Wireless Networks in industrial environments: State of the art and Issues

Xavier Carcelle, Tuan Dang, Catherine Devic
EDF Research&Development
6, quai Watier – BP 49
78401 Chatou Cedex, France
{xavier.carcelle, tuan.dang, catherine.devic}@edf.fr

Abstract. *Wireless is everywhere nowadays and WLAN (i.e. 802.11 standard family) has became used by almost any communications devices in the mass market.*
The recent achievements in the fields of modulation techniques, such as Spread Spectrum, coding methods, such as Turbocodes, CDMA2000, and frequencies allocation methods, such as OFDM and Frequency Hopping, has pushed the growing uses of reliable and low-cost wireless technologies. Among them the last standards are: IEEE 802.11 family (i.e. WiFi), HyperLAN and HyperLAN2, IEEE 802.15 (i.e. WPAN), IEEE 802.16 (i.e. WiMAX)…
However, the industrial environments are not taken into consideration in the design of those standards, because its harsh constraints has specific characteristics (reliability, interferences with existing equipments, multi-path propagation, low-power consumption, real-time reconfiguration, security…) that need specific requirements and eventually standards.
This paper will intent to give an overview of the wireless technologies and discusses the current and future possible technologies for the uses in the industrial environments (power plants and stations, factories, industrial buildings, automotive…). Our current works showed us that there is no perfect technology by it-self but the best trade-off solution is a hybrid architecture combining the right wired and wireless technologies.

1 Introduction

The last past years have been intense in terms of development of wireless standards and wireless applications. Those applications are going from mass market domestic uses including Internet access to industrial usage in the field of wireless sensors networks, wireless interconnection between computer based control devices (DCS, PLC…) and industrial asset management based on pervasive networks indoor or outdoor.

These emerging wireless technologies can give benefits in cost-reduction, and reliability in industrial applications as well as opportunities in improving operational performance. But there is still work in progress to achieve usable technologies which meet industrial requirements. Firstly we will present an overview of the current and future wireless technologies from a standardization point of view. Secondly we will analyze the work to be done in the design and implementation in the industrial environments, such as in the utilities installations (power plants, sub-stations, factories). Finally we will present our current experimentations and future works within hybrid technology networking fields.

2 Overview of wireless communication technologies

2.1 Taxonomy and technical overview

Wireless networking technologies can be divided into three main classes (see Fig). Each class addresses specific requirements and purposes in point-to-point and point-to-multipoint communication.

WPAN addresses Personal Area Network in which most of the time, point-to-point communications are involved. However, point-to-multipoint communications are possible with wireless networks protocols such as PicoNET (based on Bluetooth) or ZigBee (based on IEEE 802.15.4b). The range performances are typically from 1 meter to a few dozens meters. The WPAN are designed for low data rate (usually 100-200 kbps). This family gather the following technologies: ZigBee, Bluetooth and UWB.

WLAN addresses Wireless Local Area Networks where the main uses are inter-connecting high data rate applications (Multimedia streaming, files sharing…), building easy-to-deploy HotSpot-like networks and lately Ad-Hoc enabled networks such as Mesh Networks. The range performances are typically from a few dozens meters indoor to a few hundred meters outdoor. The WLAN are designed for high data rate (usually 1 to 20 Mbps). This family is composed with WiFi and DECT..

Finally WWAN addresses Wireless Wide Area Networks which are mainly focused for long-distance point-to-point high data rate connections. They are designed to link plant sites networks all together with date rate ranging typically over 10Mbps with distance performances over few hundred meters. This long-distance family gathers: WiMAN, WiMAX and GSM.

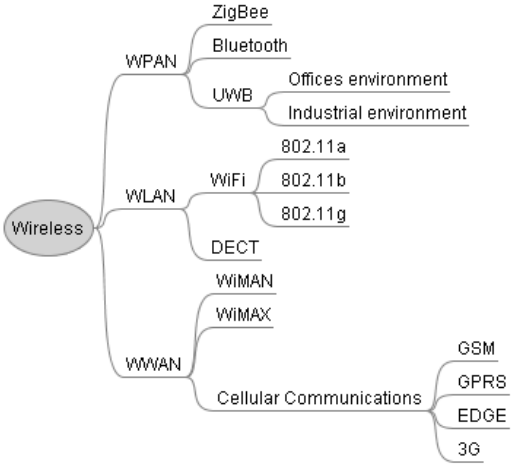


Fig.1. Wireless technologies taxonomy

From a more technical point of view, wireless networks use a lot of underlying mobile communications technologies benefiting from digital signal transmission researches. The following tables present the technical characteristics of the different wireless standards with their respective frequencies and modulation issues. In term of frequency issues, the chapter III will cover the different regulations and the co-existence problems between each wireless technology. It intents to present a brief guideline that may help to make the right choice in industrial applications.

In digital mobile communications systems, the modulation and the multiple access methods are important characteristics that has influence on the efficiency of the channel in terms of: data rate, robustness and power consumption. IEEE describes the robustness [1] as the degree to which a system or component can function correctly in the presence of invalid inputs or stressful environment conditions. Robustness can also be achieved using MIMO systems. In communication theory, MIMO refers to radio links with multiple antennas at the transmitter and the receiver side. Given multiple antennas, the spatial dimension can be exploited to improve the performance of the wireless link. The performance is often measured as the average bit rate (bit/s) the wireless link can provide or as the average bit error rate (BER). Which one has most importance depends on the application.

Most of digital transmission system uses advanced channel coding technique to prevent errors in the transmission and to correct them in the receiver when they happen. Below (see

Fig) is an example [2] of the encoding method for OFDM:

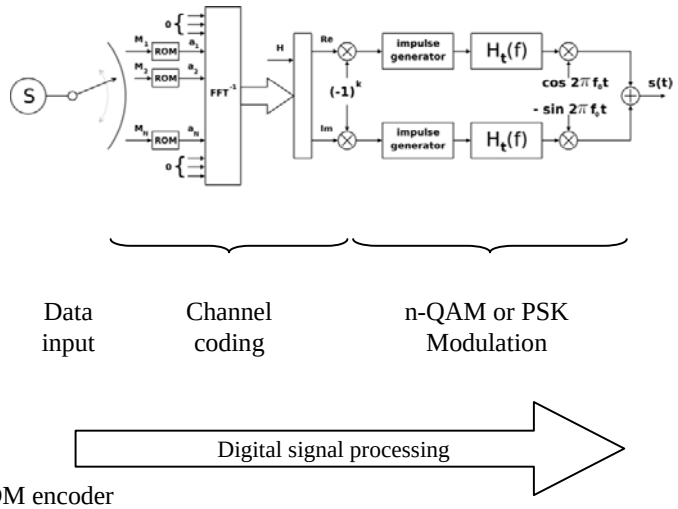


Fig.2. OFDM encoder

OFDM uses the principle of multi-carrier transmission technique that converts a serial high-rate data stream onto multiple parallel low-rate sub-streams. Each sub-stream is modulated on another sub-carrier. Below is an example of multi-carrier modulation with four sub-channels [3].

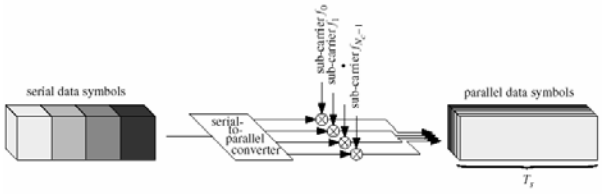


Fig.3. Example of multi-carrier modulation

In Spread Spectrum communication, the baseband signal bandwidth is intentionally spread over a larger bandwidth by injecting a higher-frequency signal. So, energy used in transmitting the signal is spread over a wider bandwidth, and appears as noise. Different Spread Spectrum techniques use different manners of injecting Pseudo Noise sequence (code) to distribute the power of the baseband signal. Below is an illustration of Direct Sequence Spread Spectrum technique [4].

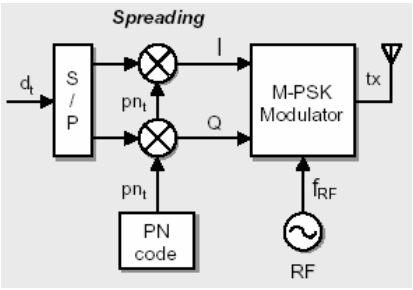


Fig.4. Typical DSSS circuit

Following the standardized OSI model for wireless protocols, the physical (PHY) and the medium access (MAC) layers can be seen as below:

Table 1.. PHY and MAC layers for wireless protocols

MAC	IEEE 802.3, IEEE 802.13, IEEE 802.15				
PHY	Multiple Access logic	CSMA/CA			
	Channel coding or decoding	Spreading, despreading, serial-to-parallel or parallel-to-serial…	**Narrowband technique:** OFDM	**Spread-spectrum technique:** FHSS, DSSS…	**Ch. multiple access:** CDMA, TDMA, FDMA
		FEC (block coding, convolutional coding, Turbocode, …)			
	Modulation or Demodulation	n-QAM or FSK or PSK…			

Each digital signal transmission technique has its own advantages and drawbacks. Following is the comparison of the different Multi-Carrier narrowband Transmission and Spread spectrum Techniques:

Table 2. Comparison of different digital signal transmission techniques

Transmission Technique	*Advantages*	*Drawbacks*
FHSS (Bluetooth, DECT)	• robust to interference • strong with jamming	• limited data rate • higher power consumption
DSSS (IEEE 802.11b, ZigBee, GSM)	• support variable data rates • resistance to multi-path • resistant to narrow-band interferences	• sensitive to jamming • limited number of same-cell access points
OFDM (IEEE 802.11g, IEEE 802.11a)	Resistance to • link dispersion • multi-path • frequency interference • burst noise	• higher power consumption • higher CPU needs

In the following paragraphs, we will analyse the characteristics of each class of wireless networking technologies:

2.2 WPAN (Wireless Personal Area Networks)

WPAN technologies are being quite heavily used these past years in the mass market industry but a very few in the industrial environment. The coming years will see a great spread out of these technologies in the factories and the industry in general. For instance the IEEE 802.15.4 working group is leading the technology standardization for such technologies matching the needs and the requirements.

Table 3. WPAN technologies

Wireless comm. technology	Bluetooth	Ultra Wide Band (HDR) (Offices environment)	"ZigBee"	Ultra Wide Band (Industrial environment)
IEEE Standards	802.15.1	802.15.3 (WG a)	802.15.4 (WG b)	802.15.4 (WG a)
Peak data rate	723.2 kbps	480 Mbps	• 20 kbps (868 MHz) • 40 kbps (915 MHz) • 250 kbps (2.4 GHz)	1 Mbps
Frequency range	2402-2480 MHz	3.1-4.8 GHz	• 2.4-2.4835 MHz • 902-928 MHz (US) • 868.3 MHz (Eu)	5.9-10.6 GHz
Channel bandwidth	1 MHz	1.368 GHz or 2.736 GHz or 528 MHz	5MHz	500MHz
Number of channels	79	2 or 13	1 (868 MHz) 10 (915 MHz) 16 (2.4 GHz)	-
Multiple access	TDMA or CDMA	Ternary CDMA or TFI-OFDM	CSMA/CA with FDMA and TDMA	Impulse Radio
Modulation	GFSK	• BPSK/QPSK (DS-SS UWB) • QPSK(MB-OFDM)	• BPSK (868/915 MHz) • OQPSK (2.4GHz)	• TH-PPM • TH-A-PAM
Power-consumption	+++	++	+	+
Range performance	+	+	++	+
Localization performance	++	+++	+	+++
Security	++	+++	+++	+++

2.3 WLAN (Wireless Local Area Networks)

WLAN technologies headed a huge development these pasts years with main applications such as Private LAN (Local Area Networks) and Public Internet Hot-Spots where the WiFi technology is now embedded in any electronic device as one

of the main features. DECT has been also extremely used in-the-homes and is now used in industrial environment for voice and data over the private phone system. For wide industrial environment, such as big factories, storage areas, docks or power plants, DECT might be a good to have a reliable, robust wireless private phone system but also add to this system data communications and emergency alarms using the worldwide ISM bands. The backbone linking the DECT base stations is usually wired.

Table 4. WLAN technologies

Wireless comm. technology	WiFi			DECT
Standards	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g	ETSI
Peak data rate	54Mbps	11Mbps	54Mbps	100kbps
Frequency range	• 5.15-5.35 GHz (US) • 5.470-5.725 GHz (Eu) • 5.725-5.825 GHz (US/China)	• 2.4-2.4835 GHz (US/Eu) • 2.471-2.497 GHz (Japan) • 2.4465-2.4835 GHz (Fr) • 2.445-2.475 GHz(Sp)	2.4-2.4835 GHz	• 1880-1900 MHz (Europe) • 1880-1990 MHz (Worldwide)
Channel bandwidth	20MHz	20MHz	20MHz	1.728MHz
Number of channels	12	3 (non overlapping)	3 (on overlapping)	10 (12 users per channel)
Multiple access	CSMA/CA	CSMA/CA	CSMA/CA	FDMA/ TDMA
Modulation	• BPSK,QPSK • 16QAM, 64QAM	• BPSK,DQPSK (Header) • BPSK,QPSK(Payload) • CCK, PBCC	• BPQK, QPSK, • 16-64QAM	GFSK
Power-consumption	++	++	++	+
Range performance	+++	++	++	++
Security	++	++	++	++

2.4 WWAN (Wireless Wide Area Networks)

WWAN technologies is used mainly for two applications nowadays is cellular phone communications and wide range IP-networks such as inter-cities point to point links. The WiMAN technology for instance is high-data rate with range performances up-to several kilometers and no mobility. Whereas the cellular communications for data transfer are usually low-to-fair data rate with complete mobility in the covered areas with GPRS services. From an industrial point of view, the two cases can be found as applications. A far remote power plant can be connected to the corporate backbone using a long-distance IP-based connection like a 802.16 link retrieving data from a sensors. Also a GPRS modem can help to regularly access a remote sensors or enabling a power plant staff to stay connected to the corporate backbone while off-site for a manual metering or a measurement task.

Table 5. WWAN technologies

Wireless comm. technology	WiMAN	WiMAX	Cellular Communications
Standards	IEEE 802.16	IEEE 802.16a	GPRS
Peak data rate	134Mbps	a:75Mbps e:15Mbps	100kbps
Frequency range	10-66GHz	a:2-16GHz e:2-6GHz	GSM bands
Channel bandwidth	20Mhz 25MHz(US) 28MHz(Eu)	a:1.5-20MHz e:>5MHz	usually 1.25MHz
Number of channels	-	a:1.5-20MHz e: under definition	depends on service
Multiple access	TDMA	OFDM	CDMA
Modulation	QPSK, 16QAM,	QPSK, 16QAM, 64QAM	QPSK, HPSK
Power-consumption	+++	+++	++
Range performance	+++	+++	+++
Localization performance	+	+	++
Security	+++	+++	+++

3 Frequency regulations and co-existence issues

3.1Frequency regulations issues

These below tables present a brief overview of the different frequency regulations for the wireless technologies discussed in the previous chapter:

3.1.1 WPAN

Table 6. WPAN frequency regulations

Region	Bluetooth	UWB (office environment)	ZigBee	UWB (industrial environment)
North America	ISM 2.4 GHz	ISM	ISM 2.4GHz, 916MHz	FCC 15.209 and FCC 2002
Europe	ISM 2.4 GHz	ECC/DECC/(06)AA	ISM 2.4GHz, 868MHz	CEPT/ECC/TG3 -41dBm/MHz
Japan	ISM 2.4 GHz	-41dBm/MHz	ISM 2.4GHz 868MHz	-41dBm/MHz

3.1.2 WLAN

Table 7. WLAN frequency regulations

Region	802.11a	802.11b	802.11g	DECT
North America	ISM	ISM	ISM	ISM
Europe	ISM	ISM	ISM	ISM
Japan	ISM	ISM	ISM	ISM

3.1.3 WWAN

Table 8. WWAN frequency regulations

Region	802.16	802.16e	Cellular
North America	Licenses	Licenses	Licenses
Europe	Licenses	Licenses	Licenses
Japan	Licenses	Licenses	Licenses

3.2 Coexistence issues in the 2.4GHz

The Steinbeis-Transfer Centre [5] has been testing the interference between ZigBee data communications (channel 11 to 26) and the other 2.4 GHz technologies. The below table summarizes the main results:

Table 9. Steinbeis-Transfer Centre coexistence tests

Technology	Packet loss results (IEEE 802.15 frames lost)
WiFi (802.11b/f=2437 MHz)	92% lost
Bluetooth	10 % lost
Microwave	1% lost

We can see both the 802.11b and the 802.15.4 are DSSS technologies that can interfere a lot between each other compared to other transmission technique in the same band.

Another test of coexistence has been led by the company Crossbow [6] measuring the perturbations of a data communications system with ZigBee technology receiving interferences from Wi-Fi radio frequencies using the 802.11b technology and namely the channel 3 at the frequency of 2.422MHz:

Table 10. Crossbow coexistence tests

802.15.4 channel	11 2.405GHz	14 2.420GHz	15 2.425GHz	20 2.450GHz	26 2.480GHz
Packet loss	0%	5%	2%	0.01%	0.01%

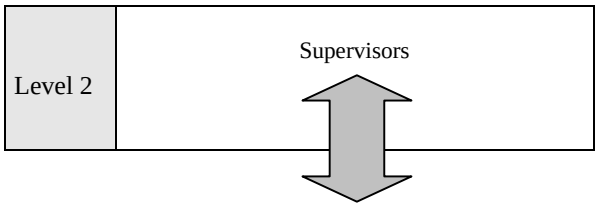
The results show that the nearest is affected by quite an important packet loss that can affect the reliability of a data communications system. This implies the best trade-off between the transmission method chosen and the frequency channel used.

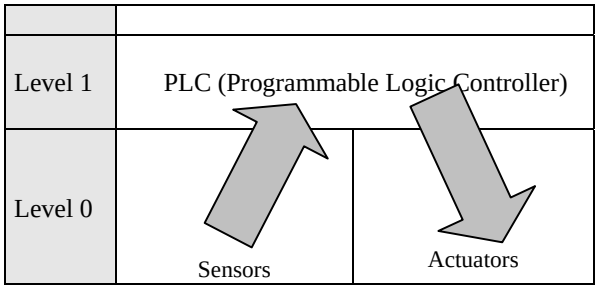
4 What needs to be done to implement industrial wireless solutions?

4.1 The environment

The industrial environments present some specific issues and requirements. For example, the I&C domain concerns instrumentation, supervisory and control of the processes. I&C focuses mainly on three levels that can be represented as below:

Table 11. Typical I&C architecture





This functional architecture has several level-to-level interfaces requirements that need to be achieved by the communications network. These requirements are:

- Level 0 to level 1: real-time control (persistent stable duplex communications links), deterministic data transfer (robustness of the LLC stack), short ranges communications, always-connected, lower data rate communications.
- Level 1 to level 2: wide range communications, hybrid-type physical medium, not-always connected, higher data rate communications, possible data aggregation.

4.2 The benefits from going wireless

The benefits one can expect from going wireless for a sensor network in the I&C domain can be listed:

- cables cost reduction
- mobile points of acquisition
- self-healing communications architecture
- low-power consumption
- adaptable topology (star, tree, mesh)
- ad-hoc communications
- harsh wiring conditions and difficult environment
- hand-over between WPAN cells and between WPAN and WLAN architecture (typical uses of wireless networks are shown in in the E.D.F. – Electricité De France - environment)

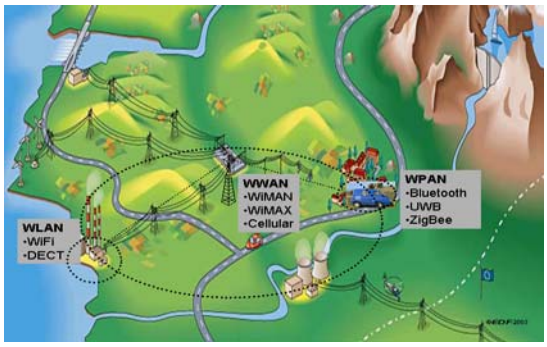


Fig. 5. Wireless technologies for utilities applications

4.3 What needs to be done?

These benefits can be obtained if the following challenges are fulfilled:

- Electro-Magnetic Compatibility satisfied despite persistent EMI (Electro Magnetic Interference) from electric welding/motors, transformers, lightning, switches, ovens, mid and high-voltage lines…
- Possible interference from same-band RF devices turned on accidentally or maliciously
- Worse large scale path-loss
- Worse fading (multipart)
- Optimised radio cell distribution
- Advanced networks protocols

The following table proposes some suggested solutions and optimizations:

Table 12. Suggested solutions and optimizations

	Challenges	Solutions	Optimizations
1	EMI	FHSS, retransmission, UWB	Notches, wide band protocols
2	Same-band RF devices	OFDM, CSMA	Random retransmission
3	Path-loss	DSSS, MIMO	Multiple antennas
4	Fading	Repeaters, smart antennas	Power regulations
5	Radio cell	RF expertise, hybrid fixed and mobile bas stations	Radio environment modeling tool
6	Network protocols	Proactive and On-demand routing protocol	Energy oriented adaptative protocol, payload balance between nodes

5 The right solutions for the right applications

Once we have gathered all these requirements and technical characteristics of the wireless technologies, one is ready to start designing the right solutions for the right applications. For instance, none technology is perfectly matching the needs of the applications and being aware of the bottlenecks of each one helps the network architect to deploy the optimized solution.

At E.D.F., we have different applications cases of wireless networks in an industrial environment such as:

- wireless tele-dosimetry
- mobile handheld devices for I&C patrols

- telecontrol of far-remote power plant sites
- geo-localization of biohazard products

The typical applications requirements in the I&C domain can be summarized into these tables:

5.1 Control applications

Table 13. Controls applications Vs wireless solutions

Constraints		*Range*		
Real-time	Yes	WPAN	WLAN	WWAN (rarely)
Harsh RF	Yes	Short-to-mid range non-beacon WiFi		GPRS
Battery life	No			
Mobility	No			
Data rate	No			802.16
Ad-hoc	No			
Security	Yes			

5.2 Measure applications

Table 14. Measures applications Vs wireless solutions

Constraints		*Range*		
Real-time	No	WPAN	WLAN	WPAN
Harsh RF	Yes	Bluetooth ZigBee	802.11b	GPRS
Battery life	Yes			
Mobility	Yes			
Data rate	No		802.11g	802.16

	Yes	UWB		
Ad-hoc	Yes			
Security	Yes			

Sometimes, we are able to find complete wireless solutions for controls or measures applications. For instance, the EDF R&D EMC laboratory specifies that wireless can interfere with old analog electronic boards.

To overcome such a barrier, we need to hybrid the technologies combining wireless and wired solutions. Concerning the wired solutions, PLC (Power Line Communications) networks can also reduce the cable cost and achieve the needed network requirements by using standardized interfaces.

5.3 Hybrid networks: wireless and power line networks

In the past years, PLC (Power Line Communications) technologies have reached a level of maturity in terms of data rate, standardization, inter-operability with the generalization of IEEE 802.3 standard and security.

That maturity allows its use in the industrial environments, such as power plants and sub-stations, by implementing the last developments in PLC networks.

Nowadays PLC Networks technologies can be described by several industrial standard-like:

Table 15. PLC Technologies

Data rate	*PLC technology*
Low	X10 LonWorks CEBus Homeplug Control and Command (2006)
High	Homeplug 1.0, AV DS2 Spidcom

Besides this list of PLC technologies, we don't look after using Homeplug BPL for industrial applications.

Finally, the cutting-edge industrial networks equipment could be a mix between:

- Zigbee and Homeplug Command and Control
- 802.11 and Homeplug AV
- UWB and Homeplug Command and Control

6 Conclusion and future works

The general feedback from our experimentation and test cases in utilities industrial environment is as follows:

- For Process Controls applications, IEEE-802.11 family standard needs to be implemented/deployed in one hand with WIPS (Wireless Intrusion Prevention System) and WIDS (Wireless Intrusion Detection System), and in the other hand with non-beacon transmission mode to reduce latency. Moreover, interference with existing analog electronic control devices is a real issue that needs to be carefully detected before any deployment. Thus, we believe that an hybrid communication architecture combining Power Line Communication technology with the IEEE-802.11 family represents a cost-effective and interesting alternative.
- For Wireless Measures applications, WPAN technologies like Zigbee and UWB are the technologies of choice as a lot of researches have been done in the area of power consumption optimisation control routing protocol [7]. Of course, careful wireless sensor network design is particularly important in terms of power conservative performance. This is an area we continue to investigate in terms of network modelling, design and deployment engineering tools that must take into account the industrial installations characteristics.

References

[1] Institute of Electrical and Electronics Engineers. IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries. New York, NY: 1990.

[2] http://www.wikipedia.org/WIKI/ofdm.

[3] K. Fazel and S. Kaiser, “Multi-Carrier and Spread Spectrum Systems”, Wiley Editor, 2003.

[4] J. Meel's (De Nayer Institute), “SS Introduction”, October 1999.

[5] http://www.ba-loerrach.de/stzedn

[6] http://www.xbow.com/Products/Product_pdf_files/Wireless_pdf/ZigBeeandWiFiInterference.pdf

[7] Ya Xu, John Hedeimann, Deborah Estrin, “Adaptive Energy-Conserving Routing for Multihop Ad hoc Networks”, USC/ISI Research report 527, October 2000.

[8] J. Karedal et al, “Statistical Analysis of the UWB Channel in an Industrial Environment”, IEEE Vehicular Technology Conference, pp. 81-85, December 2004

[9] M. Andersson, “IEEE 802.11b and Bluetooth in an Industrial Environment”, connectBlue AB, May 2001.

[10] Qixin Wang, Xue Liu, Weiqun Chen*, Wenbo He, and Marco Caccamo, Real-Time Systems Lab, CS Dept., UIUC, *ECECS, Univ. of Cincinnati “Building Robust Wireless LAN for Industrial Control with DSSS-CDMA Cellphone Network Paradigm” IEEE RTSS 2005