estar integrados en un único dispositivo físico.

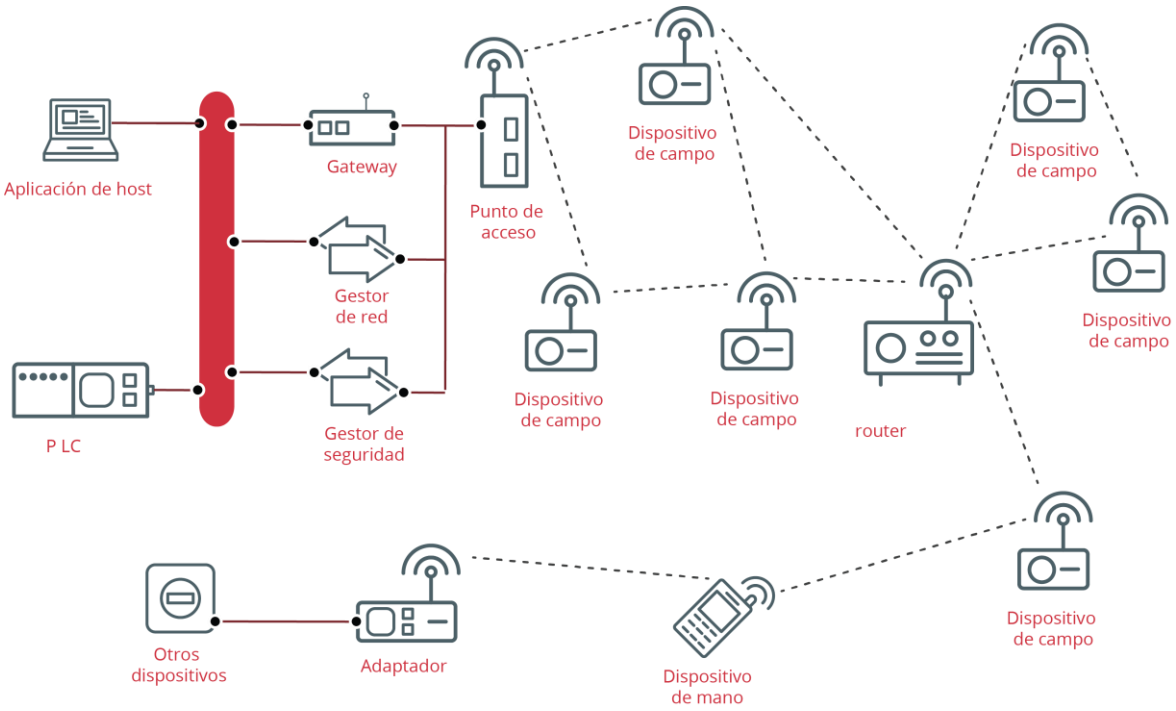

Figura 6: Disposición de dispositivos en una red WirelessHART

2.5.2. Características de seguridad

WirelessHART, como tecnología de nueva generación, ya incorpora medidas de seguridad para proteger la información y el acceso a la red.

- Las medidas de seguridad que aporta son:
  - Cifrado mediante AES de 128 bits.
  - Clave de cifrado única para cada mensaje.
  - Autenticación de dispositivos e integridad de los datos.
  - Rotación de las claves de cifrado utilizadas para unirse a la red.
  - Varios niveles de seguridad, con un mínimo siempre activado.
  - Salto de canales.
  - Potencia de emisión ajustable.
  - Varios niveles de claves de seguridad para el acceso.
  - Indicación de intento de acceso a la red fallido.
  - Reporte de fallos de integridad de mensajes.
  - Reporte de fallos de autenticación.

2.5.3. Uso en sistemas de control industrial

El uso de WirelessHART dentro de los sistemas de control industrial es exclusivo para el envío de señales definidas en el protocolo HART. Entre los sistemas que utilizan esta tecnología se puede destacar:

- Monitorización de equipamiento médico.
- Monitorización del medio ambiente, gestión de la energía.
- Entornos de condiciones extremas (alta corrosión, inundación, etc.).
- Equipamiento rotatorio.

2.5.4. Buenas prácticas

Cuando se use WirelessHART, se recomiendan las siguientes prácticas de seguridad corroboradas durante el estudio realizado:

- Por defecto, todo dispositivo WirelessHART requiere de una contraseña conocida como clave de unión (Join Key) para poder unirse a una red. La contraseña tiene que configurarse en el dispositivo antes de su asociación a la red, puesto que es necesaria para el intercambio de paquetes de control con el Gateway de la red.
- Como el uso de una única contraseña no es recomendable puesto que esta contraseña es la que se utiliza en todas las comunicaciones de tipo broadcast, lo que significa que su uso en la red es elevado. La alternativa es el uso de listas de control de acceso (ACL – Access Control List). Estas ACL controlaran el acceso a la red y funciona gracias a la comprobación por parte del Gateway del origen del paquete (mediante MAC o número de serie del emisor).
- Mezclar la opción de clave común y, una vez asociado el dispositivo a la red, crear una lista de control de accesos. Una vez que los dispositivos están asociados a una red pueden comunicarse entre ellos o con el Gateway. Las comunicaciones entre dos dispositivos son también permitidas, pudiendo utilizar una clave especifica. La negociación de esta clave se lleva a cabo con el Gateway, que la distribuirá a los dos dispositivos para que la usen en la comunicación entre ellos, que ya no dependerá del Gateway.

2.6. Resumen

WiFi, Trusted Wireless, Bluetooth, Zigbee y WirelessHART son las tecnologías más extendidas en implantaciones de comunicaciones inalámbricas que afectan al sector industrial. Dependiendo del propio sector, del entorno físico, de las necesidades del proceso y su criticidad y, sobre todo teniendo en mente la seguridad requerida, es necesario realizar un análisis concienzudo para evaluar pros y contras que determinen la mejor opción a escoger para un determinado sector.
Seguridad aparte, el siguiente diagrama permite visualizar en conjunto las capacidades de cada tecnología.

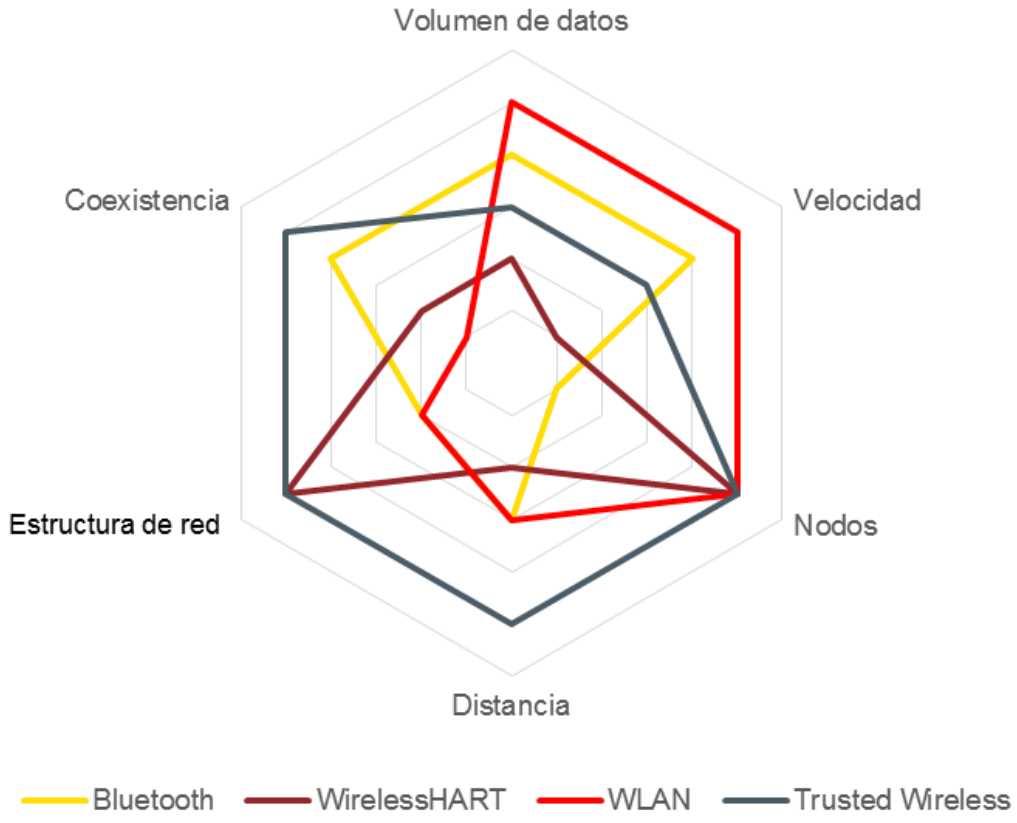

Figura 7: Comparación de características de diferentes tecnologías

Según se muestra en la Figura 7, por ejemplo, WirelessHART es una tecnología que soporta muchos nodos con varias estructuras de red, a cambio, la distancia soportada es pequeña, al igual que la velocidad; por el contrario, WLAN permite altos volúmenes de datos, velocidad y nodos, pero baja coexistencia con otras redes.

3. OTRAS TECNOLOGÍAS INALÁMBRICAS

Aparte de las tecnologías inalámbricas de uso más extendido descritos en el punto anterior, es interesante considerar otras tecnologías que si bien no tienen el mismo calado en entornos industriales, si resultan alternativas interesantes en ciertos sectores con necesidades especiales.

3.1. WiMax

La tecnología inalámbrica WiMAX (Worldwide Interoperability for Microwave Access) se encuentra dentro de las llamadas tecnologías de última milla que permite la recepción de datos por microondas y retransmitirlos por ondas de radio.

3.1.1. Descripción

Las redes WiMAX surgieron como una alternativa al cable para llevar las comunicaciones a zonas rurales aisladas a las cuales resultaba muy costoso la infraestructura física. Con esta tecnología se reducen los equipamientos y el impacto ambiental en zonas rurales, al ser necesarios solamente antenas, muchas veces situadas en ubicaciones compartidas con antenas de televisión o telefonía móvil.

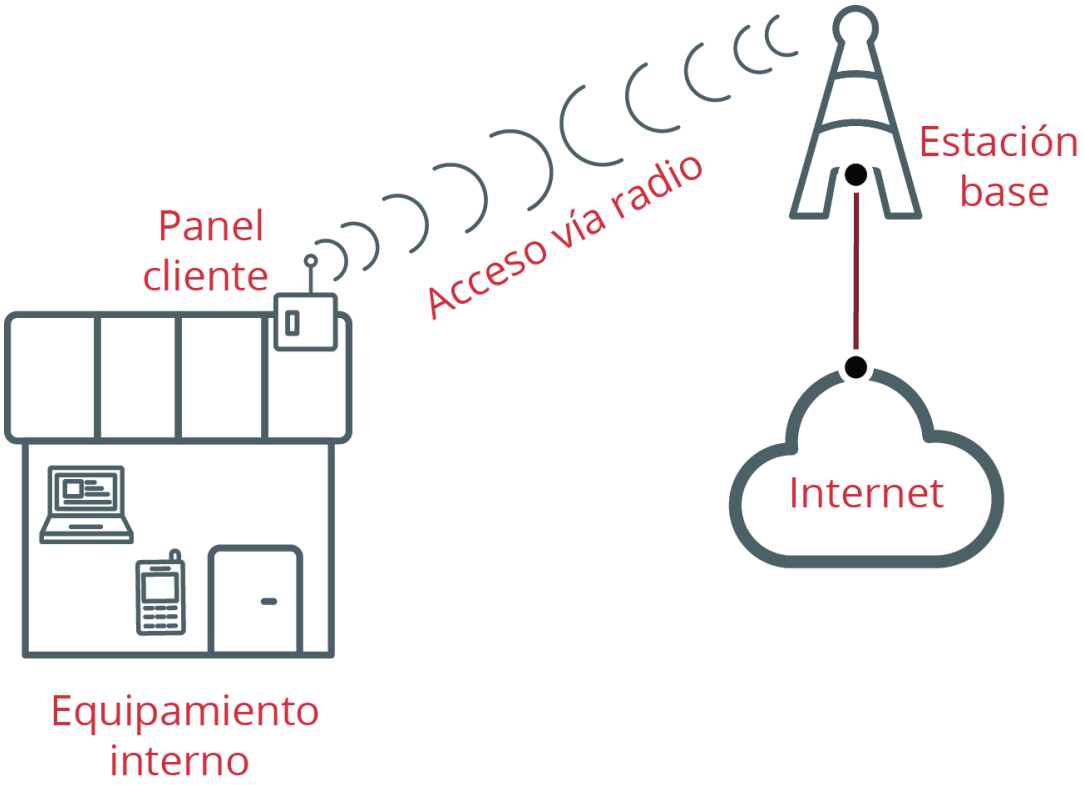

Figura 8: Red de acceso WiMAX. Fuente: Planificación mediante Atoll de red WiMAX móvil para los centros de la Universidad de Sevilla.

WiMAX posee diferentes ventajas entre las que destacan los servicios de banda ancha que ofrece en zonas donde el despliegue de cable o fibra presenta unos costos por usuario muy elevados (zonas rurales) por la baja densidad de población. Esta tecnología de comunicaciones adopta el estándar IEEE 802.16 y existen 2 variantes:

- WiMAX (802.16d-2004) o "WiMAX fijo": para zonas de baja densidad de población.
- WiMAX (802.16e-2005) o "WiMAX móvil": para aplicaciones que requieran gran ancho de banda en ambos sentidos de transmisión y en movilidad.

En la siguiente tabla se pueden observar una comparación de las características de WiMAX fijo frente a WiMAX móvil:

	802.16d	802.16e
ESPECTRO	<11 GHz - Típicamente 3.5 GHz	<6 GHz - Inicia en 2.5 GHz
FUNCIONAMIENTO	Sin visión directa (NLOS)	Sin visión directa (NLOS)
TASA DE BIT	Hasta 75 Mbit/s con canales de 20 MHz	Hasta 15 Mbit/s con canales de 5 MHz
MODULACIÓN	OFDM con 256 subportadoras QPSKI 16QAM	SOFDMA9 con 512 o 1024 subportadoras
MOVILIDAD	Sistema fijo	Sistema móvil
ANCHOS DE BANDA	Seleccionables entre 1,25 y 20 MHz	Igual que 802.16d con los canales de subida para ahorrar potencia
RADIO DE CELDA TÍPICO	5-10 km aprox. (alcance típico máximo de unos 50 km)	2-5km aprox.

Tabla 3: Resumen de características del estándar WiMAX

3.1.2. Características de seguridad

WiMAX define una subcapa de seguridad dedicada específicamente a cubrir los tres principios básicos de la seguridad en redes (Confidencialidad, Autenticación e Integridad) para proporcionar a los usuarios una navegación lo más segura posible dentro de su red.

WiMAX basa su sistema de seguridad en dos principios:

- **Autenticación:** este método garantiza a los usuarios el acceso seguro a la red, evitando que otros usuarios no autorizados hagan uso de la conexión inalámbrica. En el estándar IEEE 802.16-2009 se definen dos procesos de autenticación:
  - **OSA (Open System Authentication):** el cliente realiza una solicitud de autenticación asociada a su dirección MAC, tras esta petición, sigue una respuesta de la *Estación Base* (BS) con la aceptación o denegación de la petición. La BS realiza únicamente y de forma opcional un filtrado por dirección MAC.
  - **SKA (Shared Key Authentication):** es utilizado en procesos de claves compartidas, donde ambos extremos deberán conocer dichas claves para garantizar una autenticación más segura. Para la autenticación mediante claves compartidas WiMAX define el protocolo PKM (Privacy Key Management) para que una *Estación de Usuario* (SS) pueda intercambiar claves y obtener la autorización de la Estación Base. Además de esta tarea, el protocolo PKM también se encarga del refresco de las claves, la re-autorización periódica, etc. A continuación se describe el proceso que sigue el protocolo PKM para realizar la autenticación entre la BS y la SS.

- **Cifrado:** después de que la Estación Base autorice a la Estación de Usuario, es necesarios también un mecanismo de cifrado para velar por la confidencialidad e integridad de los datos que se comparten entre ambos. Para ello, la SS envía a la BS una solicitud de claves de cifrado llamadas TEK (Traffic Encryption Keys), que son enviadas por la BS en un mensaje de respuesta. Estos mensajes a su vez están cifrados con una clave conocida por ambas partes. El algoritmo empleado para el cifrado de las TEK puede ser de 3 tipos: *3DES (Triple Data Encryption Standard)*, *AES (Advanced Encryption Standard)* y *RSA (Rivest, Shamir y Adleman)*.
  Una vez conocidas las TEK, se pueden emplear diversas técnicas para el cifrado de datos: CBC (DES), CBC (AES), CTR (AES), CCM (AES).
  Algunas de las ventajas que poseen los mecanismos de cifrado que implementa WiMAX con respecto a otras tecnologías son las siguientes:
  - Algoritmos robustos.
  - Permite realizar un cifrado independiente para cada flujo de datos.
  - Soporta generación de claves dinámicas con tiempos de vida variables.

Por otro lado, independientemente de los mecanismos de cifrado y autenticación, el propio diseño de la tecnología WiMAX implica un valor añadido en cuestiones de seguridad:

- WiMAX no está diseñada como una red local de acceso al usuario final, sino que se diseñó como una tecnología MAN/WAN de operador, que tiene la capacidad de poder interconectar a muchos usuarios que necesariamente no tienen por qué conocerse. Al ser una red de gran escala, la propia tecnología se diseñó para poder velar por la seguridad con total garantía.
- El acceso a la red no es aleatorio, sino completamente determinista y regido por una Estación Base que actúa en todo momento como controlador de las transmisiones.

3.1.3. Uso en sistemas de control industrial

Las redes WiMAX pueden tener muchas utilidades prácticas para todo tipo de entidades, empresas o negocios. En entornos industriales poseen las siguientes características:

- Acceso a una red inalámbrica en naves industriales o a lo largo de todo el terreno perteneciente a la empresa.
- Conexión a Internet sin ningún tipo de cable con un pc, portátil, PDA o teléfono móvil.
- Servicio de Hotspot para acceso restringido por tiempo o volumen.
- Acceso a servicios VoIP sin cables que permite una comunicación entre diferentes puestos dentro de una planta industrial.

3.1.4. Buenas prácticas

Las redes WiMAX presentan debilidades de seguridad[8] que pueden corregirse con una configuración adecuada y la aplicación de algunas recomendaciones de seguridad:

- Desarrollar una política de seguridad robusta y aplicarla. Una política de seguridad se encarga del diseño, implementación y mantenimiento de tecnologías de

[8] NIST SP 800-127: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-127.pdf

seguridad adecuada. Los dispositivos de la red WiMAX deben ser configurados para cumplir con la política.

- Evaluar las contramedidas antes de su utilización. Algunos productos WiMAX emplean módulos criptográficos que cumplen determinadas normativas (Como la FIPS[9] americana). Al integrar los productos WiMAX certificados con otras soluciones de seguridad debe tenerse en cuenta que no siempre las certificaciones se extienden a toda la solución final. Las organizaciones deben trabajar en estrecha colaboración con los proveedores de WiMAX para conocer mejor las posibles limitaciones de configuración de la red.
- Requerir la autenticación mutua para dispositivos. La función de autenticación mutua está soportada pero no activada por defecto. Deben utilizarse dispositivos capaces de utilizar protocolos de autenticación confiables, como EAP. En caso de no ser posible, entonces debe aplicarse seguridad a las capas superiores utilizado más cifrado o soluciones VPN.
- Implementar algoritmos de cifrado para proteger las comunicaciones de datos. WiMAX presenta mensajes de gestión y de datos, pero el cifrado no se aplica a los mensajes de gestión para incrementar la eficiencia de las operaciones de la red, mientras que los mensajes de datos se cifran de forma nativa.

3.2. Redes móviles

Los teléfonos móviles, teléfonos inteligentes y tabletas se están haciendo cada día más imprescindibles. Su uso dentro de los sistemas de control también se ha incrementado para facilitar algunas tareas. Pero las comunicaciones móviles son solo se utilizan con estos dispositivos, comunicaciones punto a punto también son posibles con esta tecnología.

3.2.1. Descripción

Entre las redes móviles se distinguen varios tipos de tecnología diferentes a lo largo de los años.

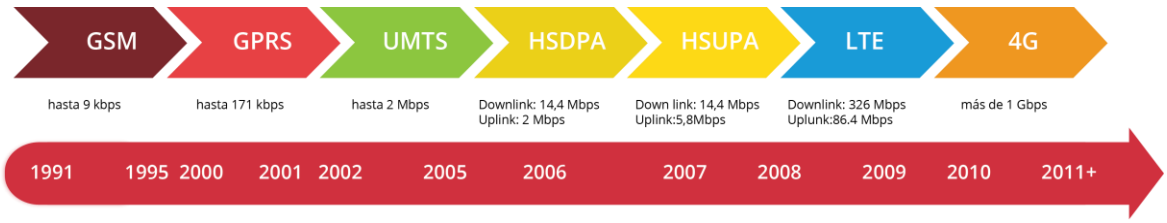

Figura 9: Evolución de las redes móviles

Principalmente, para la comunicación de mensajes y eventos se han venido utilizando dos tipos de tecnología: GSM y 3G (UMTS y HSDPA)

[9] http://csrc.nist.gov/publications/PubsFIPS.html

La tecnología GSM se basa en un sistema abierto para la comunicación móvil internacional utilizado en más de 200 países. Las principales características son:

- Alcance extensible según necesidad, mediante la utilización de antenas o repetidores.
- Velocidades de datos hasta 210 kbits/s.
- Varias bandas de frecuencias: 850, 900, 1800 y 1900 MHz.

3G designa los estándares de telefonía de la tercera generación. Comparado con su predecesor aumentaron notablemente sus prestaciones. Las características más notables son:

- Gran alcance, extensible mediante la utilización de antenas o repetidores.
- Altas velocidades de datos hasta 7,2 Mbits/s.
- Dos frecuencias: 900 y 2100 MHz.

Figura 10: Uso de tecnologías móviles en los sistemas de control. Fuente: Industrial Wireless. Transmisión inalámbrica desde el sensor hasta la red. Phoenix Contact

3.2.2. Características de seguridad

Las características de seguridad también han ido evolucionando al mismo nivel que la tecnología, cambiando algoritmos de cifrado y añadiendo nuevas medidas de seguridad.

La tecnología GSM ofrece:

- Autenticación de la Identidad del usuario.
- Confidencialidad de la Identidad del usuario.
- Confidencialidad de los datos de señalización.
- Confidencialidad de los datos del usuario.

Todas estas medidas de seguridad se realizan a nivel hardware mediante sistemas de cifrado de clave simétrica y con los algoritmos A3, A5 y A8, considerados hoy en día inseguros.

Las redes 3G ofrecen mayor grado de seguridad en comparación con sus predecesoras 2G. Entre las características más destacadas están:

- Autenticación de la red.
- Seguridad extremo a extremo.
- Sustitución del cifrador de flujo A5/1 (vulnerable) por KASUMI (hoy en día también vulnerable).

3.2.3. Uso en sistemas de control industrial

El uso de las redes móviles en sistemas de control depende de la tecnología utilizada.

La tecnología GSM, al poseer menores capacidades de transferencia de información se utiliza en el envío de señales de campo o eventos de poca transferencia de datos.

- E/S Wireless: señales de E/S analógicas y digitales.
- Wireless Serial: datos serie RS-232.
- Wireless Ethernet: datos Ethernet.
- Señalización de alarmas: SMS y correo electrónico.

Las tecnologías 3G mejoraron las capacidades de GSM, por lo que su uso en sistemas de control industrial se reserva para niveles con necesidades más altas.

- Wireless Ethernet: transmisión Ethernet a alta velocidad.
- Señalización de alarmas: SMS y correo electrónico.

3.2.4. Buenas prácticas

Las redes móviles utilizadas en los sistemas de control no difieren de las utilizadas en la vida doméstica o empresarial, por lo que las recomendaciones de seguridad a aplicar en estas redes son las mismas en todos los casos. Así, las recomendaciones más importantes son:

- Deshabilitar las redes 2G (GSM, GPRS y EDGE): por defecto son redes inseguras. Si ha de realizarse cualquier tipo de envío de información por estas redes hay que asegurarse de que ha sido cifrado previamente.
- El algoritmo A5/3 usado en UMTS es inseguro. Existen tablas de contraseñas para romper el algoritmo, por lo que se debe tratar de no usar tampoco la tecnología UMTS.

3.3. Radiocomunicaciones

Las tecnologías de radioenlace se utilizan para comunicaciones a largas distancias. Entre los radioenlaces más comunes están las comunicaciones vía satélite, las microondas y los radioenlaces terrestres.

3.3.1. Descripción

Los sistemas de radiocomunicaciones se caracterizan por disponer de un elemento emisor, otro receptor y, en ocasiones, elementos repetidores.

Los repetidores pueden ser de dos tipos:

- Pasivos: se comportan como espejos que reflejan la señal. Su misión suele ser librar obstáculos, habitualmente montes y colinas, situándose en su cima a la vista del emisor y el receptor.
- Activos: su función característica es la regeneración de la señal. La señal que llega, generalmente bastante atenuada se regenera para ser enviada hacia otra antena o hacia el receptor.

Las características que definen este tipo de comunicaciones son:

- Rango de frecuencias entre 1 y 300 GHz.
  - Dependiendo del espectro concreto se tratará de radio enlace o de enlace de microondas.
  - Las principales frecuencias son 12 GHz, 18 y 23 GHz.
- Distancias por encima de 50 km, dependiendo de la frecuencia utilizada.
- Pérdidas. Las radiocomunicaciones se ven afectadas por los fenómenos meteorológicos, aparte de otras pérdidas intrínsecas a la física de las ondas debidas a difracción, reflexión, etc.

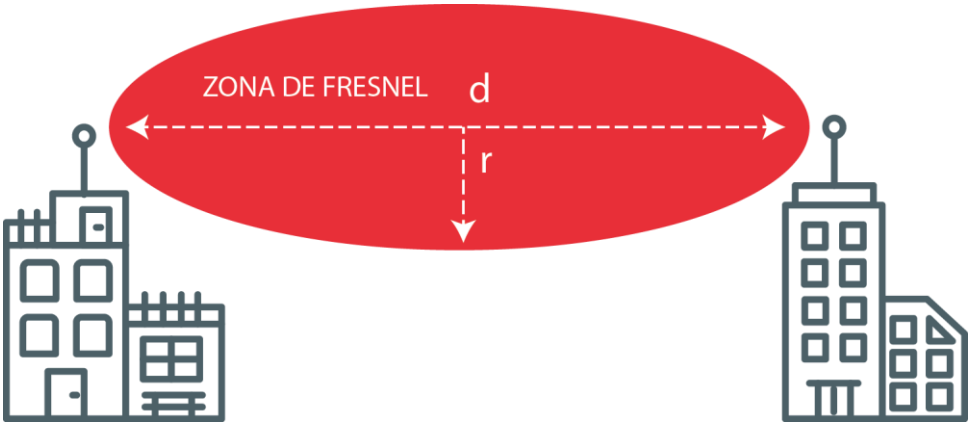

Figura 11: Cálculo de la altura de la antena según la distancia y la frecuencia de una radiocomunicación

Distancia de la conexión inalámbrica (d)	Altura de la antena (r) 2.4GHz	Altura de la antena (r) 5GHz
200 m	1,5 m	1,5 m
500 m	4 m	2,5 m
1000 m	5 m	4 m
2000 m	8 m	6 m
4000 m	11 m	8 m

Tabla 4: Valores de altura de la antena según la distancia y la frecuencia de una radiocomunicación

3.3.2. Características de seguridad

Por definición, las radiocomunicaciones no definen métodos de seguridad para sus transmisiones.

3.3.3. Uso en sistemas de control industrial

La utilización de los sistemas de radiocomunicación en los sistemas de control industrial se centra en el envío de grandes cantidades de información, habitualmente sin restricciones temporales, entre diferentes instalaciones distantes de la empresa.

3.3.4. Buenas prácticas

El principal problemas de las comunicaciones vía radio es la extensión de la zona de recepción de los mensajes, por lo que será necesario tomar medidas de seguridad en ese aspecto.

- Autenticación: las comunicaciones vía radioenlace suelen ser punto a punto, por lo que una autenticación de extremos es un proceso sencillo que va a impedir que otros elementos se unan a la red.
- Cifrado: por definición la mayoría de protocolos utilizados en radio enlace no utilizan cifrado, por lo que es necesario aplicarlo previamente a la comunicación.

3.4. RFID

Radio-Frequency IDentification (RFID) es una tecnología de identificación y captura de datos automáticos (*Automatic Identification and Data Capture*, AIDC), que se basa en campos eléctricos o magnéticos de frecuencia de radio para transmitir información.

3.4.1. Descripción

La tecnología RFID puede utilizarse para identificar, ubicar, clasificar o detectar una amplia variedad de objetos.

Un sistema RFID se compone de un máximo de tres subsistemas:

- Subsistema RF: que lleva a cabo la identificación y las transacciones relacionadas con el uso de la comunicación inalámbrica.
- Subsistema empresarial: donde se ejecuta el software especializado que puede almacenar, procesar y analizar los datos obtenidos de las operaciones del subsistema RF.
- Subsistema inter-empresarial: que se conecta a los subsistemas de la empresa cuando la información tiene que ser compartida.

A su vez, el subsistema RF consta de dos componentes:

- Etiquetas RFID (tags), son pequeños dispositivos electrónicos que se colocan en los objetos. Cada etiqueta tiene un identificador único y también puede tener otras funciones tales como memoria para almacenar datos adicionales y mecanismos de seguridad.
- Lectores RFID (interrogador), son dispositivos que se comunican con las etiquetas vía radio para identificar el objeto conectado a cada etiqueta y, posiblemente, asociar el objeto etiquetado con los datos relacionados.

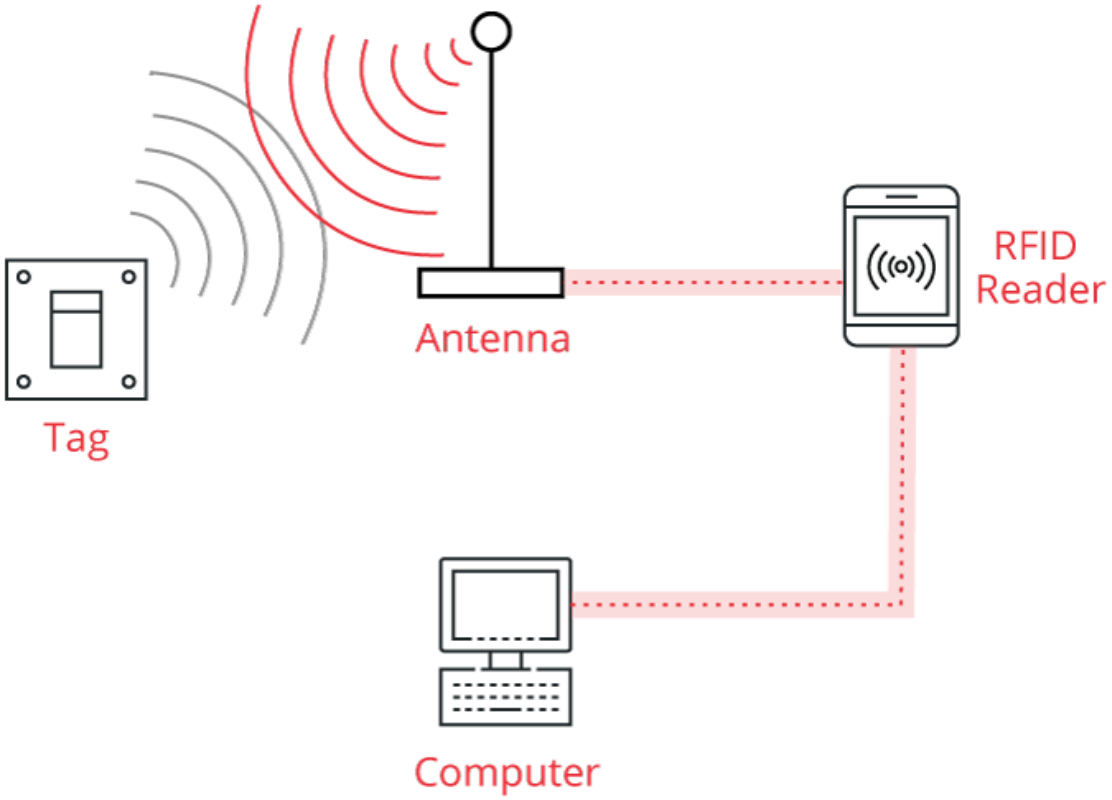

Figura 12.- Funcionamiento RFID

Para poder armonizar el desarrollo de productos basados en RFID se constituyó una organización denominada EPCglobal[10], cuyo objetivo es orientar la adopción de un sistema

[10] https://www.gs1.org/epcglobal

como estándar mundial para ser usado en la identificación inmediata de productos dentro de las cadenas de abastecimiento de cualquier empresa en cualquier lugar del mundo.

En el 2005, EPCglobal publicó las especificaciones de la última versión de EPC (Electronic Product Code), el EPC Class 1 Generation 2, versión 1.0.9. La versión fue presentada a la ISO con la intención de que se convirtiera en parte de la serie ISO - 18000 del estándar RFID, como el ISO18000 - 6C.

Características	Class 1 Gen 1	Class 1 Gen 2
Longitud del código	64/96 bits	96/256 bits
Ratio de lectura	Hasta 25 etiquetas/segundo.	Hasta 880 etiquetas/segundo (US FCC). Hasta 450 etiquetas/segundo (EU ETSI) Velocidad adaptable según el ruido del entorno en que se trabaja.
Velocidad de escritura	3 etiquetas/segundo.	Mínimo 5 etiquetas/segundo.
Verificación de datos de etiqueta	16-bit CRC (Lectura).	16-bit CRC (Lectura/Escritura).
Modo de lector	US-FCC: Salto de frecuencias EU ETSI: Escuchar después de hablar.	US-FCC: Salto de frecuencias EU ETSI: Escuchar después de hablar.
Seguridad	Contraseñas de 8 bits, kill sin bloqueo después de las preguntas incorrectas.	Contraseñas de 32 bits, bloqueo y kill.
Expansión	Código de identificación de producto de 96 bits.	Código de identificación de producto de 512 bits. Memoria de usuario ilimitada según tipo de tag.

Tabla 5.- Especificaciones RFID

3.4.2. Características de seguridad

Los objetivos de seguridad que proporcionan los sistemas RFID son la confidencialidad, la integridad, la disponibilidad y el no repudio.

Para ello se han considerado controles de seguridad que se dividen en tres grupos:

- En el grupo gestión se define la política de uso de la tecnología RFID, la política de seguridad TI para el subsistema RFID y el subsistema empresarial, y la reducción al mínimo de los datos sensibles almacenados en las etiquetas.
- En el grupo operacional se define el control de acceso físico, la colocación adecuada de etiquetas y lectores, la eliminación de las etiquetas y la no revelación del formato del identificador.
- Existen controles técnicos para todos los componentes de los sistemas RFID. Los tipos generales de control para el subsistema RF incluyen control para proporcionar servicios de autenticación e integridad de las transacciones y componentes RFID, para proteger la comunicación RF entre el lector y la etiqueta y los datos almacenados en las etiquetas.

Estándar RFID	Características			Mecanismos de seguridad	
	Banda	Alcance (m)	Datos	Confidencialidad / anonimato	Integridad
EPCglobal Class 0	UHF	3	64 o 96 bits programados desde fábrica.	"Reader Singulate Tags" usando un número aleatorio generado automáticamente.	Se usan bits de paridad y CRC para la detección de errores.
EPCglobal Class 1 Generation 1	UHF	3	64 o 96 bits programados desde fábrica.	No	El comando *lock* protege permanente contra escritura de memoria. Detección de errores CRC. Los comandos son enviados con 5 bits de paridad.
EPCglobal Class 1 Generation 2	UHF	3	Soporta identificadores de hasta 496 bits, memoria definida por el usuario, y memoria R/W.	El lector dirige la etiqueta usando un número aleatorio de 16 bits.	Pueden bloquearse áreas de memoria para proteger contra escritura de memoria. Pueden bloquearse de forma permanente áreas de memoria. Detección de errores CRC.
ISO/IEC 18000-2	LF	<0.010	ID de 64 bits, memoria R/W hasta 1 KB.	No	Pueden bloquearse de forma permanente áreas de memoria. Detección de errores CRC.

ISO/IEC 18000-3 con dos modos definidos.	HF	<2	ID de 64 bits, memoria R/W.	Modo 2 tiene 48 bits de protección de contraseña en comando *Read.*	Pueden bloquearse de forma permanente áreas de memoria. Modo 2 tiene un puntero de bloqueo que almacena la dirección de memoria. Esta característica protege la escritura de todas las áreas de memoria que se encuentran debajo de la dirección almacenada. Modo 2 tiene 48 bits de protección de contraseña en comando *Write*. Detección de errores CRC.
ISO 11784/11785	LF	<0.010	ID de 64 bits.	No	Detección de errores CRC.
ISO/IEC 14443	HF	0.07 a 0.15	Tipo A: ID de 32, 56, o 80 bits. Tipo B: ID de 32 bits.	No	Detección de errores CRC.
ISO/IEC 15693	HF	1	ID de 64 bits, memoria R/W hasta 8 KB.	No	El comando *lock* protege de forma permanente contra escritura de memoria.

Tabla 6.- Mecanismos de seguridad de RFID

3.4.3. Uso en sistemas de control industrial

La tecnología RFID es utilizada en la industria gracias a que funciona con normalidad en los entornos ambientales más adversos, así como también permite el almacenamiento de más información que otras tecnologías similares y una lectura más rápida de la información almacenada. Dentro de la industria 4.0 la tecnología RFID es utilizada para diversos aspectos:

- Controlar los procesos de la línea de producción.
- Automatizar el proceso de identificación de herramientas.
- Mantenimiento de las herramientas utilizadas en el proceso.
- Control de acceso.

3.4.4. Buenas prácticas

Además de los distintos mecanismos de seguridad que se implementan en los distintos estándares de RFID, se recomienda:

- Identificación. Se han de identificar todos los objetos etiquetados con etiquetas RFID para concienciar a los usuarios de la presencia de la tecnología y por lo tanto un mayor control sobre el acceso a los mismos.
- Destrucción de las etiquetas. Una vez finalizado el uso de las etiquetas se han de destruir para evitar el acceso a las mismas.
- Jaulas de Faraday y bloqueadores de tarjetas. Utilizando estos dispositivos podemos asegurarnos de que ningún lector accede a las tarjetas, mientras se encuentren en su radio de acción.

3.5. ISA 100.11a o ISA100 Wireless

ISA100 Wireless es un estándar internacional (IEC 62734) que define un método de comunicación inalámbrica bajo IPv6 para el internet de las cosas industrial (*Industrial Internet of Things*, IIoT). Adopta el estándar IEEE 802.15.4 para las capas bajas del modelo OSI, es decir, la capa física (PHY) y la subcapa de acceso al medio (MAC) y agrega la capa superior de enlace y la de aplicación.

3.5.1. Descripción

Las características adquiridas por ISA100 Wireless al adoptar el estándar IEEE 802.15.4 son las siguientes:

- Tasa de transmisión desde 20 kbit/s hasta 250 kbit/s dependiendo de la frecuencia.
- Uso de frecuencias en banda libre: 2.4 GHz (al igual que WiFi), 915MHz y 868 MHz.
- Dispone de 1, 10 o 16 canales de 5 MHz dependiendo de la frecuencia utilizada.
- Corto alcance, excluyendo la funcionalidad de malla, entre 10 y 200 metros.

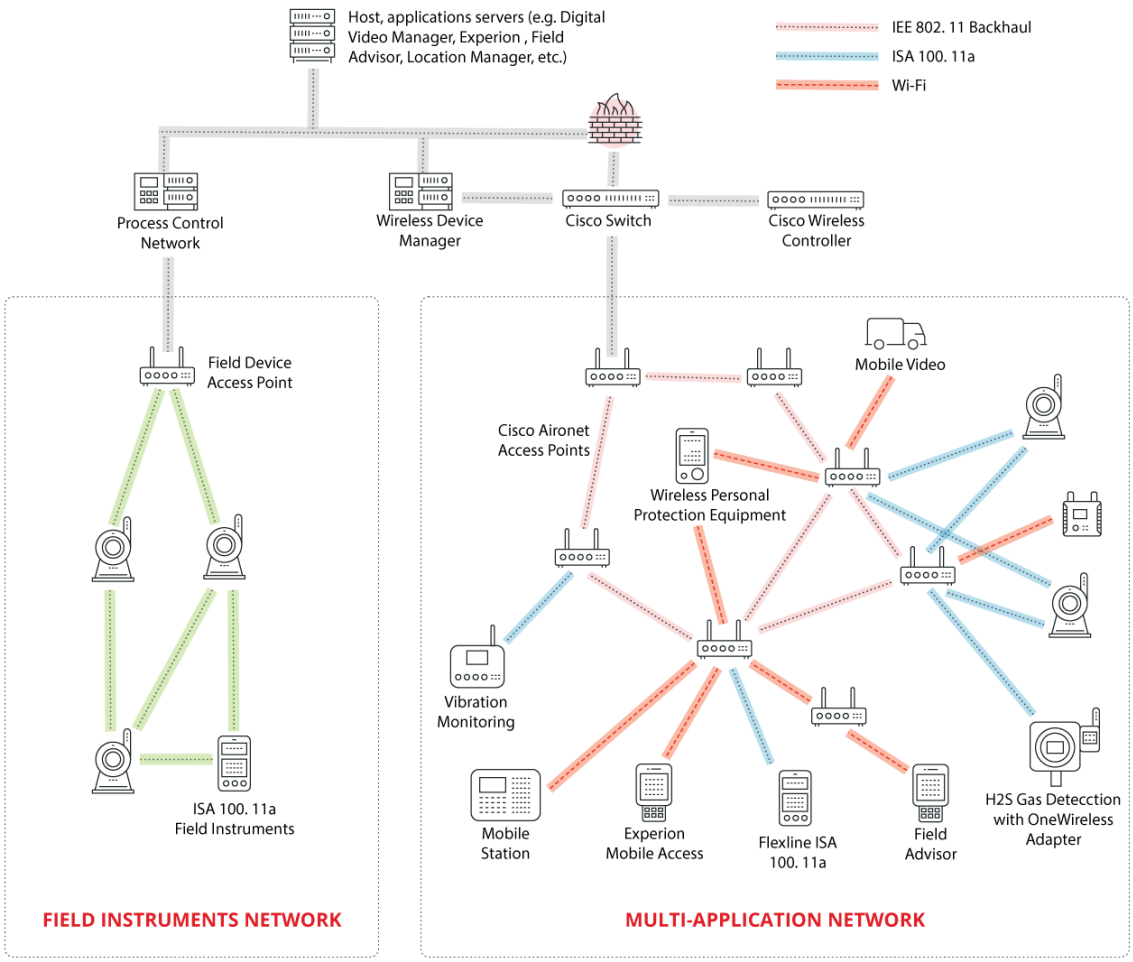

Figura 13.- Arquitectura ISA100

Los dispositivos en las redes ISA100 Wireless pueden tener diversas funciones según su rol, pudiendo implementar uno o varios de estos roles:

- Dispositivos finales: fuentes o consumidores de datos. No enrutan, son los dispositivos de entrada/salida.
- Router: es el dispositivo encargado de enrutar los mensajes de los otros dispositivos que operan dentro de la subred inalámbrica.
- Router troncal: es el dispositivo responsable de la traducción de direcciones, la expansión de paquetes y de enrutar los mensajes a la red troncal. Reduce el tráfico entre los dispositivos que operan en la subred inalámbrica y los dispositivos que operan en la red troncal.
- Administrador de sistema: conocidos como los "cerebros" de la red, son los equipos encargados de administrar todos los dispositivos de red. Para ello utilizan configuraciones controladas por políticas basadas en la recopilación de parámetros de rendimiento de los dispositivos.
- Administrador de seguridad: es el dispositivo encargado de habilitar, controlar y supervisar el funcionamiento de manera segura de todos los dispositivos presentes en la red.
- Gateway: proporciona una interfaz de aplicación entre la red inalámbrica y la red de la planta.

- Dispositivos de configuración: son los encargados del aprovisionamiento de las configuraciones requeridas para el funcionamiento dentro de la red.
- Dispositivo de tiempo: responsable de proporcionar la fuente de tiempo principal de la red.

Por otro lado, en las comunicaciones ISA100 Wireless:

- La capa de red está basada en el estándar 6LoWPAN el cual es un estándar que permite comunicaciones IPv6 en redes IEEE 802.15.4.
- El envío de los mensajes es realizado mediante paquetes UDP.
- No es necesario que la red troncal implemente direccionamiento IP.
- Se permite un PDU de aplicación de hasta 1280 bytes.
- Se implementa un mecanismo de fragmentación y desfragmentación de paquetes.
- Se incluye un mecanismo opcional de recuperación de paquetes.

3.5.2. Características de seguridad

El estándar ISA100 Wireless incorpora una metodología de seguridad de dos capas.

- Capa de enlace. En la capa de enlace la seguridad está asociada con una autenticación salto a salto y cifrado.
  - Salto a salto: las subredes inalámbricas son multisalto, los paquetes de datos se enrutan a través de la malla de subredes habilitada sobre múltiples dispositivos hasta el punto de extracción de la subred.
  - Cifrado: cada router autentica y cifra/descifra los paquetes que él enruta.
- Capa de transporte. En la capa de transporte la seguridad está asociada con una autenticación extremo a extremo y cifrado de los mensajes de datos.
  - El dispositivo origen autentica y cifra el paquete en la capa de transporte y solo el destino es capaz de autenticar y descifrar el paquete.
  - Esto se logra a través de sesiones que se establecen entre pares de dispositivos que envían mensajes a la capa de transporte.

Se pueden habilitar varios niveles de autenticación y cifrado para ambas capas. Estos niveles se heredan de las políticas de seguridad admitidas por el estándar IEEE 802.15.4. Las políticas de seguridad con material criptográfico permiten niveles de seguridad específicos de la aplicación. El dispositivo administrador de seguridad controla las políticas de todo el material criptográfico que genera. El estándar ISA100 Wireless utiliza cifrado AES de 128 bits.

Política de seguridad	Longitud del código de integridad del mensaje de autenticación (MIC)	Cifrado
MIC-32	4 bytes	No
MIC-64	8 bytes	No
MIC-128	16 bytes	No
ENC-MIC-32	4 bytes	Si
ENC-MIC-64	8 bytes	Si

Tabla 7.- Suites de cifrado ISA100

Para proporcionar protección para una variedad de ataques, el estándar ISA100 Wireless emplea marcas de tiempo para el *nonce* utilizado en la cifrado AES-128. Las redes ISA100 Wireless operan bajo una estrecha sincronización del tiempo. La base de tiempo utilizada en las redes ISA100 Wireless se basa en el TAI (tiempo atómico internacional) y todos los dispositivos dentro de la red se encuentran continuamente sincronizados con el TAI. La seguridad en la capa de transporte utiliza la marca de tiempo para indicar cuando el paquete de datos fue creado. El destinatario final intenta autenticar el paquete de datos, pero si el paquete fue creado hace más de N segundos (configurable), el destinatario descartará el paquete. Esto proporciona protección contra ataques de repetición, siendo vital para aplicaciones industriales donde un ataque malicioso puede interrumpir las operaciones.
En ISA100 Wireless se utilizan distintos tipos de claves simétricas:

- Clave global. Una clave bien conocida que no debe ser usada para garantizar ninguna seguridad.
- Clave de unión. Una clave recibida al finalizar el aprovisionamiento de clave simétrica. Se usa para unirse a la red y para recibir la clave maestra.
- Clave maestra. Clave derivada por primera vez al final del esquema de acuerdo de clave y utilizada en la comunicación entre el dispositivo administrador de seguridad y los dispositivos. Caduca y necesita ser actualizada periódicamente.
- Clave de enlace. Clave utilizada para calcular el MIC (*Message Integrity Authentication*, longitud del código de integridad del mensaje de autenticación) en la capa de enlace. Caduca y necesita ser actualizada periódicamente.
- Clave de sesión. Una clave opcional usada para encriptar y/o autenticar PDU en la capa de transporte. Caduca y necesita ser actualizada periódicamente.

3.5.3. Uso en sistemas de control industrial

ISA100 Wireless define un estándar de comunicación inalámbrica bajo IPv6 para dispositivos industriales. Los distintos dispositivos que pueden hacer uso de este estándar abarcan los de monitorización, tanto del estado del equipo como del proceso, los de alertas y alarmas, dispositivos de control y dispositivos de seguridad. El direccionamiento IPv6 convierte al estándar ISA100 Wireless en el único protocolo de red industrial compatible con el Internet de las Cosas (IoT), en este caso, Internet de las Cosas Industrial (IIoT).

3.5.4. Riesgos y buenas prácticas

El mayor riesgo al que se encuentran actualmente las comunicaciones ISA100 Wireless es el desconocimiento de las posibles amenazas de este protocolo. Al tratarse de un estándar nuevo y basado en IPv6 (tecnología actualmente en expansión), las posibles deficiencias a nivel de seguridad no son muy conocidas. Por ello se recomienda que, siempre que sea posible, los dispositivos utilicen las suites de seguridad ISA100 Wireless que implementan el cifrado de las comunicaciones.

El despliegue de redes IPv6 en la industria, si no se hace de manera correcta y con los rangos adecuados, puede hacer que dispositivos que no deben tener salida al exterior, y así han sido configurados en su red IPv4, puedan hacerlo mediante red IPv6. Esta configuración es especialmente importante en todos los equipos encargados de unir la red cableada con la red inalámbrica dentro del protocolo ISA100 Wireless.

4. COMPARACIÓN ENTRE LAS REDES INALÁMBRICAS INDUSTRIALES Y DOMÉSTICAS

4.1. Uso

Varios de las tecnologías incluidas en el estudio provienen de entornos domésticos donde cuentan con una importante presencia. Así, hoy en día, prácticamente no se entiende un hogar con conexión a Internet que no haga uso de WiFi, o un móvil sin Bluetooth para poder conectarse a cualquier accesorio desde altavoces externos hasta el sistema manos libres del coche. Esta presencia en el sector industrial, sin ser tan importante como en los entornos domésticos/empresariales es cada vez más patente. No obstante aunque la presencia es creciente en todos los casos, si existen diferencias en lo que a las tecnologías más empleadas. La siguiente tabla recoge comparativamente las tecnologías inalámbricas en orden de presencia en ambos entornos, siendo la primera posición la más utilizada en cada caso (realizando la valoración sobre las tecnologías en las que se centra el estudio y sin tener en cuenta otras).

Posición	Entorno doméstico	Entorno industrial
1	Redes móviles GSM/GPRS/UMTS	WirelessHART
2	Wifi	Trusted Wireless
3	BlueTooth	Zigbee
4	WiMax	Redes móviles GSM/GPRS/UMTS
5	Radiocomunicaciones	Wifi
6	Zigbee	BlueTooth
7	WirelessHART	Radiocomunicaciones
8	Trusted Wireless	WiMax

Tabla 8: Comparativa de uso de tecnologías inalámbricas

Algunas de las tecnologías no tienen presencia en alguno de los dos entornos, así, por ejemplo, es prácticamente imposible encontrar comunicaciones domésticas sobre WirelessHART o Trusted Wireless ya que son tecnologías exclusivamente industriales; las comunicaciones ZigBee también son infrecuentes en ambientes domésticos pero si pueden encontrarse en determinados usos como juegos o equipos electrónicos. En el sector industrial son utilizadas todas a pesar de que los casos de empleo de

Radiocomunicaciones y WiMax son muy escasos y muy lejos del nivel de uso del resto de tecnologías.

4.2. Componentes

Los dispositivos necesarios para crear las redes que utilizan estas tecnologías tanto en el entorno doméstico como en el entorno industrial son los mismos, por lo que, de forma general, los dispositivos podrían ser intercambiables.

Las diferencias son principalmente físicas y radican en que los dispositivos que se utilizan para sistemas industriales han de estar preparados para trabajar en condiciones extremas (temperatura, presión, interferencias, radiación, etc.), suelen ser más pequeños y están preparados para el montaje en carril DIN[11], y así poder incluirse en los armarios de equipamiento conjuntamente con PLC, y otros equipamientos electrónicos.

Figura 14: Router WiFi doméstico (izquierda) y router WiFi industrial (derecha). Fuente: http://www.visionsystems.de

Por estas mismas razones de condiciones de trabajo, los costes de producción aun siendo entre dispositivos domésticos e industriales son mucho mayores en el segundo caso a pesar de que funcionalmente las capacidades son similares.

4.3. Seguridad

Referente a la seguridad, y partiendo de la base de igualdad de las medidas intrínsecas en la seguridad de cada tecnología, las diferencias aparecen en el rigor con el cual se configuran, aplican y se utilizan los protocolos usados en cada tecnología en los diferentes entornos.

Por ejemplo y en referencia a las redes WiFi la diferencia radica en su compartición y su configuración de seguridad. En entornos domésticos es posible encontrar redes abiertas de acceso público, siendo este hecho más habitual en grandes superficies o en organismos públicos que dan servicio a los ciudadanos. En cuanto a la compartición, existen clientes finales con redes WiFi instaladas en sus casas o negocios que deciden compartir una parte de su ancho de banda. Estas condiciones y configuraciones son impensables en entornos industriales donde todas las comunicaciones tratan de mantenerse lo más cerradas posibles con accesos restringidos.

[11] https://es.wikipedia.org/wiki/Carril_DIN

Si lo que se tiene en cuenta es el cifrado, en ambos entornos se tratarán de utilizar correctamente los protocolos disponibles de la tecnología en uso que permitan un cifrado suficientemente robusto. Puede darse el caso de que por una mala configuración o por un descuido, las medidas disponibles no se encuentren activas. Es por ello que las revisiones de seguridad en las redes de la organización son tan importantes y necesarias.

5. ANÁLISIS DE SEGURIDAD EN LABORATORIO

5.1. WiFi

Las redes WiFi están muy extendidas en entornos domésticos, y aunque en entornos industriales no es tan común, no resulta extraño encontrar alguna conexión de este tipo aunque sea en la red corporativa. Sobre seguridad en comunicaciones WiFi existe amplia documentación[12] y al tratarse de una tecnología bastante conocida y más ligada al mundo de TI que al de TO, no se va a entrar en detalle en este estudio para, directamente, centrar la atención en otras tecnologías inalámbricas más utilizadas en la industria.

5.2. Bluetooth

En las pruebas realizadas en laboratorio, se ha contado con tres dispositivos Bluetooth configurados uno como maestro, otro como esclavo y el tercero utilizado para la captura de los paquetes transmitidos por los otros.

Las pruebas llevadas a cabo han consistido en diversas lecturas de datos con diferentes configuraciones de seguridad, capturando en todo momento los paquetes intercambiados, que han sido posteriormente analizados.

5.2.1. Conexión Bluetooth

La primera prueba que se ha llevado a cabo es realizar una comunicación Bluetooth y comprobar todos los estados por los que pasa y la seguridad que aplica en cada uno de ellos. Bluetooth permite conexiones punto a multipunto, pero para limitar y hacer más sencillo el análisis se va a trabajar con conexiones punto a punto entre dos elementos.

El primer estado es el establecimiento de la conexión. Para ello, el dispositivo esclavo envía tramas de presencia de forma continua hasta que un maestro, realizando un proceso de descubrimiento recibe los paquetes e inicia el proceso de establecimiento de la conexión.

[12] Véase por ejemplo: https://www.incibe.es/CERT/guias_estudios/guias/GuiaManual_wifi_pymes

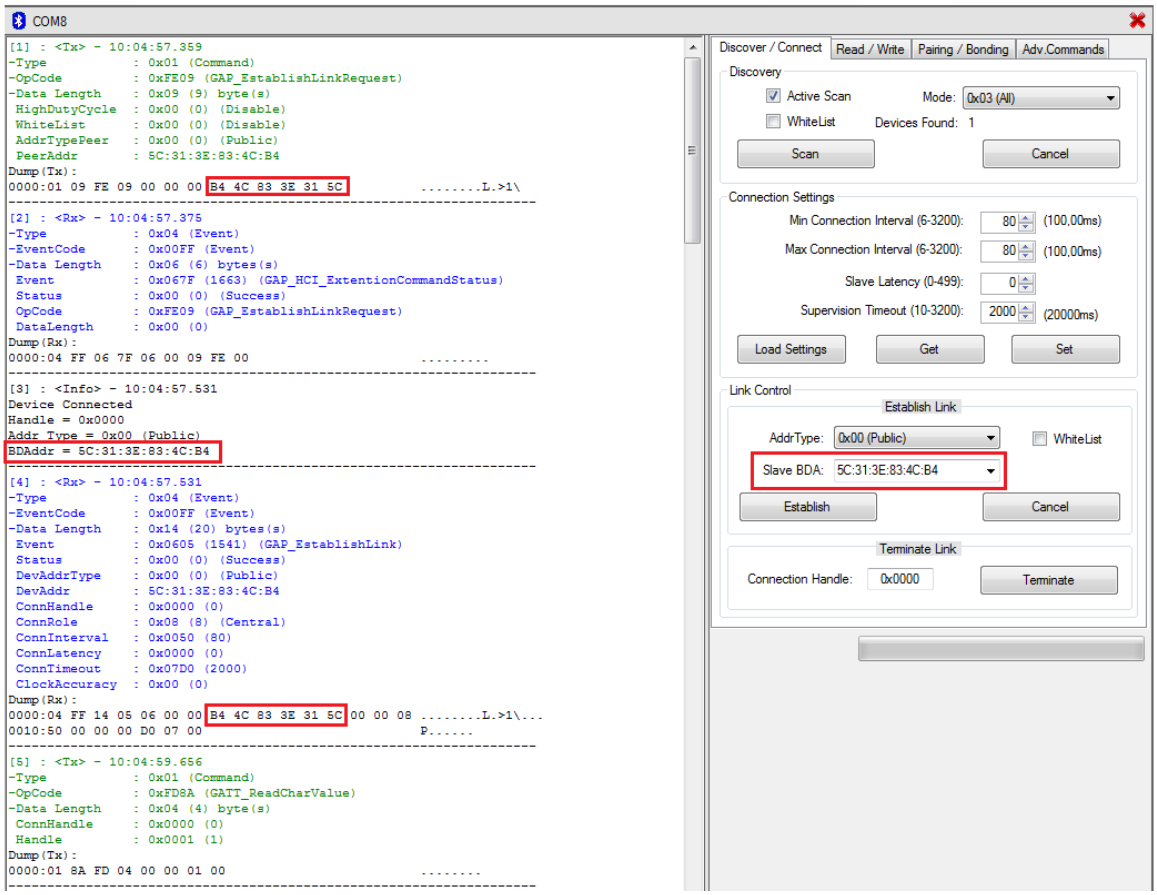

Figura 15: Establecimiento de la conexión maestro/esclavo

La primera petición mostrada en la imagen (en verde) representa el intento de establecimiento de la conexión por parte del maestro, las dos respuestas posteriores (en azul) muestran la interacción del esclavo para realizar el establecimiento de la conexión.

Una vez establecida la conexión entre el maestro/esclavo se sincroniza el reloj y el orden de salto en los canales de frecuencia. Posteriormente, se realizan intercambios de información de forma ininterrumpida siguiendo las especificaciones de la tecnología Bluetooth con saltos de canal constantes.

Del análisis de las tramas de datos capturadas se concluye que los saltos de canal, si bien comienzan de manera aleatoria entre los canales, llega un determinado momento en que se repite toda la secuencia de saltos en el mismo orden. A raíz de lo observado en las pruebas, se podría concluir que la predictibilidad que poseen los saltos a lo largo de todos los canales en los que trabaja Bluetooth, podría ser aprovechada por un potencial atacante para realizar ataques avanzados puesto que conoce el canal en el que ha de ir el siguiente mensaje, originando ataques de denegación de servicio u otros más complejos.

Para añadir un nivel extra de seguridad, Bluetooth ofrece un intercambio de información de autenticación mediante un proceso de emparejamiento o pairing. Este proceso proporciona la certeza de que los dispositivos que se intercambian los datos son quienes dicen ser.

ACK Status	Data Type	Data Header					L2CAP Header		SM_Pairing_Req					CRC	RSSI (dBm)	FCS
		LLID	NESN	SN	MD	PDU-Length	L2CAP-Length	ChanId	Opcode	IOCap	OOBDataFlag	AuthReq	MaxEncKeySize	InitKeyDist	RespKeyDist			
OK	L2CAP-S	2	1	1	0	11	0x0007	0x0006	0x01	0x04	0x00	0x05	0x10	0x07	0x07	0x70CB29	-35	OK
ACK Status	Data Type	Data Header					L2CAP Header		SM_Pairing_Rsp					CRC	RSSI (dBm)	FCS
		LLID	NESN	SN	MD	PDU-Length	L2CAP-Length	ChanId	Opcode	IOCap	OOBDataFlag	AuthReq	MaxEncKeySize	InitKeyDist	RespKeyDist			
OK	L2CAP-S	2	1	0	0	11	0x0007	0x0006	0x02	0x00	0x00	0x05	0x10	0x07	0x07	0xFF1393	-31	OK
ACK Status	Data Type	Data Header					L2CAP Header		SM_Pairing_Confirm			CRC	RSSI (dBm)	FCS		
		LLID	NESN	SN	MD	PDU-Length	L2CAP-Length	ChanId	Opcode	ConfirmValue						
OK	L2CAP-S	2	0	0	0	21	0x0011	0x0006	0x03	72 FB 1A 63 8A CD 97 5F 46 1A 2B D5 05 5F 56 55		0x160D89	-34	OK		
ACK Status	Data Type	Data Header					L2CAP Header		SM_Pairing_Confirm			CRC	RSSI (dBm)	FCS		
		LLID	NESN	SN	MD	PDU-Length	L2CAP-Length	ChanId	Opcode	ConfirmValue						
OK	L2CAP-S	2	0	1	0	21	0x0011	0x0006	0x03	9A 79 6B 85 F8 8D BC 55 63 7A 5B E9 27 BC 0F C6		0x9E34C1	-30	OK		
ACK Status	Data Type	Data Header					L2CAP Header		SM_Pairing_Random			CRC	RSSI (dBm)	FCS		
		LLID	NESN	SN	MD	PDU-Length	L2CAP-Length	ChanId	Opcode	RandomValue						
OK	L2CAP-S	2	0	0	0	21	0x0011	0x0006	0x04	63 81 4E E8 24 76 FA 5B A3 81 92 38 1D 2F E5 8A		0xC68201	-30	OK		
ACK Status	Data Type	Data Header					L2CAP Header		SIG Pkt Header			SIG_Connection_Param_Update_Req				CRC	RSSI (dBm)	FCS
		LLID	NESN	SN	MD	PDU-Length	L2CAP-Length	ChanId	Code	Id	Data-Length	IntervalMin	IntervalMax	SlaveLatency	TimeoutMultiplier			
OK	L2CAP-S	2	1	0	0	16	0x000C	0x0005	0x12	0x05	0x0008	0x0050	0x0320	0x0000	0x03E8	0x6F3FD8	-31	OK
ACK Status	Data Type	Data Header					L2CAP Header		SIG Pkt Header			SIG_Connection_Param_Update_Rsp		CRC	RSSI (dBm)	FCS
		LLID	NESN	SN	MD	PDU-Length	L2CAP-Length	ChanId	Code	Id	Data-Length	Result				
OK	L2CAP-S	2	1	1	0	10	0x0006	0x0005	0x13	0x05	0x0002	0x0000		0xF9F9DD	-32	OK
ACK Status	Data Type	Data Header					L2CAP Header		SM_Pairing_Random			CRC	RSSI (dBm)	FCS		
		LLID	NESN	SN	MD	PDU-Length	L2CAP-Length	ChanId	Opcode	RandomValue						
OK	L2CAP-S	2	0	1	0	21	0x0011	0x0006	0x04	B2 BC 24 74 B9 58 E4 72 85 08 1B 23 86 09 CB E3		0xA532A1	-30	OK		

Figura 16: Tramas de un proceso de pairing

El proceso de emparejamiento requiere el uso de una clave o PIN (passkey), que debe ser conocida de antemano, evitando así que dispositivos maliciosos se puedan incorporar a la red. Tras el intercambio del PIN se finaliza el proceso y se proporciona la autenticación de extremos. El PIN no es transferido en la comunicación inalámbrica, ya que se basa en un esquema desafío-respuesta en el cual es comprobado el conocimiento de una clave secreta por parte del solicitante. Gracias al emparejamiento es posible evitar ataques del hombre del medio (MiTM).

5.2.2. Lectura de datos

Las pruebas de lectura de datos permiten analizar las capacidades de cifrado de las que dispone Bluetooth. Para llevar a cabo una lectura de datos, a única condición es que se haya realizado el establecimiento de la conexión entre dos dispositivos. Como mediante el establecimiento no se autentican los dispositivos, las lecturas no son cifradas, pudiendo interceptarse e interpretarse todo el tráfico de la transmisión.

Tras el emparejamiento las lecturas siguen manteniéndose sin cifrar, pues sólo se ha realizado la autenticación de los extremos, por lo que las escuchas de tráfico de red siguen siendo efectivas.

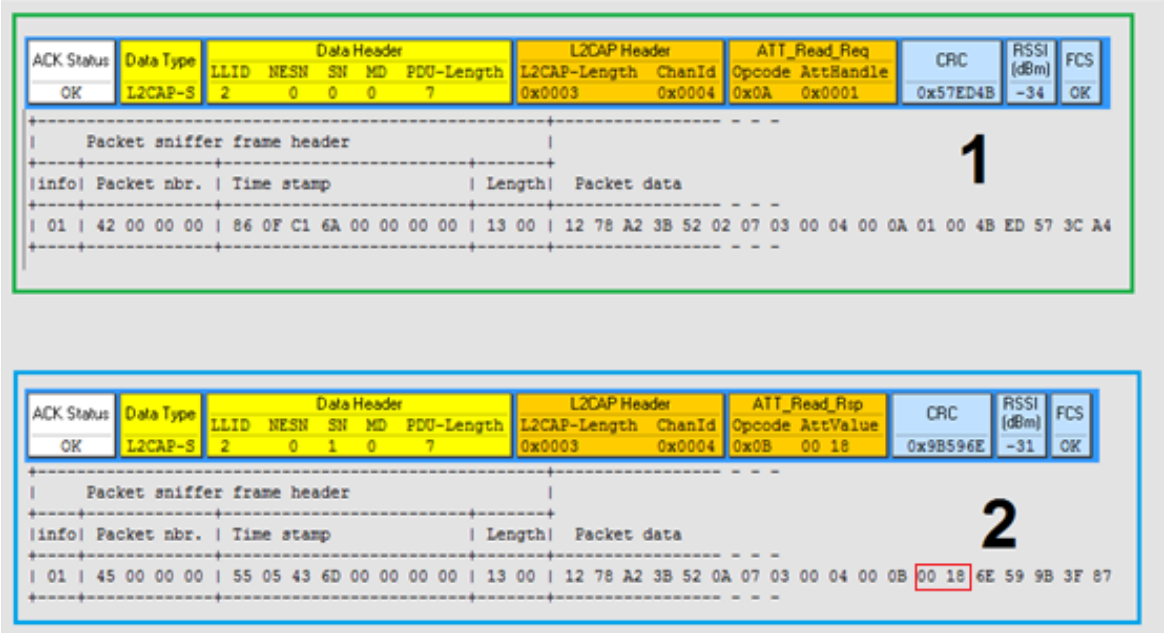

Figura 17: Captura de tramas enviados sin cifrar

Cuando se establece un canal de comunicación sin seguridad, las lecturas y escrituras realizadas pueden ser fácilmente capturadas. Como solo se realiza una identificación de extremos, cualquiera de ellos podría ser suplantado y podría continuar con la comunicación.

Para poder llevar a cabo el cifrado del canal e impedir la interpretación de los datos capturados existe la posibilidad de utilizar una clave a largo plazo (LKT – Long Term Key). El uso de la LTK es posterior al emparejamiento, esta clave ha de ser conocida por los dos integrantes de la comunicación en el momento de la activación de la medida de seguridad.

Figura 18: Captura de tramas enviados con cifrado

Durante el proceso de emparejamiento existe la posibilidad de almacenar la clave a largo plazo. Esta clave persistente se utiliza para conocer previamente a una comunicación entre

dispositivos la clave que cifrará la comunicación, pudiendo realizar intercambios de información cifrada sin tener que volver a realizar los pasos previos de pairing y autenticación. La LTK puede ser utilizada por ambos dispositivos siempre y cuando estos conserven almacenada la clave sin que sea borrada de forma manual.

5.3. Zigbee

Para las pruebas en laboratorio con Zigbee, se utilizó un kit de desarrollo compuesto por cuatro dispositivos autónomos, con función de router o dispositivo final, y un dispositivo de gestión, con funciones de coordinador de la red.

Para mostrar de manera práctica el tráfico intercambiado entre dispositivos ZigBee, se han realizado diferentes pruebas. En ellas se han analizado capturas de tráfico de red correspondientes a operaciones de lectura y escritura de parámetros de un nodo.

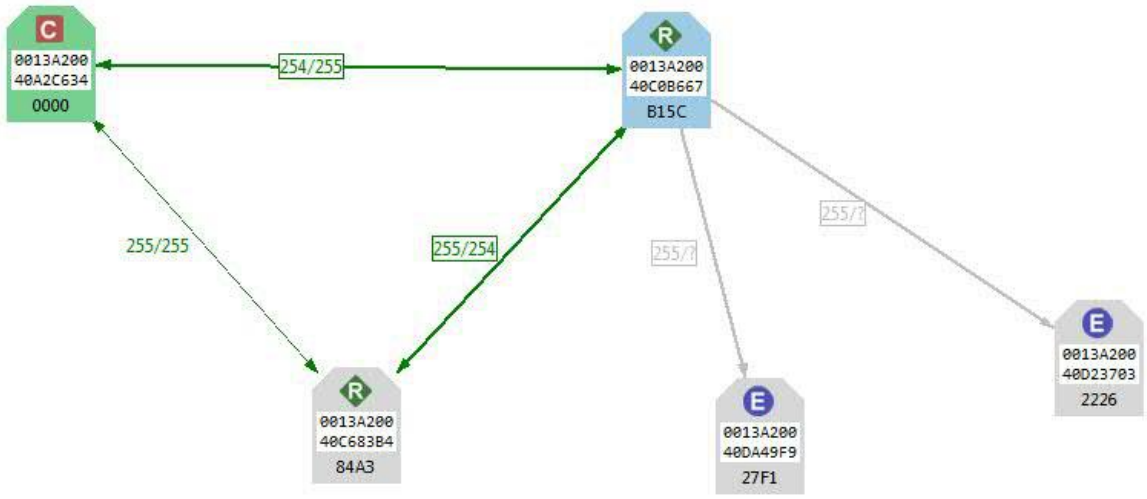

Figura 19: Red Zigbee del laboratorio. Coordinador (C), Routers (R) y dispositivos finales (E)

5.3.1. Escuchas en la red

Las escuchas de red son el ataque más sencillo a realizar sobre cualquier comunicación inalámbrica.

Un dispositivo ZigBee utilizado para capturar la información intercambiada en la red Zigbee, permite recoger información de las comunicaciones de forma transparente para el resto de dispositivos en la red.

La información obtenida de la comunicación proporciona a un atacante conocimiento sobre la red, identificando al dispositivo coordinador y a los dispositivos que funcionan como router, que luego podría utilizar para realizar otro tipo de ataques. Además, también se obtienen los datos transmitidos, permitiendo conocer los datos solicitados y los valores leídos de diferentes variables. Esta información puede utilizarse para realizar acciones como el reenvío de paquetes o la suplantación de dispositivos. En pruebas de laboratorio se verificarán estas posibilidades y su impacto.

5.3.2. Reenvío de paquetes

El reenvío de paquete (también conocido como replay), consiste en la captura de tramas que posteriormente son reenviadas, ya sea modificadas o con la misma estructura, con el objetivo de desestabilizar la red o un nodo concreto.

El reenvío de paquetes es frecuentemente utilizado en ataques de denegación de servicio. Mediante un script construido para construir e inyectar tramas ZigBee se comprueba el éxito de un ataque de reenvío de paquetes previamente capturados.

La siguiente figura muestra las opciones de la aplicación utilizada para el reenvío de tramas desde el dispositivo atacante. En este caso permite hacer un reenvío de una de las tramas capturadas (seleccionable en el segundo paso) modificando o no el número de secuencia.

```
Modo de inyeccion:
        0) replay de existente.
        1) replay de existente con cambio de numero de secuencia.
        2) construir trama entera.
        --> 0

Elegir trama para realizar replay...
        0) 02 00 10 39 a5  ---> len = 5
        1) 63 88 10 91 31 a9 00 50 65 04 b2 63  ---> len = 12
        2) 02 00 0f 4f 4d  ---> len = 5
        3) 63 88 0f 91 31 a9 00 50 65 04 78 89  ---> len = 12
        4) 02 00 0e c6 5c  ---> len = 5
        5) 63 88 0e 91 31 a9 00 50 65 04 c7 08  ---> len = 12
        6) 02 00 0d 5d 6e  ---> len = 5
        7) 63 88 0d 91 31 a9 00 50 65 04 17 82  ---> len = 12
        8) 02 00 0c d4 7f  ---> len = 5
        9) 63 88 0c 91 31 a9 00 50 65 04 a8 03  ---> len = 12
        10) 02 00 0b 6b 0b  ---> len = 5
        11) 63 88 0b 91 31 a9 00 50 65 04 a6 9f  ---> len = 12
        12) 02 00 0a e2 1a  ---> len = 5
        13) 63 88 0a 91 31 a9 00 50 65 04 19 1e  ---> len = 12
        14) 02 00 09 79 28  ---> len = 5
        15) 63 88 09 91 31 a9 00 50 65 04 c9 94  ---> len = 12
        16) 02 00 08 f0 39  ---> len = 5
        17) 63 88 08 91 31 a9 00 50 65 04 76 15  ---> len = 12
        18) 02 00 07 07 c1  ---> len = 5
        19) 63 88 07 91 31 a9 00 50 65 04 c4 a4  ---> len = 12

Paquete a inyectar:
        --> 10
        Probando la inyeccion del paquete 10...
        02 00 0b 6b 0b  ---> len = 5
        Exito al inyectar paquete 10, longitud 3 (sin contar CRC).
```

Figura 20: Replay de trama capturada

Para evitar este tipo de ataques es necesario el uso de la característica de integridad que posee ZigBee para la comprobación de tramas, verificando así que no han sido reemplazadas por otras. El controlador de red comprueba estas tramas de refresco y su valor, para ver si son las esperadas.

5.3.3. Tramas de datos

ZigBee permite el uso de un cifrado robusto usando criptografía de clave simétrica con rotación periódica de claves de red, lo que aporta un nivel extra de seguridad en el intercambio de información. No obstante si no se configura específicamente, la comunicación ZigBee se realiza sin cifrar.

En una trama ZigBee se pueden identificar campos en diferentes capas (red, aplicación) cuyos valores fijan la activación de la seguridad. Si los valores están a 0 significa que no se aplica seguridad. La activación del cifrado de los datos se indica colocando el bit a 1.

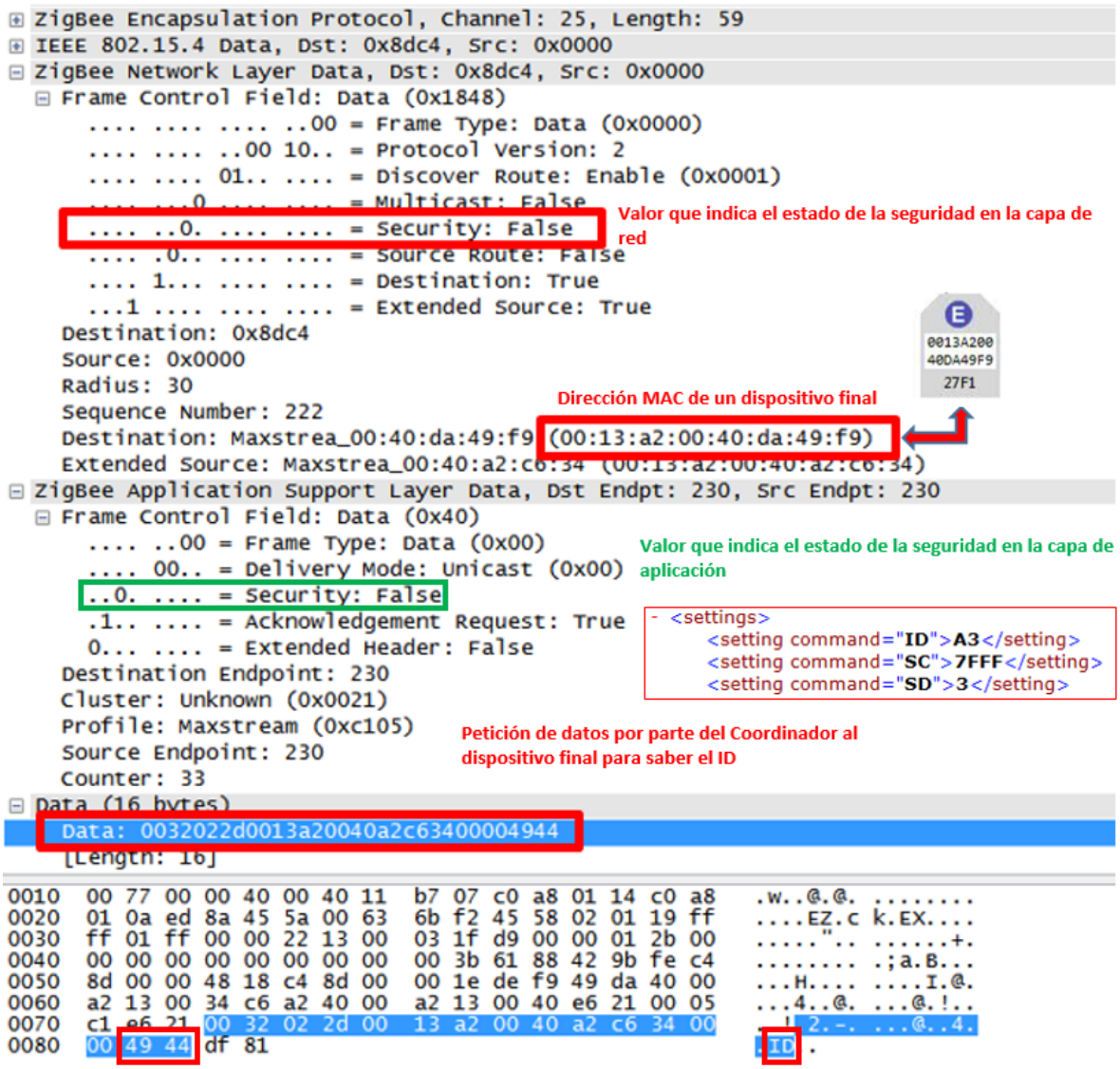

Figura 21: Petición del parámetro ID con datos sin cifrar

5.3.4. Denegación de servicio

Un posible escenario en el que puede darse una denegación de servicio es la incorporación de múltiples dispositivos gracias a la inyección de tramas falsas al coordinador de la red

tratando de exceder el máximo permitido por una red ZigBee, que puede constar de un máximo de 65535 nodos distribuidos en subredes de 255 nodos.

Por otro lado, y como ocurre con todas las comunicaciones inalámbricas, es posible realizar ataques mediante técnicas de jamming[13] o inhibición. Cuando los nodos se asocian a una red ZigBee envían su petición de asociación al coordinador o a uno de los routers. Aquel que recibe la petición se convierte en el padre del nodo. En caso de que un nodo pierda el contacto con su nodo padre, éste deberá realizar una reasociación con la red y obtener un nuevo padre. Esta reasociación implica actualizar las rutas de la red.

La realización de estos ataques puede provocar la inestabilidad de las rutas en la red, y en consecuencia, las comunicaciones en ésta pueden quedar anuladas, además de incrementar el consumo de batería por parte de los nodos.

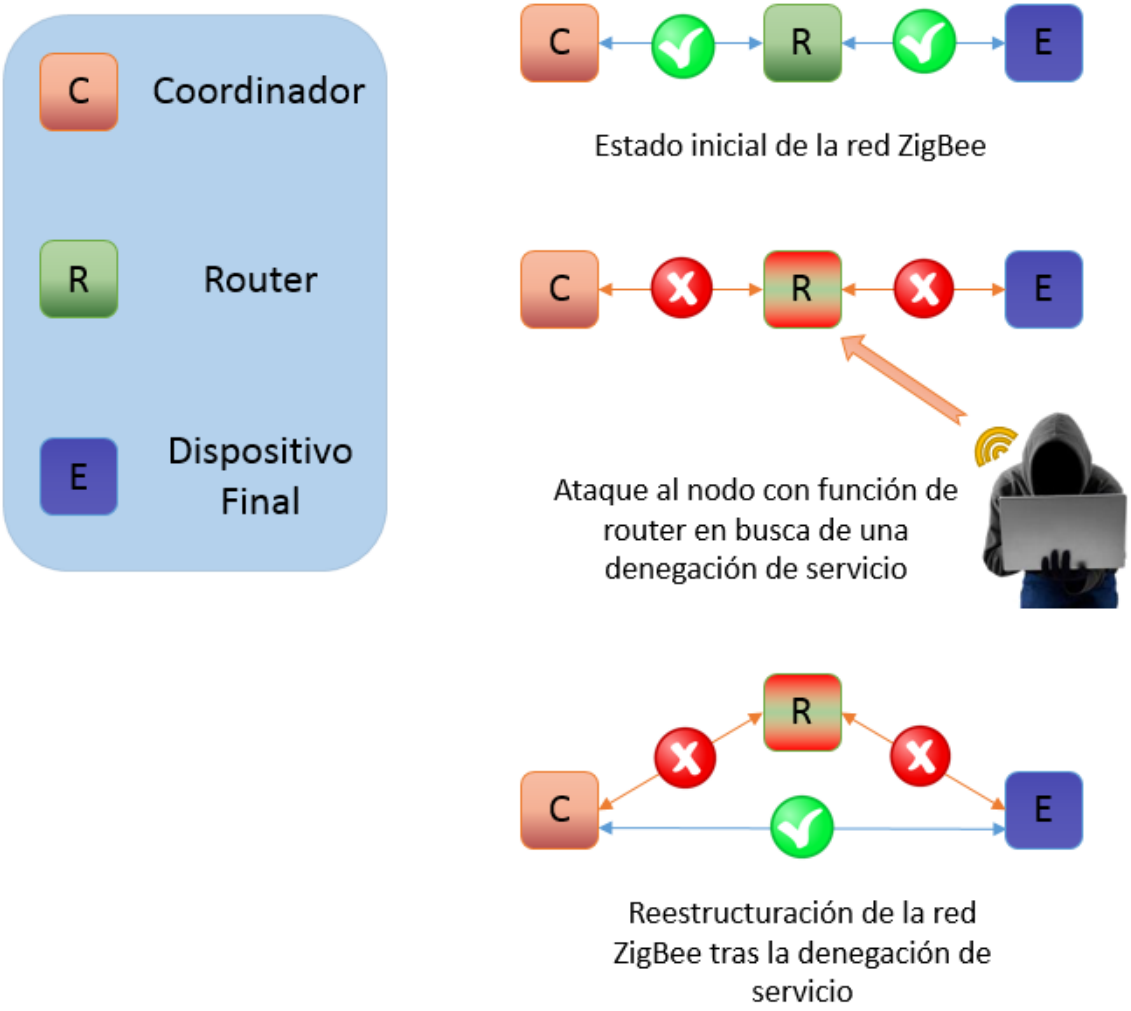

Figura 22: Ejemplo de denegación de servicio sobre un nodo en una red ZigBee

Para evitar ataques de solicitudes de asociación de dispositivos falsos se pueden usar listas blancas de dispositivos, para tratar sólo las peticiones de dispositivos autorizados.

[13] http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/nocedal_d_jm/capitulo3.pdf

5.3.5. Suplantación vía spoofing

Usurpar la identidad de un nodo, requiere del conociendo previo su dirección MAC, ya sea para realizar denegaciones de servicio o para transmitir o solicitar datos a terceros es otro ataque posible dentro de la red ZigBee.

En el laboratorio se ha probado la suplantación mediante el envío constante de mensajes, por parte de un nodo de la red, indicando que la dirección anunciada ya estaba ocupada. Este ataque obliga a la retransmisión de muchos mensajes a la broadcast, saturando el ancho de banda.

La otra prueba realizada ha consistido en generar tramas dirigidas a direcciones ZigBee falsas. Un nodo atacante envía datos dirigidos a direcciones no existentes provocando problemas en el encaminamiento y en consecuencia el mal funcionamiento de la red ZigBee.

Al igual que en el caso anterior, una lista blanca de dispositivos minimiza el problema,

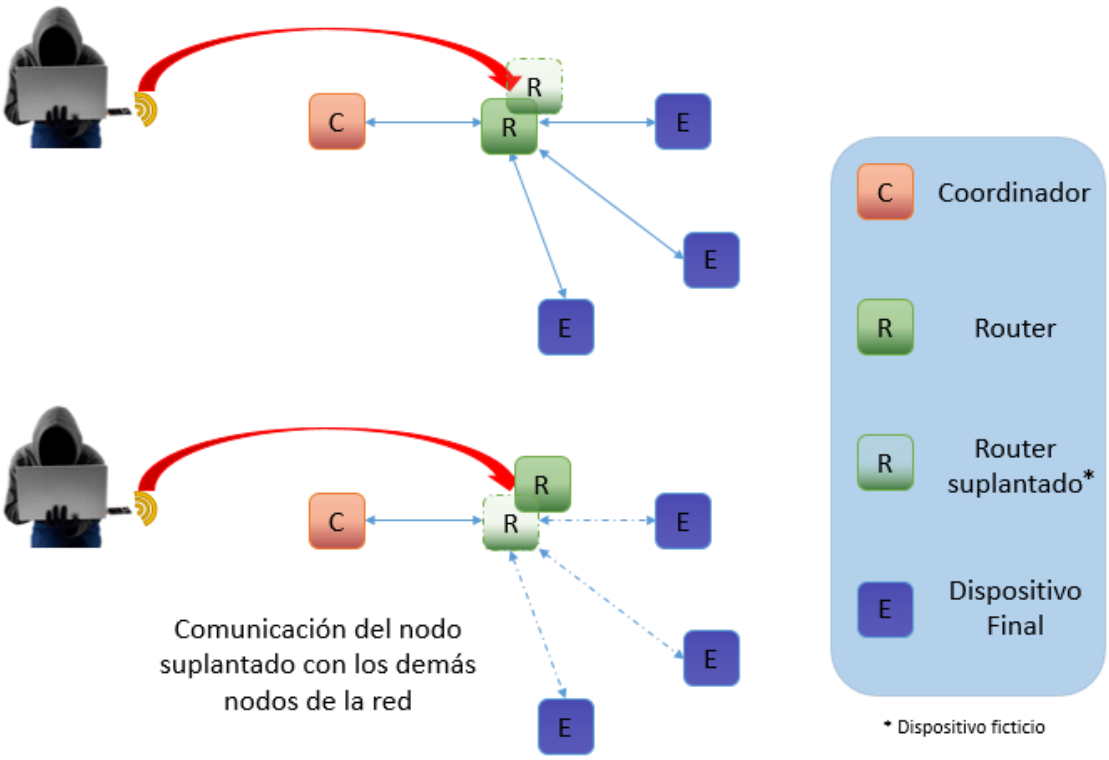

Figura 23: Router suplantado por un atacante

5.4. WirelessHART

Para el análisis de WirelessHART se ha contado con un kit de desarrollo compuesto por cinco dispositivos autónomos que realizan la lectura del valor de temperatura ambiente y lo transmiten al punto de acceso de la red para que sea tratado adecuadamente por las aplicaciones. No se disponía de elementos a mayores para realizar capturas o inyección de tramas de forma sencilla, lo que ha limitado en parte las pruebas a realizar.

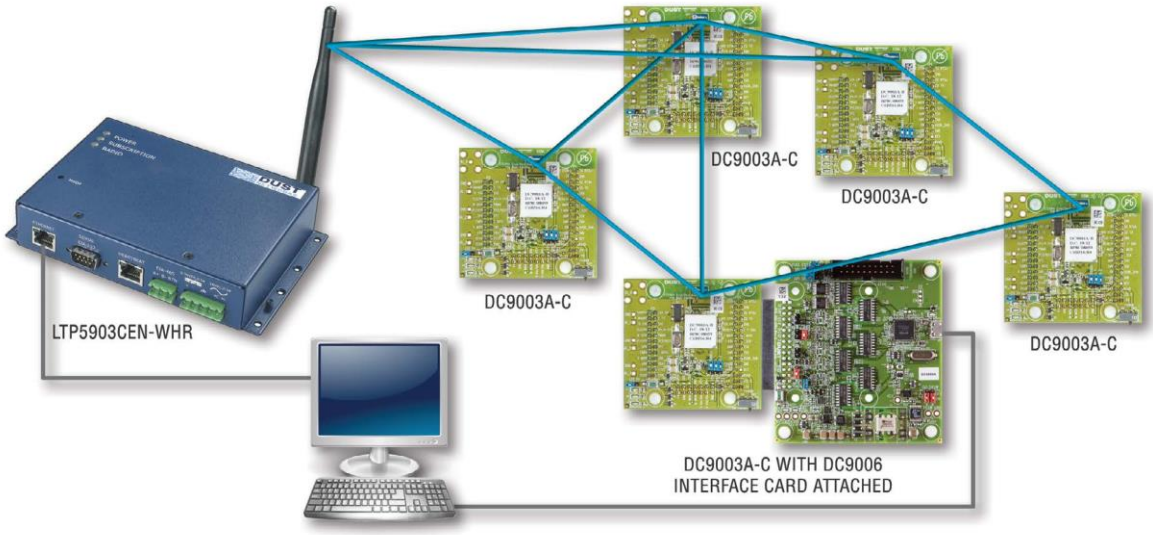

Figura 24: Red WirelessHART del laboratorio

Las medidas de seguridad del WirelessHART no pueden ser deshabilitadas, y se puede distinguir entre las que afectan al nivel lógico y las que afectan a nivel físico.

5.4.1. Captura de información

WirelessHART dispone de una clave de cifrado para el tráfico de red, pero también permite el intercambio cifrado de paquetes únicamente entre dos dispositivos, que dispondrán de una clave específica para ellos.

Esta característica hace que todos los datos de la comunicación no puedan ser interpretados de forma sencilla, pero sí las cabeceras y otro tipo de información, que se envía sin cifrar en todos los mensajes.

5.4.2. Comunicación con el resto de la red

La comunicación de la parte inalámbrica de la red con la parte cableada de la misma (dispositivos como gestor de red o seguridad), así como con otros dispositivos del protocolo HART, es el punto crítico del despliegue. Estos dispositivos utilizan otros protocolos (HART u otros) que pueden ser más vulnerables que WirelessHART y poner en riesgo a toda la red. Este tipo de ataques no se analizaron por no formar parte de la tecnología WirelessHART.

5.4.3. Denegación de servicio

Los ataques de denegación de servicio por inhibición no son mitigables en ninguna red inalámbrica, por lo que WirelessHART también se ve afectada por ellos.

También pueden conseguirse ataques de denegación de servicio mediante el envío continuo de peticiones de asociación a la red, llegando a saturar el ancho de banda disponible.

BIBLIOGRAFÍA

[1] http://www.redeswimax.info/
[2] Trusted Wireless 2.0. Wireless Technologies in Industrial Automation
[3] Industrial Wireless. Transmisión inalámbrica desde el sensor hasta la red. Phoenix Contact
[4] http://en.hartcomm.org
[5] System Engineering Guidelines. IEC 62591 WirelessHART.
[6] Planificación mediante Atoll de red WiMAX móvil para los centros de la Universidad de Sevilla. Proyecto fin de carrera. Antonio Carmona Sánchez. 2008
[7] Hoja de producto XBEE® AND XBEE-PRO® ZIGBEE
[8] Hoja de producto SmartRF05EB User's Guide (Rev. A)
[9] Hoja de producto CC2540 Development Kit User's Guide (Rev. A)
[10] SmartMesh WirelessHART Easy Start Guide

GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMÍA Y EMPRESA

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

incibe cert_