Cybersecurity in wireless comunications in industrial enviroments

CERT DE SEGURIDAD
E INDUSTRIA

certsi_

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

September 2017

CERTSI_GUIA_SCI_003_ComunicacionesInalambricas_2017_v1

INDEX

GRAPHICS

TABLES

1. INTRODUCTION

Today, in an increasingly more connected world, wireless communication is beginning to play a greater role than the use of cable thanks to the advantages and conveniences it provides. With regard to industrial environments, concepts such as Industry 4.0 and the Industrial Internet of Things (IIOT) have a very important role to play in this development, with ever greater numbers of increasingly more sophisticated wireless devices.

The proliferation of mobile devices such as tablets, PDAs or smartphones and their influence in industrial environments is an example of the evolution of this sector in relation to access to industrial process information. Today it is common for this information to be available online on servers with restricted access. Often, they are accessed regularly as a reference to verify values, but also, on occasion, there will be the possibility of modifying said values remotely and swiftly thanks to communications between ever more intelligent machines and the interconnection of sensor networks for capturing data.

The use of technologies like ZigBee, WirelessHART and Trusted Wireless among others, already implemented in our industry as resources to provide these services has already become consolidated.

The aim of this study is to raise awareness of different wireless technologies used in many applications in the domestic environment but that are opening the way into industrial environments. In addition to the features and peculiarities of each technology, this study aims to verify the applied security in each and proposes countermeasures so that communication can be carried out in a way that is secure and that, at the same time, takes advantages of all the security features available in the protocols used.

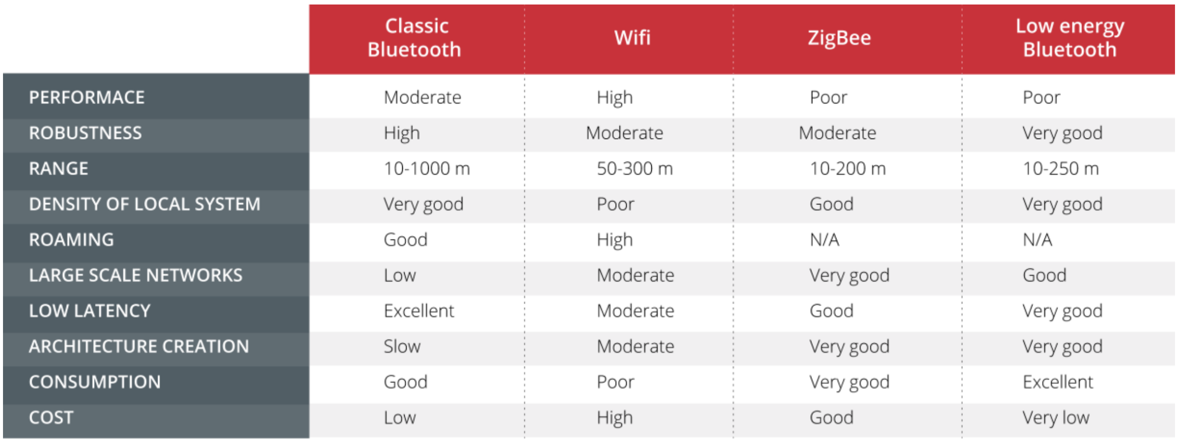
2. MOST COMMON WIRELESS TECHNOLOGIES

Wireless technologies are implemented in both the corporate and industrial sector for various reasons, although mainly for reasons of simplicity of roll out and cost reduction. These factors ensure that their use is ever more popular and progressively more modern wireless protocols that offer the same functionalities as cabled, or even better, continue to emerge.

Industrial control systems demand certain security and robustness characteristics, both physically and logistically, that wireless communications must satisfy in order for their use to be considered. The main features are:

- Reliable and robust communication
- Advanced security functions
- Configuration and function similar to commonly used automation tools.
- Real time and deterministic behaviour
- Wide range of temperature
- Compatibility with existing wireless technology (without interference)
- Low energy consumption for certain areas of the application

The following table describes the desirable features of wireless technologies used frequently in industrial environments.



	Classic Bluetooth	Wifi	ZigBee	Low energy Bluetooth
PERFORMACE	Moderate	High	Poor	Poor
ROBUSTNESS	High	Moderate	Moderate	Very good
RANGE	10-1000 m	50-300 m	10-200 m	10-250 m
DENSITY OF LOCAL SYSTEM	Very good	Poor	Good	Very good
ROAMING	Good	High	N/A	N/A
LARGE SCALE NETWORKS	Low	Moderate	Very good	Good
LOW LATENCY	Excellent	Moderate	Good	Very good
ARCHITECTURE CREATION	Slow	Moderate	Very good	Very good
CONSUMPTION	Good	Poor	Very good	Excellent
COST	Low	High	Good	Very low

Table 1: Comparison of different wireless technologies in industrial environments

On the other hand, the frequency bands used in each technology is also a point to consider when it comes to adopting a wireless communication resource in an industrial system that can be sensitive to interference.

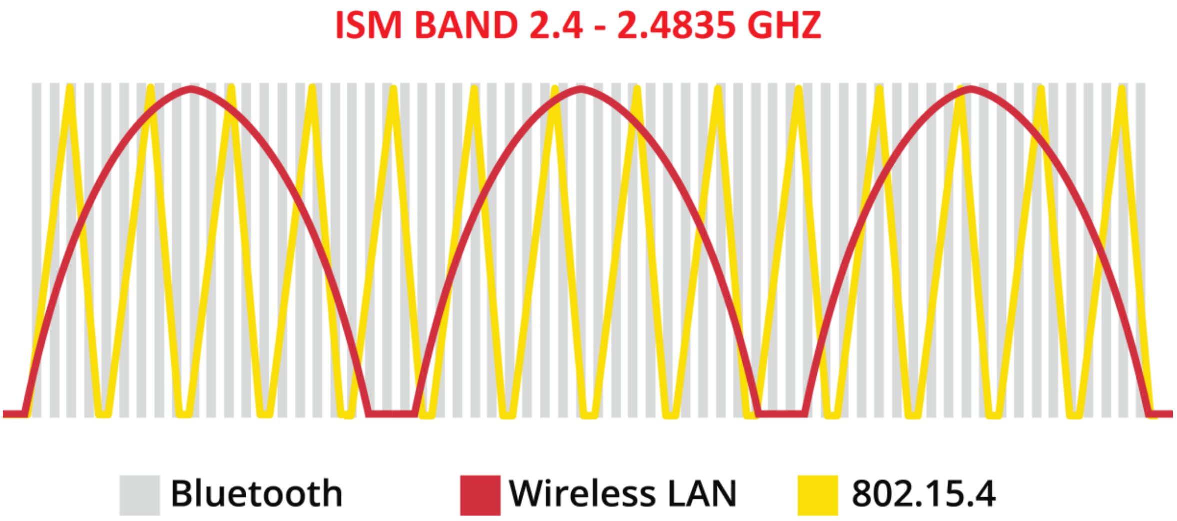


Figure 1: Comparison of range of frequencies of various wireless technologies

All adequate wireless technologies comply with the requirements of control systems. In addition, some general functionalities intrinsically provided by wireless systems and that are interesting from an industrial perspective are:

- Greater mobility and possibility of connecting other devices like tablets and smartphones
- Removal of expensive and heavy transmission material like copper cables and supports.
- Communication across great distances and where physical cables cannot be used.
- Flexibility for modification of the facility
- Scalability
- Increased security of people as not necessary to be close to a device during configuration or maintenance.

Having outlined the basic reasons for the use of airborne communications in industry, it is interesting to analyse the specific characteristics and security of the main technologies that can be considered applicable to industrial environments.

2.1. WiFi

WiFi network are the most used for the exchange of data from all existing wireless networks both in the industrial and in the corporate sector.

2.1.1. Description:

WiFi or WLAN technology (Wireless Local Access Network) is regulated by standard IEEE 802.11 in its versions a/b/g/n/ac. The main features are:

- Frequency of use of free band, located in 2.4 GHz or 5 GHz
- High speeds, depending on the standard that might reach 300 Mbits/s
- Fast roaming
- Provides mobility in large surface networks
- High reliability through the use of MiMo technology (Multiple-input Multiple-output)

- Range of action of 50 metres (5GHz) to 200 (2.4 GHz), although can be increased if it is in a visible straight line.
- 23 channels for frequency of 5 GHz and 13 channels for 2.4 GHz
- High availability of products

2.1.2. Security Features

WiFi technology allows for encryption of communications. For that, several methods have been used that have evolved to remedy the difficulties that appeared over time. The security of WiFi communications can be established:

- **Without Encryption** A password for the encryption in the connection is not established, therefore any device can join and communicate. Often, WiFi connections without encryption are known as free or open.
- **WEP (Wired Equivalent Privacy):** First encryption mechanism, included in the first IEEE standard 802.11. It is based on the RC4 encryption algorithm, using a 40 or 104 bit secret key combined with a 24 bit Initialization Vector (IV), which makes for a total of 64 or 128 bits. This encryption method is strongly advised against due to the vulnerabilities it presents and many devices no longer allow its use as it is considered so vulnerable.
- **WPA (Wi-Fi Protected Access):** Developed as a solution to the problems of WEP encryption, it boasted the main characteristic of use of an authentication server (Type RADIUS[1] or similar) (WPA-Enterprise) through the EAP protocol. It is also possible to use Pre-Shared Keys (PSKs) (WPA-Personal), although this lowers security. It incorporates TKIP[2] which is responsible for the dynamic change of the key. There is also the option to use AES encryption:
- **WPA2 (Wi-Fi Protected Access 2):** This is an improvement on WPA which corrects certain deficiencies in its predecessor. It uses AES encryption by default. In principle it is the most secure security protocol for WiFi at this time.

2.1.3. Use in Industrial Control Systems

Within industrial facilities it is common to use WiFi at control centres for acquisition, monitoring and configuration, but it is also possible to find it at field level to control the critical actions in time. On occasion it is necessary to use particular solutions (proprietary software) or perform a frequency study before roll-out.

2.1.4. Best Practice

As it is a quite well-known technology, more linked to the world of Information Technology than Operational Technology and many documents have been written on how to apply security measures. Consequently, this study will not enter into further detail here, in order to focus on other wireless technologies used more in Industry.

2.2. Trusted Wireless

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

[2] TKIP - Temporal Key Integrity Protocol

Trusted Wireless is a technology developed specifically to be used in industrial control systems.

2.2.1. Description:

The current version (2.0) has the following features:

- Reach of several kilometres depending on the frequency used.
- Speed of adjustable data (from 16 to 500 kbps)
- Mesh networks with a maximum of 250 nodes
- Robust communications through frequency hopping spread spectrum[3]
- Uses 900 Hz band (free band in America) or 2.4 GHz band (global free band)

Allows several types of architecture in its implementation:

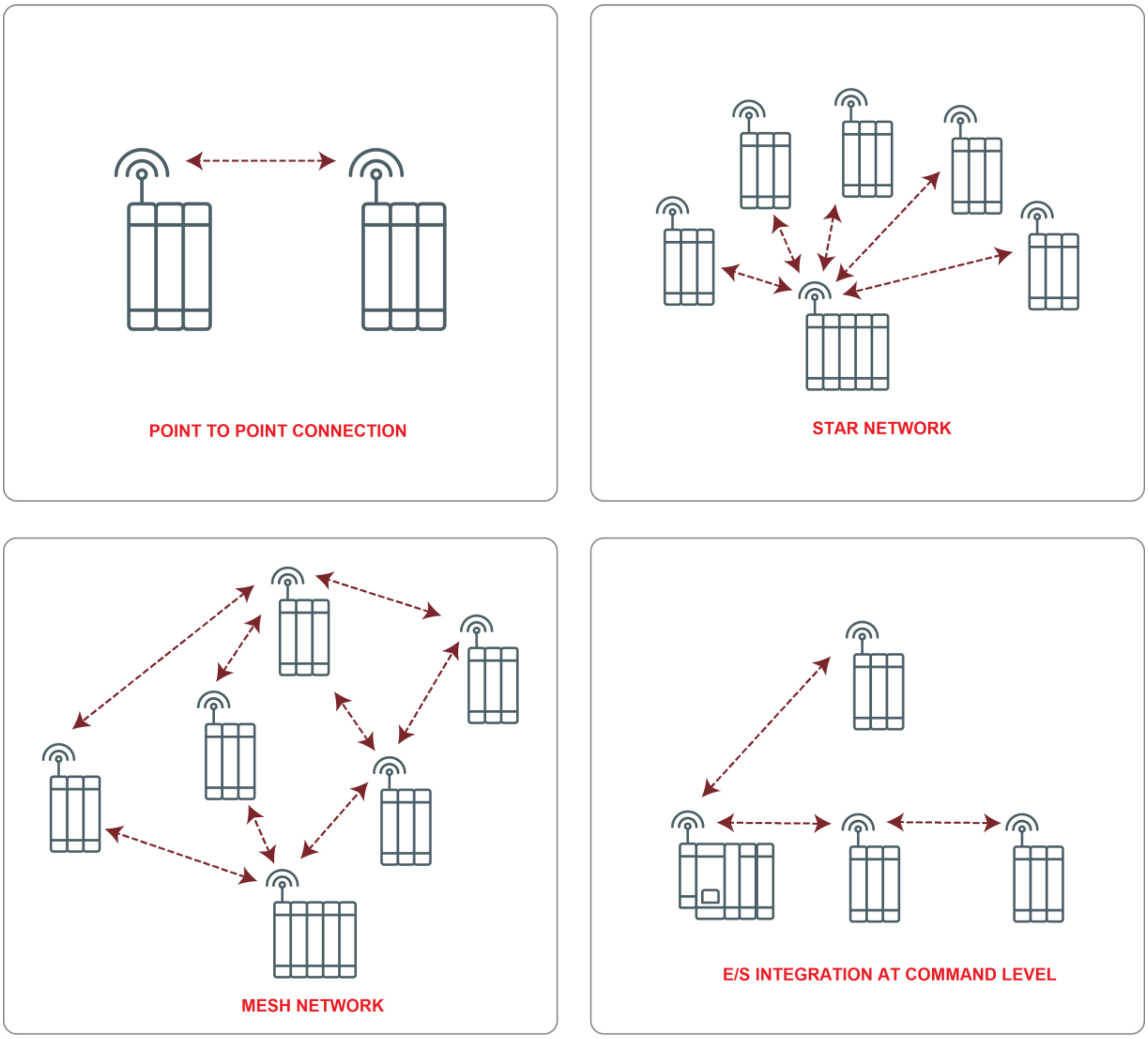


Figure 2: Typologies Source: Industrial Wireless. Wireless transmission from sensor to network. Phoenix Contact

[3] FHSS - Frequency Hopping Spread Spectrum

POINT TO POINT CONNECTION

2.2.2. Security Features

The security of Trusted Wireless is based on proprietary components and frequency hopping. Nevertheless it adds two very important features:

- Authentication in accordance with RFC 3610[4]
- 128 bit AES Encryption (Pre Shared Keys)

2.2.3. Use in Industrial Control Systems

Trusted Wireless is use to transmit data and signals across great distances within an industrial sector. Its use is focussed on:

- E/S Wireless: E/S analogue and digital signals captured by devices
- Wireless Serial: Sending of series data RS232, RS485, from other equipment, through the conversation of same to Trusted Wireless.

Trusted Wireless offers a high degree of reliability, robustness, security and flexibility.

2.2.4. Best Practice

In the case of Trusted Wireless, this is a robust technology in its design that uses frequency hopping and allows for encryption through 128 bit AES.

It must be taken into account that this technology is based on a private specification, something that was quite frequent some years ago in the field of industrial control systems, which means it is not subject to the same level of testing on the part of the community like other technologies with public specifications.

2.3. Bluetooth

Bluetooth technology began to be developed in the year 1994 by Ericsson as an alternative to cable. For communication it uses FHSS.

2.3.1. Description:

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

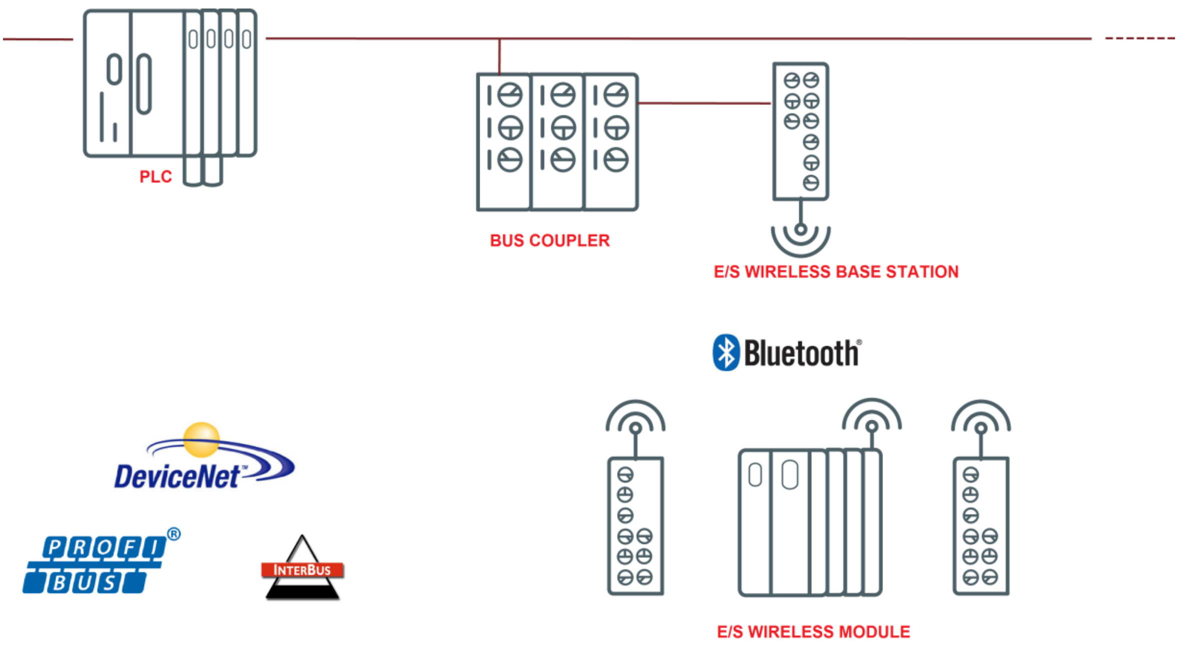


Figure 3: Network infrastructure with Bluetooth communication sensors. Source: Industrial Wireless. Wireless transmission from sensor to network. Phoenix Contact

Bluetooth technology is governed by standard IEEE 802.15.1. There exist two specifications of the technology:

- Classic Bluetooth: It is a specific technology for devices with high demand of small transmission demands, low energy consumption and that are profitable.
- Bluetooth Low Energy: This technology is ideal for applications that require the communication of small quantities of data on an occasional or periodic basis.

Bluetooth technology stands out for the following features:

- Communication distance of up to 1 km (in a straight line with no obstacles).
- Use of frequency on the free 2.4 GHz. band.
- High-reliability transmission through redundant transmission channels.
- Reduced delay time (5-10 minutes).
- Capacity to function in environments where there are large numbers of devices due to the use of frequency.

Focussing on the two Bluetooth technologies, the most important features of each are:

- Classic Bluetooth
  - Rapid and cyclical transmission of small quantities of data
  - Transmission of up to 780 kbit/s
  - Large quantity of devices connected to the same radio environment functioning without interferences
  - High availability of consumer products
- Bluetooth Low Energy
  - Allows a large number of communication nodes with low latency requirements
  - Very low energy consumption

  - Similar level to Classic Bluetooth.
  - Very little latency if the number of nodes connected is not high.
  - Very brief awakening and reconnection time.

2.3.2. Security Features

The security features of Bluetooth are similar to those of other wireless technologies. The following stand out:

- 128 bit encryption
- Robustness, achieved through:
  - Adaptive Frequency Hopping (AFH)[5]
  - Forward Error Connection (FEC), allows the receiver to correct errors in the transmission if it is necessary to resend.
  - Channels with narrow frequencies, which implies lower interference with other devices
  - Low sensitivity to reflection or multiple routes

Bluetooth security can have various functioning modes:

- ***No security.*** All security mechanisms (authentication and encryption) are turned off. Devices allow all other devices to connect with them.

- ***Services level security.*** Security is initialized after establishing a channel between the LM (Link Manager) level and the L2CAP level. The security policies and confidence levels are applied independently, allowing access to applications with different requirements.

- ***Link level security.*** All the routines are within the Bluetooth chip and nothing is transmitted on the level. Security is initialized before establishing a channel and all communications are encrypted. In addition to the encryption of communication, it uses a shared secret Link Key (PIN) between the two devices communicating and the MAC security level. This methodology consists of sharing the secret Link Key between a pair of devices every time they communicate for the first time.

2.3.3. Use in Industrial Control Systems

The use of Bluetooth technology in industrial control systems is centred on the exchange of data both at a low level and at a high level. Thus we can find it in:

- E/S Wireless: E/S analogue and digital signals
- Wireless Serial: Series data RS-232 and RS-422/485
- Wireless Ethernet: Ethernet data exchange

Classic Bluetooth is oriented more towards integration in atomization devices in series and field networks; however, Bluetooth Low Energy is designed for sensors, actuators or small devices that require very small consumption levels.

[5] It uses the same system as FHSS

2.3.4. Best Practice

After the tests are carried out, the following security practices are concluded when it comes to using Bluetooth technology in any device:

- Use of encryption where possible. The use of LTK[6] allows communication to be encrypted between the master and the slave from the first moment. All devices from a control network that uses Bluetooth should make use of LTK
- Do not accept connections from unknown devices. Activate the white list option in the master and require pairing with a key of at least 5 characters, thus avoiding malicious devices connecting without permission.
- Continuously review the list of registered trusted devices in order to avoid malicious devices joining.
- Assign a name to the devices that do not reflect extra information such as the brand, the device model, the location or service. This practice will prevent possible attackers from taking advantage of known vulnerabilities associated with certain devices in order to perpetrate direct attacks.
- Maintain device configuration in invisible mode to make it difficult to detect from other devices.

This device will make it difficult for attacks like:

- Discovery of hidden devices
- Interception of communications
- Frame injections
- Exploitation of known vulnerabilities
- Association of malicious devices to the network

2.4. ZigBee

ZigBee is a technology developed by ZigBee Alliance7 which adopts the IEEE standard 802.15.4 for the lower layers of the OSI model, that is, the physical layer (PHY) and the MAC sublayer and adds the network and application layer.

2.4.1. Description:

The main characteristic of ZigBee is its low energy consumption which makes it adequate for devices whose functioning does not have continuous electrical supply and requires the use of external batteries. These devices can function for up to 2 years using batteries.

The characteristics acquired by ZigBee when adopting the IEEE standard are the following:

- Transmission rate between 20 kbit/s up to 250 kbit/s depending on the frequency
- Use of free band frequencies: 2.4 GHz (sane as WiFi), 915MHz and 868 MHz.
- 1, 10 or 16 channels of 5 MHz depending on frequency.
- Short reach excluding functionality of mesh between 10 and 200 metres.

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

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

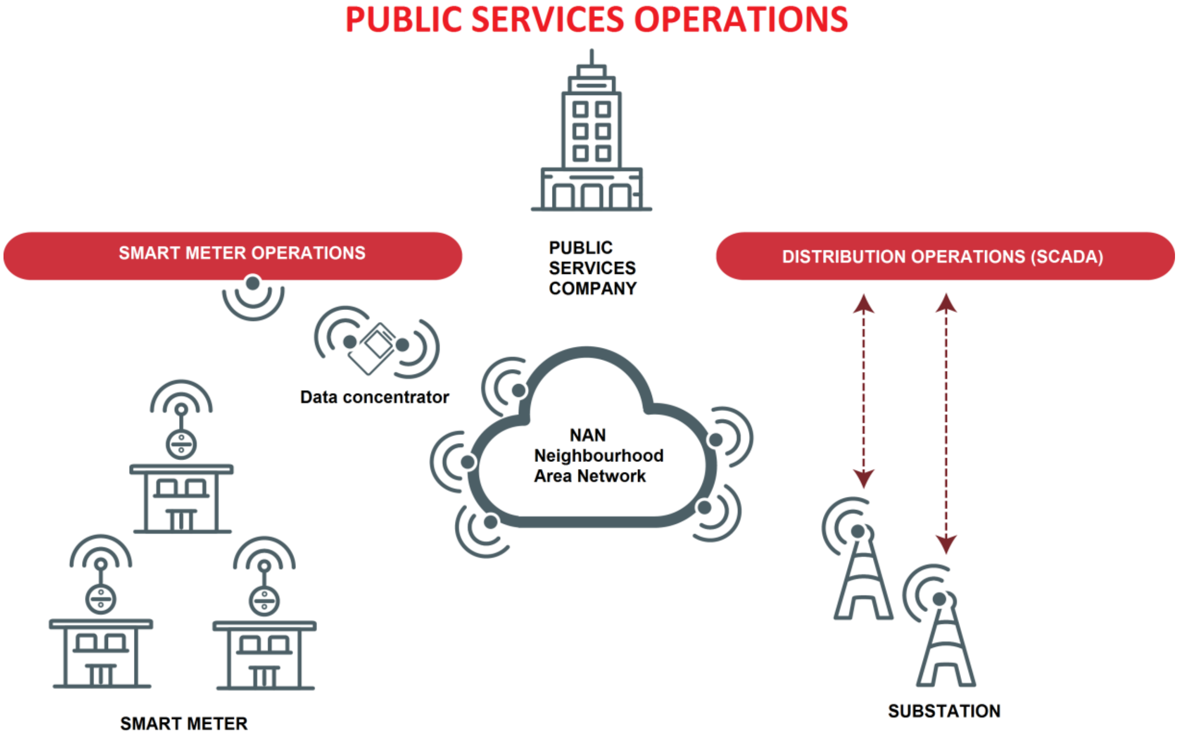

PUBLIC SERVICES OPERATIONS
SMART METER OPERATIONS
PUBLIC SERVICES COMPANY
DISTRIBUTION OPERATIONS (SCADA)
Data concentrator
NAN Neighbourhood Area Network
SMART METER
SUBSTATION

Figure 4: Use of ZigBee in industrial environments Source: http://www.ZigBee.org

In a ZigBee network, three different types of behaviour are distinguished for the devices:

- **Final Device:** Responds to discovery requests for devices sending your own IEEE address to the NWK address (depending on request) and does not have capacity to re-route packets. These types of devices must always act through the parent node, whether a coordinator or a router. Normally these devices are fed by batteries.
- **Router:** Responds to requests sending its IEEE or NWK address and the IEEE or NWK addresses of all associated devices such as ZigBee router (depending on request) maintaining information on the network to determine the best route to transmit the information packet. This component must be able to join a ZigBee network before being able to act as a re transmitter of packets of other routers or final devices.
- **Coordinator:** The node of the network has the sole function of forming part of a network, assuming responsibility for establishing the channel of communications and the network identifier (PAN ID) for the entire network. Responds to the request sending its IEEE or NWK addresses, which have ZigBee associated as a coordinator (depending on the type of request). Once the network is created, the Coordinator performs the functions of the routers, participating in the routing of packets. The coordinator also intervenes in functions related to the management of the security of the communications, acting as Trust Center.

2.4.2. Security Features

The security of transmissions and the data are key points in ZigBee technology. For that reason ZigBee uses the security model of the MAC IEEE sublayer, which specifies 4 security services:

- Use of AES 128 bit encryption: ZigBee uses symmetrical key cryptography and moreover allows for rotation of network keys, which provides an extra level of security in the exchange of information, thus preventing devices external to the network from being able to join it.
- Control of access to devices, maintaining a list of devices "checked" in the network.
- Integration of frames to protect data from being modified by others.
- Refresh sequences to check that the frames have not been replaced by others. The network controller checks these refresh frames and their value, to see if they are those expected.

In ZigBee, the keys are the base of the security architecture and therefore, the protection of same is fundamental. To understand a little more about this architecture, we briefly describe below the 128 bit keys used in same:

- **Master Key:** Key from which the different link keys are generated. The security of the entire network is dependent upon it, as the different services will use unidirectional variations of the link key to avoid security risks. Given the importance of this key, the initial master key must be obtained through secure means, by transport or by pre-installation.
- **Link Key:** They provide security for point to point communications at application level. It is a key only known for its elements that participate in specific communication.
- **Network Key:** Key used at network level by all of the elements belonging to same.

The keys can be obtained by 3 different methods:

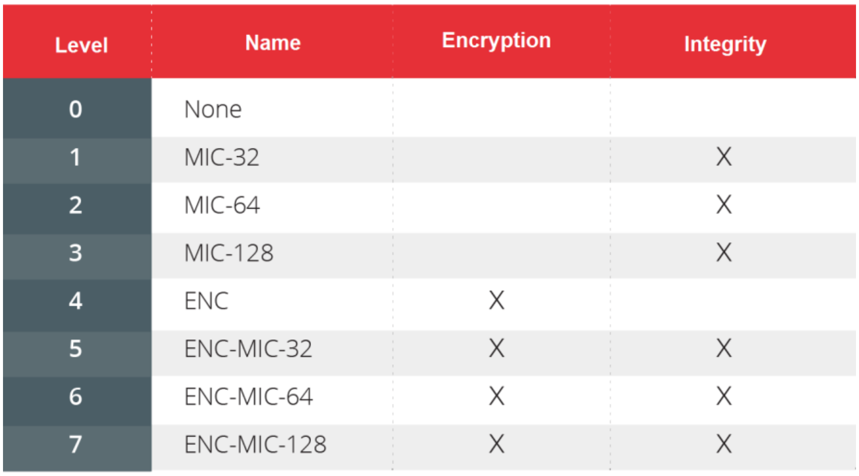
- **Pre-installation:** The manufacturer includes the key in the device itself. In some cases, the user can select one of the keys installed through a set of jumpers in the device in those in which more than one has been pre-installed, but only one will be active at any time. This method is used for the incorporation of master keys.
- **Key transport:** The devices sends a request to a Trust Center so that a key is sent. The trust center represents the origin of trust responsible for performing the distribution of security keys. The trust center has 2 modes of operation:
  - *Commercial Mode:* The trust center maintains a list of devices, master keys, link keys and network keys. In this mode, the memory space required in the trust center increases with the number of devices associated with the network.
  - *Residential Mode:* the network key is the only one that it is compulsory to maintain in the Trust Center. The memory required for the storage of the keys is independent of the size of the network.
- **Establishing the Key:** It is a method of generating keys randomly for two devices without the need to communicate them. This ZigBee service is based on the SKKE (Symmetric-Key Key Establishment) protocol. The destination devices of the key must have a common key, called a master key, which may have been assigned in accordance with the pre-installation method or key transport.

With the security features it offers, ZigBee provides two levels of security for its infrastructure:

- **Standard Security Mode:** Intended for residential installations where there is no criticality of information. The devices are communicated between each other and with the Trust Center using the network key, which can be pre-installed or obtained through transport, in this case without additional security.

- **High Security Mode:** Intended for commercial applications. The devices can communicate through the network key or link key, in such a way that the Security Center must maintain a list of all the keys and perform transport and establishment operations. The network key must be change periodically automatically by the Trust Center. The link key with the Trust Center may be pre-installed or obtained via establishment through the master key, which itself may be re-inserted or obtained via transport.

The specification clarifies that the high security mode must comply with all the features that define it, while the standard mode may implement some features of the upper mode.
Depending on the ZigBee hardware, there may be limitations with respect to the application of security modes, allowing the mode without security or standard mode in normal hardware, while hardware designated PRO allows any security mode or the mode without security to be applied.



Level	Name	Encryption	Integrity
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

Table 2. ZigBee Security Levels

The integrity of the message is verified through an MIC (Message Integrity Code)

2.4.3. Use in Industrial Control Systems

This technology is primarily used for monitoring energy consumption, gathering data from processes and automating buildings. It is common for small sensors to work with this technology, using it to coordinate the infrastructure of a device like an RTU or PLC which will be used to process information.

2.4.4. Best Practice

Over the course of the tests carried out within the study to check the robustness of ZigBee thanks to the configuration and use of bets practice as commented below:

- Use of white lists for access to the ZigBee network devices, thus preventing attacks like DoS DDoS, impersonation of devices, etc.

- ZigBee allows AES 128 bits encryption (the strongest of those defined in the standard IEEE 802.15.4) using symmetric key cryptography and also allowing the period rotation of network keys, which support an extra level of security and ensuring external network devices cannot join it.
- Use of the integrity characteristic of the ZigBee protocol for checking the frames as a countermeasure against replacing them with a possible attacker.

2.5. WirelessHART

WirelessHART, like ZigBee, is based on the standard IEEE 802.15.4 and is used for the wireless connection of HART field devices in the industry.

2.5.1. Description:

WirelessHART technology is developed between 2004 and 2007 and its function is that of providing wireless communications that use the HART protocol. In the year 2010, IEC 62591 was approved as a standard.

The features that define this communication are:

- Confidential and manipulation-proof transmission
- High reliability thanks to Full-Mesh routing
- Low energy consumption thanks to synchronized communication
- 2.4 GHz
- 15 broadcast channels

Within the operating features of the technology, we also distinguish between the following advantages over cabled methods:

- Fewer authorizations and delays
- Use of the same maintenance and diagnostic tools as with traditional cabled HART devices
- Does not require extensive planning or study of radio emissions

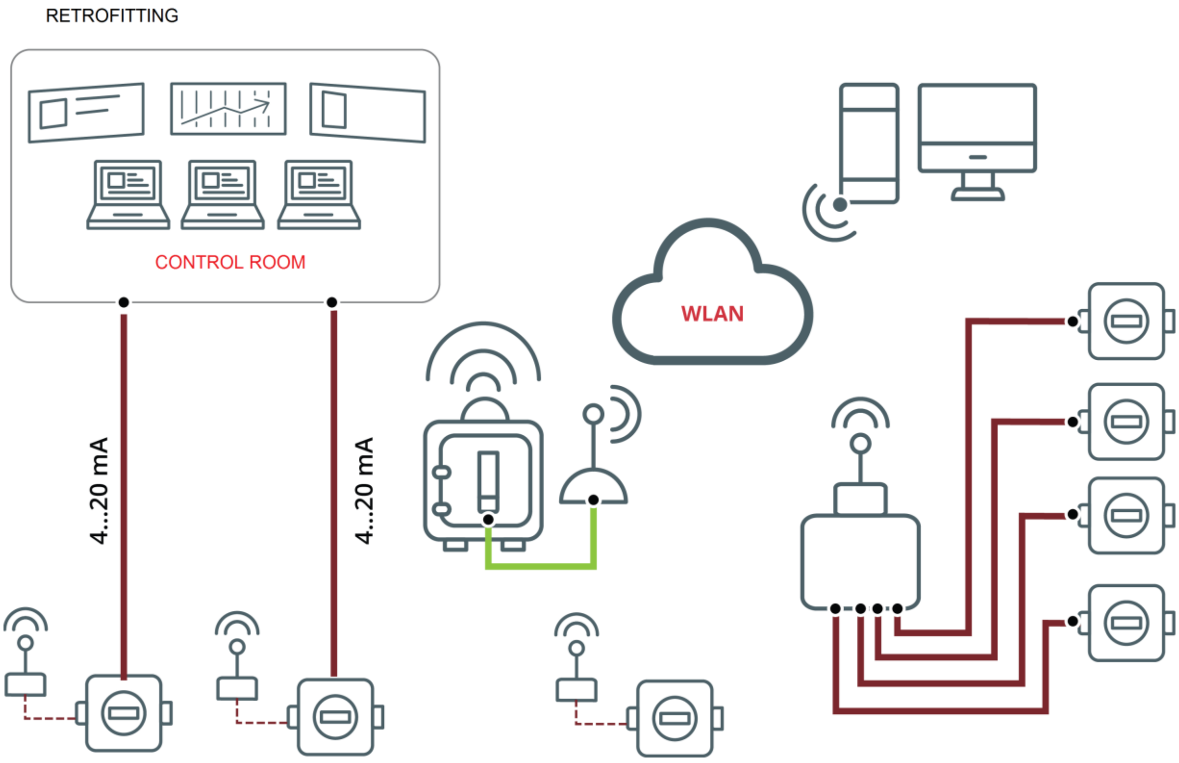


Figure 5: Infrastructure with HART and WirelessHART devices. Source: Industrial Wireless. Wireless transmission from sensor to network. Phoenix Contact

The WirelessHART specification defines the following devices:

- **Network Devices**:
  - **Field Devices:** Sensors and actuators communicated through WirelessHART. They have capacities to route packets from other devices.
  - **Handheld Devices:** Devices to interact in the System. Used by operators.
- Routers or repeaters: Device solely responsible for redirecting packets. In general, these computers are not necessary as any field device can perform the function.
- **Adaptors:** Allow for HART devices to join the WirelessHART network. Have of a cabled interface and a wireless interface. Must be capable of interpreting security material for equipment prior to HART 7 specification.
- **Gateway**: Responsible for connecting the WirelessHART network with other networks. It is the connection point with WirelessHART network.
- **Access Point:** Responsible for providing the wireless network. Communicates directly with the Gateway. Various access points can communicate with the Gateway.
- **Network Manager:** Maintains and updates routes, contains the device list and manages bandwidth.
- **Security Manager:** Responsible for creating and managing the keys used for the network and encrypting communication.

Not all devices are compulsory and must be present in all networks but are used as needed. The Gateway devices, access point, network manager and security manager can all be integrated in a single physical device.

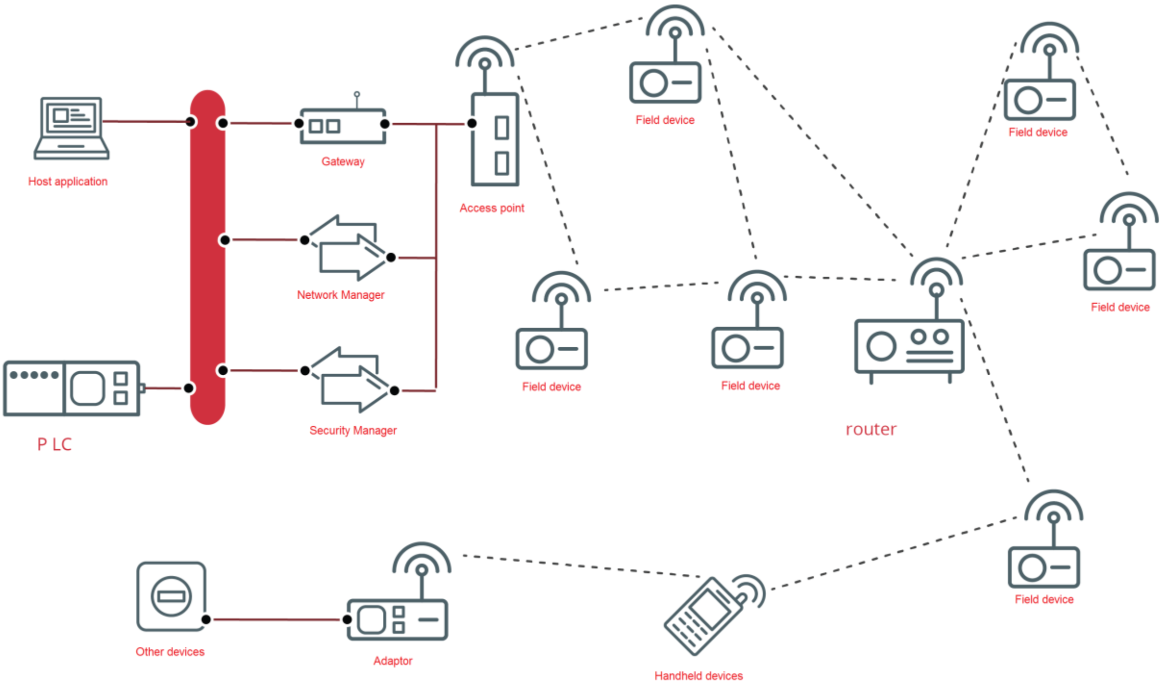


Figure 6: Arrangement of devices in a WirelessHART network

2.5.2. Security Features

WirelessHART, as new generation technology, already incorporates security measures to protect information and access to the network. The security measures it provides are:

- The security measures it provides are:
  - 128 bit AES encryption.
  - Unique encryption key for each message
  - Authentication of devices and data integrity
  - Rotation of keys used to join the network
  - Various levels of security with a minimum always activated
  - Channel hopping
  - Adjustable emission power
  - Various levels of security keys for access
  - Indication of failed attempt to access network
  - Message integrity failure report
  - Authentication failure report

2.5.3. Use in Industrial Control Systems

The use of WirelessHART within industrial control systems is exclusive for sending signals defined in the HART protocol. Among the systems that use this technology, the following can be highlighted:

- Monitoring of medical equipment
- Monitoring of environment, energy management
- Extreme environmental conditions (high corrosion, flooding, etc.)
- Rotary equipment

2.5.4. Best Practice

When using WirelessHART, the following security practices are recommended, corroborated during the study carried out:

- By defect, all WirelessHART devices require a known password such as a Join Key to be able to join the network. The password must be configured on the device before it's associated with the network, which is necessary for the exchange of control packets with the network Gateway.
- Like the use of the single password, it is not recommended as this password is that used in all broadcast type communications, which means that its use in the network is high. The alternative is to use the ACLs (Access Control Lists). These ACLs will control access to the network and function thanks to checking on the part of the Gateway of the origin of the packet (through MAC or issuer number series).
- Mix the common key option and, once the device is associated with the network, create an access control list. Once the devices are associated with a network, they can communicate between themselves and with the Gateway. The communications between the two devices are also permitted and a specific key can be used. The negotiation of this key is carried out with the Gateway, which is distributed to the two devices so that they use it in communication between them, as it will no longer depend on the Gateway.

2.6. Summary

WiFi, Trusted Wireless, Bluetooth, ZigBee and WirelessHART are the most widely used technologies for wireless communications systems in the industrial sector. Depending on the specific sector, the physical environment, the process requirements and their critical nature, and, above all, the required security standards, it is necessary to analyse the pros and cons in order to establish the best options for a specific sector.

Security aside, the following diagram allows us to compare the capacities of each of the technologies together.

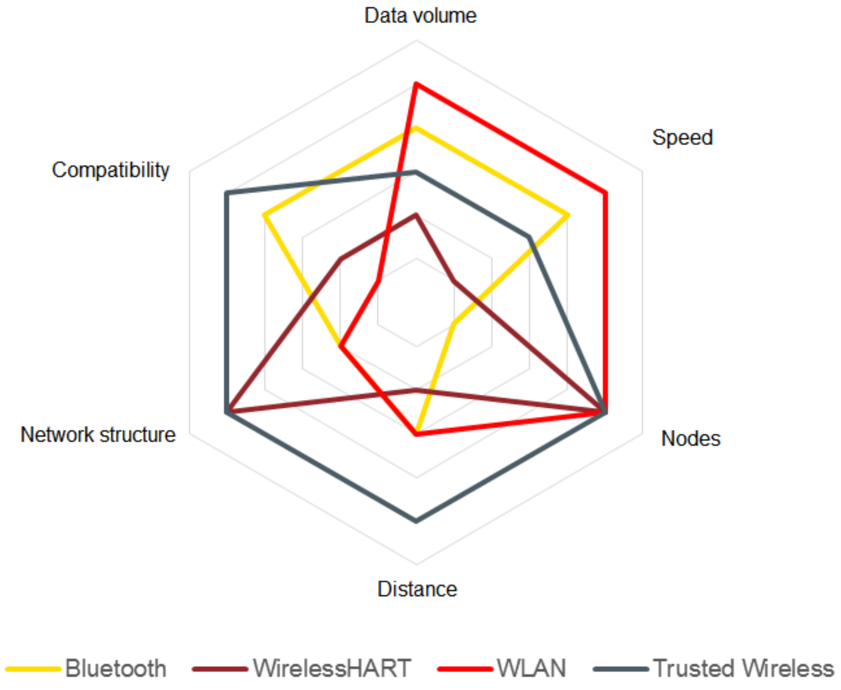


Figure 7: Comparison of features of the different technologies

As shown in Figure 7, for example, WirelessHART is a technology that supports many nodes with various network structures, however, supports only short distances and relatively slow speeds. On the contrary, WLAN allows for high volumes of data, high speeds and nodes but offers poor consistency with other networks.

3. OTHER WIRELESS TECHNOLOGIES

Apart from the most widely used wireless technologies described in the last section, it is interesting to consider other technologies that, while they may not be used on the same scale in industrial environments, are certainly interesting alternatives in specific sectors with special requirements.

3.1. WiMax

WiMax wireless technology (Worldwide Interoperability for Microwave Access) is among the so-called last mile technologies that allow data to be received by microwaves and retransmitted by radio waves.

3.1.1. Description:

WiMax networks arose as an alternative to cable to bring communication to isolated rural areas where the physical infrastructure proved very costly. With this technology, the degree of equipment and the environmental impact on rural areas was reduced as only antennae were used, often located in shared areas with television and mobile phone antennae.

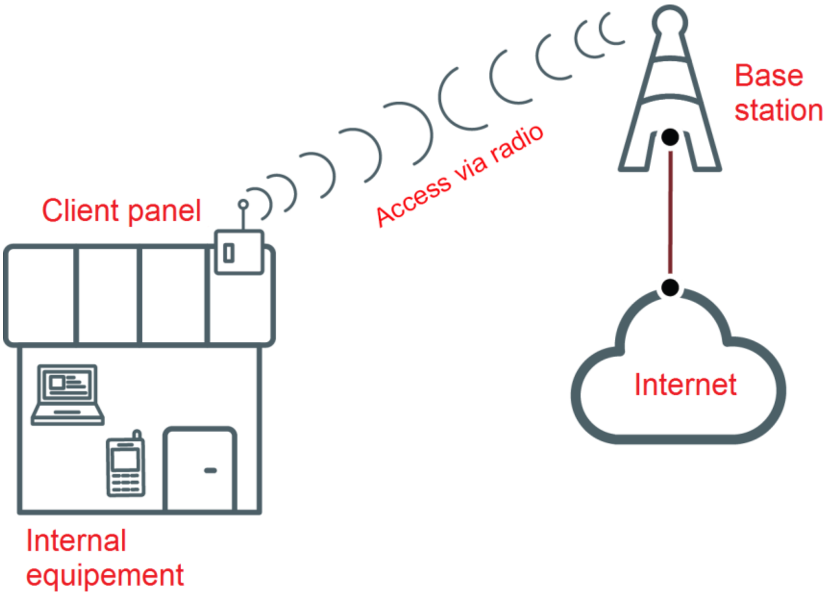
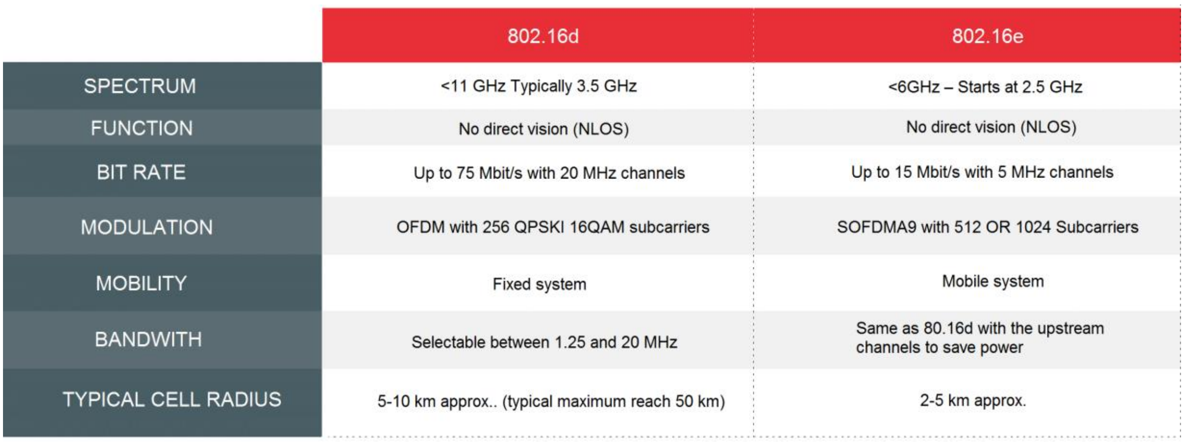


Figure 8: WiMax Access Network. Source: Planning via Atoll of WiMax mobile network for centres of the University of Seville.

WiMax poses different advantages including the bandwidth advantages it offers in areas where the roll-out of cable or fibre-optic is very costly for the user (rural areas) due to the low population density. This communication technology adapts to the standard IEEE 802.16 and there are 2 variants:

- WiMAX (802.16d-2004) or “Fixed WiMAX”: for areas with low population density.
- WiMAX (802.16e-2005) or “Mobile WiMAX”: for applications that require greater bandwidth in both transmission directions and in mobile form.

In **¡Error! No se encuentra el origen de la referencia.** we can observe a comparison of he features of WiMax fixed and WiMax mobile:



	802.16d	802.16e
SPECTRUM	<11 GHz Typically 3.5 GHz	<6GHz – Starts at 2.5 GHz
FUNCTION	No direct vision (NLOS)	No direct vision (NLOS)
BIT RATE	Up to 75 Mbit/s with 20 MHz channels	Up to 15 Mbit/s with 5 MHz channels
MODULATION	OFDM with 256 QPSKI 16QAM subcarriers	SOFDMA9 with 512 OR 1024 Subcarriers
MOBILITY	Fixed system	Mobile system
BANDWITH	Selectable between 1.25 and 20 MHz	Same as 80.16d with the upstream channels to save power
TYPICAL CELL RADIUS	5-10 km approx.. (typical maximum reach 50 km)	2-5 km approx.

Table 3: Summary of standard WiMAX features

3.1.2. Security Features

WiMax defines a sublayer of security dedicated specifically to covering the three basic principles of security in networks (Confidentiality, Authentication and Integrity) to provide users with as secure a browsing experience as possible in their network.

WiMAX is based on a security system with two principles.

Authentication: This method guarantees users secure access to the network, preventing other unauthorised users from making use of the wireless connection. In the IEEE 802.16.2009 standard, two authentication processes are defined.

- **OSA (Open System Authentication):** The Client makes an authentication request associated with the MAC address after the request, following a response from the Base Station (BS) with the acceptance or denial of the request. The BS only uses an option filter by MAC address.
- **SKA (Shared Key Authentication):** Used in shared key processes, where both ends must know said keys to guarantee a more secure authentication. For authentication through shared keys, WiMax defines the PKM (Privacy Key Management) protocol so that a Subscriber Station (SS) can exchange keys and obtain the authorisation of the Station Base. In addition to this task, the KPM is also responsible for refreshing the keys, the periodic re-authorisation, etc. Described below is the process the follows the PKM protocol to carry out the authentication between the BS and the SS.

Encryption: After the Station Base authorises the Subscriber base, an encryption mechanism is also necessary to ensure confidentiality and integrity of the data shared between the two. For that, the SS send a request for the encryption keys called the TEKs (Traffic Encryption Keys) to the BS, which are sent by the BS in the response message. These messages are also encrypted with a key known by both parties. The algorithm used for the encryption of the TEKs can be one of 3 kinds: *3DES (Triple Data Encryption Standard)*, *AES (Advanced Encryption Standard)* or *RSA (Rivest, Shamir y Adleman)*.

Once the TEKs are known, various techniques can be used to encrypt the data: CBC (DES), CBC (AES), CTR (AES), CCM (AES).

Some of the advantages of the encryption mechanisms that implement WiMAX with respect to other technologies are the following:

- Robust algorithms.
- Allow independent encryption for each data flow.
- Support dynamic key generation with variable life times.

On the other hand, independently of the encryption and authentication mechanisms, the design of the WiMAX technology itself implies added value IN questions of security:

- WiMax is not designed as a local access network for the final user, but was designed as a MAN/WAN operator technology, which has the capacity to interconnect with many users who don't necessarily have to know each other. As it is a large scale network, the technology itself is designed to be able to ensure security with full guarantees.
- Access to the network is not random, but entirely determined and ruled from a Base Station that acts as the controller of transmissions at all times.

3.1.3. Use in Industrial Control Systems

WiMax networks can have many practical uses for all kinds of organizations, companies and businesses. In industrial environments they have the following features:

- Access to a wireless network in industrial units across all the land belonging to the company.
- Internet connection with no type of cable to a pc, laptop, PDA or smartphone.
- Hotspot service for access restricted by time or volume.
- Access to VoIP services without cables that allow for communication between different locations within the industrial plant.

3.1.4. Best Practice

WiMAX networks have weaknesses in security[8] that can be resolved with the appropriate configuration and the application of some security recommendations:

- Develop a robust security policy and implement it. A security policy is responsible for the design, implementation and maintenance of adequate security technologies. The WiMAX network devices must be configured to comply with the policy.
- Assess countermeasures before use. Some WiMAX products use cryptographic models that meet specific standards (Such as the American FIPS[9]). When integrating WiMAX certificates with other security solutions it must be taken into account that certifications do not always stretch to the definitive solution. Organizations must work closely with WiMAX providers to ensure they know the possible limitations of network configuration.
- Require mutual authentication for devices. The function of mutual authentication is supported, but not activated, by default. They must use devices capable of using reliable authentication protocols, such as EAP. Where this is not possible, security must be applied in superior layers using encryption or VPN solutions.

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

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

- Implement encryption algorithms to protect data communications. WiMAX presents management and data messages, but the encryption does not apply to management messages to increase the efficiency of network operations, while data messages are encrypted on a native basis.

3.2. Mobile networks

Mobile phones, smartphones and tablets are becoming more essential every day. Their use within control systems has also grown in order to facilitate certain tasks. But mobile communications are only used with these devices; point-to-point communications are also possible with this technology.

3.2.1. Description:

Various types of technology can be found in the different mobile networks over the years.

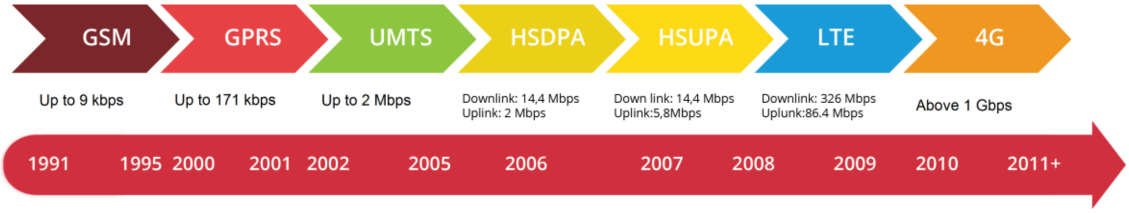


Figure 9: Evolution of mobile networks

Principally, for communication of messages and events, two types of technology have been used: GSM and 3G (UMTS and HSDPA)

GSM technology is based on an open system for international mobile communication used in over 200 countries. The main features are:

- Extensive reach according to need, through the use of antennae and repeaters.
- Data speeds of up to 210 kbit/s
- Various band frequencies: 850, 900, 1800 y 1900 MHz

3G designates third generation telephone standards. Compared to its predecessor, it considerably improved services. The most notable features are:

- Extensive reach according to need, through the use of antennae and repeaters
- High data speeds of up to 7.2 Mbits/s
- Two frequencies: 900 and 2100 MHz

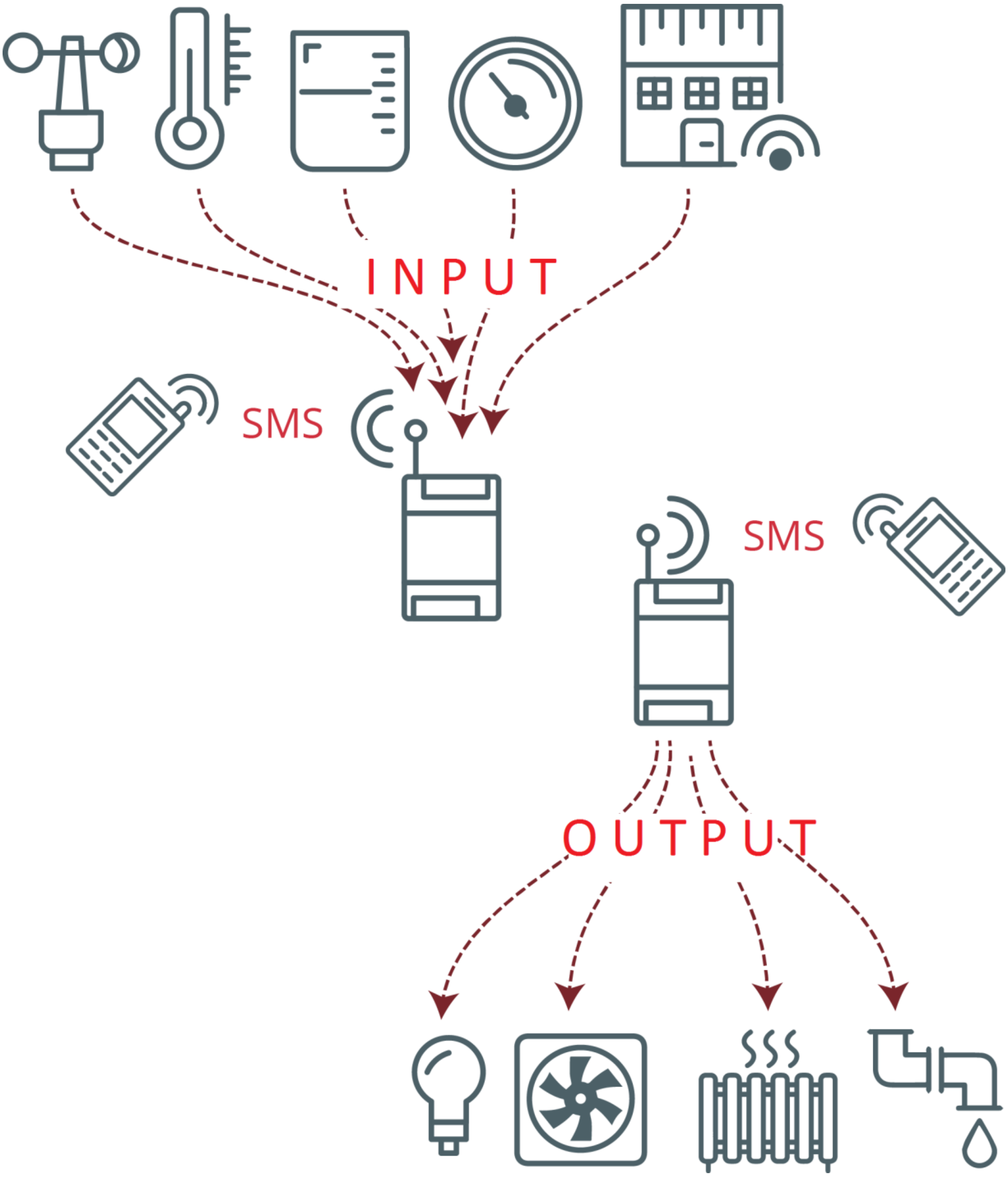


Figure 10: Use of mobile technologies in control systems Source: Industrial Wireless. Wireless transmission from sensor to network. Phoenix Contact

3.2.2. Security Features

The security features have also evolves at the same level as the technology, changing encryption algorithms and adding security measures.

GSM technology offers:

- Authentication of the identity of the user
- Confidentiality of the identity of the user
- Confidentiality of signalling data
- Confidentiality of user data

All of these security measures are carried out at hardware level through symmetric key encryption systems and with A3, A5 and A8 algorithms, today considered insecure.

3G networks offer a greater degree of security in comparison with their 2G predecessors. Among the most outstanding features are:

- Network authentication
- End to End security
- Replacement of A5/1 flow (vulnerable) with KASUMI (now also vulnerable)

3.2.3. Use in Industrial Control Systems

The use of mobile network in control systems very much depends on the technology used.

GSM technology, as it has lower capacity for the transfer of information, is used for sending field signals or events with low data transfer.

- E/S Wireless: E/S analogue and digital signals
- Wireless Serial: RS-232 data series
- Wireless Ethernet: Ethernet data
- Alarm signalling: SMS and email

3G technologies improved the capacity of GSM and therefore its use in industrial control systems is reserved for levels with greater needs.

- Wireless Ethernet: Ethernet transmission
- Alarm signalling: SMS and email

3.2.4. Best Practice

Mobile networks used in control systems are no different from those used in the domestic or business environments, and therefore the security recommendations for these networks are the same in all cases. The most important recommendations are:

- Disable 2G networks (GSM, GPRS y EDGE): they are insecure networks by default. If any type of information must be sent via these networks, you must ensure that it has been encrypted in advance.
- The A5/3 algorithm in UMTS is insecure. There are tables of passwords to break the algorithm and therefore you should also try to avoid using UMTS technology.

3.3. Radiocommunications

Radiolink technologies are used for long distance communications. Among the most common raidolinks are satellite communications, microwaves and terrestrial raidolinks.

3.3.1. Description:

Radiocommunications systems are characterised by the availability of a sender element, another receptor and sometimes repeater elements.

There are two types of repeaters:

- Passive: They act as mirrors that reflect the signal. Their function is usually to negotiate obstacles, normally mountains and hills by positioning them at the peak of sender and receptor's view.
- Active: Their characteristic function is the regeneration of the signal. The signal that arrives, generally fairly diminished, is regenerated to be sent to another antenna and to the receptor.

The features that define this communication are:

- Range of frequencies between 1 and 300 GHz.
  - Depending on the specific spectrum, it will be radio link or microwave link.
  - The main frequencies are 12 GHz, 18 and 23 GHz.
- Distances above 50 km, depending on the frequency used.
- Losses. Radiocommunications are affected by meteorological phenomenon, as well as other intrinsic physical losses in the wave due to diffraction, reflection, etc.

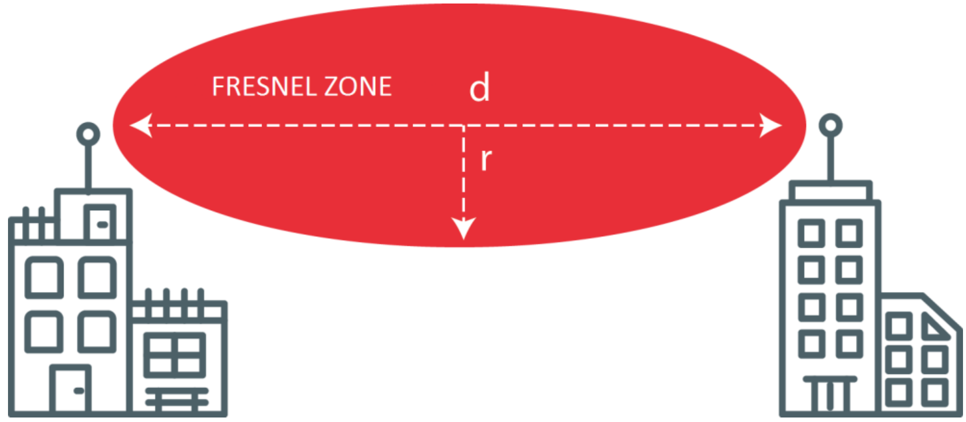
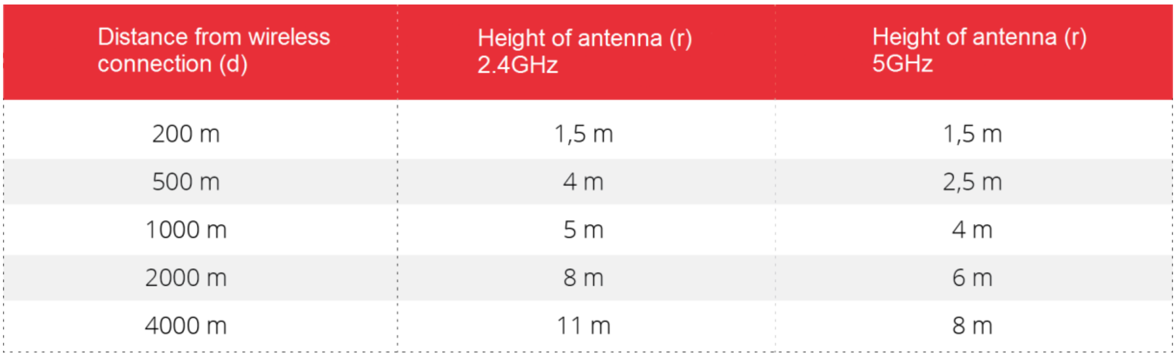


Figure 11: Calculation of height of antennae due to distance and frequency of radiocommunication



Distance from wireless connection (d)	Height of antenna (r) 2.4GHz	Height of antenna (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

Table 4. Height values of antennae by distance and frequency of radiocommuunication

3.3.2. Security Features

By definition, radiocommunications do not define security methods for transmissions.

3.3.3. Use in Industrial Control Systems

The use of radiocommunications systems in industry control systems in centred on sending large quantities of information, usually with no time restrictions, between different, remote facilities of the company.

3.3.4. Best Practice

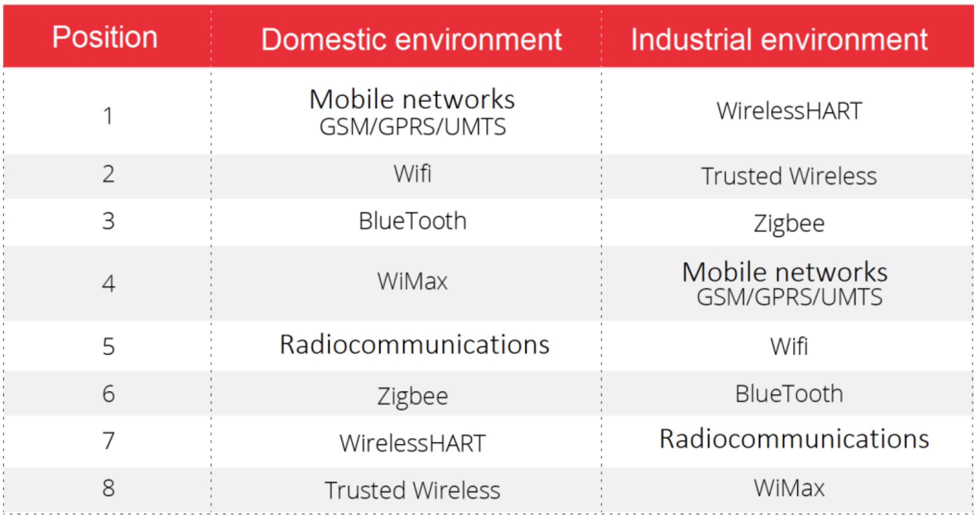
The main problem with communications via radio is the extent of the reception area of messages, which will make it necessary to take security measures in this respect.

- Authentication: Communications via radiolink area usually point to point, and therefore authentication of both ends is a simple process which will impede other elements from joining the network.
- Encrypted: by definition, most protocols used in radio link do not use encryption, therefore it is necessary to apply encryption prior to communication.

4. COMPARISON BETWEEN INDUSTRIAL AND DOMESTIC WIRELESS NETWORKS

4.1. Use

Several technologies included in the study come from domestic environments where they have an important presence. Today, the idea of a home with an internet connection that does not use WiFi or a phone without Bluetooth to be able to connect to another device, from external speakers to a hands-free car system, is unthinkable. This presence in the industrial sector, while not as important as in domestic/business environments, is increasingly common. Nevertheless, although their presence is growing in all cases, there are differences with more widely used technologies. The table below is a comparison of wireless technologies in order of their presence in both environments, the first position being the most used in each case (completing the evaluation of the technologies on which to focus the study and without taking others into account).



Position	Domestic environment	Industrial environment
1	Mobile networks GSM/GPRS/UMTS	WirelessHART
2	Wifi	Trusted Wireless
3	BlueTooth	Zigbee
4	WiMax	Mobile networks GSM/GPRS/UMTS
5	Radiocommunications	Wifi
6	Zigbee	BlueTooth
7	WirelessHART	Radiocommunications
8	Trusted Wireless	WiMax

Table 5. Comparison of use of wireless technologies

Some of the technologies have no presence in either of the two environments, thus, for example, it is practically impossible to find domestic communications over WirelessHART or Trusted Wireless as they are exclusively industrial technologies; ZigBee communications are also uncommon in domestic environments but can be found in certain uses such as gaming or electronic devices. In the industrial sector all are used despite the fact that uses of Radiocommunications and WiMax are few and far between and far from the extent of the other technologies.

4.2. Components

The devices necessary to create networks that use these technologies, in both the domestic and the industrial environments, are the same, therefore, in general, the devices can be interchangeable.

The differences are mainly physical and lie in the fact that the devices used for industrial systems must be prepared to work in extreme conditions (temperature, pressure, interference, radiation, etc.) are usually smaller and are prepared for assembly on a DIN rail[10], and can thus be included in equipment cabinets together with PLC and other electronic equipment.

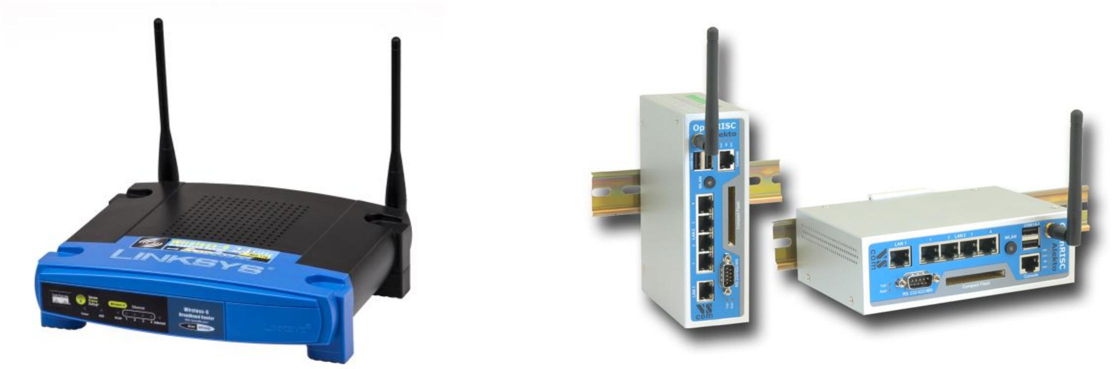


Figure 12: Domestic WiFi router (left) and industrial WiFi router (right) Source: http://www.visionsystems.de

For these same reasons of working conditions, the costs of production are still between domestic and industrial devices are much greater in the latter case despite functionally similar capacities.

4.3. Security

Regarding security, and starting from an equal base of intrinsic measures in the security of each technology, the differences arise in the rigour with which the protocols are configured, applied and used in each technology in the different environments.

For example, in reference to WiFi networks, the difference lies in their sharing and security configuration. In domestic environments it is possible to find open access public networks, this being most common in large spaces or in public bodies that provide services to citizens. In terms of sharing, there are final clients with WiFi networks installed in their homes or business that decide to share part of their bandwidth. These conditions and configurations would be unthinkable in industrial environments where the aim to keep all communications as closed as possible with access restricted.

If we consider encryption, in both senses they attempt to correctly use the protocols available for the technology in use that permits a sufficiently robust encryption. The case may arise where by either poor configuration or carelessness, available measures are not activated. That is why security reviews of an organization's networks are so important and necessary.

[10] https://en.wikipedia.org/wiki/DIN_rail

5. LABORATORY SECURITY ANALYSIS

5.1. WiFi

WiFi networks are widely used in domestic environments, and although they are not as common in industrial settings, it is not strange to find a connection of this type, even if it is a corporate network. With regard to the security on WiFi communications, there is a wide array of documentation[11] and, given that this is a well-known technology which is more linked to the IT world than the OT world, we will not discuss it in detail in this study in order to directly focus attention on other wireless technologies which are more commonplace in the industry.

5.2. Bluetooth

The laboratory tests were carried out with three Bluetooth devices, one was configured as the master, another as the slave and the third was used for capturing packets transmitted by the others.

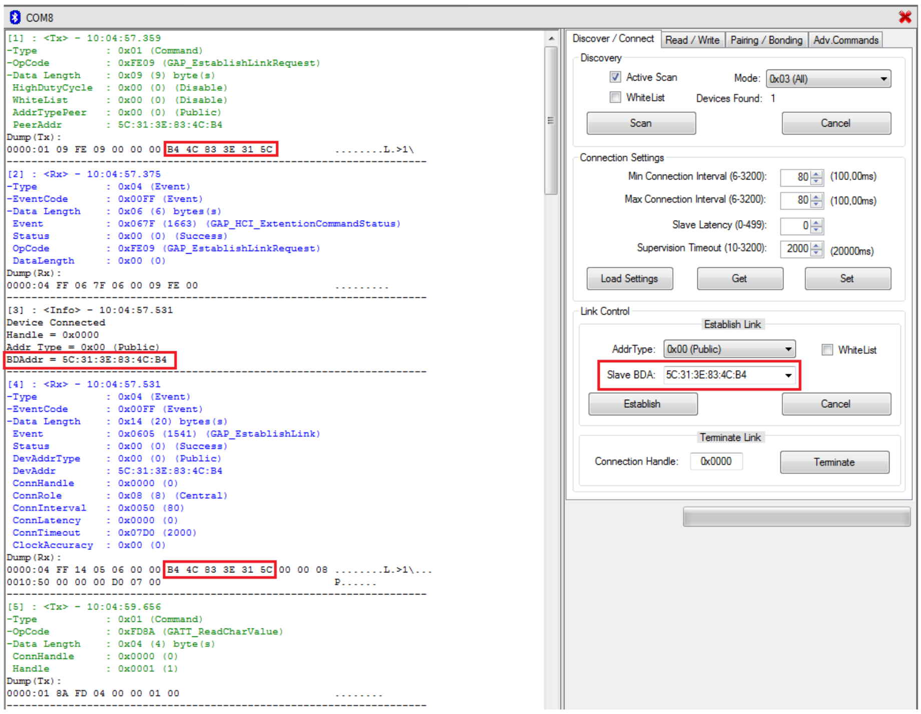
The tests carried out consisted of diverse data reading with different security configurations, capturing the exchanged packets at all times and subsequently analysing them.

Bluetooth Connection

The first test carried out was the undertaking of a Bluetooth communication and checking all of the stages through which it passed and the security applied in each of them. Bluetooth allows for multipoint connections, but in order to limit the analysis and make it simpler, only point to point connections between to elements will be worked on.

The first stage is the establishing of the connection. For this, the slave device sends messages continuously until a master, which is undertaking a discovery process, receives the packets and starts the process of establishing the connection.

[11] See the example: https://www.incibe.es/CERT/guias_estudios/guias/GuiaManual_wifi_pymes



COM8

```
[1] : <Tx> - 10:04:57.359
-Type               : 0x01 (Command)
-OpCode             : 0xFE09 (GAP_EstablishLinkRequest)
-Data Length        : 0x09 (9) byte(s)
 HighDutyCycle      : 0x00 (0) (Disable)
 WhiteList          : 0x00 (0) (Disable)
 AddrTypePeer       : 0x00 (0) (Public)
 PeerAddr           : 5C:31:3E:83:4C:B4
Dump(Tx):
0000:01 09 FE 09 00 00 00 B4 4C 83 3E 31 5C          ........L.>1\
-------------------------------------------------------------------
[2] : <Rx> - 10:04:57.375
-Type               : 0x04 (Event)
-EventCode          : 0x00FF (Event)
-Data Length        : 0x06 (6) bytes(s)
 Event              : 0x067F (1663) (GAP_HCI_ExtentionCommandStatus)
 Status             : 0x00 (0) (Success)
 OpCode             : 0xFE09 (GAP_EstablishLinkRequest)
 DataLength         : 0x00 (0)
Dump(Rx):
0000:04 FF 06 7F 06 00 09 FE 00                      .........
-------------------------------------------------------------------
[3] : <Info> - 10:04:57.531
Device Connected
Handle = 0x0000
Addr Type = 0x00 (Public)
BDAddr = 5C:31:3E:83:4C:B4
-------------------------------------------------------------------
[4] : <Rx> - 10:04:57.531
-Type               : 0x04 (Event)
-EventCode          : 0x00FF (Event)
-Data Length        : 0x14 (20) bytes(s)
 Event              : 0x0605 (1541) (GAP_EstablishLink)
 Status             : 0x00 (0) (Success)
 DevAddrType        : 0x00 (0) (Public)
 DevAddr            : 5C:31:3E:83:4C:B4
 ConnHandle         : 0x0000 (0)
 ConnRole           : 0x08 (8) (Central)
 ConnInterval       : 0x0050 (80)
 ConnLatency        : 0x0000 (0)
 ConnTimeout        : 0x07D0 (2000)
 ClockAccuracy      : 0x00 (0)
Dump(Rx):
0000:04 FF 14 05 06 00 00 B4 4C 83 3E 31 5C 00 00 08 ........L.>1\...
0010:50 00 00 00 D0 07 00                            P......
-------------------------------------------------------------------
[5] : <Tx> - 10:04:59.656
-Type               : 0x01 (Command)
-OpCode             : 0xFD8A (GATT_ReadCharValue)
-Data Length        : 0x04 (4) byte(s)
 ConnHandle         : 0x0000 (0)
 Handle             : 0x0001 (1)
Dump(Tx):
0000:01 8A FD 04 00 00 01 00                         ........
-------------------------------------------------------------------
```

Discovery

☑ Active Scan Mode: 0x03 (All)
□ WhiteList Devices Found: 1

Connection Settings

Min Connection Interval (6-3200): 80 (100,00ms)
Max Connection Interval (6-3200): 80 (100,00ms)
Slave Latency (0-499): 0
Supervision Timeout (10-3200): 2000 (20000ms)

Link Control

Establish Link
AddrType: 0x00 (Public) □ WhiteList
Slave BDA: 5C:31:3E:83:4C:B4

Terminate Link
Connection Handle: 0x0000

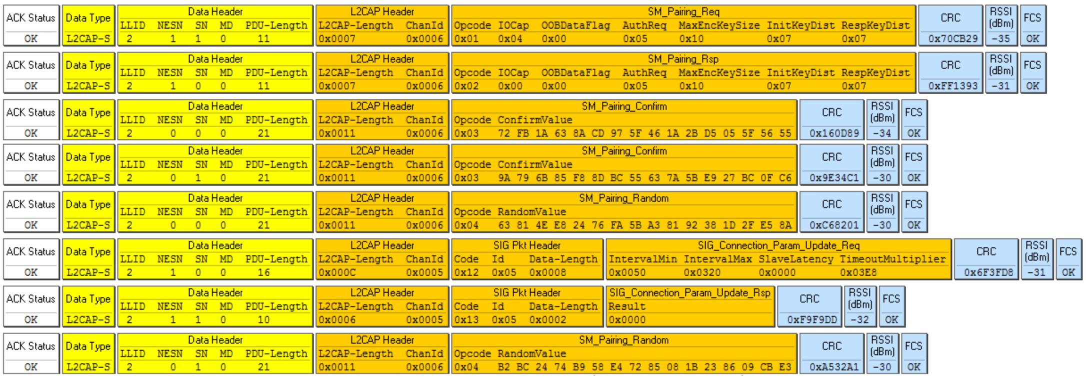
Figure 13: Establishing the master/slave connection

The first request shown in the image (in green) represents the master's attempt at establishing the connection, the two following responses (in blue) show the interaction of the slave to establish the connection.

Once the connection between master and slave has been established, the clock is synchronised as is the order of frequency channel hopping. Subsequently, information is exchanged on an uninterrupted basis following the specifications of Bluetooth technology with constant channel hopping.

By analysing the data messages captured, it can be concluded that if the channel hopping starts in a random way among channels, a determined moment arises in which the entire hopping sequence is repeated in the same order. As a result of the test observations, it can be concluded that the predictability of the hopping throughout all of the channels in which Bluetooth works could be taken advantage of by a potential attacker in order to carry out advanced attacks given that in knowns the channel the next message must go to, and thus creating denial of service or other, more complex attacks.

In order to add an extra level of security, Bluetooth offers an exchange of information authentication via a pairing process. This process ensures that the devices exchanging information are what they claim to be.



```
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
```

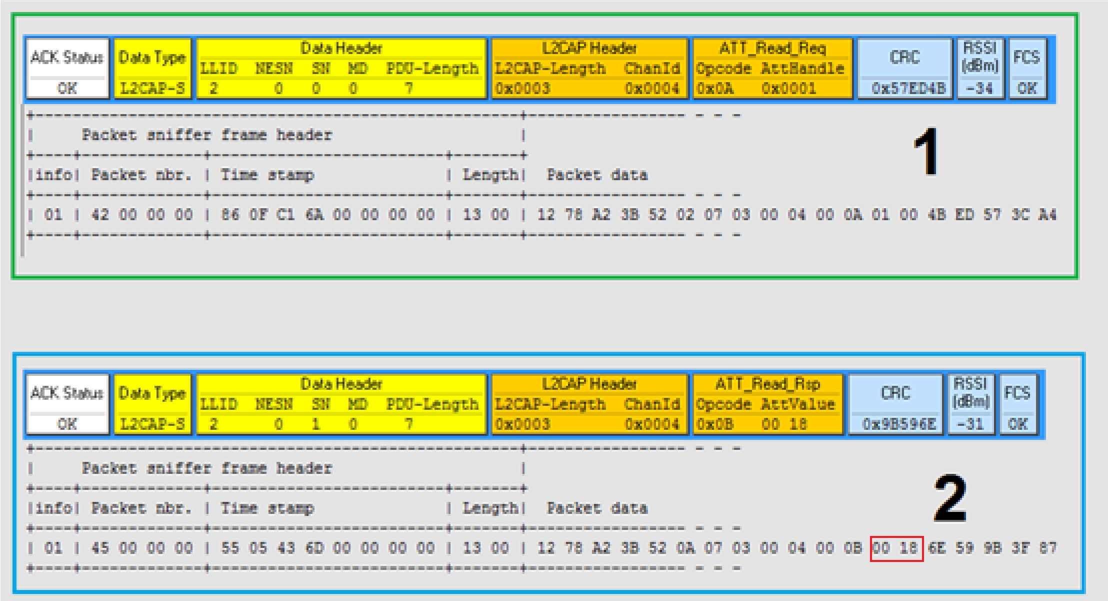
Figure 14: Frames of a pairing process

The pairing process requires the use of a key or PIN (passkey) that must be known beforehand, thus preventing malicious devices from joining the network. After exchanging the PIN the process is finished and authentication of ends is provided. The PIN is not transferred in wireless communication, since it is based on a challenge-response scheme in order to verify that the participant has knowledge of the secret key. Thanks to pairing, it is possible to avoid man-in-the-middle (MiTM) attacks.

Data reading

The reading of data allows for the analysis of the encryption capacities that Bluetooth has. The only condition is for data reading to be carried out is that a connection has been made between the two devices. Due to the fact that through the establishing of the connection the devices are not authenticated, the readings are not encrypted and so all types of transmission traffic could be intercepted and interpreted

Through the pairing, the reading continues to not be encrypted as the only the ends have been authenticated, and so the bugging of network traffic continues to be effective.



```
ACK Status | Data Type | Data Header                          | L2CAP Header               | ATT_Read_Req         | CRC      | RSSI (dBm) | FCS
           |           | LLID NESN SN MD PDU-Length           | L2CAP-Length ChanId        | Opcode AttHandle     |          |            |
OK         | L2CAP-S   | 2    0    0  0  7                    | 0x0003       0x0004        | 0x0A   0x0001        | 0x57ED4B | -34        | OK

+----------------------------------------------------------+------------------ - - -
|     Packet sniffer frame header                          |
+----+-------------+--------------------------+-------+
|info| Packet nbr. | Time stamp               | Length|  Packet data
+----+-------------+--------------------------+-------+------------------ - - -
| 01 | 42 00 00 00 | 86 0F C1 6A 00 00 00 00 | 13 00 | 12 78 A2 3B 52 02 07 03 00 04 00 0A 01 00 4B ED 57 3C A4
+----+-------------+--------------------------+-------+------------------ - - -
```

1

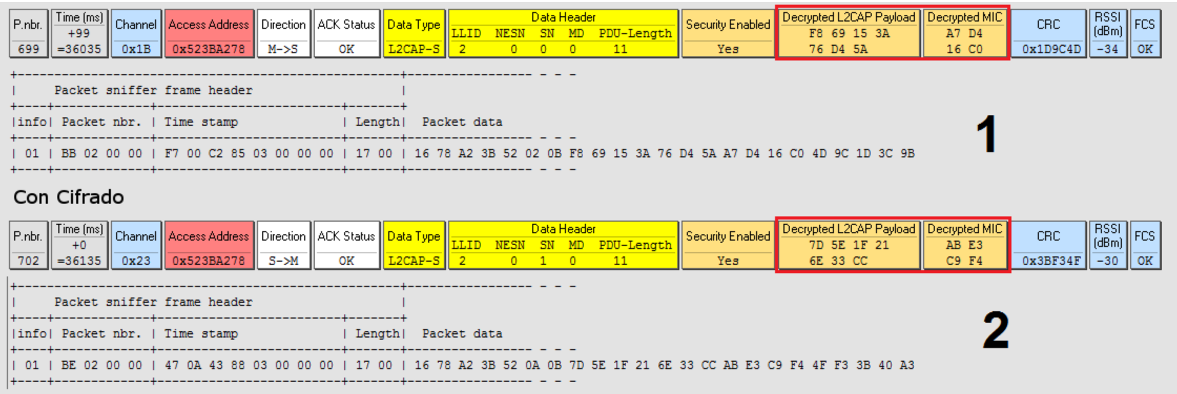
```
ACK Status | Data Type | Data Header                          | L2CAP Header               | ATT_Read_Rsp         | CRC      | RSSI (dBm) | FCS
           |           | LLID NESN SN MD PDU-Length           | L2CAP-Length ChanId        | Opcode AttValue      |          |            |
OK         | L2CAP-S   | 2    0    1  0  7                    | 0x0003       0x0004        | 0x0B   00 18         | 0x9B596E | -31        | OK

+----------------------------------------------------------+------------------ - - -
|     Packet sniffer frame header                          |
+----+-------------+--------------------------+-------+
|info| Packet nbr. | Time stamp               | Length|  Packet data
+----+-------------+--------------------------+-------+------------------ - - -
| 01 | 45 00 00 00 | 55 05 43 6D 00 00 00 00 | 13 00 | 12 78 A2 3B 52 0A 07 03 00 04 00 0B 00 18 6E 59 9B 3F 87
+----+-------------+--------------------------+-------+------------------ - - -
```

2

Figure 15: Capturing of non-encrypted sent frames

When a communication channel is established without security, reading and writing performed can be easily captured. As only the identification of ends has been carried out, any of them could have been impersonated and continued with communication.

In order to carry out the encryption of a channel and impede the interpretation of captured data, there is the option of using a long term key (LKT). The LKT is used after the pairing, this key must be known by those involved in the communication at the time of activating the security measure.



P.nbr.	Time (ms)	Channel	Access Address	Direction	ACK Status	Data Type	Data Header					Security Enabled	Decrypted L2CAP Payload	Decrypted MIC	CRC	RSSI (dBm)	FCS
							LLID	NESN	SN	MD	PDU-Length						
699	+99 =36035	0x1B	0x523BA278	M->S	OK	L2CAP-S	2	0	0	0	11	Yes	F8 69 15 3A 76 D4 5A	A7 D4 16 C0	0x1D9C4D	-34	OK

```
+----------------------------------------------------+----------------- - - -
|     Packet sniffer frame header                    |
+----+-------------+--------------------------+-------+
|info| Packet nbr. | Time stamp               | Length|  Packet data
+----+-------------+--------------------------+-------+----------------- - - -
| 01 | BB 02 00 00 | F7 00 C2 85 03 00 00 00 | 17 00 | 16 78 A2 3B 52 02 0B F8 69 15 3A 76 D4 5A A7 D4 16 C0 4D 9C 1D 3C 9B
+----+-------------+--------------------------+-------+----------------- - - -
```

Con Cifrado

P.nbr.	Time (ms)	Channel	Access Address	Direction	ACK Status	Data Type	Data Header					Security Enabled	Decrypted L2CAP Payload	Decrypted MIC	CRC	RSSI (dBm)	FCS
							LLID	NESN	SN	MD	PDU-Length						
702	+0 =36135	0x23	0x523BA278	S->M	OK	L2CAP-S	2	0	1	0	11	Yes	7D 5E 1F 21 6E 33 CC	AB E3 C9 F4	0x3BF34F	-30	OK

```
+----------------------------------------------------+----------------- - - -
|     Packet sniffer frame header                    |
+----+-------------+--------------------------+-------+
|info| Packet nbr. | Time stamp               | Length|  Packet data
+----+-------------+--------------------------+-------+----------------- - - -
| 01 | BE 02 00 00 | 47 0A 43 88 03 00 00 00 | 17 00 | 16 78 A2 3B 52 0A 0B 7D 5E 1F 21 6E 33 CC AB E3 C9 F4 4F F3 3B 40 A3
+----+-------------+--------------------------+-------+----------------- - - -
```

Figure 16: Capturing of encrypted sent frames

During the pairing process there is the option of storing the long term key. This persistent key is used to ascertain in advance a communication between devices, the key of which will encrypt communication, being capable of carrying out encrypted information exchange without having to carry out the previous steps of pairing and authentication again. The LTK can be used by both devices provided that these retain the key saved without it being deleted manually.

5.3. ZigBee

For the laboratory tests with ZigBee, a development kit was used which was made up of autonomous devices, with the function of router or final device, and a management device, with network coordinating functions.

In order to show the traffic exchanged between ZigBee devices in a practical way, different tests were carried out, among which captures of network traffic corresponding to the reading and writing parameters of a node were analysed.

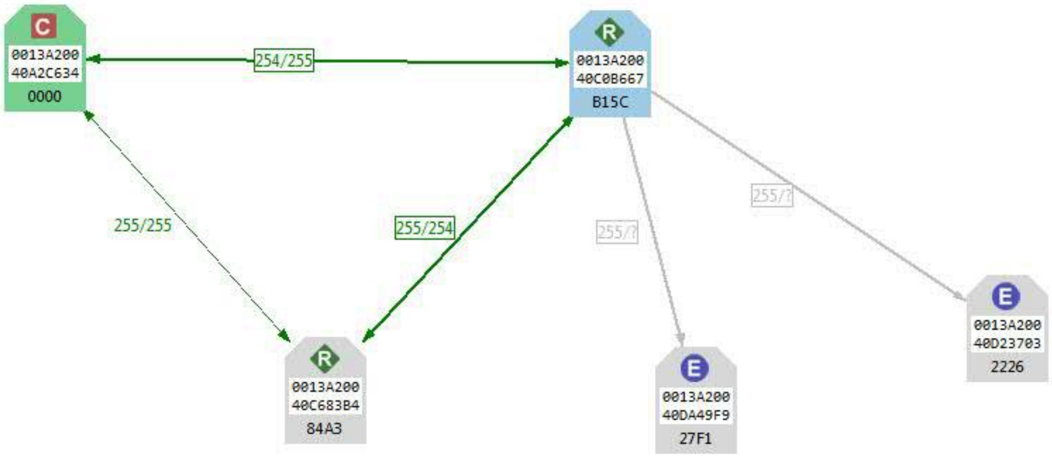


Figure 17: Laboratory ZigBee network. Coordinator (C), Routers (R) and Final Devices (E)

Bugging on the network.

Bugging on the network is the simplest attack to carry out on any wireless communication.

A ZigBee device used for intercepting information exchanged on the ZigBee network allows for the gathering of information from communications in a transparent way for the other devices in the network.

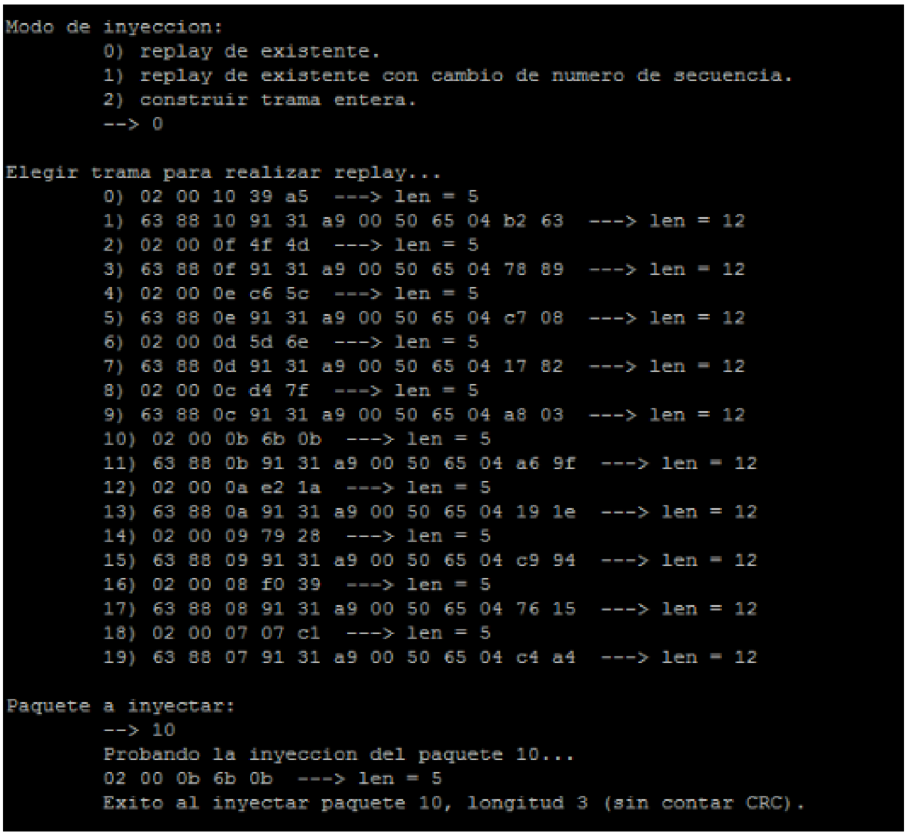
The information obtained from the communication provides an attacker with knowledge about the network, identifying the coordinating device and the devices that work as routers, which could then be used to carry out another type of attack. Furthermore, the data transmitted is also obtained, allowing for the requested data and the read values of different variables to be known. This information could be used in order to carry out actions such as the forwarding of packets or the impersonation of devices. In laboratory tests these possibilities and their impact will be verified.

Forwarding of data packets

The forwarding of packets (also known as replay), consists of the interception of frames that are then sent on, either after being modified or with the same structure, with the aim of destabilising a specific network or node.

The forwarding of data packets is frequently used in denial of service attacks. By means of a script constructed to build and inject ZigBee frames, the success of a previously captured forwarding of packets attack can be checked.

Figure 18 shows the application options used for the forwarding of frames from the attacker device. In this case, the forwarding of one of the captured frames (selectable in the second step) is permitted, whether the sequence number has been modified or not.



```
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).
```

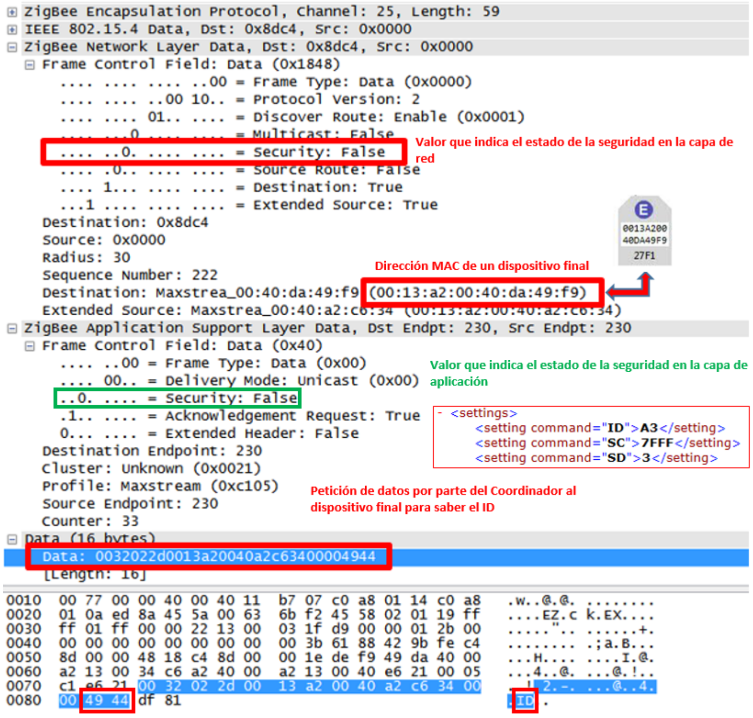
Figure 18: Replay of captured frame

In order to prevent these types of attacks, it is necessary to use the integrity characteristic that the ZigBee protocol has, in order to check and verify frames to ensure they have not been replaced by others. The network controller checks these refresh frames and their value, to see if they are those expected.

Data framing

ZigBee allows the use of a strong encryption, using key symmetric cryptography with periodic rotation of network keys, which provides an extra level of security in the exchange of information. However, if this is not specifically configured, the ZigBee communication is carried out without encryption.

In a ZigBee frame fields can be identified in different layers (network, application) whose values set the security activation. If the values are at 0 it means that the security has not been applied. The activation of the data encryption is indicated by placing the bit at 1.



```
⊞ ZigBee Encapsulation Protocol, Channel: 25, Length: 59
⊞ IEEE 802.15.4 Data, Dst: 0x8dc4, Src: 0x0000
⊟ ZigBee Network Layer Data, Dst: 0x8dc4, Src: 0x0000
  ⊟ Frame Control Field: Data (0x1848)
      .... .... .... ..00 = Frame Type: Data (0x0000)
      .... .... ..00 10.. = Protocol Version: 2
      .... .... 01.. .... = Discover Route: Enable (0x0001)
      .... ...0 .... .... = Multicast: False
      .... ..0. .... .... = Security: False
      .... .0.. .... .... = Source Route: False
      .... 1... .... .... = Destination: True
      ...1 .... .... .... = Extended Source: True
    Destination: 0x8dc4
    Source: 0x0000
    Radius: 30
    Sequence Number: 222
    Destination: Maxstrea_00:40:da:49:f9 (00:13:a2:00:40:da:49:f9)
    Extended Source: Maxstrea_00:40:a2:c6:34 (00:13:a2:00:40:a2:c6:34)
⊟ ZigBee Application Support Layer Data, Dst Endpt: 230, Src Endpt: 230
  ⊟ Frame Control Field: Data (0x40)
      .... ..00 = Frame Type: Data (0x00)
      .... 00.. = Delivery Mode: Unicast (0x00)
      ..0. .... = Security: False
      .1.. .... = Acknowledgement Request: True
      0... .... = Extended Header: False
    Destination Endpoint: 230
    Cluster: Unknown (0x0021)
    Profile: Maxstream (0xc105)
    Source Endpoint: 230
    Counter: 33
⊟ Data (16 bytes)
    Data: 0032022d0013a20040a2c63400004944
    [Length: 16]

0010  00 77 00 00 40 00 40 11  b7 07 c0 a8 01 14 c0 a8   .w..@.@. ........
0020  01 0a ed 8a 45 5a 00 63  6b f2 45 58 02 01 19 ff   ....EZ.c k.EX....
0030  ff 01 ff 00 00 22 13 00  03 1f d9 00 00 01 2b 00   .....".. ......+.
0040  00 00 00 00 00 00 00 00  00 3b 61 88 42 9b fe c4   ........ .;a.B...
0050  8d 00 00 48 18 c4 8d 00  00 1e de f9 49 da 40 00   ...H.... ....I.@.
0060  a2 13 00 34 c6 a2 40 00  a2 13 00 40 e6 21 00 05   ...4..@. ...@.!..
0070  c1 e6 21 00 32 02 2d 00  13 a2 00 40 a2 c6 34 00   ..!.2.-. ...@..4.
0080  00 49 44 df 81                                     .ID.
```

Valor que indica el estado de la seguridad en la capa de red

Dirección MAC de un dispositivo final

Valor que indica el estado de la seguridad en la capa de aplicación

```
- <settings>
      <setting command="ID">A3</setting>
      <setting command="SC">7FFF</setting>
      <setting command="SD">3</setting>
```

Petición de datos por parte del Coordinador al dispositivo final para saber el ID

Figure 19: ID parameter request with non encrypted data

Denial of Service Attacks

One possible scenario in which service can be denied is through the incorporation of multiple devices thanks to the influx of false frames to create false devices that connect the coordinating element to the network, trying to exceed the maximum allowed by a ZigBee network, which can be a maximum of 65535 nodes distributed in sub-networks of 255 nodes.

On the other hand, just as is the case with all wireless communications, it is possible to reject attacks via jamming[12] or inhibition techniques. When the nodes are associated with a ZigBee network, they send their association request to the coordinator or to one of the routers. The one which receives the request becomes the parent node. Where a node loses contact with its parent node, it must be re-associated with the network and obtain a new parent. This re-association involves updating the network routes.

These attacks can cause instability in the network routes, and consequently, their communications can be cancelled and it also increases the node's battery consumption.

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

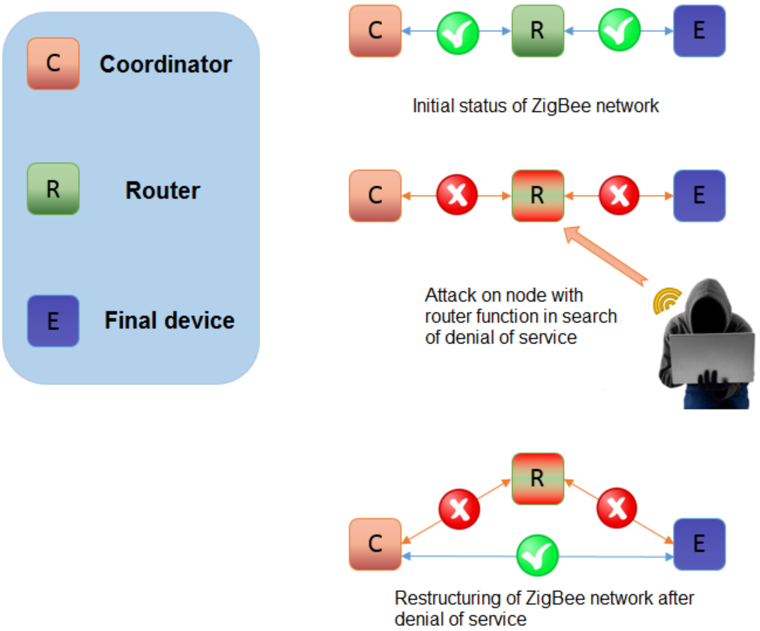

C Coordinator
R Router
E Final device
C
R
E
Initial status of ZigBee network
Attack on node with router function in search of denial of service
Restructuring of ZigBee network after denial of service

Figure 20: Example of denial of service on a node in a ZigBee network

To avoid attacks requesting the association of false devices, white lists of devices can be used in order to uniquely deal with the requests of authorised devices.

Impersonation via spoofing

Stealing the identity of a node requires prior knowledge of its MAC address, whether to carry out denial or services, or to transmit or request data to or from third parties, and this is another possible attack within a ZigBee network.

In the laboratory, impersonation was tested via the constant sending of messages from a node in the network, indicating that that advertised address was already busy. This attack forces the re-transmission of many broadcast messages, thus saturating the bandwidth.

The other test carried out consisted of generated frames directed to false ZigBee addresses. An attacker node sends data directed to non-existent addresses causing problems in the routing and, as a result, the malfunction of the ZigBee network.

Just as in the previous case, a white list of devices minimizes this problem.

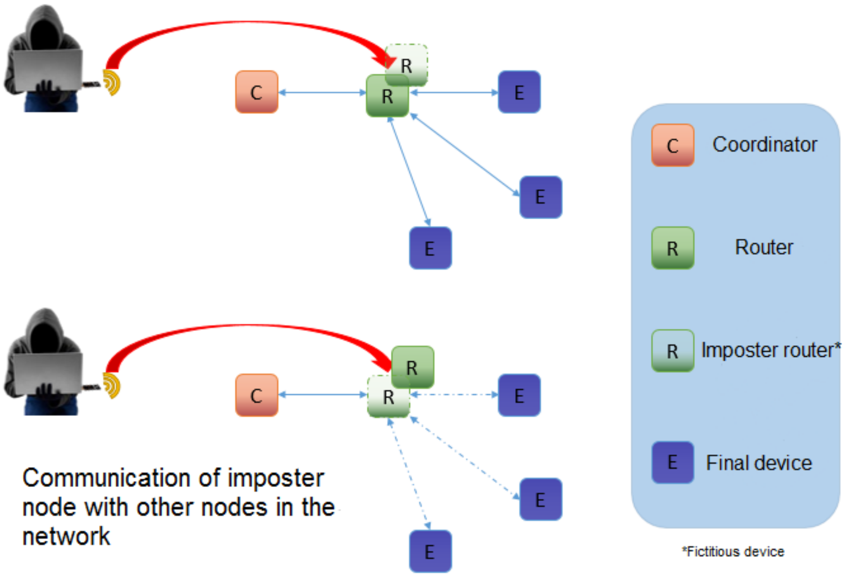


Figure 21: Router impersonated by an attacker

5.4. WirelessHART

For the analysis of WirelessHART a development kit has been used, made up of five autonomous devices which carry out the reading of the value of the environmental temperature and transmit that to the network's access point so that is is adequately dealt with by the applications. Larger elements were not available in order to perform frame captures or injections in a simple way. This partially limited the tests carried out.

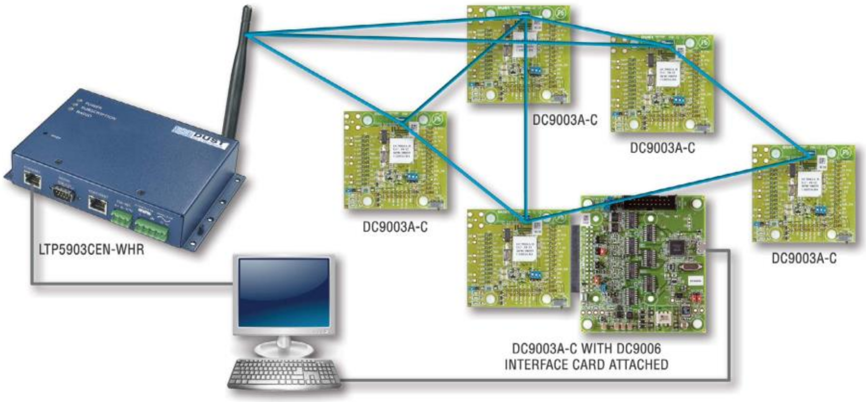


Figure 22: Laboratory WirelessHART network.

The WirelessHART security measures cannot be disabled, and a distinction can be made between those that affect the logical level and those that affect the physical level.

Capturing of information

WirelessHART has an encryption key for the network traffic, but it also allows the encrypted exchange of packets solely between two devices, which have a specific key for this.

This characteristic means that all of the communication data cannot be easily interpreted, however headers and other types of information can be as they are sent without encryption in all the messages.

Communication with the rest of the network

The communication of the wireless part of the network with the cabled part (devices such as network or security manager) and other HART protocol devices, is a critical point of roll-out. These devices use protocols (HART and others) that can be more vulnerable than WirelessHART and put an entire network at risk. This type of attack was not analysed because they do not form part of WirelessHART technology.

Denial of Service Attacks

Denial of service attacks by inhibition cannot be mitigated in any wireless network, therefore WirelessHART is also affected by them.

Denial of service attacks can also be launched via the continuous sending of requests to join the network, leading to the saturation of the available bandwidth.

REFERENCES

[1] http://www.redeswimax.info/
[2] Trusted Wireless 2.0. Wireless Technologies in Industrial Automation
[3] Industrial Wireless. Wireless transmission from sensor to network. Phoenix Contact
[4] http://en.hartcomm.org
[5] System Engineering Guidelines. IEC 62591 WirelessHART.
[6] Planning via Atoll of WiMax mobile network for centres of the University of Seville. End of degree project. Antonio Carmona Sánchez. 2008
[7] XBEE® AND XBEE-PRO® ZigBee product sheet
[8] SmartRF05EB User's Guide (Rev. A) product sheet
[9] CC2540 Development Kit User's Guide (Rev. A) product sheet
[10] SmartMesh WirelessHART Easy Start Guide

GOBIERNO DE ESPAÑA MINISTERIO DEL INTERIOR

GOBIERNO DE ESPAÑA MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

certsi_

CERT DE SEGURIDAD E INDUSTRIA