Hochschule Ostwestfalen-Lippe
University of Applied Sciences

Institut Industrial IT
www.init-owl.de

Wireless Automation Systems

Optimizing Reliability, Security and Coexistence

Users' Guide

Institute Industrial IT
University of Applied Sciences Ostwestfalen-Lippe

M.Sc. Kaleem Ahmad
Prof. Dr. rer. nat. Stefan Heiss
Prof. Dr.-Ing. Uwe Meier

Lemgo, 10.06.2008

Institut *Industrial IT*
Hochschule Ostwestfalen-Lippe
Liebigstrasse 87
D-32657 Lemgo

kaleem.ahmad@hs-owl.de
stefan.heiss@hs-owl.de
uwe.meier@ hs-owl.de

www.init-owl.de
www.hs-owl.de/fb5

Table of Contents

Document Conventions

1. All terms in `Courier New` font are defined at the end in the definitions and explanations section.
2. Only Bluetooth, ZigBee, IEEE 802.11g, CSS based nanoNET, and Atmel's narrowband FSK transceiver are considered in this document. Where 'all systems', or 'systems', or 'all technologies', or 'technologies' are used, it refers to only these systems.

1 Introduction

In recent years, the desire for connectivity and physical mobility has caused an exponential growth in wireless systems. The information being communicated in industrial environments are typically sensor and actuator signals and as such in normal operation it takes the form of recurring streams of small packets. At the same time, these packets are associated with critical tasks having strict timing requirements even under harsh environments. The latter may include extreme temperatures, high humidity levels, intense vibrations, explosive atmospheres, corrosive chemicals and excessive electromagnetic noise. Thus, in general, the required data throughput of the network is relatively low, but its reliability needs to be very high.

Furthermore as a result of wireless technology, the traditional ways of wired networks have become inadequate in meeting the challenges of present arena posed by our collective lifestyles. Wireless technology provides us with cheap and flexible wireless access. It is also easy to be installed on campuses, airports, in stock markets, factories, offices, hospitals, and other places. Mobility, ease and speed of installation, flexibility and cost are the core characteristics that place wireless solutions on great demand in today's commercial market.

In many innovative applications in the area of industrial automation wireless technologies are more and more desired. Meanwhile, a great variety of commercial wireless technologies are available which are offered as a great selection of OEM products. To avoid later disappointments technological limits should be considered early in the initial planning stage.

The purpose of this document is to encircle these technological limits for selected wireless technologies. In addition, this guide shall assist prospective users in adapting the best available wireless technology for the intended application.

There are many wireless technologies available today but only those listed below are selected for investigation in this report; a common feature of all these technologies is that all these operate in the 2.4 GHz ISM band:

- IEEE 802.11g; wireless local area networking standard (also called WLAN/Wi-Fi)
- IEEE 802.15.1; the Bluetooth® wireless personal area networking standard
- ZigBee based on IEEE 802.15.4; low rate wireless personal area networking standard.
- IEEE 802.15.4a; CSS based low rate wireless personal area networking standard.
- Narrowband FSK

ISM: The 2.4 GHz industrial, scientific and medical (ISM) band is an unlicensed radio frequency band that in most parts of the world is 83.5 MHz wide with a lower limit of 2.400 GHz and an upper limit of 2.4835 GHz as shown in Fig. 1.

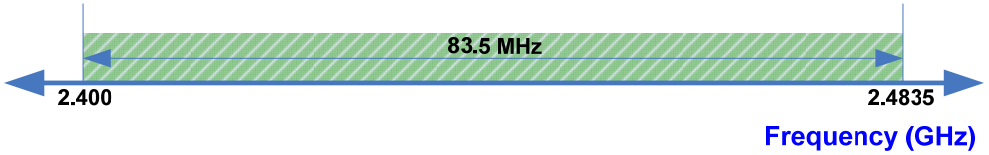

Figure 1: *2.4 GHz ISM band*

Because of being globally available and license free, it is fast becoming the frequency band of choice for an increasing number of applications. So it is a crowded neighborhood, with more devices in the home, office and industry using these frequencies, it is expected that at some point interference will result from these devices.

Although the 2.4 GHz band is unlicensed, it does not mean that it is unregulated. Products using this band come under various regulations depending on the country. For instance, only certain modulation techniques can be used in this ISM band, and output power levels for devices using these techniques are also regulated.

Despite the advantages a single wireless technology might offer on the factory floor, it will be often required to run multiple WLAN/WPAN networks in parallel in different or overlapping regions of the plant. Because of this fact, the `coexistence` of multiple networks of either the same or varying types needs to be investigated.

2 Industrial Requirements

In nearly every factory floor and industrial setting, communication links carry vital information between machinery, control, and monitoring devices. From periodic updates to ongoing process and manufacturing management, reliable data flow is critical to operations. To understand the requirements of industrial systems properly it is important to comprehend the hierarchy of industrial systems which is shown in Fig. 2.

The typical requirements of industrial systems nearly remain the same at all hierarchy levels but the value to be met vary from one level to the other. For example the data typically exchanged between different control processes or production plants is acyclic and need to travel long distances, on the other hand the data exchanged within a single process of a production plant is real-time cyclic data and the distances are medium.

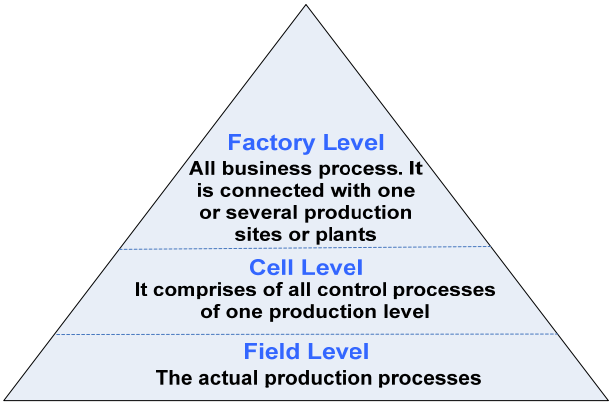

Figure 2: *Process hierarchy of the industrial systems*

The requirements for industrial automation can be categorized in two types [1], the *system-driven requirements* or *basic requirements*, which can be derived from the overall structure of the automation system and the *application-specific requirements* resulting from the application in question. These two types of requirements are listed in subsequent sections. The lists do not claim to be meticulous, but are primarily supposed to provide the user of this guideline a basic understanding of the system-driven and the application-specific requirements.

System-driven requirements

Table 1 lists all system-driven requirements and their corresponding values at all hierarchical levels. It is important to mention that the so called fieldbus systems are implemented at field level. The fieldbus systems are specially designed for solving automation or control tasks that rely on the interconnection of digital controllers with other digital controllers as well as sensors and/or actuators. The main objective of these systems is to provide services for predictable and reliable real-time communication, i.e., to provide certain guarantees on eventual delivery of packets and delivery times. Most of the time the packets are short in size and occur cyclically and a bounded jitter between subsequent packets is required. Some important acyclic packets e.g. alarm may also occur, which require reliable transmission with bounded latencies. The field level implementation of wireless technologies is the primary focus of this document.

Table 1: System-driven or basic requirements of industrial automation systems

Requirement	Hierarchical levels

	Factory level	Cell level	*Field level
Availability	Low to medium	high	high to very high
Typical data traffic	acyclic	cyclic and acyclic	mainly cyclic, acyclic
Safety	Medium to high	high	high to very high
Real-time data transmission	no	yes	yes
Typical data length	long	medium	short
Bandwidth	broadband	medium	Narrow/Broadband
Number of stations	High to very high	medium	medium to high
Type of stations	stationary and mobile peripherals	stationary and mobile peripherals	stationary and mobile devices
Distance	long	medium	short to medium

**The so called field-bus systems are implemented at this level*

Application-specific requirements

Any wireless technology considered for deployment in industrial systems should be evaluated in terms of performance and flexibility against environmental threats. Following are the application-specific requirements which need to be met by any particular wireless technology:

Integration ability

Most of the time some communication systems already exist in any industrial system where the new system is to be installed. Therefore a radio system considered for deployment should be provided with appropriate interfaces and networking options to allow its integration into existing systems.

Network Architecture Flexibility

Modern industrial automation installations are not merely restricted to point-to-point connections. Rather complex communication networks are required to allow an integration of stationary and mobile plant components. This network topology in turn increases the requirements with respect to the reliability of transmission and availability of the radio channel.

Mobility support

The inherent mobility support of wireless systems is an advantage on one hand but on the other hand the mobility can impair the transmission due to time-varying effects. The requirement of integrating mobile plant components into a communication system is an important reason for the use of wireless technologies in industrial automation. Any technology in question should be evaluated for its ability to combat with motion effects. The radius within which the component can move and its speed are two important parameters which should be determined by the application. Robot arms with a maximum speed of 60 km/h and a coverage range below 10 m are typical examples of such mobile components. Transport devices moving in the area of a production plant is another example of it. The speed of such transport remains usually less than 20 km/h, the radius ranging from few meters to approximately 100 m.

Reliability and Safety

Industrial automation systems demand strict requirements in terms of reliability and functional safety. The bit error rate (BER) of an existing cable based fieldbus system is usually below 10^{-9}. When radio based field bus solutions are proposed similar levels of reliability are expected. Multipath and motion based environments of industrial environments make it rather challenging to provide a reliable transmission. The so called `coexistence` phenomenon pose another threat to the reliability of a radio system. The transmission method employed by the intended radio system must therefore offer a sufficient level of immunity in multipath, motion based, and coexistence environments.

Different to wire-based systems, the wireless channel is strongly time dependent. Reliability in terms of bit error rate or packet losses might be sufficient for most of the time, but if the wireless system shows too many dropouts, its availability will be too low. This will prevent the successful usage of this wireless system, especially for safety applications.

Besides the desire to realize wireless safety applications, a wireless system shall not cause any inadmissible interference. This is an issue of electromagnetic compatibility (EMC). Additionally, a wireless system should not impose any threats especially in explosive environments.

Security

Wireless systems are not only vulnerable to the same security threads as wired networks, but are more difficult to secure, because of the openness of its physical medium. Physical access can not be controlled, allowing attackers to easily eavesdrop traffic in wireless networks. Also, it may be possible for an attacker to insert (manipulated) packets, in order to violate the integrity or availability of a wireless network. A determination of the possible distance from which such attacks could be launched, should take the usage of high gain unidirectional antennas under consideration. Because of the openness of its physical medium, most wireless specifications define (optional) measures at the data link layer (layer 2 of the ISO/OSI network model) to provide for the integrity and confidentiality of transmitted data. Integrity can be obtained by the attachment of message authentication code (MAC) values and confidentiality by the usage of an `encryption` algorithm.

Power consumption

The power consumption of radio devices is of particular importance as these devices often operate on batteries. Power consumption of the radio devices must be low in order to make it capable to work for long duration on a single battery. The power supply demands of sensors and actuators are especially very low and such devices need to work for years on a small battery.

Costs

The cost of the radio based module is another factor which should be considered and it must not drastically increase the overall cost of the system.

3 Overview of Selected Radio Technologies

The protocol architecture of most fieldbus systems covers only the physical layer, the data link layer including the medium access control (MAC) sublayer, and the application layer of the OSI reference model. Fig. 3 provides a graphical comparison of protocol architecture of selected technologies. This section also provides an overview of these technologies.

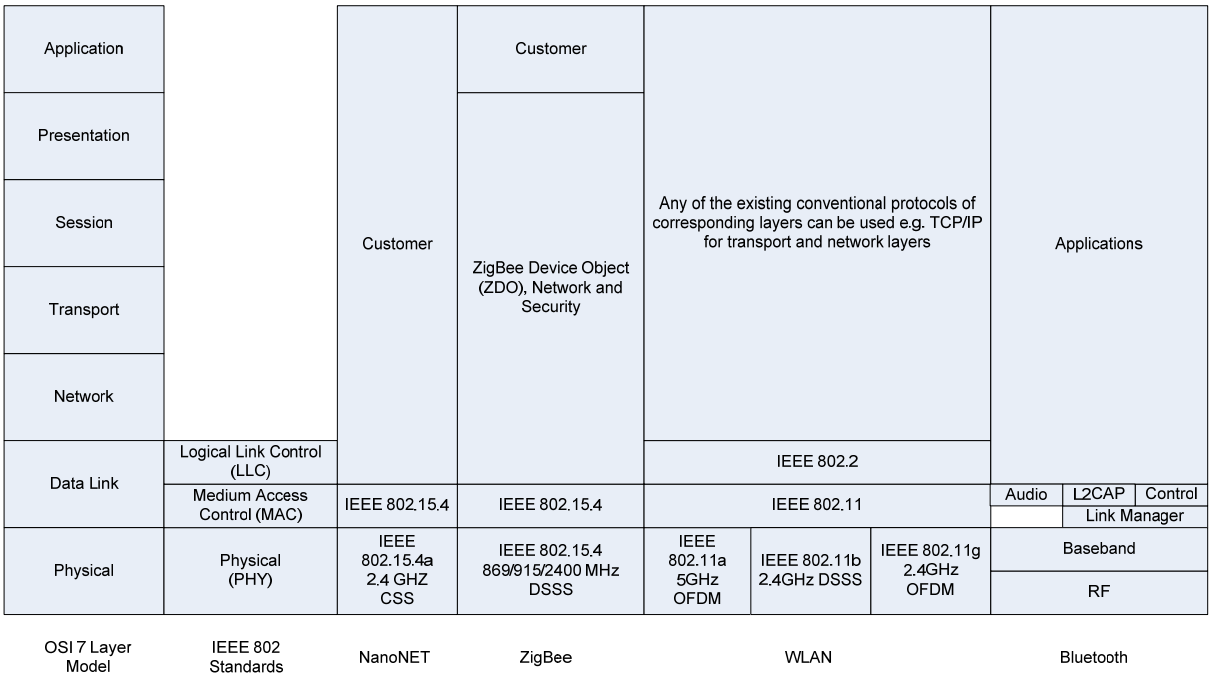

Figure 3: *Protocol architecture of selected wireless technologies*

3.1 IEEE 802.15.1 – Bluetooth

Bluetooth based on IEEE 802.15.1 [2] was originally designed as a cable replacement technology. In order to allow for worldwide deployment, the BT Special Interest Group (SIG) placed the technology in the ISM band at 2.4 GHz. For Bluetooth transmission 79 radio frequency channels with 1 MHz spacing are defined over a total bandwidth of 79 MHz. The following formula is used to calculate the transmitting frequencies:

$$f = (2402 + k)\ \text{MHz} \quad \text{where} \quad k = 0,...,78 \text{ (channel number)}$$

Gaussian Frequency Shift Keying (GFSK) is used to modulate the digital data symbols. Thereby the transmitting frequency for the transfer of a logical '1' is increased by at least 115 kHz and is correspondingly decreased for the transfer of a logical '0'. A Gaussian filter is used to round off the steep transitions in the base band to avoid a widening of the power density spectrum and therefore to avoid a high power consumption. The channel bandwidth is about 1 MHz and the symbol rate is 1 Msps and a bit rate of 1 Mbps according to Bluetooth specification v1.2. A gross bit rate of 3 Mbps can be achieved by using enhanced data rate (EDR) introduced in Bluetooth specification v2.0.

In the standard the transmitting power level is classified into three classes: 0 dBm = 1 mW (class 3), 4 dBm = 2.5 mW (class 2) and 20 dBm = 100 mW (class 1). With 1 mW transmitting power a range of approximately 10 m can be reached and with 100 mW distances of 30 m to 100 m are achieved. The requirement for a Bluetooth receiver is an actual sensitivity level of -70 dBm or better.

Frequency Hopping Spread Spectrum technology (FHSS) is applied to combat `interference` and fading. The Bluetooth channel is represented by a pseudo-random hopping sequence over the 79 RF channels. The hopping sequence is unique for the generated net and is determined by the Bluetooth

device address of the master. The timing of the hopping sequence is determined by the Bluetooth clock of the master. The channel is divided into time slots where each slot corresponds to an RF hop. Consecutive hops correspond to different RF hop frequencies. The nominal hop rate is 1600 hops/s and therefore the slot length is 625 µs. All Bluetooth units participating in one net are time and hop synchronised to the channel. Prior to participating in a net the initiating Bluetooth node must enter the paging mode. With frequency hopping it is possible to get statistically out of the way of other interferers in the ISM-band. On the other side Bluetooth is now acting itself as interferer distributed in time over the whole ISM band. Signal break downs due to interferences caused by multiway `spreading` are limited to the short hopping periods. A disadvantage caused by frequency hopping is the long time of up to 5 s (sometimes 10 s) to build up the Bluetooth connections.

For full duplex transmission, a Time-Division Duplex (TDD) scheme is used. On the channel, information is exchanged through packets. Each packet is transmitted on a different hop frequency. A packet nominally covers a single slot, but can be extended to cover up to five slots. The Bluetooth protocol uses a combination of circuit and packet switching. Slots can be reserved for synchronous packets. Bluetooth can support an asynchronous data channel, up to three simultaneous synchronous voice channels, or a channel which simultaneously supports asynchronous data and synchronous voice. Each voice channel supports a 64 kb/s synchronous (voice) channel in each direction. The asynchronous channel can support maximal 723.2 kb/s asymmetric (and still up to 57.6 kb/s in the return direction), or 433.9 kb/s symmetric. These data rates are reduced by other systems in the ISM band like microwave ovens, WLAN, door opening systems or other independent Bluetooth nets.

3.2 IEEE 802.15.4 – ZigBee

ZigBee technology is a low data rate, low power consumption, low cost technology. Wireless networking protocols target towards automation and remote control applications. The IEEE 802.15.4 [3] committee started working on a low data rate standard a short while later. Then the ZigBee Alliance and the IEEE decided to join forces and ZigBee is the commercial name for this technology. The IEEE 802.15.4 standard specifies a low data rate MAC and physical layer solution with multi-month to multi-year battery life and very low complexity. It is operating in an unlicensed, international frequency band. It specifies three physical layers (PHYs). The first operates in 868-868.6 MHz and provides 20 kb/s. The second operates in 902-928 MHz and supports 40 kb/s bit rate. Both of theses physical layers implement BPSK. The third physical layer specified by this standard works in 2400-2483.5 MHz and provides a bit rate of 250 kb/s. It implements O-QPSK modulation. DSSS is used for spreading the modulated signal. Two additional optional physical layers are also specified working in 868/915 MHZ and can support up to 250 kb/s bit rate. A total of 27 channels numbered 0-26 are available, sixteen of which are in 2.4 GHz band, 10 in 915 MHz band and 1 in 868 MHz band. The center frequency of these channels is defined as follows:

$f_c = 868.3$ MHz, for $k = 0$;

$f_c = 906 + 2(k - 1)$ MHz, for $k = 1, 2, ..., 10$;

$f_c = 2405 + 5(k-11)$ MHz, for $k = 11, 12, …., 26$;

where k is the channel number. IEEE 802.15.4 focuses on the specification of the lower two layers of the protocol (physical and data link layer). On the other hand, the ZigBee Alliance aims to provide the upper layers of the protocol stack (from network to the application layer) for interoperable data networking, security services and a range of wireless home and building control solutions. It further provides interoperability compliance testing, marketing of the standard, advanced engineering for the evolution of the standard.

3.3 IEEE 802.15.4a - CSS

There are two transceivers based on IEEE 802.15.4a/CSS [4][5] available, both of which are developed by Nanotron technologies GmbH, Germany. These are nanoNET [6] (nanoPAN 5360, nanoPAN 5361), and nanoLOC. Only nanoNET is investigated and discussed in this document.

NanoNET: It operates in the 2.4 GHz ISM band. This system achieves a maximum data rate of 2 Mbit/s, although 1 Mbit/s and 500 kbit/s can also be selected. The targeted range for nanoNET is a maximum outdoor range at LOS of approximately 900 m and an indoor range of approximately 60 m (typical). The transmission power can vary from -42 dBm to +6.9 dBm without any additional external power amplifier or attenuator. The sensitivity (see 5.2.6) of the nanoNET transceiver is defined by the raw data mode (data not coded or encrypted in any way). The sensitivity is -92 dBm @ 1 Mbps and the `processing gain` is 17 dB.

The nanoNET chip produces up chirp and down chirp signals with a symbol duration of 1µs and an effective frequency bandwidth of 64 MHz. The bit processing methods of nanoNET TRX includes scrambling, CRC (Cyclic redundancy check) generation and checking, 128 bit `encryption/decryption`., and FEC (`forward error correction`) with a (7,4) HAMMING code. Additional to these bit processing methods it also includes automatic repeat request (ARQ, see 5.2.7) with maximum 14 retransmissions. But the application software can choose any value between 0-14 retransmissions.

3.4 IEEE 802.11 – WLAN

IEEE 802.11 is composed of a number of specifications that primarily define the physical and MAC layers of WLAN systems. While IEEE 802.2 LLC is used as a standard interface between MAC and higher layers. The most common variations and extensions of WLAN systems include the general 802.11 MAC, IEEE 802.11a [7], IEEE 802.11b [8], and IEEE 802.11g [9] [On 12 June 2007 IEEE has issued a single reaffirmed document which is available here [10] and all previous versions are rolled into it. Whereas the previous documents are retired] for physical layers. The most prominent features of IEEE 802.11 a/b/g are discussed below:

- *IEEE 802.11a* [7] operates in 5 GHz bands that are license exempt in Europe (5.15–5.35 GHz and 5.47–5.725 GHz) and unlicensed in the United States (UNII bands, 5.15–5.35 GHz and 5.725–5.825 GHz). Over the entire available spectrum, 21 systems are allowed to be running in parallel in Europe and eight in the United States. The IEEE 802.11a physical layer (PHY) is based on the multicarrier system orthogonal frequency-division multiplexing (OFDM). Eight modes called RATE-dependent parameters are defined. These are BPSK with code rate 1/2 (6Mbps) and rate 3/4 (9Mbps), QPSK with rate 1/2 (12 Mbps) and rate 3/4 (18 Mbps), 16-QAM with rate 1/2 (24 Mbps) and rate 3/4 (36Mbps), and 64-QAM with rate 1/2 (48 Mbps) and rate 3/4 (54 Mbps). But the maximum achievable data rates depend on the transmitted packet size. E.g. in the 54 Mb/s mode, the transmission of a packet with 1500 bytes long user payload results in a maximum data rate of about 30 Mb/s. However smaller throughput value is of primary interest for industrial applications, as small packet sizes are often used in such networks.

- There are three PHYs defined in the original IEEE 802.11 standard: DSSS, FHSS and infrared for bitrates up to 2Mbps. *IEEE 802.11b* [8] is a high-rate extension to the original IEEE 802.11 DSSS mode and operates in the 2.4 GHz ISM band. This extension builds on the data rate capabilities, to provide 5.5 Mbit/s and 11 Mbit/s payload data rates in addition to the 1 Mbps and 2 Mbps rates. To achieve the higher rates, 8 chip complementary code keying (CCK) is employed as the modulation scheme. Although in principle 13 different channels

each with a 20 MHz bandwidth can be used for DSSS (Europe except France and Spain), but only three non-overlapping channels can be selected to operate in parallel.

- *IEEE 802.11g* [9] is an extension to the IEEE 802.11b specification called "Further Higher Data Rate Extension in the 2.4 GHz Band". This extension defines extended PHYs named as extended rate PHY (ERP) and extends the maximum bitrate to 54 Mbps. This PHY operates in the 2.4 GHz ISM band. It supports four different physical layers of which two are mandatory: ERP-DSSS/CCK, the PHY that is identical to IEEE 802.11b and ERP-OFDM that uses the same modulation and coding combinations as IEEE 802.11a. The channel description remains the same as in IEEE 802.11b.

3.5 Narrowband FSK

Though a variety of FSK (Frequency Shift Keying) based transceivers are available in the market only Atmel's ATR 2406 [11] transceiver is included in this document. It is a narrowband FSK transceiver which operates in the 2.4 GHz ISM band.

3.6 Comparison

Table 2 summarizes main parameters of selected technologies while the channel scheme of all these technologies is shown in Fig. 4.

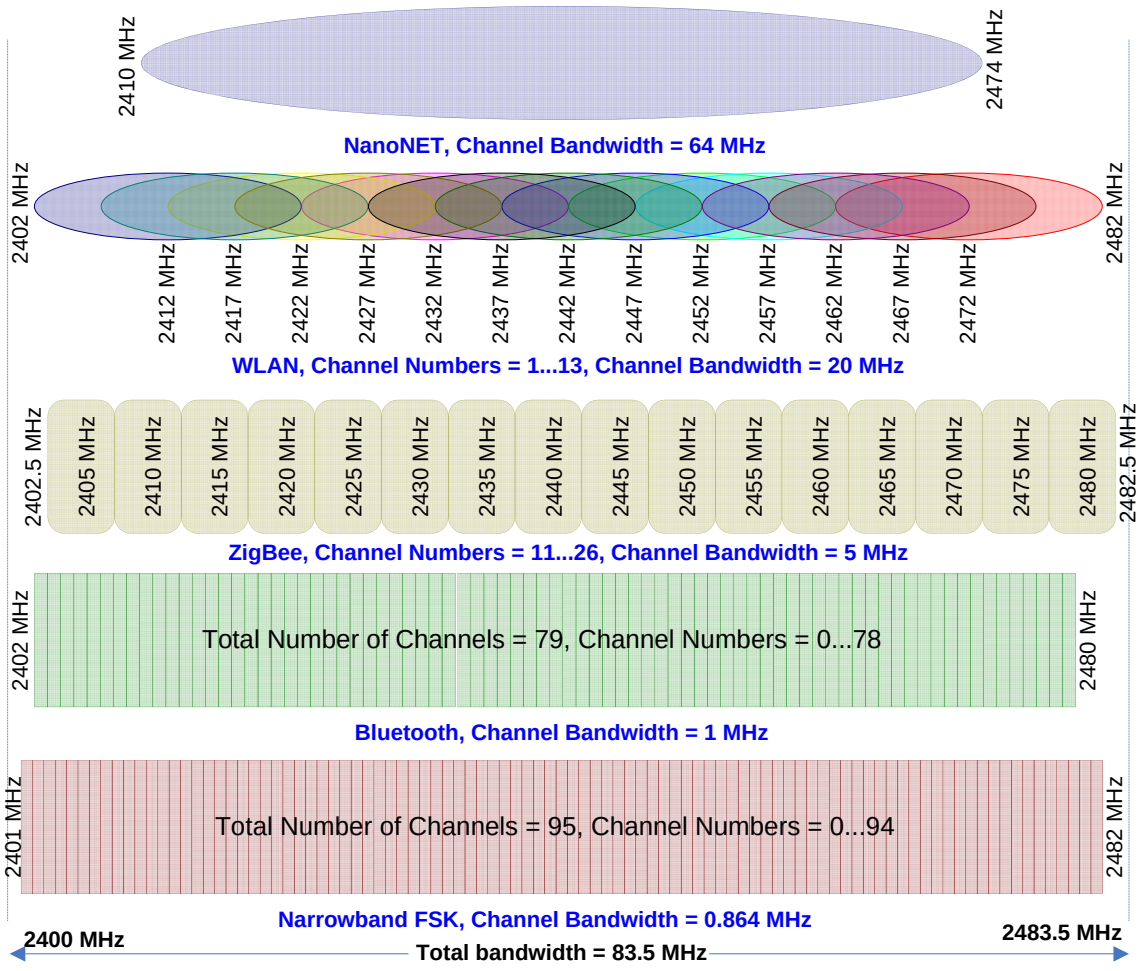

Figure 4: *Investigated technologies in the 2.4 GHz ISM band*

Table 2: *Technology summary*

	NanoNET	FSK	Bluetooth®	WLAN	ZigBee
Modulation	*CSS*	*FSK*	*FHSS/GFSK*	*DSSS/OFDM*	*DSSS/O-QPSK*
Standard	*IEEE 802.15.4a*	-	*IEEE 802.15.1*	*IEEE 802.15.11g*	*IEEE 802.15.4*
Range	*60m Indoor 900m outdoor*	*~20-30m*	*10m-100m*	*100m*	*10m-75m*
Bitrate	*500 kbps, 1Mbps, 2Mbps*	*500 kbps 72 kbps*	*1 Mbps*	*54 Mbps*	*20kbps, 40 kbps, 100 kbps, 250 kbps*
Operating Band	*2.4 GHz ISM*	*2.4 GHz ISM*	*2.4 GHz ISM*	*2.4 GHz ISM*	*2.4 GHz ISM, 915 MHz, 868 MHz*
Bandwidth	*64 MHz*	*0.864 MHz*	*1 MHz*	*20 MHz*	*5 MHz*
Frequency Range	*2.4 GHz - 2.4835 GHz*	*2.4342 GHz- 2.4334 GHz*	*2.4 GHz - 2.4835 GHz*	*2.4 GHz - 2.4835 GHz*	*2.4 GHz - 2.4835 GHz*
Total number of channels available	*1*	*95*	*79*	*13*	*16(2.4GHz), 10(915MHz), 1(868MHz)*
Battery Life	*Years*	*Years*	*Days*	*Hours*	*Years*
Power Requirement	*Very Low*	*Low*	*Medium*	*High*	*Low*
Max. Transmission Power	*-42dBm…6.90 dBm*	*+4 dBm*	*+20 dBm*	*+20 dBm*	*+4 dBm*
Network Topology	-	-	*Star*	*Star*	*Star, Tree, Cluster*
Number of parallel systems	*1*	*47*	*15-50 depending upon the application*	*3*	*16*
Channel access method	*CSMA/CA*	-	*TDMA*	*CSMA/CA*	*CSMA/CA*
Security	*MAC & Encry. (AES-128 with CCM* mode)*	-	*Encry. (additive stream cipher) & device authent.*	*WEP (insecure), WPA / IEEE 802.11i (TKIP & AES-128-CCM)*	*MAC & Encryption (AES-128 with CCM mode)*

4 Selecting a Suitable Radio Technology

This section is divided into three subsections. In the first subsection a performance evaluation matrix is presented in Table 3. The table shows how specific user requirements are related to the corresponding features of the radio system. It also relates the radio system parameters which effect other radio systems in a coexistence environment. While the second subsection briefly presents the role of these parameters in co-existing environments and also discusses how these parameters can be selected to optimize the performance in such environments. A `coexistence` measurement setup is proposed in the third subsection. The user of this guideline can follow the layout and instructions given in this setup to evaluate the performance of any interfering radio systems.

4.1 Application Requirements vs. Radio System Features

Table 3: *Application requirements and associated features of radio systems (see definition in 'Definitions and Explanations' section)*

Application Requirement	Radio system features	Comments/Side effects
Distance that can be covered		
Range of mobile stations Largest range between stationary stations	Range	Increasing the distance by the factor 2 adds 6 dB pathloss (see 4.2.1) for an ideal channel. Real line-of-sight channels (LOS) add 6...12 dB pathloss. Each radio system offers some level of `interference` to other coexisting systems in its coverage area. High range radio systems are more vulnerable to interference.
	Transmitter power	6 dB more transmission power (see 5.2.5) increases the distance by the factor 2 for an ideal channel. 6...12 dB are necessary for a real LOS channel. Increasing the transmission power results in stronger `interference` to other systems.
	Symbol duration	A radio system transmitting with longer symbol durations enables higher transmission ranges. Systems with longer symbol duration suffer from more data collisions in coexisting environments. For example, when narrowband FSK use 71.482 kbps bitrate (symbol duration = 14 µs) it sees more collisions with other coexisting systems (impairing the transmission of its own and of others as well) than when it uses 500 kbps bitrate (symbol duration = 2 µs)[12].
	Receiver sensitivity	A radio system with better receiver sensitivity (see 5.2.6) requires less transmission power to achieve a given transmission range. Such systems offer less `interference` to coexisting systems. Receiver sensitivity for nanoNET is -92 dBm @ BER 10^{-3}, Atmel is -93 dBm @ BER 10^{-3}, and maximum (according to Bluetooth standard) Bluetooth receiver sensitivity is -70 dBm @ BER 10^{-3} (but different

		companies develop Bluetooth receivers with better receiver sensitivity). In [12] it was found that NanoNET and FSK (with smaller symbol duration) offer less `interference` to other coexisting systems.
	Antenna design	Directional antennas have very high `antenna gain` in some directions, while omni-directional antennas have low gain. Directional antennas can be used to increase the transmission range (in specific directions only). They are not useful in moving applications. Directional antennas reduce `interference` in coexisting environments.
Number of stations		
Number of stations	Addressing	The maximum number of stations which can be accommodated in a network by a radio system is limited to the addressing capabilities of it. Furthermore a radio system may offer some or all sort of data casting techniques (`broadcasting`, `unicasting`, `multicast`).
	Multiple Access Procedure	Each radio system implements `multiple access procedures` in order to share the channel among several stations. Each multiple access procedure has its own inherent advantages and disadvantages (see 5.1.12 for more detail).
Network Architecture		
Topology	Radio Network	Not all network topologies are supported by a specific radio system. An application requiring some specific network structure must check the candidate radio systems for the availability of the required topologies. For example Bluetooth offers only star topology. It offers to built small networks, called piconets, which consists of two or more devices that occupy the same physical channel. By *'same physical channel'* it means that these devices are synchronized to a common clock and hopping sequence. The common clock is identical to the clock of one of the devices in the piconet, known as the *master* of the piconet. All other devices are known as *slaves*.
	Relay Station	Some radio systems support the use of relay stations in the network to increase the range of the network. However, the use of relay stations increases packet delay.
	Mobility Support	Moving stations are subject to change their physical locations and hence the physical shape of the network continuously. The maximum speed and motion range are two important parameters of such stations. It is important to evaluate the mobility support of the contender radio system according to these

		parameters of the application's moving stations.
Availability and reliability		
Bit Error rate Packet Loss Rate	Modulation	The performance of different modulation techniques is different in different environments. A modulation technique having low BER and PLR in one environment (e.g. an environment with stationary objects) does not necessarily perform at similar level in another environment (e.g. with environment with many moving objects).
	Transmission Power, Adjustable Range	High transmission power always improves the quality of the signal at the receiver antenna and is always an obvious choice to improve BER and PLR of a radio system in any environment. But in a coexisting environment it is very critical to increase the transmission power of one system as it decrease SIR for other coexisting systems and hence increase BER and PLR for those systems. A radio system providing fine adjustable range of transmission power is preferable as it gives more control to the user to adjust the transmission power to high or low in low and high density coexisting environments respectively.
	Antenna diversity, Array gain	`Diversity` or `array gain` by using multiple antennas can be exploited to achieve low BER and PLR. But multiple transmit antennas will increase interference for coexisting systems. On the other hand multiple antennas either at transmit or receive or both sides will also increase processing time, complexity and cost of the radio system.
	ARQ	`ARQ` is a very popular choice to improve the BER and PLR of radio systems. But it has some drawbacks as well. First of all it increases the packet delay and jitter considerably. Secondly it increases the channel traffic due to the transmission of several copies of the single packet.
	FEC, CRC	`FEC`, and `CRC` are often implemented by radio systems to provide higher level of transmission reliability. But these are also not without drawbacks. They increase the packet size and hence cause the wastage of not only channel resources but also increase the processing time of both sender and receiver and hence increase the packet delay and `jitter`.
	Receiver Sensitivity	Receivers with better sensitivity need lower transmission power to achieve a desired BER, PLR. Furthermore a little increase in transmission power can lead to considerably reduced bit and packet errors. Such radio systems are especially well suited in coexisting environments.

	Spread Procedure	Due to high `processing gain`, `spread procedures` improve the transmission reliability in multipath (see 4.2.2) and coexisting environments but are considered highly `bandwidth inefficient`. WLAN, Bluetooth, ZigBee, and nanoNET all use some kind of spreading procedure (see Table 3).
	Preamble length	Better synchronization between transmitter and receiver can be achieved with a long `preamble`, which results in high reliability of transmission. But it means an increased overhead and causes the wastage of precious system resources such as channel capacity and processing time.
	Frequency band	Some frequency bands are more used than others, especially unlicensed frequency bands such as 2.4 GHz ISM band. Due to high usage there is more interference in such frequency bands which threats low data reliability. All systems presented in Table 3 operate in 2.4 GHz ISM band.
Type of Stations		
Stationary Temporary Portable Mobile	Mobility Support	What maximum speed and movement radius can be accommodated by a specific radio system? This question is particularly more important in applications which have high density of mobile stations. For example Bluetooth based SAI's were tested in [14] for different environments including some motion based environments. It was found that the path loss was significantly high (up to 107 dB, without moving objects it was in the range of 55dB…78dB) and error rate, in motion based environments was also increased by a factor of 10.
	Addressing	Efficient `routing` and address management (How new nodes are being accommodated and how the leaving ones are handled, how mobile nodes are handled, how temporary nodes are accommodated) are often important questions to consider.
Services		
Real-time communication Download data	Bitrate	The bitrate is often among the primary considerations of a specific application. WSAN and WPAN usually need low bitrates, but applications with high download traffic need high bitrate.
	BER, PLR	The type of application also define the level of reliability required. Real-time communication especially WPAN and WSAN need very low BER and PLR. On the other hand comparatively higher BER and PLR can be affordable in download-specific applications. The acceptability of higher BER and PLR is because of the usage of reliable high level

		protocols such as TCP/IP in download-specific applications.
	Jitter	Response time such as packet delay is critical for WSAN and WPAN networks. Such application particularly need small `jitter`.
	FEC,CRC	In some applications where the packet sizes are very short (typically up to few bytes in WPAN and WSAN) FEC and CRC is a significant overhead.
	Bandwidth	Download-specific applications need high bandwidth to increase the download data rate (e.g. WLAN = 20 MHz). On the other hand WSAN and WPAN based applications can work with low bandwidth (e.g. Bluetooth = 1 MHz, narrowband FSK = 0.864 MHz, ZigBee = 5 MHz) because high data rate is not a compulsory requirement for these systems. Although some specific modulation techniques employed in such systems may need higher bandwidth due to its own reasons (but not to increase data rate) e.g. CSS in nanoNET requires 64 MHz bandwidth but still offers maximal 2 Mbps bit rate.
Time Response		
Packet delay Jitter Cycle Time Processing time Response time	Baud, bitrate	Using low `baud` means using longer symbol duration, which increases the length of overhead bits (such as `preamble` bits, error correction bits) and the packet size on the time axes (e.g. in a binary FSK system for 1 Msymbol/sec and 2 Msymbol/sec bauds, bit duration is 1 µsec and 0.5 µsec respectively. A packet with 20 overhead bits will have 20 µsec and 10 µsec overhead length (on time axis) respectively for above mentioned bauds). It will eventually increase the time response of the system.
	Encryption	Data `encryption` makes the data more secure against eavesdropping though but it also increase the processing time of both sender and receiver of the radio system.
	Packet Loss Rate	High PLR may need more retransmissions (If some retransmit mechanism such as `ARQ` is used) and consequently can increase response time, delay and `jitter`.
	ARQ	Retransmissions increase the delay and the jitter of the radio system. Moreover it also effects the minimum possible cycle time (To understand, suppose a radio system which uses `ARQ` with 5 retransmissions, takes 32 ms when all 5 retransmissions are utilized. In this case the radio system must wait for more than 32 ms before the transmission of a next packet, i.e. it should have a cycle time longer than 32 ms). Bluetooth, nanoNET, and ZigBee implement ARQ and give the option to users to enable or

		disable it.
	Authentication	The `authentication` mechanism is subject to protect the system against unauthorized access but it also introduce some extra processing time of both sender and receiver of the radio system
	Sleep mode	Some radio systems put the transceiver in sleep mode while no transmission is taking place and hence save useful energy which is especially very important for battery operating systems. But the awakening process after each sleep increase the response time of the system.
	Multiple access procedure	Some specific `multiple access procedures` may effect the response time of the radio system. For instance using TDMA a node need to wait for its turn to transmit, hence increasing the time response
	Bit error rate	High BER may necessarily need some error correction mechanisms which eventually increase the processing time of the radio system.
	FEC, CRC	Using `FEC` and `CRC` increases the reliability of the system on one hand but on the other hand increase the processing time of the radio system.
	Preamble Length	A longer `preamble` needs more time to transmit and hence introduces some extra delay and processing time over each packet.
Data Security		
Authentication Integrity Confidentiality/Privacy Protection against Denial of Service attacks	MACs (Message Authentication Codes)	Authenticity of the origin and integrity of data packets can be ensured by adding MAC values to the data packets. (See `Authentication` in 'Definitions and Explanations'.) MAC calculations need additional computational resources and add some time overhead to the processing of data packets. MAC values add some additional overhead to each data packet's payload (typically 20 bytes per packet). Devices have to be configured with a secret key. These keys have to be stored in a secure way, such that they can not easily be retrieved from a device by a non-authorized person. Key replacement schemes have to be designed.
	Encryption	`Encryption` provides protection against eavesdropping (sniffing). `Encryption` and `decryption` need additional computational resources and may add some time overhead to the processing of data packets. Devices have to be configured with a secret key. These keys have to be stored in a secure way, such that they can not easily be retrieved

		from a device by a non-authorized person. Key replacement schemes have to be designed.
	Range	The limited range of a wireless system restricts the options for a potential eavesdropper. However, using directional antennas may increase the possible distances for eavesdropping significantly. The possible range for active denial of service attacks (DoS) should be considered as well.
	Access procedures	Some `channel access techniques`, e.g. CSMA, may allow denial of service attacks by deliberately violating the access rules.
	Spreading	`Spreading` techniques provide some protection against jamming attacks.
Location		
Range of mobile stations Greatest range between stationary stations Indoor/Outdoor Industrial structural conditions Robustness with respect to mobile obstacles Robustness against multipath effects Path Loss	Range	The inherent range of any radio system may pose some limitations if it does not match with the maximum required range of the application.
	Transmission Power, Adjustable range	Different transmission powers are needed for indoor and outdoor transmission to achieve the same level of transmission quality. For that reason better control over adjusting the transmission power is required.
	Receiver Sensitivity	Radio receiver with better sensitivity can perform better in any environments using a lower transmission power.
	Antenna Design/Antenna gain	Directional antennas may perform better in outdoor LOS applications. While an omni directional antenna can be a better choice in an NLOS indoor environment to exploit the multipath effects.
	Antenna Diversity/Array gain	Depending upon the location based characteristics (e.g in a channel with very high path loss) it can be necessary for the radio system to implement some kind of antenna diversity or array gain to achieve the desired QoS.
	Modulation	Different modulations techniques offer different advantages in different environments. One modulation may be better in indoor environment while the other in outdoor, similarly one modulation technique may have better capabilities to combat against multipath and motion effects or high path loss than the other.
	Spread procedure	`Spreading techniques` perform better in multipath environments.
	Frequency Range	Path loss (see 4.2.1 for further detail) is different for different frequency ranges. For example free space path losses measured in [13] for 1 m T-R separation were as follows: 450 MHz = 18 dB,

		900 MHz = 25 dB, 1.35 GHz = 30 dB, 1.89 GHz is 32 dB. In another study [14] ideal free space path loss for 2.4 GHz frequency for 1 m T-R separation was almost 40 dB. Path loss increases as T-R separation distances increases.
Environmental Conditions		
Co-existence Electromagnetic compatibility (EMC)	Frequency band	Unlicensed frequency bands have more usage and many co-existing systems can be there in such bands. Different frequencies may also offer different electromagnetic radiation. 2.4 GHz ISM band is a well known example of it. This is used by Bluetooth, WLAN, ZigBee, FSK based Atmel 2406, and CSS based nanoNET. 902 MHz-928 MHz, and 5.800 GHz-5.925 GHz are other unlicensed frequency bands.
	Transmission Power/Adjustable	Higher power increase the transmission quality for a single system but signal-to-interference ratio (SIR, see 5.2.5) is decreased for coexisting systems in the area. The power adjustabiliy feature of a radio transmitter give the user more control over it. For example the transmission power of nanoNET can be programmed in small steps in the range of -27 dBm...6.90 dBm.
	Antenna Design/Antenna gain	Omni directional antennas, because of their transmission in all directions may offer unnecessary interference in directions which are not even needed. It is better to have high antenna gain in required directions while low in others to reduce the interference for coexisting systems.
	Range	A radio system with inherent higher range has a larger coverage area and hence a larger affected area because of its signals.
	Modulation	Each modulation technique has different levels of performance in different coexisting environments. Furthermore modulation 'A' may perform better in the coexistence of modulation 'B' while may perform bad in coexistence of 'C'. Because of this it is also important to find the combination of radio systems which can perform well in the presence of each other.
	Spread procedure	`Spreading techniques` have inherent capabilities to combat against interference. That's why they perform better in coexisting environments. WLAN and ZigBee systems use DSSS, Bluetooth uses FHSS, and nanoNET uses the CSS technique for spreading its signal.
	Multiple Access	Each `channel access mechanisms` has some positive features to offer in

	Procedure	coexisting environments. E.g. FDMA can be used to separate coexisting systems in the frequency domain while TDMA separates them in the time domain and reduces the chances of collision. CDMA generally implemented using DSSS offer less interference to coexisting systems by spreading the signal.
Design		
Dimensions Integration, extension Electrical Power Consumption	Antenna Design/Antenna gain	The antenna design (e.g. Directional, Omni directional) is particularly important with respect to the nature of application.
	Receiver Sensitivity	Lower receiver sensitivity is always preferable.
	Transmission Power, Adjustable power range	The maximum and minimum transmission power and the adjustable range can make a radio system more flexible.
	Sleep Mode	This feature is particularly well suited for battery powered systems. The systems having this feature can go in sleep mode during idle times to save energy.
	Components available	The availability of components may be important while system integration and extension phases.
	Suppliers	Different suppliers may offer different product support.
Cost		
Component Cost License	Components available, Suppliers	The availability of the components can effect the cost. Widely available components and multiple suppliers not only make it easier to get the components but also give the customer more bargaining options to reduce the cost.
	License	Some times some software doesn't need any license and is available free of cost which considerably reduces the overall cost of the system.
	Frequency Band	Free ISM bands don't need any license. That's why these are highly used for industrial, educational, and scientific purposes. This reduces the implementation cost of systems significantly.

The parameters of radio channels or radio systems itself which are important while selecting a technology without coexistence considerations are discussed below:

4.2 Requirements of Wireless Industrial Channels

When planning to install a system in an industrial environment it is not sufficient to consider only the features of the proposed radio system but the nature of the channel should also be considered as different systems can be suitable for different kind of channels.

4.2.1 Path Loss

The strength of a transmitted radio signal decreases as the distance between the transmitter and the receiver is increased. This decrease in signal strength is known as path loss. There are many

parameters which the path loss depends on, most important of these are the antenna technology, the frequencies used, the T-R distance, and the environmental conditions (e.g. outdoor will have different path loss than a closed environment like a room. It is the most important parameter for optimal system operation. Fig. 5 shows two linear increasing prediction curves for ideal free space (blue line) and a laboratory environment (green line) measured in [14]. They are based on the following equation:

$$L/\mathrm{dB} = 40.15 + 10 \cdot n \cdot \log10(d/\mathrm{m}) \quad (3)$$

with path loss exponents $n = 2$ for ideal free space and $n = 3$ for lab environment. All measured path loss values were found between these two prediction curves.

The performance of one radio system can be better than some other radio systems if there is no line of sight (LOS) between the communicating nodes. Therefore if the channel which the radio system is desired for, has no line of sight (NLOS) between the communicating nodes then it could be important to first investigate which system can perform better in NLOS before selecting a particular technology for any industrial application.

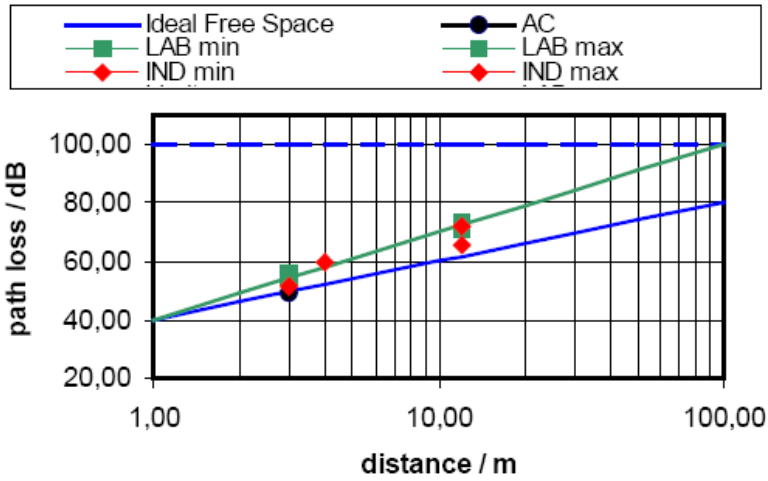

Figure 5: Average path loss of different environments in the 2.4 GHz band with 0 dBi antennas. Measurements: anechoic chamber (AC), university lab (LAB), industrial environments (IND) [14]

4.2.2 Multipath Effects

Multipath propagation causes two effects i.e. time dispersion and frequency selective fading of the channel. Time dispersion is to stretch the signal in time in such a way that the received signal is of longer duration than that of the transmitted signal. Frequency selective fading filters the transmitted signal resulting in good transmission at some frequencies and bad at others. Root mean square delay spread (T_{RMS}) and coherence bandwidth (B_c) are two parameters of the channel to measure multipath effects. To get a better transmission quality in such kind of channels the signal bandwidth (B_S) and the symbol duration (T_S) should be related to the above mentioned channel parameters in the following way:

$$B_S \langle B_C \quad and \quad T_S \rangle T_{RMS} \quad (1)$$

While planning a radio system for an industrial multipath environment it is important to consider which technology combat better with multipath effects.

4.2.3 Motion Effects

Some kind of movement involved in the channel whether it is the movement of transceiver (transmitter or receiver) or movement of some other objects within the area of transmission causes DOPPLER

effects. It makes the channel time varying and hence causes time selective fading. Another consequence of DOPPLER Effect is frequency dispersion (also called spectral broadening). DOPPLER spread (B_D) and coherence bandwidth (T_C) are two parameters to measure such kind of channel behavior. To achieve better transmission the signal parameters signal bandwidth(B_S) and symbol duration (T_S) should be related to above mentioned channel parameters in the following way:

$$B_S \rangle B_D \quad and \quad T_S \langle T_C \tag{2}$$

If possible, the packet duration should be less than the coherence time. While planning radio system for an industrial environment where there is significant movement in the area or if the transceivers will be installed on moving objects it is important to consider which technology works better in the presence of DOPPLER Effects.

Fig. 6. shows how multipath and DOPPLER effects fade the signal.

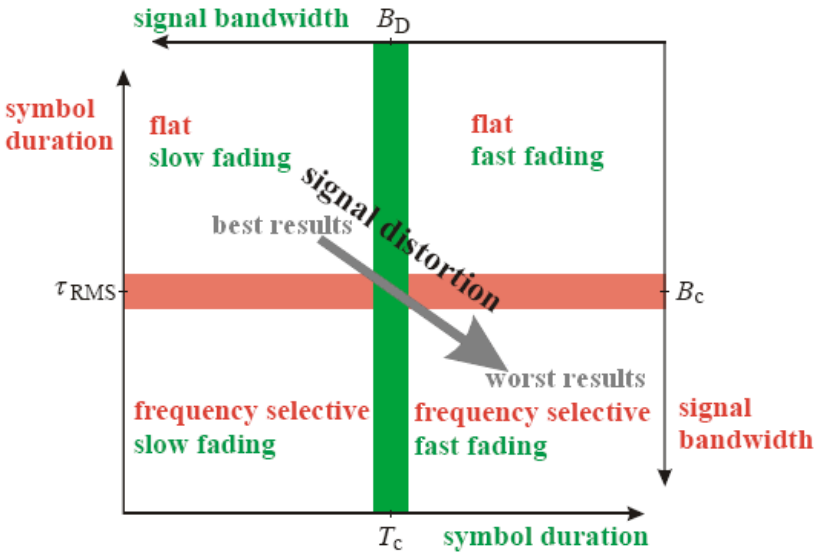

Figure 6: *Fading types experienced by a signal*

5 Performance Optimization with respect to Coexistence

The performance of a single technology can vary in different environments and under different conditions and the selection of a particular technology depends upon the customer requirements. The performance evaluation becomes further complex when more that one technologies are required to operate in the same area. In this case it is important to investigate the performance of candidate systems in the coexistence of each other to find which radio system performs best in presence of each other. Such investigations include to test different system parameters to optimize the performance of radio systems in coexistence environments. Performance optimization requires the control of time, frequency, polarization, space, and power of signals and interferers. This section discuss the role of different system parameters in coexistence environments.

5.1 Coexistence Test-Sites

It is often required to run multiple WLAN/WPAN networks in parallel in different or overlapping regions of the industrial units. To avoid future disappointments it would be always better to not only investigate the performance of individual technologies but also to test these technologies in the coexistence of each other. This section presents a simple coexistence test setup which a user of this guideline can use to test the desired systems.

The test setup suggests to investigate only two radio systems at a time to keep the investigation process simple. The system can be investigated as a function of some or all of the following parameters depending upon the radio system and the requirements of the user:

- Transmission power
- Distance/Range
- Retransmissions
- Error handling and bit processing methods (E.g. FEC, CRC, Scrambling etc.)
- Antenna
- Cycle time
- Packet size
- Frequency band and channel
- Environment
- Security procedures
- Adaptive procedures
- Bitrate
- Duty cycle
- Diversity

It is worth mentioning that the above list is not exhaustive and a radio system can be accessed for other parameters as well, even some new parameters can be defined. The parameters to be measured can be set according to the demands of the application. For industrial applications these are BER, PLR, packet delay, and jitter. Where jitter is the difference of maximum and minimum delay. The layout of the proposed setup can be seen in Fig. 7 for an equal-distance model. Fig. 8 and Fig. 9 show anechoic chamber based and cable based versions of this model respectively. Whereas Fig. 10 represents a co-existence test setup where the distances of the radio being tested and the interferer are different.

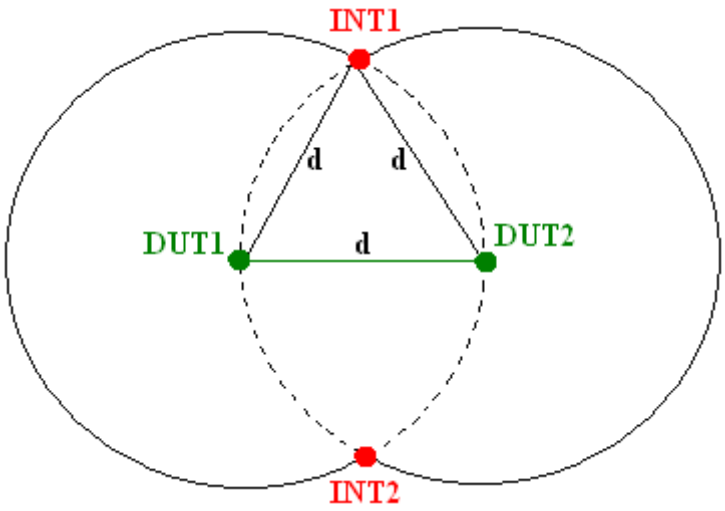

Figure 7: *Recommended equal-distance co-existence test setup*

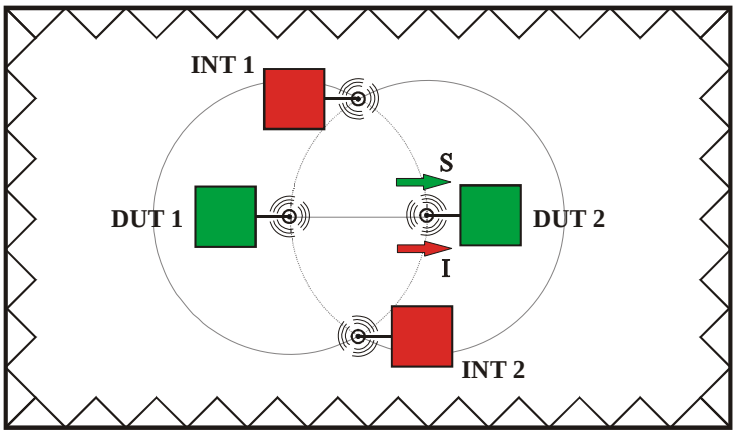

Figure 8: *Recommended equal-distance coexistence test site in anechoic shielded chamber*

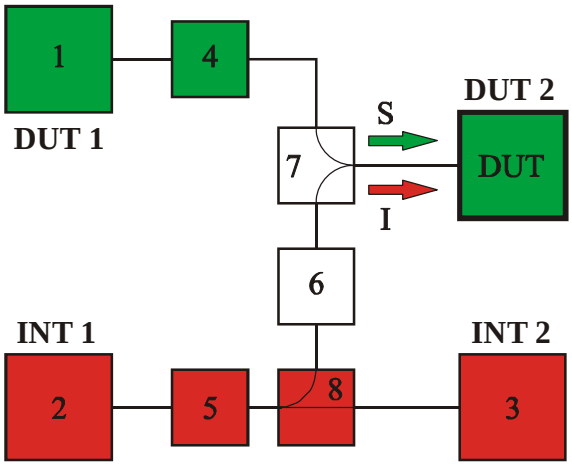

Figure 9: *Recommended wired equal-distance coexistence test*

Two distances are important, which are defined and named as follows:

- *D1:* The distance between transmitter and receiver of the test system
- *D2:* The distance between transmitter of the interfering system and receiver of the test system

In Fig. 7 d1 and d2 are the same i.e. equal to d. The signal-to-interference ratio at the DUT receiver in this model can simply be obtained by the following formula:

$$SIR = \frac{\text{transmission power of the test transmitter}}{\text{transmission power of the interfering transmitter}}$$

The transmission power might be taken from the data sheets. In a second model which is more realistic, the distances d1 and d2 are not the same and measurements are taken for many values of d1. In this model the coexistence of systems is mainly tested as a function of distance and the worst level of interference can be measured in this way. A spectrum analyzer is needed in this case to measure the received power of both transmitters at the receiver antenna. The following formula can be used to measure the signal-to-interference ratio.

$$SIR = \frac{\text{received power of the test system at the test receiver}}{\text{received power of the interfering system at the test receiver}}$$

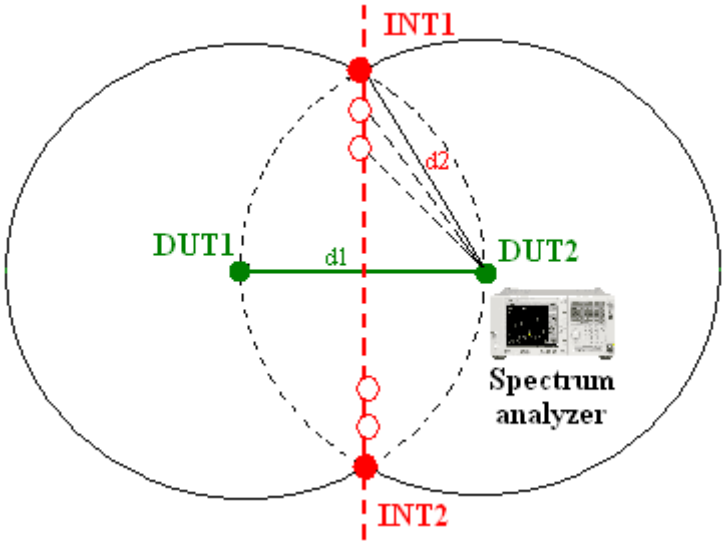

Figure 10: *Co-existence test setup with different distances*

5.2 Parameter Optimization

5.2.1 Frequency

It is possible for coexisting systems to avoid or minimize the interference by choosing channels which do not overlap with each other. If possible, the operating frequency of the DUT system should be selected with respect to existing frequency allocations. As for example most WLAN systems choose the channels 1 (center 2412 MHz), 6 (center 2437 MHz) or 11 (center 2462 MHz), ZigBee systems should use the channel 15 (center 2425 MHz), 20 (center 2450 MHz), 25 (center 2475 MHz), or 26 (center 2480 MHz) and narrowband FSK systems should use the channels 25 ... 29 (2422.6 … 2426.92 MHz), 54 … 58 (2447.65 … 2451.97 MHz), or 83 … 94 (2472.71 … 2482 MHz). A possible channel allocation model is shown in Fig. 11.

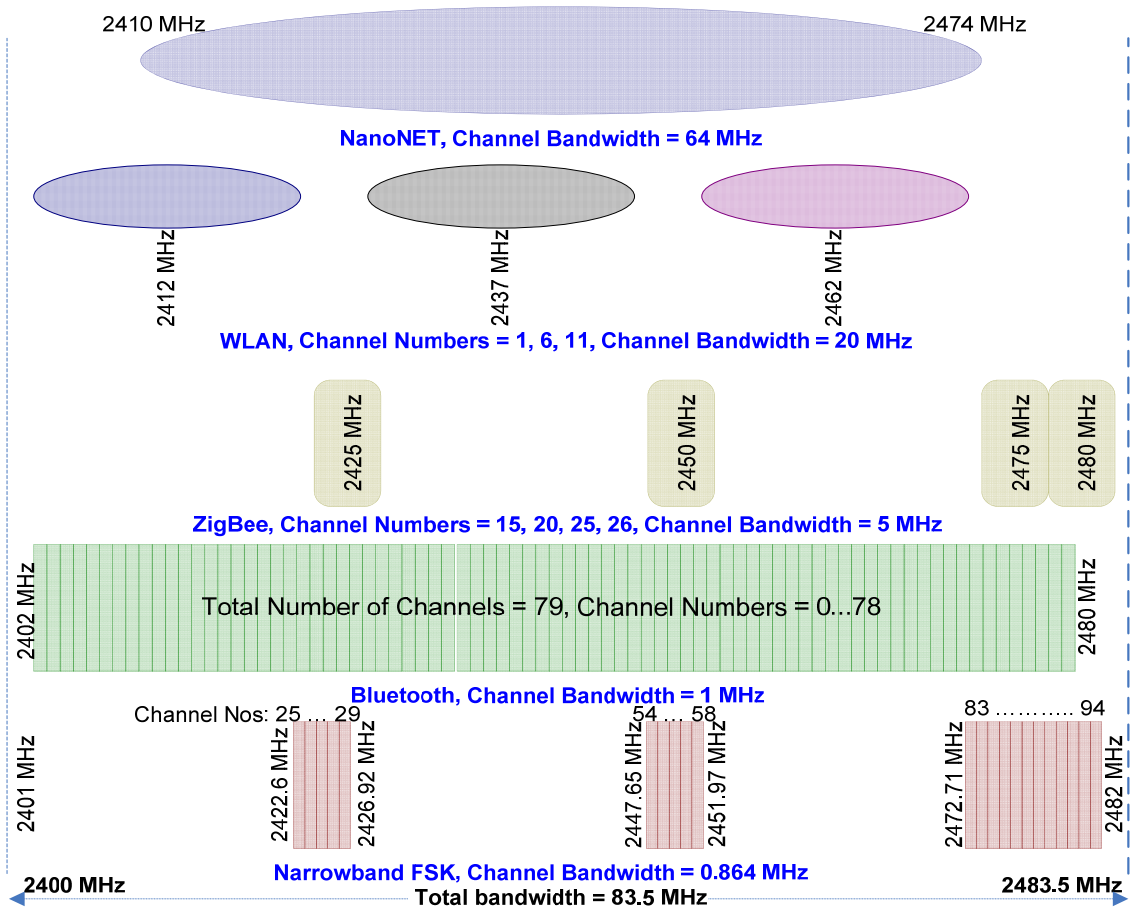

Figure 11: *Channel recommendation model*

5.2.2 Bandwidth and Number of Parallel Systems

The systems using high bandwidth provide smaller number of channels and hence offer less number of parallel systems. Higher bandwidth also make the channel selection process (as proposed in Fig. 11.) less flexible. On the other hand the radio systems with smaller bandwidth are more flexible in terms of channel adjustment to avoid channel overlapping with other coexisting systems. Furthermore the systems using high bandwidth offer more interference to coexisting systems and it is important to use low transmission power (Maximum allowed power and channel bandwidth for all systems is shown in Fig. 12) if a system uses high bandwidth. The nanoNET and WLAN systems are two high bandwidth systems with 64MHz and 20MHz bandwidths, respectively. The nanoNET system because of its very high bandwidth provide only one channel and has no choice to adjust some other channel while WLAN offers 3 parallel systems running in the same area without channel overlapping.

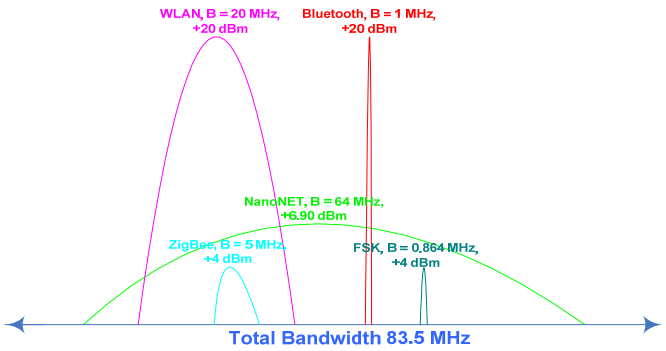

Figure 12: *Maximum transmission power and Channel Bandwidth in 83.5 MHz ISM band*

5.2.3 Duplex Method

A communication channel is often divided into forward and reverse channel to separate the outward and reverse signals. Time division duplex (TDD) and frequency division duplex (FDD) are two very well known examples of it. FDD increases the required bandwidth of a particular system and hence ends up with smaller number of parallel frequency channels. On the other hand TDD increases the usage of a particular channel in the time domain.

5.2.4 Cycle Time-Synchronization

Cycle time is defined as the time interval between successive packet transmissions. This parameter is important when the devices are generating cyclic traffic. A careful selection of cycle time can help to arrange the transmission of coexisting systems in the time domain and hence to avoid or minimize the possibility of packet collisions. This phenomena is shown in Fig. 13.

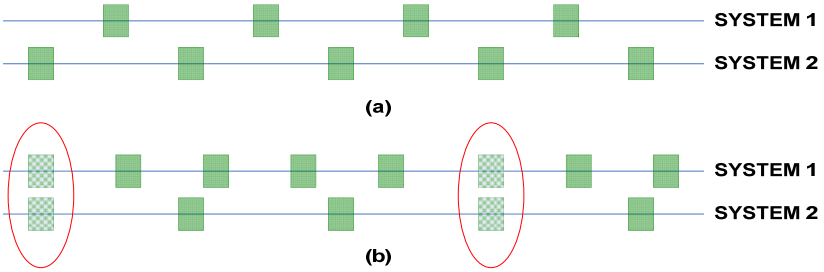

Figure 13: *Collision avoidance with optimized cycle time*

The complexity to synchronize the systems with respect to cycle time increases as the number of coexisting systems grows. The synchronization can be done by tuning the systems with the help of some sophisticated equipment like an oscilloscope.

5.2.5 Transmission Power and SIR

The transmission power of the device is another important factor to decide the transmission quality. It should be selected carefully especially when there are more than one radio systems working in the same area. The received signal quality at a receiver is typically measured by the *signal-to-interference ratio (SIR)*, which is the ratio of the power of the wanted signal to the total residue power of the unwanted signals. In order to correctly interpret the wanted signal, the SIR must be above a given threshold. For each receiver all those signals are unwanted signals which are not generated by its peer transmitter. In case of a single system the higher transmission power would generally guarantee a better transmission quality as it results in higher SIR for that system. But this is not true when more then one radio systems are working close enough to each other. In this case increasing the transmission power of one system would although increase the SIR for that particular system but would however lower the SIR for all other systems in the area.

5.2.6 Receiver Sensitivity

Receiver sensitivity is normally taken as the minimum input signal required to produce a specified output signal having a specified signal-to-noise ratio (SNR). It is an inherent feature of any transceiver and varies from device to device. The receiver with a better sensitivity can detect a weaker signal and can still achieve a desired output signal quality. E.g. receiver sensitivity = -92 dBm @ BER = 10^{-3} is better than receiver sensitivity = -80 dBm @ BER = 10^{-3}.

5.2.7 Retransmission (ARQ)

The ARQ is a famous mechanism to improve the transmission quality. A transmitter keeps on retransmitting the same packet after a predefined time interval called timeout if it does not receive an acknowledgement from the receiver. The maximum number of retransmissions can be configured as per demand of the application.

ARQ is a critical factor and has its effect in two different ways on the transmission. One way the impact of ARQ should be considered is that increasing the number of retransmissions results in an increased traffic in the area. This increased traffic can degrade the quality of transmission of all systems in the area. In an extreme case if more and more systems are using ARQ in the area and each system keeps on increasing the number of retransmissions, the overall traffic of the area will eventually reach to a maximum extent. It can threat very high collision rates and hence very high PLR and BER for most of the systems. Another way to see the role of ARQ is its impact on packet delay. Very good results in terms of PLR can be achieved with the retransmission method but it results in a high packet delay and jitter. As packet delay and jitter might be critical parameters for industrial systems, a compromise needs to be achieved between packet delay and PLR. In any case, the number of allowed retransmissions should be limited.

5.2.8 Channel Error Handling (FEC, Scrambling, CRC, FCS)

Channel error handling mechanisms like FEC, Scrambling, CRC, FSC, antenna diversity can increase the transmission quality of radio systems in noisy and coexisting environments but on the other hand it increase the processing time for the packet and hence increasing the time based parameters like packet delay, and packet jitter etc. Furthermore a specific mechanism does not result in good results in all environments but can even worsen the transmission quality. That is why it is important to choose correct channel error handling mechanism.

5.2.9 Antenna / Antenna Gain

Antennas are very important elements of a radio system and careful selection of antenna can not only improve the performance of a single system but also of the coexisting systems. Directional antennas of the systems can reduce interfering radiation. But unfortunately, fixed spatial pattern allocations require stationary applications. As wireless PAN systems are mainly used in portable or mobile sensor actuator networks, this parameter is less effective but wherever only stationary stations are involved this can be beneficial.

5.2.10 Operating Range

The longer the operating range of the radio system, the larger would be the affected area because of its radiation. Unnecessary long operating ranges of the radio system need to be restricted to required areas only. It is important to note that the figures for the ranges often mentioned with devices are average values which may vary significantly depending on the specific environment structure.

5.2.11 Distance

The distance between the stations of DUT and between DUT and interferers is one of the deriving factors for the level of interference. The distance between DUT stations should be kept as small as

possible and on the other hand the distance between DUT and interferers should be kept as large as possible.

5.2.12 Channel Access Method

A channel access method or multiple access method allows several stations to be connected to the same physical medium to transmit over it and to share its capacity. Time division multiple access (TDMA), space division multiple access (SDMA), code division multiple access (CDMA), carrier sense multiple access (CSMA), and frequency division multiple access (FDMA) are some well known channel access methods. Each of these have its own inherent benefits and may offer different level of performance in different environments.

5.2.13 Adaptive Algorithm/Approach

An adaptive channel allocation scheme can be very helpful to improve the performance of a radio system in noisy and coexisting environments. Using this technique a radio system can avoid the channels which have more disturbance at a particular time and can transmit in other channels. Current Bluetooth systems use this technique to provide high quality transmission.

5.2.14 Bitrate/Symbol Duration

The higher the bitrate the smaller is the symbol duration and vice versa. Using low bitrates means transmitting with long symbol durations and hence high collision probability between coexisting systems. During the research being done for this project it was found that the PLR and BER are very high for all coexisting systems when any one of these are using low bit rates.

5.2.15 Duty Cycle/Packet Size

The duty cycle is the proportion of time during which a device, or system operates or keeps the channel busy. High duty cycles mean more busy channels and hence increased chances of collision with coexisting systems. Furthermore, larger packet sizes impose not only more interference to coexisting systems but also degrade the performance of the system itself. Thus, small packet sizes reduce the collision probability and should be preferred in coexistence environments.

5.2.16 Network Topology/Relay Station/Node density

The network topology, the presence of any relay stations, and the average number of nodes present in a particular network may also affect the performance of a system. For example the presence of relay stations can extend the range of the network on one hand but on the other hand it may increase the interference to other systems in the area. The level of interference offered by one network topology may be different from some other technology. For example in a star topology with a single master station only one pair of devices can be communicating with each other but on the other hand in a peer-to-peer topology there can be many pairs of devices communicating with each other at the same time. The level of interference would be higher in the latter case. Similarly, the networks with higher node density can have more traffic and may offer more interference to other systems in the area.

References

[1] VDI/VDE-Richtlinien: Funkgestützte Kommunikation in der Automatisierungstechnik - Radio Based Communication in Industrial Automation; December 2003, VDI2185.pdf

[2] http://standards.ieee.org/getieee802/download/802.15.1-2005.pdf

[3] http://standards.ieee.org/getieee802/download/802.15.4-2006.pdf

[4] http://www.ieee802.org/15/pub/TG4a.html

[5] Kaleem Ahmad, Uwe Meier: Performance Investigation and Optimization of Chirp Spread Spectrum Systems for Wireless Sensor Actuator Networks, IEEE WCSN-2007, Allahabad, India.

[6] http://www.nanotron.com/EN/docs/nanoNET-TRX/NA1TR8/datasheet/nanoNET_TRX_Transceiver_NA1TR8_DS_Ver2.08.pdf

[7] http://standards.ieee.org/getieee802/download/802.11a-1999.pdf

[8] http://standards.ieee.org/getieee802/download/802.11b-1999.pdf

[9] http://standards.ieee.org/getieee802/download/802.11g-2003.pdf

[10] http://standards.ieee.org/getieee802/download/802.11-2007.pdf

[11] http://www.atmel.com/dyn/resources/prod_documents/doc4779.pdf

[12] Ahmad, Kaleem; Meier, Uwe: Coexistence Optimization of Wireless PAN Automation Systems; 7th IEEE International Workshop on Factory Communication Systems - WFCS 2008, Dresden, Germany, May 2008, Mar 2008

[13] Ashok Chandra, Dak Bhawan, Ambuj Kumar , P. Chandra: Comparative Study of Path Losses From Propagation Measurements at 450 MHz, 900 MHz, 1.35 GHz and 1.89 GHz in the Corridors of a Multifloor Laboratory-cum-Office Building, Vehicular Technology Conference, 1999. VTC 1999 - Fall. IEEE VTS 50th

[14] U. Meier, S. Witte, K. Helmig, M. Höing, M. Schnückel, H. Krause: Performance Evaluation and Prediction of a Bluetooth Based Real-Time Sensor Actuator System in Harsh Industrial Environments, 12th IEEE Conference on Emerging Technologies in Industrial Automation, Patras, Greece.

[15] http://standards.ieee.org/getieee802/download/802.15.2-2003.pdf

[16] Jing Zhu, Alan Waltho, Xue Yang, and Xingang Guo: Multi-Radio Coexistence: Challenges and Opportunities. IEEE, 2007.

Definitions and Explanations

Antenna gain: Antenna gain is the ratio of the power density of an antenna's radiation pattern in the direction of strongest radiation to that of a reference antenna. If an isotropic antenna is used as a reference antenna then dBi is used and if a dipole antenna is used as reference antenna then dBd is the unit used for antenna gain. The power is not added by the antenna, but simply redistributed to provide more radiated power in a certain direction than would be transmitted by an isotropic antenna. The energy is conserved by the antenna, so if an antenna has high gain in some directions, it must have low gain in some other directions.

Array gain: It is the average increase in SNR due to the coherent combining effect of multiple antennas at transmitter, receiver or both.

Authentication: Authentication is the means of establishing the validity of a (often implicitly) claimed identity, thereby preventing unauthorized people (or unauthorized processes) from entering a network. Identification and authentication is the basis for most types of access control and for establishing user accountability. To authenticate every single data packet send by an legitimate user or device, a so called message authenticate code (MAC) can be calculated and added to the data by the sending end and verified by the receiving end. MAC calculations depend on a pre-shared secret (often derived from a password). The distribution and configuration of these pre-shared secrets may require the establishment of a well organized key distribution scheme (key management). Such authentication and key management schemes may be supported by technical means, like the implementation of centralized authentication servers. Most wireless standards specify authentication mechanisms for data packets on the data link layer.

Automatic Repeat-reQuest (ARQ): It is an error control mechanism for data transmission. It uses ACK (acknowledgment) and timeouts to achieve reliable data transmission. An ACK is a message sent by the receiver to the transmitter if the packet is correctly received by it. If the sender does not receive an ACK before the timeout, it usually re-transmits the packet until it receives an acknowledgment or exceeds a predefined number of re-transmissions.

Bandwidth Efficiency: Bandwidth efficiency is a measure of how well a particular modulation scheme is making use of the available bandwidth of a communication channel. It is given by the total number of transmitted bits/sec over the channel bandwidth,

i.e: $k\frac{bits/\sec}{Hz}$

Baud/Symbol rate: The distinct number of symbols transmitted over transmission medium per second. It is different from bitrate, as one symbol may carry more than one bits in it.

Broadcast: The data transmitted by one station is received by all stations of the network.

Coexistence: Ability of a system, to work *sufficiently* in the presence of other systems and to avoid disturbing other systems.

Collaborative and non-collaborative coexistence [15]: A *collaborative* coexistence mechanism can be realized if the coexisting wireless networks can communicate with each other to exchange information in order to reduce mutual interference. If there is no method to exchange information between the two wireless networks then only *non-collaborative* coexistence mechanisms can be considered.

Cyclic Redundancy Check (CRC): CRC is a powerful and easy-to-implement technique to obtain data reliability. The block of data is called frame. Using this technique, the transmitter appends an extra n-bit data to every frame called Frame Check Sequence (FCS). The FCS holds redundant information about the frame that helps the transmitter to detect errors in the frame.

Diversity gain: Multiple antennas can be used to achieve diversity gain. It can be receive antenna diversity or transmit antenna diversity or a combination (MIMO) of both. In receive antenna diversity the antennas see independently faded versions of the same signal. The receiver can either select best of these or can combine all received signals so that the resultant signal exhibits considerably reduced fading in comparison with the signal at any one antenna. In transmit antenna coding the transmitter adds some redundancy in space by sending the same signals (but orthogonal) by multiple antennas. The receiver receives with one antenna but is able to distinguish between the multiple copies because the signals are orthogonal.

Encryption/Decryption: Data confidentiality can be achieved through the transformation of intelligible data (plain text) into so called ciphertext by various encryption algorithms. Symmetric encryption algorithms have to be initialized by some secret information (secret key) before they can be used. Recovering the plain text from the ciphertext is possible by the application of an related decryption algorithm after its initialization with the same secret key. An important design aim of encryption algorithms states, that a given ciphertext should not allow the disclosure of any information of the plain text (besides its length), as long as the secret key is not known. In the context of encrypting network traffic, secret keys are also known as preshared keys. They are often derived from passphrases. Most wireless standards specify symmetric encryption algorithms for an (optional) usage at the data link layer.

Forward error correction (FEC): It is an error correction mechanism where the sender adds some redundant data to the user data which is some times known as an error correction code. This code allows the receiver to detect and correct errors without the need to ask the sender for additional data.

Heterogeneous or homogeneous coexistence: *Heterogeneous* coexistence refers to radio systems which use different technologies. Whereas *homogeneous* radio systems make use of the same wireless technology.

Interference (general definition): Superposition of two or more waves.

Interference (definition according to radio systems): Interaction of a desired signal (DUT) with an interfering signal.

Jitter: Maximum packet delay – Minimum packet delay

Multicast: Not all but a specific group of stations in the network are the recipient of the data sent by a station.

Multipath Effects: It is the propagation phenomenon due to which the transmitted signals by a single source reach the receiver by more than one path. This can be because of reflection, refraction or diffraction as shown in the following figure.

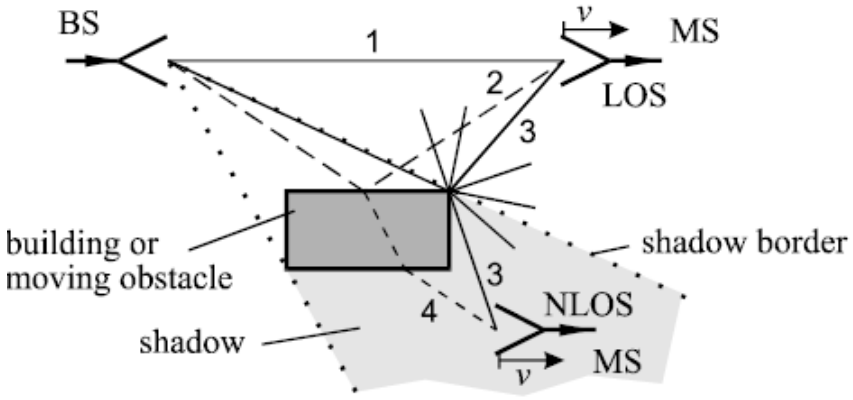

Figure 14: *Multipath propagation, (BS: Base station, MS: Mobile station, LOS : Line of sight, NLOS : Non line of sight), 1: Direct wave, 2: reflected wave, 3: diffracted wave, 4: refracted wave*

Multiple Access Method or Channel Access Method: A channel access method or multiple access method enables multiple stations which are connected to the same physical medium, to transmit over it and to share its capacity. The frequency division multiple access (FDMA), code division multiple access (CDMA), time division multiple access (TDMA), space division multiple access (SDMA), orthogonal frequency division multiple access (OFDMA) are some well known examples of it.

Network Topology: It is the arrangement or mapping of the elements (stations, nodes, etc.) of a network, especially the physical (real) and logical (virtual) interconnections between nodes. It can be seen as the shape or structure of the network and defines how the data communicates in the network. The ring, mesh, star, bus, and tree are some well known network topologies.

Preamble: To allow bit synchronization an extra training sequence of well-known symbols is used at the physical layer level of wireless systems. It is called preamble when it appears in the beginning of a packet. Such physical layer overheads should be kept as small as possible for better utilization of channel resources.

Processing Gain: $Spread\ Bandwidth / Unspread\ Bandwidth$, It is expressed in dB.

Proximity and collocation coexistence [16]: *Proximity* is described as if devices are not operating from a single platform but are working in the same area close enough to interfere with each other. The interference is caused by antenna radiation, where the stations are located in the antenna far field ranges. Whereas heterogeneous *collocation* is the case when multiple radios are in the same physical unit so that mutual interference can be caused by conduction, parasitic circuit radiation or antenna near field radiation.

Receiver sensitivity : Sensitivity in a receiver is normally taken as the minimum input signal required to produce a specified output signal having a specified signal-to-noise ratio (SNR). The receiver sensitivity indicates how faint a signal can be to be successfully received and understood by the receiver to achieve a specific QoS (for instance -90dBm @ 10^{-3} BER). The lower the value of receiver sensitivity the better will be the system performance.

Relay station: An intermediate station that passes information between terminal stations or other relay stations.

Routing: It is the process of selecting suitable paths in a network to transmit data.

Signal-to-interference ratio (SIR): Ratio of signal power over interference power. This is usually taken at the input of a DUT receiver or DUT transceiver.

Spreading Techniques: Spread-spectrum techniques are methods by which the signal is deliberatly spread over a wider bandwidth than actually required. Direct sequence spread spectrum (DSSS), and frequency hopping spread spectrum (FHSS) are popular systems. These techniques not only offer security against eavesdropping and jamming but also provide robustness against interference and multipath effects.

Unicast: The data transmitted by one station is received by one specific (specified by the address of the receiver) station in the network.

Abbreviations

AM	Amplitude Modulation
ARQ	Automatic Repeat reQuest
ACK	Acknowledge
ASK	Amplitude Shift Keying
BER	Bit Error Rate
BPSK	Binary Phase Shift Keying
BT	Bandwidth Time
CRC	Cyclic Redundancy Check
CSS	Chirp Spread Spectrum
DDL	Dispersive Delay Line
DQPSK	Differential Quadrature Phase Shift Keying
DSSS	Direct Sequence Spread Spectrum
e.g.	For Example
FEC	Forward Error Correction
FHSS	Frequency Hopping Spread Spectrum
FM	Frequency Modulation
FSK	Frequency Shift Keying
IEEE	Institute of Electronic and electrical Engineering
ISI	Inter symbol interference
ISM	Industrial, Scientific, Medical
LFM	Linear Frequency Modulated
MDMA	Multi Dimensional Multiple Access
OQPSK	Offset Quadrature Phase Shift Keying
QAM	Quadrature amplitude modulation
QPSK	Quadrature Phase Shift Keying
PAN	Personal Area Network
PDA	Personnel Digital Assistant
PLR	Packet Loss Rate
PM	Phase Modulation
SAI	Sensor Actuator Interface
SAW	Surface Acoustic Wave
T-R	Transmitter-Receiver
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WSAN	Wireless Sensor Actuator Network

List of Figures

List of Tables