Electrical Measurement Engineering
Helmut-Schmidt-University
University of the German Federal Armed Forces Hamburg

Wireless Automation

Gerd Scholl, Ralf Heynicke, Dirk Krüger, Rainer Hornung
Electrical Measurement Engineering
Helmut Schmidt University / University of the Federal Armed Forces, Hamburg, Germany
gerd.scholl@hsu-hh.de

Abstract:
Resource conserving weight, material and energy savings, achievement of compliance with new environmental and safety requirements, cost-efficient retrofitting of already existing monitoring and control systems, improvement of labor productivity, inventory optimization, mobile operation and tracking, remote control and maintenance or alleviation and acceleration of awkward or laborious installations are still the main reasons for the employment of wireless technologies in automation applications. Therefore, more and more radio chips in combination with low-power microcontrollers are embedded into machines, tools, sensors and actuators. During the last years the the high market potential of wireless technologies has been recognized by nearly all important industrial players and various standards have been defined and are now paving their way into the markets, which can roughly be subdivided into transportation and logistics, building automation, factory and process automation and infrastructure plants. Still the wireless automation market offers opportunities for creative ideas, e.g. solutions for wireless coexistence or engineering tools for a fast and simple installation of wireless systems, but for nealy all market segments standardized wireless solutions are now available so that the application field for innovative proprietary solutions is steadily shrinking.

Key words: wireless standards, factory- and process automation, smart metering, smart grid

1 Introduction

While proprietary wireless technologies have been used for automation applications in a limited fashion since the 1980s, users were reluctant to adopt wireless technologies originally determined for office or consumer applications. Main concerns were high security and safety requirements, battery lifetime, interoperability and scalability, interference of radio signals with other radio services and electromagnetic radiation, emitted from e.g. spot welding robots, induction heaters or inverter controlled motors. All of these concerns have been addressed by the suppliers of wireless technologies during the last years so that the speed of market penetration of wirelessly embedded sensors, actuators, identification tags and communication modules is steadily increasing. This effect is supported by potential users, which today normally have a good understanding of the pros and cons of the wireless solutions for their target applications, which was not the case several years ago. Analysis of inter-device industrial wireless communications by the International Society of Automation (ISA) resulted in a partitioning of industrial communication systems into three categories: monitoring, control and safety. For all safety levels wireless products are already available. Examples for extremely robust wireless data transmission systems are [1-5]. By modifying the eleven-chip Barker spreading sequence employed in 802.11b Wi-Fi modules a very high interference immunity against other Wi-Fi systems also operating in the 2.45 GHz ISM band could be achieved. Depending on the application a wireless PROFIsafe data transfer, which is the extension of the standard PROFIBUS or PROFInet to address special requirements for safety related information, can be realized with various Wi-Fi standards, Bluetooth, DECT or upbanded DECT radio solutions [1]. In [2] a highly robust wireless data transmission is achieved on the basis of chirp spread spectrum technology. With a bandwidth of 64 MHz and a symbol length of 1μs the processing gain is 64 or 18 dB, which allows to detect very weak signals even in strong interference situations or noise. A frequency hopping spread spectrum technology with up to 830 individual hop-channels for industrial applications was developed by [3]. Fail-safe point-to-point wireless transmission via PROFInet was realized using two redundant wireless links in the 2.45 GHz and/or 5 GHz ISM-bands [4]. Even in a heavily interference-prone environment wireless technologies can be integrated into an industrial communication

Review Paper for the 16th International Conference On Sensors and Measurement Technology, Nürnberg Exhibition Center, SENSOR 2013, Germany, May, 15th, 2013.

system employing leaky wave cables [4] or slotted waveguides [5]. Today, Wi-Fi and Bluetooth are well established for secure and robust factory and process automation applications [1-10]. Wi-Fi systems can provide an excellent backbone for data concentration and networking. They also allow wireless access to field devices for configuration and testing, linking of communication segments for rapid commissioning, communication with dynamic stations as stacker trucks, conveyor lines or trolleys, and also give mobile workers access to up-to-date control and maintenance data, wherever they are. As Bluetooth uses tiny, inexpensive, short-range radio transceivers, this technology is ideally suited to be embedded into sensors or actuators connecting them to a programmable logic controller (PLC). Other applications are serial cable replacement or wireless access points [7-9]. A Bluetooth piconet can have up to eight devices, typically, but also wireless systems, where up to 250 Bluetooth modules can be clustered, are already available [10]. A multi-hop Bluetooth tree-network can be automatically established using the standard serial port profile so that almost any commercially available Bluetooth device can be integrated into the network. The first commercially available wireless sensor network solution for low-data rate home, building and industrial automation applications was ZigBee. Since 2004, when the standard has been ratified, Zigbee has been improved with additional functionalities. In 2012 Zigbee was enhanced by the green power feature, which now also allows batteryless devices to securely join ZigBee PRO networks. The first company and the originator of patented energy-harvesting wireless sensor technology was EnOcean. Meanwhile the International Electrotechnical Commission (IEC) has ratified the new standard ISO/IEC 14543-3-10 for wireless applications with ultra-low power consumption. It is the first and only wireless standard that is also optimized for energy harvesting solutions and, therefore, for EnOcean's self-powered wireless technology. Together with the EnOcean Equipment Profiles drawn up by the EnOcean Alliance, this international standard lays the foundation for fully interoperable, open wireless technology comparable to standards such as Bluetooth and Wi-Fi. This is one reason why EnOcean seems to become the de-facto standard for wireless energy harvesting applications in building automation.

2 Smart Metering

The smart grid is envisioned as providing a communications network for the energy industry, offering new business opportunities for different kind of industries, such as smart-meter vendors, electric utilities and telecom operators from all around the world. A key element of the smart grid is the availability of a sophisticated advanced metering infrastructure (AMI), capable of real-time communication with the utility company, i.e. the metering unit represents the interface between the grid and the end user. To standardize the communication of consumption meters so that interoperability is guaranteed, associations and companies have joined together to form the OMS-Group and have developed the “Open Metering System Specification” by selecting options from the European norm EN 13757-x. All the OMS-meters are interoperable, regardless of the source they come from or which kind of consumption they measure. Tools are available to test and certify interoperability. Intelligent OMS meters are a prerequisite for energy saving via smart grids and smart homes and the optimum integration of renewable energies such as wind power or solar energy. OMS is compatible with the well-known KNX standard, so that beyond metering of consumption the building automation system can also be directly integrated e.g. for energy management. Requirements for future services such as tariff or load management can thus also be implemented cost-effectively with OMS. For data transfer between the gas, water or electric energy meters and the data concentrator, the multi-utility communication (MUC) controller, which is defined as primary communication, EN 13757-x was identified as the currently applicable norm, which describes the M-Bus as the physical interface, both hard-wired and wireless (Wireless M-Bus), as well as the data protocol. For wireless communication, the norm EN 13757-4 is being used by the OMS-specification as well as by the KNX standard. Both, metering data and data from the building automation can thus be transferred via the same system. Long distance communication uses proven internet standards. With its recommendation for specification of the MUC controller, the VDE Forum Netztechnik/Netz-betrieb has supported the standardization work of smart metering systems, significantly. The MUC controller communicates with all standard IT systems for remote metering as well as household consumer meters for electricity, gas, water and heating and is an essential prerequisite for realising a smart metering system. Following national implementation of the EU Energy Efficiency Directive (EDL) by the Energy Economy Law (EnWG) and the Measuring Instrumentals Directive (MessZV), the issue of “Smart Metering“ has gained significance. Since the 1st of January 2010 metering equipment must be installed in new buildings and in the course of larger renovation measures in accordance with § 21b EnWG, so that actual energy consumption and usage time can be made visible for the end user. This is realised by the electronic basic meter (EDL21 meter). In accordance with § 40 EnWG electricity consumers are to be offered additional load-variable tariffs or tariffs which are dependent on the time of day representing an incentive to save energy or control energy consumption. This is possible by supplementing the basic meter with the MUC controller (EDL40 system). The new electronic household meters which are also capable of saving, displaying and transferring consumption data via standardised interfaces will totally replace the well-known Ferraris meters within a few years.

3 Process Automation

As wireless communication in an industrial environment is exposed to interference, especially when operated in the 2.45 GHz ISM-band, frequency of operation should be adjusted dynamically and channels, where interference is persistent or communication is blocked, should be ignored. The network should also be easy to install, flexible, scalable, self-organizing and self-healing. Other requirements are: cost and time saving installation, low maintenance costs, engineering and diagnosis tools should be based on standards already known by the technical staff, simple integration of additional sensors or actuators into the existing sensor network and an efficient power management for long-term operation.

During the last years WirelessHART is maturing to become the de-facto standard in process automation. WirelessHART relies on the physical layer of IEEE standard 802.15.4, but additionally specifies to the transport and applications layers its own data-link layer. More than 26 million wired HART devices are already installed in the field. The compatibility in the transport and application layers ensures the compatibility in the protocol stacks of HART and WirelessHART, allowing the user to employ the same engineering tools and practices he already knows. WirelessHART is a contention-free, time-synchronized protocol with an accuracy of 1 ms across the entire network. The basics for network synchronization were developed by DustNetworks [11]. Time division multiple access (TDMA) is used to provide collision free and deterministic communications. All devices must support superframes, which are formed by a sequence of time slots, each having a length of 10 ms. Typically, a communication transaction between two devices are assigned to a given time slot. To enhance reliability, channel hopping is combined with TDMA so that each slot may be used on multiple channels at the same time by different nodes. All devices in the network share an identical channel list indicating which channel can be used. For easy network installation and expansion WirelessHART only specifies one single type of network device, so that each device in a self-organizing multi-hop mesh network can act as router for other nearby devices, passing messages along until they reach their destination. Also star and hybrid network types are possible. The complete network is organized by the network manager, who is responsible for e.g. initializing and maintaining network communication parameter values, scheduling, management of dedicated and shared network resouces, collection of system performance and diagnostic information, and provision of mechanisms for devices joining or leaving the network. The network manager maintains a complete list of all devices and has full knowledge of the network topology resulting in a collection of routing graphs, where each edge of the graph represents a possible transmission link between two devices. Each graph is denoted by a unique graph ID to identify the route through the mesh network. As the network is established multiple redundant communication paths are formed and continuously verified. To ensure path diversity each device should have at least two neighbours in each routing graph. In real plant settings, typically 30% of the devices communicate directly with the gateway and 50% are one hop away. The remaining 20% may take 3-4 hops [12]. Source routing is a second method for routing information between two devices. The source specifies a single route to the destination without providing any path diversity. Therfore, source routing is only used for testing and trouble shouting. Well-engineered WirelessHART products are already available [12-17] and are continuously penetrating into the market.

4 Factory Automation

One of the first wireless systems in the market was the WISA system, which has proven feasibility by many installations in the field. An excellent description of the system is given in [18]. Sensor/actuator communication is based on IEEE 802.15.1 radios. The protocol stack has been modified to achieve a high transmission reliability, to meet the requirement of short cycle times and to support a large number of sensors and actuators. The system is able to handle a communication load of 120 sensor/actuator modules per base station. The downlink signal is always available for frame and slot synchronization by the sensors/actuators. Uplink information from the sensors/actuators to the base station is organized in four parallel uplink channels. The power supply unit is connected to primary wire loops generating a varying magnetic field with a frequency of 120 kHz.

The interface wireless system delivered by Phoenix Contact is also based on IEEE 802.15.1 standard radios but uses the Bluetooth stack [3]. More than 10,000 Bluetooth networks illustrate that this system works well even in difficult industrial metallic dominated environments. The Phoenix Contact system also employs Bluetooth security, encryption and error correction features. Bluetooth networks with up to 7 devices achieve latencies between 8 ms and 16 ms.

As a steadily increasing number of different wireless technologies are used in industrial environments there is an increased probability for collisions with already installed Wi-Fi networks. Therefore, ETSI started new activities to regulate usage of the 2.45 GHz ISM-Band. These regulations aim to improve coexistence, especially for different Wi-Fi standards. They also include mechanisms like “listen before talk” or limitations of the duty cycle, transmission power, bandwidth, channel separation and total number of channels in use, what complicates the implementation of simple low-cost wireless systems for sensor/actuator-communication on the shop floor. Coexistence with other wireless systems can be increased by a limitation of time intervals required for active communication. Another way is to use only a minimum of transmission power. Without increasing frame error rate this can, e.g., be achieved with intelligent frequency hopping mechanisms. In our case the adaption of the system to the wireless channel is done during an automated initialization routine and an update is made in predefined time intervals during normal system operation. Generally, wireless channels in an industrial environment can be classified into three different groups [19]. They show a chaotic behavior if small changes in time or position lead to a totally different receive power and/or group delay. Therefore, it is impossible to derive any systematics and there is no chance to find good or bad channels for data transmission. Simple frequency hopping is the only way to cope with the randomly varying radio channel. A radio environment without moving objects or moving nodes results in a second class of wireless channels. By definition, if there is no time-variance the radio channel can be described by only a frequency-dependent channel transfer function. This can be observed in Fig. 1, where signal levels are mainly constant over time (horizontal axis) and are only slightly disturbed across the frequency range (vertical axis). In a radio scenario like this an effective mechanism to improve system performance is to use only frequencies where a high signal level can be guaranteed, i.e. to blacklist all frequencies with low absolute values in the channel transfer function. Manufacturing processes in factory automation environments often follow a cyclic sequence of process steps. The periodicity of the cyclic sequence results in a periodicity over time in the channel transfer function. Thus, a third class of wireless channels with a cyclic behavior due to a dominant process in the surrounding area of the wireless system can be defined. Fig. 3 shows a measurement of a wireless channel in a production cell with a cyclic process. In such scenarios a wireless system should be able to hop on the best frequencies dynamically. A two dimensional correlation was used to find combinations of sensor nodes with a similar behavior of the channel transfer function. At all times the optimal frequencies for each combination of sensor nodes were determined and stored in frequency hopping lists. Afterwards, the operation of the wireless system was synchronized with the cyclic process. Also rotating machines can be found in factory automation environments very often. Such a scenario has been used to verify the benefit of adaptive frequency hopping and to compare the results with a standard pseudo random frequency hopping sequence. Fig. 4 shows both sequences in a measured spectrogram of the radio channel between base station and a sensor node.

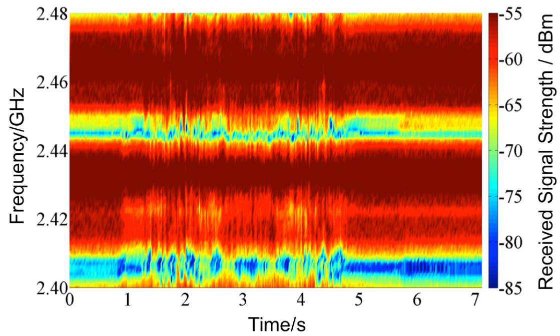

Fig. 1. Measurement result of a wireless channel with static behavior.

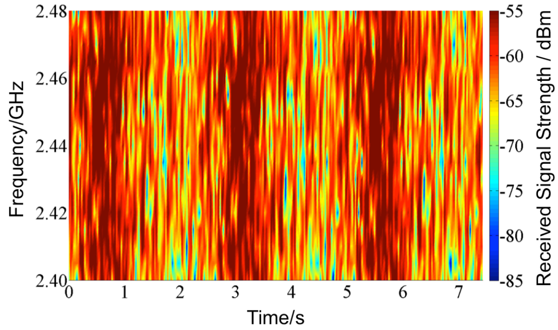

Fig. 2. Measurement result of a wireless channel with cyclic behavior.

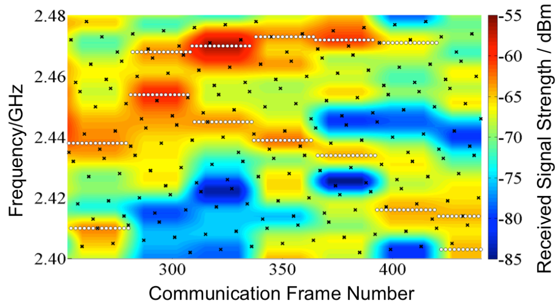

Fig. 3. Comparison of a pseudo random frequency hopping sequence (black crosses) with an adaptive blacklisting sequence (white dots).

A typical result of an adaptive frequency-hopping algorithm is shown in Fig. 4, where histograms of the received signal strength indicator (RSSI) are depicted for both hopping algorithms. In direct comparison both histograms have the same axes scale. It is obvious that the centre of the red histogram (pseudo random frequency sequence) is located left to the blue one (adaptive frequency sequence). This means that the mean level of the received signal strength increased due to the adaptive frequency sequence. In this application the mean improvement is about 7 dB. The pseudo random frequency sequence shows a variation of about 57 dB and a minimum of -90 dBm. The adaptive frequency hopping sequence has a minimum of -74 dBm and a variation of only 36 dB.

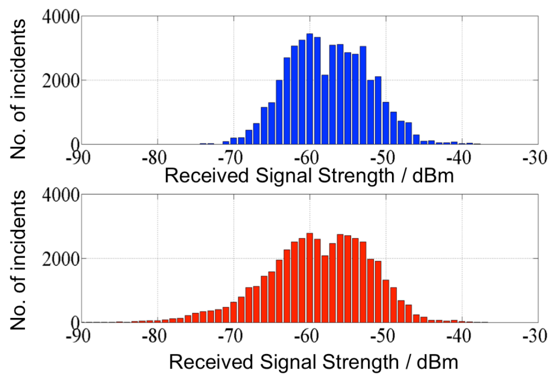

Fig. 4. Histogram of the received signal strength of a pseudo random frequency hopping sequence (red) with a adaptive blacklisting sequence (blue) in the cyclic wireless channel.

References

[1] Schildknecht AG, “Wireless Data Primer,” http://www.schildknecht.info.

[2] Nanotron Technologies, “nanoNET Chirp Based Wireless Networks,” White Paper, Version 1.04, Feb. 2007.

[3] Phoenix Contact, “Truted Wireless – in Detail,” Application Note 103146_C00_en, Jan. 2007.

[4] Siemens AG, “Industrial wireless communication: reliable, rugged, secure,” Scalance W Brochure, Oct. 2007.

[5] Vahle Electrification Systems, http://www.vahle.de.

[6] Sensicast, http://www.sensicast.com.

[7] Wago, http://www.wago.com.

[8] Phoenix Contact, http://www.phoenixcontact.de.

[9] connect Blue, http://www.connectblue.com.

[10] Stollmann Entwicklungs- und Vertriebs GmbH, “BlueCluster+,” http://www.stollmann.de.

[11] Dust Networks, “Technical Overview of Time Synchronized Mesh Protocol,” http://www.dustnetworks.com.

[12] HCF – Hart Communication Foundation, “HART 7 Specification,” Sept. 2007.

[13] Emerson Process Management, http://www.emersonprocess.com.

[14] A.N. Kim, F. Hekland, S. Petersen, P. Doyle, “When HART Goes Wirless: Understandig and Implementing the Wireless HART Standard,“ IEEE Int. Conf. On Emerging Techn. and Factory Autom.,” 09/2008, pp. 899 – 907.

[15] Endress+Hauser, “Wireless Adapter and Fieldgate,“ http://www.endress.com.

[16] Pepperl+Fuchs GmbH, “A request becomes reality,” http://www.pepperl-fuchs.com.

[17] G. Lohmann, “Bereit für die breite Anwendung, Wireless HART als offener Standard für die Funkkommunikation in der Prozessautomation,” P&A Spezial Wireless-Kommunikation, May 2008.

[18] R. Steigmann, J. Endresen, “Introduction to WISA and WPS,” White Paper, ABB Stotz-Kontakt, Aug. 2004.

[19] R. Heynicke, D. Krüger and G. Scholl, “Steigerung der Robustheit drahtloser Sensor/Aktor- Feldbussysteme durch prozessorientiertes adaptives Frequency-Hopping,” Wireless technologies Congress, Bochum, Germany, September 2010.