OPEN ACCESS

future internet

ISSN 1999-5903

www.mdpi.com/journal/futureinternet

Article

Survey on Wireless Sensor Network Technologies for Industrial Automation: The Security and Quality of Service Perspectives

Delphine Christin [1,⋆], Parag S. Mogre [2] and Matthias Hollick [1]

[1] Secure Mobile Networking Lab, Center for Advanced Security Research Darmstadt, Department of Computer Science, Technische Universität Darmstadt, Mornewegstr. 32, 64293 Darmstadt, Germany; E-Mail: matthias.hollick@seemoo.tu-darmstadt.de

[2] Multimedia Communications Lab, Department of Computer Science, Technische Universität Darmstadt, Rundeturmstr. 10, 64283 Darmstadt, Germany;
E-Mail: parag.mogre@kom.tu-darmstadt.de

[⋆] Author to whom correspondence should be addressed;
E-Mail: delphine.christin@seemoo.tu-darmstadt.de; Tel.: +49 6151 16-70923

Received: 30 January 2010; in revised form: 19 March 2010 / Accepted: 24 March 2010 / Published: 8 April 2010

Abstract: Wireless Sensor Networks (WSNs) are gradually adopted in the industrial world due to their advantages over wired networks. In addition to saving cabling costs, WSNs widen the realm of environments feasible for monitoring. They thus add sensing and acting capabilities to objects in the physical world and allow for communication among these objects or with services in the future Internet. However, the acceptance of WSNs by the industrial automation community is impeded by open issues, such as security guarantees and provision of Quality of Service (QoS). To examine both of these perspectives, we select and survey relevant WSN technologies dedicated to industrial automation. We determine QoS requirements and carry out a threat analysis, which act as basis of our evaluation of the current state-of-the-art. According to the results of this evaluation, we identify and discuss open research issues.

Keywords: Wireless Sensor Networks; Industrial Automation; Quality of Service; Security; State-of-the-art; WirelessHART; ISA100.11a-2009; ZigBee; Wireless Interface for Sensors and Actuators ; 802.15.4e Factory Automation MAC Layer

1. Introduction

Industrial automation has been successfully introduced in a countless amount of industries ranging from food to energy industries. Even if the products differ from one industry to another, the automated processes can be classified according to three main layers as proposed by [1]: the plant-floor automation layer, the manufacturing execution system layer and the enterprise resource planning layer. Internet technology can be considered as the link that interconnects all these layers and allows for information exchange. For example, it serves as a backbone to interconnect different production locations within one enterprise, to transfer production control data in near real-time to the headquarters or to integrate suppliers into a production workflow.

Within the scope of this survey, we focus on the plant-floor automation layer including sensors, switches, programmable controllers and motor starters (Fig. 1) that ensure the correct operation of machines and execution of processes, while the remaining layers are dedicated to the optimization of the production by managing resource allocation and operation scheduling for example. In addition to productivity gain and precision improvement, the automation of processes at the plant-floor automation layer allows the replacement of workers in harsh and hazardous environments or assigned to tedious tasks [2]. The WSNs are part of this layer and can be used for multiple purposes, such as monitoring synchronous or asynchronous events that require periodic data collection or detecting exceptional events, respectively [3]. For example, vibration, heat or thermal sensors can be deployed in proximity of machines to monitor their health. The analysis of the measured parameters can allow the detection of abnormal operating conditions and aids therefore in preventing potential machine failure. In addition to machine monitoring, WSNs can be deployed to measure basic physical quantities such as pressure, temperature, flow or more complex events such as process quality or automotive performance in industrial environments [4].

Although wired sensor networks can also be deployed for such monitoring scenarios, WSNs present additional advantages. In fact, their wireless capability allows deployments in hostile environments, where vibrations or moving parts may prevent the use of cables that would be damaged or even broken. In addition to reduce cabling costs, the WSNs provide network flexibility, as the sensor nodes may be relocated quickly without necessitating time-consuming cable installation and maintenance. However, the nature of the wireless medium opens up security and QoS issues. For example, potential attackers may easily eavesdrop or manipulate wireless communication in absence of security mechanisms and the wireless channel has to be efficiently allocated between the different devices to provide the required QoS.

Our contributions are as follows:

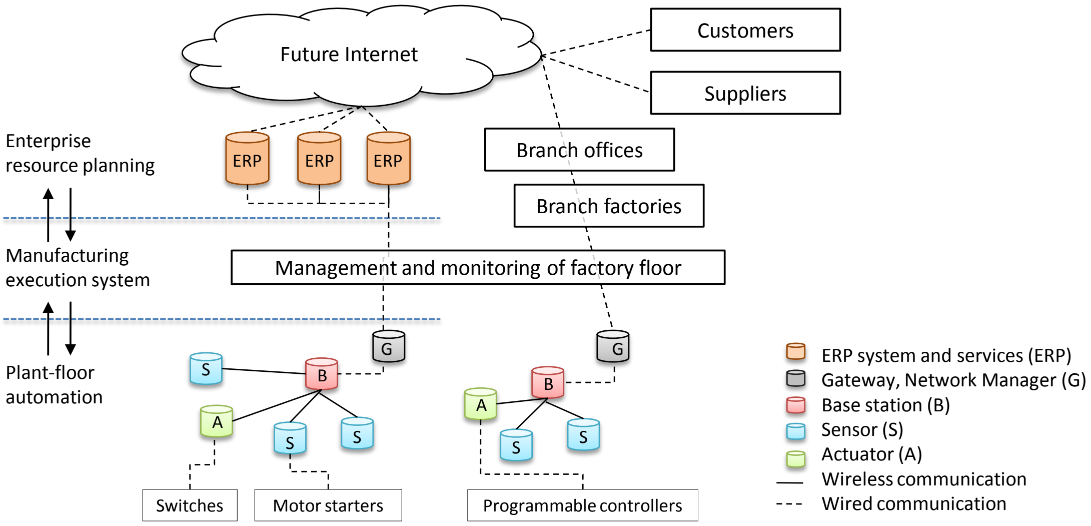
1. We first select relevant WSN technologies dedicated to industrial automation and we provide an exhaustive survey of their characteristics.

2. We then analyze industrial automation applications to determine QoS requirements and evaluate the selected standards according to each identified QoS requirement. Open issues are discussed based on the results of this evaluation.

3. We carry out a threat analysis to identify pertinent security requirements and we investigate if and how the selected standards fulfill the previously identified security requirements. Related open issues are finally highlighted and discussed.

The paper is structured as follows. Section 2 provides a detailed overview of the following WSN technologies: Wireless Interface for Sensor and Actuators (WISA), WirelessHART, ISA100.11a, ZigBee, ZigBee PRO, and 802.15.4e Factory Automation MAC Layer. Section 3 and Section 4 focus on QoS and security respectively. Both sections are composed of an analysis of the respective requirements and an evaluation of the selected specifications. Open issues are listed and discussed at the end of both sections. Section 5 concludes our work.

Figure 1. From the sensors to the customers.



2. Selected Wireless Sensor Networks Standards: State-of-the-art

Wireless communication in industrial automation is mostly based on standardized technologies, such as the IEEE 802.11 [5] and IEEE 802.15 standard families [6], also designated as *Wireless Local Area Networks* (WLAN) and *Wireless Personal Area Networks* (WPAN). Both of these standard families were conceived for application purposes different than industrial automation. In fact, the IEEE 802.11-based standards offer high data rates in the order of tens of Mbit/s and ranges up to tens/hundreds of meters, while the IEEE 802.15-based standards only supports data rates of hundreds of kbit/s to several Mbits/s with ranges from a few meters up to hundreds of meters. However, to provide greater data rate and range, IEEE 802.11 technology consumes a greater energy budget that can limit the benefits obtained by wireless communications. Indeed, the sensor nodes are either powered by cables or batteries. In the former case, the advantages provided by wireless communication are partially negated, whereas in the latter case, the scarce energy resource has to be parsimoniously consumed in order to avoid frequent human interventions to recharge the batteries. Energy is thus a major concern in both previous cases and we therefore focus on the IEEE 802.15-based standards, and particularly on the IEEE 802.15.1 [7] and IEEE 802.15.4 [8] standard, within the scope of this work.

2.1. IEEE 802.15.1-based Standards

The IEEE 802.15.1 standard, also known as Bluetooth®, can be classified to fall between the IEEE 802.11 and IEEE 802.15.4 standards in terms of energy consumption and data rates. With medium data rates and lower energy consumption than the IEEE 802.11 standard, IEEE 802.15.1 offers an interesting compromise between energy consumption and data rate, and is therefore particularly suited for high-end applications requiring high data rates as well as applications with strong real-time requirements such as *factory automation*. The Wireless Interface for Sensor and Actuators (WISA) has been selected as a representative 802.15.1-based specification for further discussion.

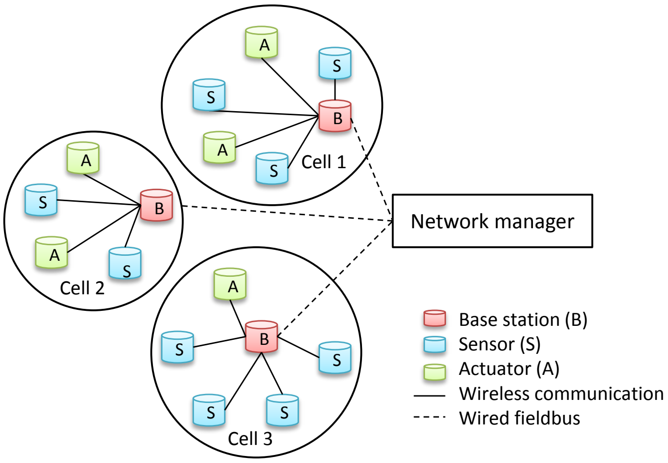
Wireless Interface for Sensor and Actuators (WISA)

Released by ABB and presented in [9], the proprietary *Wireless Interface for Sensors and Actuators* (WISA) specification is based on the IEEE 802.15.1 physical layer and targets factory automation WSNs with packet error rate less than 1^{-9} and cycle time of 2ms [10].

Network Elements

WISA networks [11] can be deployed in cellular topology with up to three cells (Fig. 2). Each cell uses a different transmission frequency, and is composed of a *base station* and up to 120 *end devices* including sensors and/or actuators organized in a star topology. The end devices communicate wirelessly via standard Bluetooth transceivers, while the base station is equipped with a specific transceiver, which is able to receive up to four channels in parallel [12]. Additionally, the base stations exchange information with the network manager via wired fieldbus such as DeviceNet [13] and Modbus [14].

Figure 2. WISA network elements.

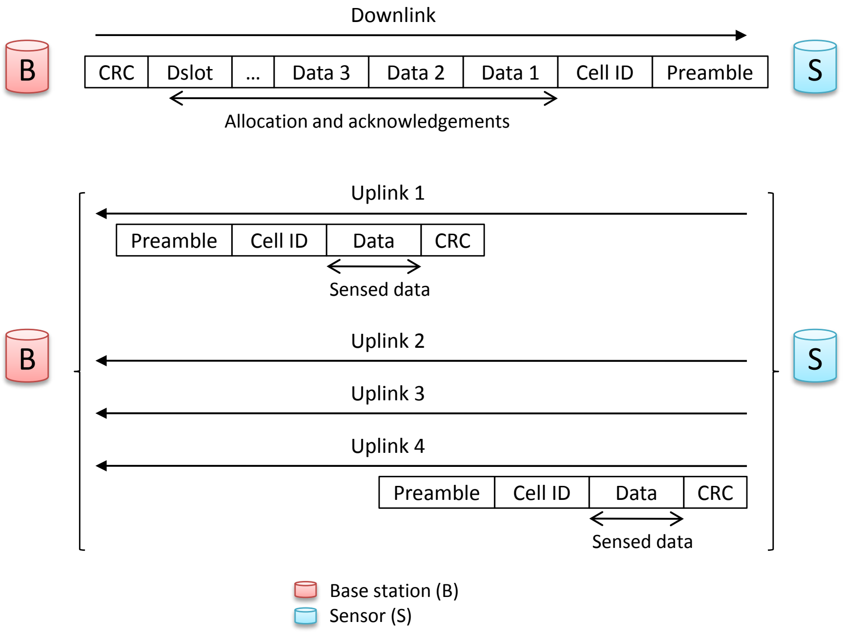


Architecture

The WISA architecture is limited to the physical and MAC layers, as sensors and actuators communicate exclusively with a central base station in a star topology within each cell. As mentioned previously, the

WISA specification relies on the physical layer of the IEEE 802.15.1 standard operating in the 2.4 GHz frequency band at a data rate of 1 Mb/s. The WISA specification [15] is based on *Time Division Multiple Access* (TDMA) and *Frequency Division Duplex* (FDD), meaning that communication from base station to sensors, defined as *downlink* direction, and from sensors to base station, defined as *uplink* direction, occur at different frequencies. The downlink direction is exclusively reserved for the base station that remains continuously active and manages the TDMA scheme occurring in the uplink direction. The four uplink channels are divided into superframes of 2048 μs, which are composed of 30 timeslots able to support packets up to 64 bit length (Fig. 3). These time slots are allocated by the base station to each sensor willing to transmit data. In case of successful transmission of the sensor data, an acknowledgement is sent by the base station in the downlink. Otherwise the sensor retransmits the data in the next frame. To avoid interference and improve the reliability, frequency hopping is additionally applied after each superframe with a carrier spacing of 1 MHz.

Figure 3. WISA superframe structure [16].



2.2. *IEEE 802.15.4-based Standards*

In comparison with Bluetooth®, the IEEE 802.15.4 standard presents lower data rates, but requires also lower energy budgets. According to [6], the standard is appropriate for infrequent exchanges of small packets, when power consumption is an important issue. The standard is therefore suited for *process automation applications*, where continuous production streams are monitored.

The IEEE 802.15.4 physical layer is common to all the following standards and operates in the 2.4 GHz frequency band as well as the 868 MHz and 915 MHz bands in Europe and North America, respectively. The 2.4 GHz frequency band is divided into 16 channels with a maximal data rate of 250 Kbits/s per channel and separated by a 5 MHz gap, while the 915 MHz band is divided into 10 channels with a maximal data rate of 40 Kbit/s each. The single channel in the 868 MHz frequency band presents a data rate of 20 Kbit/s. However, the effective data rates are smaller than the announced nominal values in reality, as mentioned in [6]. In addition to WISA, we have selected the WirelessHART, ISA100.11a, ZigBee, ZigBee PRO, and 802.15.4e Factory Automation MAC Layer technologies. These technologies address the complete protocol stack from the physical layer to the application layer (Table 1) and thus provide a complete system, except for the 802.15.4e FA MAC and the WISA technology that mainly focus on the data link layer.

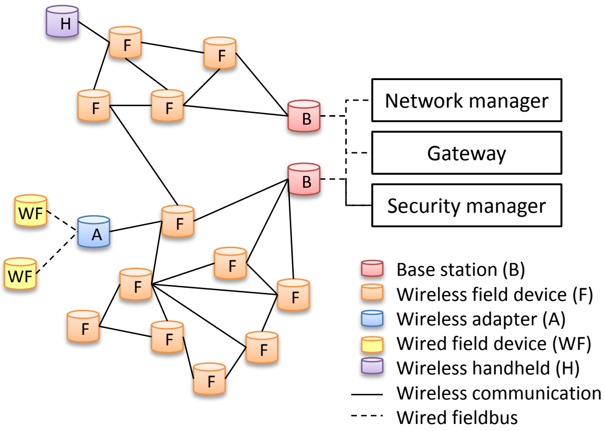
Table 1. Scope of the selected technologies.

	WISA	WirelessHART	ISA100.11a	ZigBee	802.15.4e MAC
PHY/MAC layers	802.15.1-based	802.15.4-based	802.15.4-based	802.15.4-based	802.15.4-based
NET/TRANS APP layers	unspecified	specified	specified	specified	unspecified

WirelessHART

The HART Communication Foundation is an independent and not-for-profit organization that ensures the development of the HART Protocol. As technology owner and central authority, the foundation released the open WirelessHART™standard in 2007, considered by [17] as the only released open wireless standard suitable for process measurement and control applications.

Figure 4. WirelessHART network elements [19].



Network Elements

WirelessHART networks are composed of different devices as illustrated in Fig. 4, including field devices, gateways, network and security managers. The *field devices* are organized in either star or mesh topology. However, the star topology is not recommended by [18]. The *gateway* is a bridge between the field device network and the host application. The gateway is configured by the *network manager* using HART commands and allows buffering large sensor data, event notifications, diagnostics, and command responses. In addition to the gateway configuration, the network manager configures the remaining devices and maintains the whole network. WirelessHART networks may include several network managers for redundancy reasons, however only one should be active at a time. The active network manager also schedules communication, manages routing tables, and monitors network health. In addition, the network manager can receive input from the host application and also queries the field devices about particular information via the gateway. The *security manager* collaborates with the network manager and prevents intrusion and attacks against the network by generating session keys, joint keys and network keys. Each security manager can collaborate with several network managers responsible for the key distribution to the concerned field devices. Additionally to these devices required by the standard, *adapters* and *handheld devices* may be added. The adapters connect HART devices to WirelessHART networks, whereas handheld devices configure and maintain WirelessHART compliant devices.

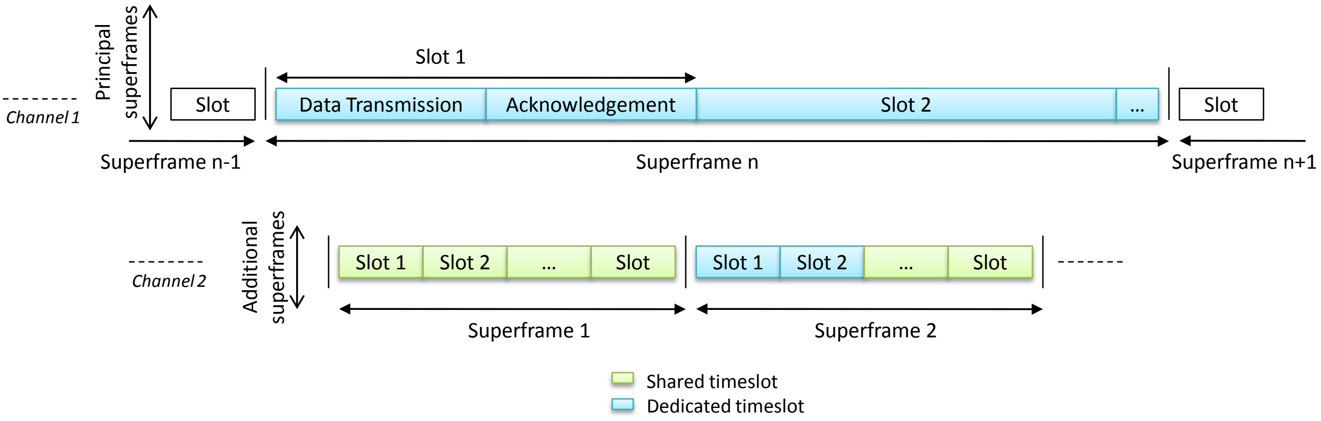
Architecture

The WirelessHART standard is presented by the HART Communication Foundation, as a reliable, secure, and robust standard. We consider successively the data link, network as well as transport and application layers that compose WirelessHART's protocol stack. At the data link layer, the WirelessHART standard coordinates and manages each device's transmission time by using TDMA with timeslots of 10 ms. Each time slot may be allocated to one source or may be shared between several sources using the *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA) mechanism. In the former case, minimal latency can be reached, whereas the latter case supports efficient bandwidth utilization. Possible collisions due to multiple sources sending simultaneously are reduced by setting random back-off intervals for each source. During the timeslot assignment, the data to transmit are first prioritized by the network manager. The data originating from the network manager have the highest priority, followed by sensed data and event information. The timeslot allocation is then communicated by the network manager in the superframe to each device. At least one superframe (Fig. 5) is continuously repeated at fixed rate and further superframes can be added to support additional traffic [20]. The length of the superframes can be adapted to the needs of the application. However, the length is fixed once the superframe becomes active. In addition to the timeslot allocation, the network manager indicates the transmission channel in the superframe. This frequency hopping helps in reducing multi-path fading and interferences. Moreover, the faulty channels are eliminated by blacklisting.

The WirelessHART standard uses two possible routing protocols [22] at the network layer: graph and source routing. In *graph routing*, the network manager determines the different paths forming the graph. The paths are stored by each device and are then used to identify the next node to forward the packet. In case of *source routing*, the packet header contains the list of the devices from the source to the destination. In addition to the paths stored for the graph routing, each device maintains tables about its communication statistics and neighbor activities. Furthermore, the WirelessHART network layer offers broadcast, multicast and unicast transmissions.

At the transport layer, the WirelessHART standard supports connection-oriented as well as connectionless communication. The *connection-oriented* communications are set up for applications requiring a reliable transfer of data between the host application and the field device for example. The connection

Figure 5. WirelessHART superframes [21].



set up starts by opening a dedicated port on the targeted field device with a specific HART command and the transmission data rate is then negotiated with the network manager, before the data transmission between the both entities can begin. Once all packets have been transmitted, the connection established between both entities is removed. The reliability of the data transfer is ensured by the acknowledgement and the order of the packets is maintained from the source to the destination. Nevertheless, these guarantees introduce additional overhead and a trade-off between reliability and overhead has to be found. For applications supporting out-of-order packet delivery, *connectionless* communication can be sufficient. Each datagram contains the full destination address and is routed independently from the others through the network [23]. Depending on the required level of reliability and the tolerance of packet loss, end-to-end acknowledgement can be introduced, but would also cause additional overhead. In connection-oriented and connectionless communication, the transport layer is also responsible for the segmentation of the data blocks at the source and their reassembling at the destination in order to allow transparent transfers for the upper layers. The WirelessHART application layer is based on the HART commands and extended by additional features allowing data publishing only when required for example.

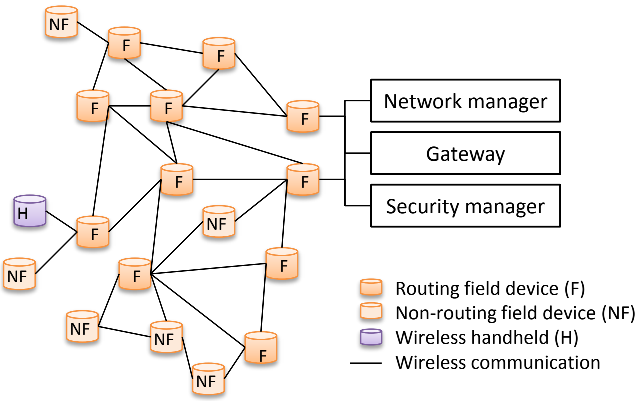
ISA100.11a

The ISA100.11a-2009 standard [24] has been developed by the ISA100 standards committee, part of the non-profit International Society of Automation (ISA) organization, and approved by the ISA Standards and Practices Board in September 2009. This first release focuses only on process applications that tolerate delays up to 100ms [12]. However, further releases addressing factory and building automation applications are expected in the next years. In parallel to the main ISA100.11a working group, different working groups address complementary issues including the compatibility of the ISA100.11a standard with existing wired and wireless standards.

Network Elements

ISA100.11a WSNs can be organized according to different topology schemes and are composed of field devices, gateway(s), and handheld device(s) as depicted in Fig. 6. Some of the *field devices* responsible for sensor data collection and actuator management can also provide routing functionalities. According to the standard, there is no limitation of the amount of subnets that form the network, and therefore the total amount of devices is not limited. However, the amount of devices per subnet is restricted by the addressing space to 30 000 devices. One or several *gateways* ensure the connection between the WSN and the user application. The gateways also support the interoperability with different standards such as WirelessHART by translating and tunneling information between the networks and could act as security and network managers. Moreover, *handheld devices* support device installation, configuration and maintenance.

Figure 6. ISA100.11a network elements [25].



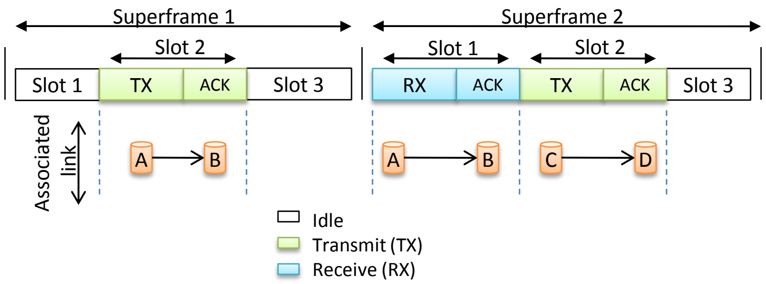
Architecture

The ISA100.11a standard addresses all OSI layers: physical, data link, network, transport and application layers. The *physical layer* is based on the IEEE 802.15.4 standard. However, additional requirements were defined. First of all, the ISA100.11a-2009 supports only the frequency band at 2.4 GHz; the lower sub-bands are not supported. In addition to the IEEE 802.15.4 standard, the ISA100.11a standard supports frequency hopping and also blacklisting that eliminates faulty frequency bands in order to improve the robustness against interferers. Additionally, the carrier sensing scheme can be disabled to reduce possible delay transmission.

The ISA100.11a *data link layer* is responsible for the management of the employed TDMA schemes by configuring the timeslot durations and managing the superframes. The configuration of timeslots can be done according to two different patterns: slotted channel hopping and slow channel hopping. The former scheme optimizes the bandwidth utilization and is adapted to energy-constrained routers, while the latter smooths the time synchronization requirements between neighbors by powering their receivers continuously during well-defined periods. The last scheme is therefore only adapted to routers offering unlimited energy budget. Both patterns can however be combined in a hybrid fashion by mixing superframes of both types. In addition to manage TDMA, the network manager assigns paths and links between the devices composing the WSNs. Each link is associated to one or multiple timeslots of a superframe and its type can be *transmit* and/or *receive* (Fig. 7). Information about the neighbors, the channel offset from the superframe hopping scheme as well as possible alternatives for the transmission and reception are also included. The ISA100.11a data link layer supports the previously described graph routing as well as source routing.

The *network layer* provides schemes for routing and QoS. It allows energy and bandwidth savings by mapping and translating the 128-bit addresses of the application endpoints to 16-bit short addresses used within subnets and vice versa. These savings can be increased by adapting the packet formats in function of the desired addressing, routing or QoS. Moreover, the network layer headers are compatible with the headers specifications conceived by the IETF 6LoWPAN working group and described in [26] in order to support future compatibility. Packet fragmentation and reassembly are also ensured at this layer. The packets can be routed at the backbone and the mesh levels, as defined in the standard. The first routing level is ensured by the data link layer, while the second is performed at the network layer by the end devices with routing capabilities. QoS is addressed in detail in the next section.

Figure 7. ISA100.11a superframes [24].



Depending on the level of reliability required by the application, the ISA100.11a *transport layer* can support end-to-end acknowledgements as well as unacknowledged communication. Additionally, flow control, segmentation and reassembly as well as security (see Section 4) are supported at transport layer, whereas the application layer ensures standard interoperability by using tunneling and native protocols at the gateways. The former carry protocols used in existing standards such as HART or FOUNDATION Fieldbus, while the latter provide efficient bandwidth utilization and therefore increase the battery lifetime.

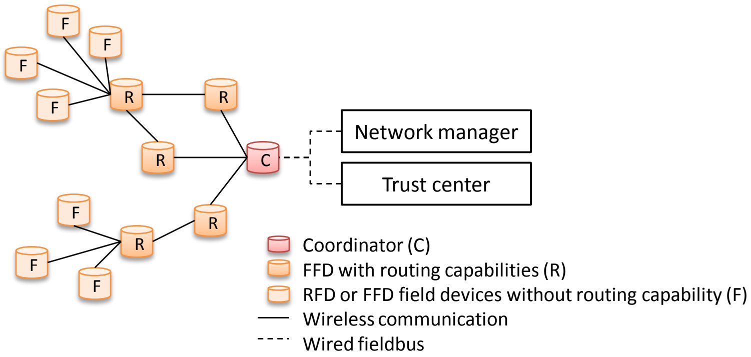
ZigBee and ZigBee PRO

The ZigBee®standard, described in [27], was developed by the ZigBee Alliance and was originally designed for home automation. A new ZigBee PRO variant was released in 2007 to fulfill the industrial requirements. The ZigBee PRO standard is still based on the IEEE 802.15.4 physical and MAC layers and provides network and application layers with enhanced security features. However, the ZigBee PRO standard supports only frequency agility that consists of scanning available channels to determine the channel with the least interference, which is then selected and used by all ZigBee devices. Within the scope of this survey, we refer to both ZigBee and ZigBee PRO variants as ZigBee, except for the explicitly mentioned specificities.

Network Elements

ZigBee networks support hundreds of devices and should thus be suitable even for large deployments. They can be organized into star, tree or mesh topologies. The ZigBee standard is based on the two defined IEEE 802.15.4 device classes including *Full-Function Device* (FFD) and *Reduced-Function Device* (RFD) and proposes three different types of devices: ZigBee coordinator, ZigBee router and ZigBee end devices (Fig. 8). A unique FFD *ZigBee coordinator* manages the network by supervising the network formation as well as information storage, and bridges it with others ZigBee networks. The *ZigBee routers* are complementary to the network manager and also FFD devices with additional routing capabilities, responsible for linking group of devices and supporting multi-hop communications. *ZigBee end devices* are either RFD or FFD. They transmit the collected sensor or actuator data to a unique FFD including router or coordinator functionality. Consequently, a FFD becomes the master of RFDs organized according to a star topology. Furthermore, the ZigBee specifications introduce a *trust center* to manage the keys and the end-to-end configuration. Only one center trusted by all devices should be active and be associated with all network devices.

Figure 8. ZigBee network elements [28].

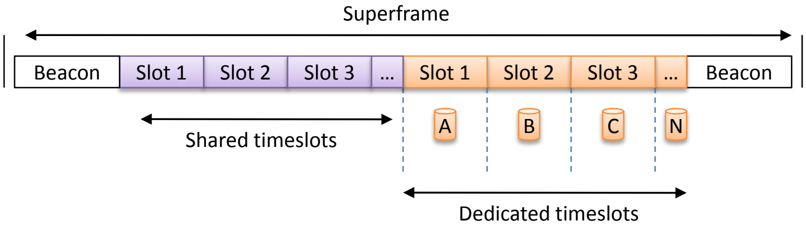


Architecture

The ZigBee stack is composed of the IEEE 802.15.4 physical and MAC layers as lower layers, and of the network and application layers specified by the ZigBee standard. After having set the selected common frequency for all devices, data transfers between ZigBee devices are possible. Two data transmission mechanisms are possible in ZigBee networks: with or without beacon. In the mode *with beacon*, the FFD sends a first beacon to synchronize all RFD sleeping phases and announces the superframe structure to manage the communication from end devices to the FFD. The first part of the superframe is slotted and CSMA/CA is used as channel access mechanism, while the second is composed of slots reserved for particular nodes by the network coordinator (Fig. 9). The FFD announces first the data transfer in the beacon to transfer data from the FFD to the RFD. Then, the concerned RFD must send a data request to the FFD to begin the data transmission. In case of FFD to FFD communication, the mechanism is similar, as one FFD acts as end device and is synchronized by the beacon originating from the second FFD. In the mode *without beacon*, no beacon and superframe are transmitted . The channel access is based on unslotted CSMA/CA. Each FFD coordinator remains continuously active to receive data coming from end devices during their limited active phase. RFDs send data requests to the FFD to receive data from the FFD. FFDs are permanently active and can thus communicate easily. In addition to transmission management, the MAC layer partially supports the admission of new devices in the network. The admission process starts by the scan procedure, during which the RFDs listen for beacon requests sent by a FFD. Request and acceptance notification are then exchanged at the MAC layer to complete the admission process. However, the decision to accept or reject a device is left to the security mechanisms supported by the upper layers and in case of acceptance, a 16-bit short address is assigned to the new device.

The *network layer* is specified by the ZigBee standard and is responsible for network formation, address assignment as well as routing over the ZigBee network. The network layer is complementary to the MAC layer and takes part in the join procedure by initiating a network discovery mechanism to detect surrounding ZigBee networks. After the selection of the network by the application layer, the network layer chooses a parent to attach the joining device and requests the MAC layer to begin an association procedure, where the network layer assigns the 16-bit address to the joining device. The ZigBee network layer employs the *Ad hoc On Demand Distance Vector* routing algorithm (AODV) as route discovery mechanism to manage routing in mesh networks.

Figure 9. ZigBee superframe.



The ZigBee *application layer* proposes a framework for distributed application development and communication [27]. This application framework is composed of up to 240 *Application Objects* (APO). They consist of software units controlling dedicated device hardware and are disseminated over network devices. Each APO manages a set of variables and offers the possibility to set and read its values as well as report value changes. These functions are accessible by using the APO local number, which extends the device address. Additionally, the *Application Sub Layer* (APS) provides an interface to ensure security and data services between APO and *ZigBee Device Objects* (ZDO), which manage APO discovery services. Finally, application profiles described in the ZigBee specifications define formats and protocols for intra APO communication allowing the interoperability of ZigBee devices with the same application profile.

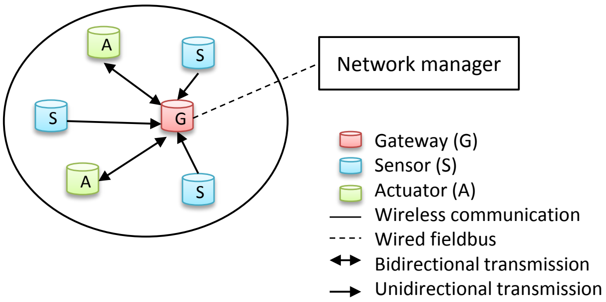
802.15.4e Factory Automation MAC Layer

The IEEE 802.15 Task Group 4e is currently developing a MAC layer [29] dedicated to factory automation and based on the IEEE 802.15.4 standard. The 802.15.4e Factory Automation MAC layer defines a deterministic TDMA communication scheme to fulfill the real-time requirement.

Network Elements

The network is composed of *sensors* and *actuators* organized in star topology around a *gateway* (Fig. 10). The *network manager* configures each end device via the gateway and allocates the dedicated time slots. After the configuration phase, sensor to gateway communication is unidirectional, whereas actuator/gateway communication is bidirectional.

Figure 10. 802.15.4e Factory Automation MAC Layer network elements.



Architecture

The 802.15.4e Factory Automation MAC layer is based on the IEEE 802.15.4 physical layer and develops particular superframe formats as well as transmission modes to support deterministic TDMA [29]. The gateway supports three main transmission modes: discovery mode, configuration mode and online mode.

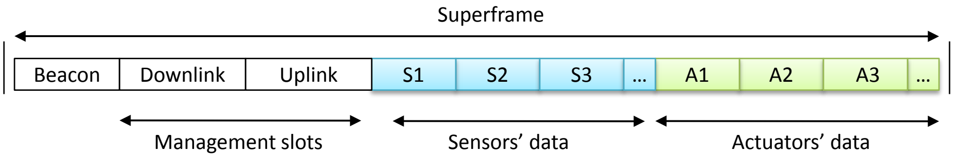
The *discovery mode* takes place during either network setup or joining procedure. The gateway sends superframes with beacons to indicate the discovery mode. When a device wanting to join the network receives such a beacon, it tries to access the transmission medium to send a *Discover Response* frame to the gateway with its current configuration parameters. The frame will be retransmitted by the device until the gateway receives it or changes its transmission mode.

During network setup or reconfiguration, the gateway is in a *configuration mode* and indicates this status in the superframe beacon. When the device receives the beacon and gets access to the transmission medium, it sends a *Configuration Response* frame to the gateway with its current configuration until the gateway receives it or changes its mode. As soon as the gateway receives the *Configuration Response* frame, it sends a *Configuration Request* frame with the new device configuration parameters and the device sends an acknowledgement in the next superframe.

In the *online mode*, devices can send data to the gateway in the timeslots allocated during the configuration mode and the gateway acknowledges the received data in the following superframe.

The superframes are sent to the end devices by the gateway and their structures depend on the current gateway transmission mode. The first slot is designed as the beacon slot (Fig. 11) and is common to all superframe structures. The end devices can detect the start of a new superframe at the reception of this first slot and synchronize themselves with it. Additionally, the beacon specifies the current trans-

Figure 11. 802.15.4e FA MAC superframe structure [29].



mission mode and also acknowledgements for data transmitted in the previous superframe. In discovery, configuration and optionally online modes, the beacon is followed by up to two management time slots, which manage the bidirectional transmission between gateway and actuators. During online transmission mode, the next time slots are allocated to sensors. These timeslots can be either dedicated to a particular device or shared by a group of devices using CSMA/CA. In the first case, no addressing information is necessary, whereas the second case requires a simple addressing scheme. Then, actuator time slots are reserved in the superframe. The direction of the communication between actuators and gateway is indicated in the beacon, and each time slot can be either dedicated or shared.

3. Quality of Service

Quality of Service (QoS) refers to "*the collective effect of service performance which determine the degree of satisfaction of a user of the service*" [30]. More technically, QoS can be defined as the "*well-defined and controllable behavior of a system with respect to quantitative parameters*" [31]. Interesting parameters to monitor for computer networks can be delay, jitter, throughput, fairness, and packet losses for example. However, the requirements of industrial automation networks are different from usual computer networks. The harsh industrial operation environment may degrade the wireless communication performance due to path loss and shadowing, multi-path propagation, and interference [12]. Moreover, the traffic is mainly composed of short packets containing sensor measurements or actuator commands that need to be delivered timely, instead of large multimedia streams or interactive traffic that prevails in computer networks. We next identify the specific QoS requirements and evaluate the aforementioned selected specifications with respect to their compliance to these requirements. Open issues are identified and discussed based on the results of this evaluation.

3.1. Requirements

Industrial automation applications can be divided into two main categories of systems [32]: close-loop[1] and open-loop systems[2] as defined in [33]. The applications based on either close or open-loop systems have different QoS requirements, as close-loop systems monitor discrete operations, such as actuator control, and open-loop systems monitor continuous processes, such as cooking raw material.

[1] In closed-loop systems, "*the control action is somehow dependent of the input*". The input is"*the stimulus, excitation or command applied to a control system*" and the output is "*the actual response obtained from a control system*". The control action refers to the "*quantity responsible for activating the system to produce the output*". More precisely, in closed-loop systems, also designated as feedback control systems, "*the output [. . .] is compared with the input to the system [. . .] so that the appropriate control action may be performed at some function of the output and input*" [33].

[2] In an open-loop system, "*the control action is independent of the input*" [33].

Table 2. Industrial automation applications classified according to their real-time requirements [35].

	Real-time requirements			
	None	Soft	Hard	Isochronous
Cycle duration		greater than 10 ms	1 ms to 10 ms	250 μs to 1 ms
Jitter				less than 1ms
Application examples	Maintenance Diagnosis	Process automation Data acquisition	Control Machine tools	Motion control

In close-loop applications, the sensors generate traffic that needs to be transmitted timely, reliably and accurately [33] to the control system, whereas in open-loop applications, real-time processing is typically not required, but the energy consumption is a crucial point. An additional classification [35] of the industrial applications refines these categories and is based on the degree of the required real-time guarantees. The classification is composed of four classes presenting increasing real-time requirements that are summarized in Table 2. We next focus on the support of real-time traffic and the reliability offered by the selected specifications.

3.2. Evaluation of the Selected Specifications

To evaluate the support of real-time transmission, the medium access control mechanisms including priority management schemes of the selected specifications are compared. Different diversity parameters including frequency and space diversity as well as protocol features such as acknowledgements are additionally considered in order to estimate the reliability provided by the different specifications.

Real-time Support

The selected specifications are mainly based on the IEEE 802.15.4 data link layer, except for the WISA specification relying on the IEEE 802.15.1 standard. As 802.15.4e FA MAC Layer and WISA only address the specifications of the physical and data link layers, the comparisons of the selected technologies are mainly based on the features of their two first layers. To complete this comparison, the 802.15.4 FA MAC needs to be evaluated in the context of a whole system. However, this aspect is outside the scope of this survey.

Medium Access Control Mechanisms

Each standard uses TDMA as medium access control mechanism (Table 3). However, TDMA is not the main medium access scheme in the ZigBee standard, which uses primarily CSMA/CA, but can also provide guaranteed timeslots in its beacon mode. Even if all specifications make use of TDMA access mechanisms, some differences between them can be observed. First of all, the timeslot length can be configured in the ISA100.11a, ZigBee and 802.15.4e FA MAC standards, while it is fixed in the others standards. Adapting the timeslot length to the needs of the applications allows taking into account the specific characteristics and optimizes the timeslot duration. Without such optimization, time can be lost between two successive slots if the slot is longer than the data to send. Configuring the length of the timeslots is thus an important feature to allow for optimizing the real-time support. However, all timeslots inside each superframe have the same length that limits a real adaptation to the requirements of individual applications, as only the overall traffic mix can be optimized. Another feature is the selection of the type of the timeslots, which can be either shared or dedicated. Most of the selected specifications offer both kinds of timeslots. Only the WISA specification uses exclusively dedicated timeslots. The choice between dedicated and shared timeslots is made difficult by the trade-off between real-time support and optimized utilization of the medium. Indeed, the dedicated timeslots are assigned to one particular device only. If this device wants to send commands or measurements, the data are transmitted immediately within the reserved timeslots. Otherwise the timeslot is lost and other devices wanting to transmit information may be constrained to wait longer. In case of shared slots, the devices have to compete to access the medium. The medium utilization is thus optimized because slots can be utilized by the stations in need of bandwidth, but the data transmission cannot always be immediate due to random back-off mechanisms for example.

Superframe Management

Furthermore, the WirelessHART, ISA100.11a and the ZigBee standards allows optimizing the transmission of superframes to fit the real-time communication constraints. The ISA100.11a standard supports insertion, removal and activation of superframes during the operating process, whereas additional superframes can be transmitted in parallel to the mandatory superframe in the WirelessHART standard. In the *without beacon* mode of the ZigBee standard, no superframe is transmitted and the devices do not have to wait for the next timeslot to transmit their data. However, this solution has also drawbacks. If one device has a great amount of data to send, the channel would be occupied for a long period of time and data requiring real-time transmission could not be send during this period. Moreover, the time to get access to the channel may be longer than in case of dedicated slots, if all the devices have data to be sent. The management of dedicated and shared timeslots has therefore to be tailored to application characteristics and the traffic patterns.

Priority Management

In addition to medium access control, flow control with assignment of priority to the packets can be introduced to support real-time at higher level. A priority flag indicates to each device on the path if the arriving packet has to be transmitted without delay or can be buffered. The WirelessHART standard defines four main priority levels according to classes of data [36]. Control and configuration information as well as network diagnostic messages have the highest priority, followed by a second category composed of process data measurements and network statistic messages. The lowest priority is assigned to the fourth category, which includes packets reporting information about events and alarms. Additional classes of data are classified into the third category. In comparison, the ISA100.11a standard allows to prioritize the QoS contracts established between the devices and the system manager in addition to

Table 3. Features relevant for real-time operation.

	WISA	WirelessHART	ISA100.11a	ZigBee	802.15.4e MAC
TDMA	x	x	x	x[3]	x
CSMA/CA				x	
FDD	x				
Superframe	x	x	x	x[4]	x
Fixed timeslot duration	x	x			
Duration	64 and 128 μs	10 ms			
Shared timeslots		x	x	x[4]	x
Dedicated timeslots	x	x	x	x[4]	x
Superframe optimization		x	x		
Message-based priority		x	x		
Priority levels		4	2		
Contract-based priority			x		
Priority levels			4		

message priorities. The device wanting to transmit data first sends the required priorities in a contract proposal, as well as other additional parameters including reliability, periodicity and negotiability. The system manager replies to this request in a contract response and indicates the provided QoS for the requested communication. Depending on the traffic conditions, the system manager might not be able to provide the requested QoS. If the device indicates that the contract is negotiable, the system manager can propose another QoS level or postpone the contract to provide the requested QoS level. The contract priority is set during the contract establishment and concerns all messages exchanged during the contract duration. Depending on these priorities, the system manager manages the routing and the load balancing to provide the guarantees defined in the contract. Four levels of contract priority are available at network layer: network control, real time buffer, real time sequential and best effort queued. The first priority level can be used by the system manager to communicate critical information about the network management; whereas the second category is used for periodic data exchanges with buffer overwrite operations in case of fresher messages. The third class, real time sequential, is appropriate for applications requiring sequential and real-time data delivery like video or voice-based applications. The last level is adapted for client-server communications. Within the contract, message priority can also be assigned by setting one bit to either low or high. However, the contract priority takes precedence over the message priority.

Each standard supports real-time communication in a different way. While the WISA specification and the 802.15.4e FA MAC layer target applications with strong real-time requirements, the ZigBee

[3] In the beacon mode, the second part of the superframe is composed of timeslots assigned and reserved by the network manager in a similar manner as TDMA.

[4] Only in the beacon mode.

and the WirelessHART standard are more adapted to applications with softer requirements. The recent ISA100.11a standard supports currently soft real-time requirements. More precisely, the evaluation of the selected technologies has shown that:

- Dedicated timeslots are supported by all standards. Their utilization is a key feature to fulfill strong real-time requirements and is particularly appropriate, if the complete set of the sensors have a continuous stream of information send. To optimize the transmission, dedicated as well as shared timeslots can be combined to support fluctuations of the traffic load. Such hybrid modes can be envisaged in most of the considered technologies except for the WISA standard, which only support dedicated timeslots.

- Tuning the timeslot length is a second key feature that allows to support application-specific traffic as well as optimize the real-time support. Except for the WISA and the WirelessHART standards, all standards offer this option. However, the timeslot length is common to all timeslots within a superframe, which limits the adaptation to variations of traffic as well as real-time requirements. Although this property may be useful for applications with various length of data to send, it would introduce additional overhead and complexity and may therefore unnecessary.

- Superframe management is an additional means to maintain real-time communication in case of very high traffic load. However, the superframe optimization proposed by WirelessHART and ISA100.11a remains a minor contribution to the real-time support in comparison to the aforementioned dedicated timeslots and adaptable timeslot lengths.

- Priority mechanisms are provided by the WirelessHART and the ISA100.11a standards. Both standards support message-based priority, while the ISA100.11a standard offers contract-based priority additionally. Although the proposed contracts are promising in terms of QoS guarantees, the overhead and the complexity introduced by their management as well as the additional resulting traffic may limit their practical feasibility. Even if message-based priorities may be less efficient than contracts, their utilization allows to reach a balance between overhead and efficiency and provides a complementary method to support real-time traffic.

Reliability Support

Industrial WSNs are located in spaces, where equipment moves, conditions change and interference perturbs the communication. Mechanisms, such as space and frequency diversity as well as acknowledgements (Table 4), are thus required to protect the wireless networks from these disturbances [37].

Space Diversity

Space diversity allows bypassing obstacles and interference by modifying the routing within networks organized in mesh topology. Such ability is however impossible with star topologies, as each device communicates exclusively and directly with a central coordinator. In case of obstacles that block the wireless communication, no alternative path is available and the communication cannot be established. Within the selected standards, the WISA specification and the 802.15.4e FA MAC standard are foreseen to be

Table 4. Features relevant for robust/reliable features.

	WISA	WirelessHART	ISA100.11a	ZigBee	802.15.4e MAC
Mesh topology		x	x	x	
Channel agility				x[5]	?[6]
Channel hopping	x	x	x		?[6]
Channel blacklisting		x	x		?[6]
DDL acknowledgements	x	x	x	x	x
TL acknowledgements		x	x		
Automatic repeat request	x	x	x	x	?[6]

deployed in star topology only. Their protection against wireless channel obstructions and fluctuations is therefore reduced in comparison with the other standards. However, the maximal distance between the central coordinator and the sensors is shorter than between devices deployed in mesh topology. The probability of an obstacle breaking the communication is therefore low, if careful network planning is performed.

Frequency Diversity

In addition to space diversity, frequency diversity reduces the effects of the environment on the wireless communication by limiting the interference. Two frequency diversity schemes are possible: channel hopping and channel blacklisting. The channel hopping allows avoiding interference by changing the transmission frequency, while the devices maintain lists of frequencies to avoid due to their significant interference with the channel blacklisting scheme. The WirelessHART and the ISA100.11a standards use both of them and possess therefore an efficient response against interference. The WISA specification uses channel hopping, but does not blacklist faulty channels. In comparison, the ZigBee and 802.15.4e FA MAC standards do not provide any mechanism to avoid potential interference, which may lead to erroneous transmissions or even worse to a total transmission break down. However, the ZigBee PRO standard proposes an enhancement of the ZigBee standard by offering frequency agility. The available channels are scanned during the network setup phase to select a frequency without interference. Then, the frequency is shared by all ZigBee compliant devices and remains unchanged until the next network setup period. Even if the frequency agility may limit the effects of potential interference during the network formation, it can rapidly become inefficient in case of additional sources of interference.

Acknowledgement Management

Interferences or obstacles can also lead to packet loss. To ensure transmission reliability, *acknowledgements* (ACK) at *Data Link Layer* (DLL) are supported by all the selected standards, as well as end-to-end acknowledgements at *Transport Layer* (TL) for the WirelessHART and ISA100.11a stan-

[5] Frequency agility is only supported by the ZigBee PRO version.

[6] Not addressed by the currently available documentation.

dards. Each standard however manages its ACK mechanisms according to its transmission scheme. For example, the WISA specification transmits each ACK in the downlink channel, whereas each ACK is transmitted during the same timeslot as the received data in the WirelessHART standard. Once an ACK is missing, all standards[7] support the automatic retransmission of the data.

The comparison of the aforementioned mechanisms summarized in Table 4 shows that:

- The technologies targeting *process automation* applications provide a good protection against potential obstacles and node failures, as mesh topology is supported.
- The WirelessHART and ISA100.11a standards offer the most complete set of mechanisms with channel blacklisting and frequency hopping to avoid perturbations caused by interference. While channel blacklisting allows saving time and energy by avoiding scanning channels previously identified as faulty, the obtained benefits are minor in comparison with the frequency hopping capability that is fundamental. Even if the ZigBee PRO version shows some improvements, the frequency diversity proposed by the ZigBee standards is insufficient to fulfill the strong reliability requirements of industrial applications.
- All selected technologies use acknowledgements at data link layer and automatic repeat request to ensure reliable transmissions and identify packet losses. At transport layer level, only the WirelessHART and ISA100.11a standards support acknowledgements.

3.3. Open Issues

The previous evaluation has highlighted that the selected specifications differ with respect to the supported QoS requirements for industrial applications, particularly concerning real-time support and reliability.

Open Standard for Factory Automation

The first conclusion that can be drawn is that no standard provides currently an open solution to *factory automation* with strict real-time requirements. The WISA specification is dedicated to this kind of deployments, but it is based on the IEEE 802.15.1 standard that consumes more energy than the IEEE 802.15.4-based standards. Moreover, the WISA specification is proprietary, thus locking the user into a single vendor as well as the design and maintenance of a proprietary set of interfaces. Even if WISA successfully fulfills the requirements of factory automation, it does not support openness and interoperability. The 802.15.4 Factory Automation MAC provides a promising perspective, but is still under development. Furthermore, the recently released ISA100.11a standard is expected to be enhanced by future addenda to make it fit to applications with stronger real-time requirements. As a consequence, additional research and development is necessary in order to obtain open and IEEE 802.15.4-based standards, which suit the needs of factory automation.

[7] Except for the 802.15.4e FA MAC standard that does not address this issue in the current proposal.

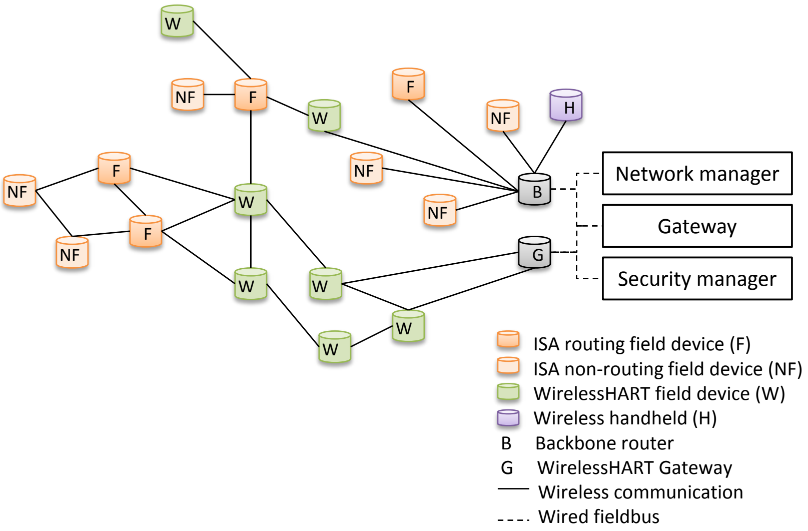
QoS Support in Heterogeneous Networks

In the *process automation* domain, the standards WirelessHART and ISA100.11a occupy the first positions and a potential convergence is analyzed by the ISA100.12 Working Group. WirelessHART devices are foreseen to be deployed within ISA100.11a-based WSNs, as illustrated in Fig. 12. In parallel to the ISA100.12 Working Group, the ISA100 Wireless Backhaul Backbone Network Working Group addresses potential interoperability between the ISA100.11a and the ZigBee-based standards. Additionally, the ISA100.11a standard is compatible with existing wired standards including HART, FOUNDATION Fieldbus, Modbus, and Profi bus. The ISA100.11a standard offers therefore a wide panel of compatible standards, which allows manufacturers to reuse existing devices. However, questions regarding the provided QoS capabilities among heterogeneous WSNs have to be raised. Indeed, such compatibility requires translation between the standards at the gateways, which may increase the end-to-end transmission delay of end systems belonging to different kinds of networks. Moreover, options implemented in one standard may not be supported or may have to be disabled to support interoperability. In such case, segments of the network that do not support the same priority scheme or the QoS contracts established in the ISA100.11a standard may ignore the indicated priority leading to a best-effort QoS. Thus, the efforts to support the QoS requirements would be wasted. A central network manager for both or more network segments based on different standards would be a possible solution because options, configuration settings and capabilities could be centrally managed. The network manager would be able to obtain a global view of the network and thus is able to take the appropriate decisions. However, a single central network manager remains a single point of failure that threatens the resilience of the network, if it is not deployed redundantly. In case of malfunctions, the whole network would be affected and could catastrophically fail. Therefore, the support of interoperability between the investigated standards remains an open issue. Although addressing the heterogeneity has a number of interesting research challenges, its practical feasibility may be limited by the technical complexity and financial costs incurred to adapt different technologies.

QoS Support in Multi-hop Networks

The surveyed standards dedicated to *process automation* can also be deployed in mesh topology, thus raising the question of QoS support over multi-hop routes. The WirelessHART and ISA100.11a standards propose solutions based on priority mechanisms, which are centrally managed by the network manager. While the standards provide the basic mechanisms to support differentiated QoS, the detailed specification to support operation in a multi-hop network is outside the scope of the standard. Although mechanisms that support QoS in multi-hop networks were developed for other applications, e.g. the Internet, their reuse is limited as they do not provide sufficiently strong real-time guarantees and are mainly adapted to multimedia streams, which differ from data streams in sensor networks. Further research is therefore mandatory to provide an exhaustive description of the required mechanisms to support QoS in multi-hop networks.

Figure 12. Interoperability of WirelessHART and ISA100.11.a networks [38].



4. Security

In addition to the previously considered quantitative QoS parameters, security guarantees play an important role within industrial WSNs. Indeed, without any protection mechanism, the network could suffer from attacks or malfunctions that degrade the desired QoS by introducing additional delays, or not delivering correctly and timely the needed information. For example, these malfunctions can perturb the production chain, as one of the machines would move at an unexpected time or in the wrong direction. Such perturbations can have important consequences going from delayed and damaged production to broken equipment. Additional costs are not the only consequence; employee's lives can be endangered in the worst case; for example in case of explosions due to false temperature measurements in chemical industries. A threat analysis is conducted in this section followed by an evaluation of the selected standards in order to determine whether the WSNs are protected against the identified threats. Within the scope of this survey, only attackers located within the range of the WSNs and taking advantage of the wireless characteristics of the industrial networks are considered, as many methods like firewalls [12] are efficient to protect the networks against attacks coming from the outside. Moreover, attacks requiring physical capture of sensor platforms are excluded from this analysis.

4.1. Threat Analysis

To protect industrial WSNs efficiently against potential attackers, the following main security criteria have to be considered: confidentiality of information, integrity of information, authentication of communication peers and availability of information [35]. The first criterion ensures that the data access is restricted to authorized parties only, while the second ensures their protection against alteration and modifications by either malicious parties or the harsh surrounding environment. The authentication of communication peers allows guaranteeing that the exchanged data are coming from trusted devices. At last, the information availability ensures that data and services are accessible even in case of attacks.

To perturb or even break down industrial WSNs, the attackers can therefore target one or several of the aforementioned criteria and conduct the appropriate attack(s).

Confidentiality of Information

The wireless nature of the communication between the sensors and devices eases these attacks, as there is no strict physical boundary of the transmission medium. An attacker located close to the network can thus easily eavesdrop the communication and threaten the confidentiality of the transmitted information. The content of the packets can be revealed to the attacker, who can benefit from stolen information like network configuration data to conduct further attacks. Eavesdropping can also be coupled with network monitoring to perform traffic analysis. The aim of this attack is to determine the responsibility of each sensor and identify the data sink for example. An analysis of the packet content is not mandatory to success; the amount of exchanged packets can be a sufficient clue [39]. However, an attack directed against the data sink can be very efficient, as the entire data set may be damaged or lost.

Integrity of Information

In addition to the confidentiality of the exchanged information, its integrity can be threatened by attackers adding additional fragments to the packets or manipulating the data. However, malicious behavior is not the only source of packet manipulations; errors due to the harsh industrial environment are also possible. The modifications of the packet content may cause misbehavior of the equipment and thus have inconvenient effects on the production, or even worse.

Authenticity of Communication Peers

Packet manipulation can be one sign that one or several malicious nodes have succeeded in integrating itself with the network. Such intrusions widely open the doors to further attacks like Sybil [40] and node replication [41] attacks. Both attacks profit from weaknesses of the authentication mechanisms to insert malicious nodes. In the former case, these nodes take illegitimately multiple identifiers; while in the latter, they capture and use existing device IDs. The identifier manipulation allows the attacker to modify the content of the traffic exchanged between the devices as well as control messages such as routing messages. These attacks can therefore be the basis of further routing attacks like wormhole [42] or black hole [43] attacks, where the attackers are able to disconnect part of the network or make it totally inoperable.

Availability of Information

Such routing attacks also threaten the last criterion, as the data may not be delivered timely or even at all and the information are therefore not available. Additional attacks can be conducted at different layers to disturb the availability of information. At the physical layer, jamming may cause interference at different frequencies in an intermittent or constant manner that make the communication impossible. Jamming may be caused by malicious attacks or unintentionally by surrounding equipment. To fight against malicious jamming, the physical protection of the industrial sites is one of the first measures to adopt. However, most of the industrial sites still accept external visitors. Even if their visits may be strictly controlled, attackers might benefit from security weaknesses to introduce jammers within the factory. Additionally, uninterrupted transmission of data by the attacker can generate collisions and force retransmissions at data link layer. The energy budget of the node decreases rapidly due to the retransmissions and the sensor is made inoperable. Additional energy consumption can also be caused by flooding the network with many connection requests at transport layer for example.

4.2. Evaluation of the Selected Standards

The selected standards are evaluated to determine how the current industrial WSNs are protected against the aforementioned threats. The set of considered standards is restricted to the WirelessHART, ISA100.11a and the ZigBee standards[8].

Confidentiality of Information

The evaluation begins with data confidentiality including protection against eavesdropping and traffic analysis. The most efficient way to protect the industrial WSNs against eavesdropping is to encrypt the exchanged data. The WirelessHART, the ISA100.11a as well as the ZigBee standards use the 128-bit AES encryption [44] coupled with different keys depending on the layer of encryption. For example, WirelessHART uses the session key to encrypt the message at transport layer, while link and network keys are used at data link layer and at network layer respectively in the ZigBee standard. As mentioned by [45], AES remains an efficient mechanism to keep the data secret. Moreover, its efficiency is increased by the utilization of keys with short lifetime and unique for each device such as the session key used in WirelessHART. Eavesdropping is consequently made difficult or even impossible in networks running the three considered standards. However, the confidentiality is not ensured at all layers. For example, even if the packets are encrypted at transport layer, header and payload of packets sent at network layer are transmitted unencrypted in the WirelessHART standard [45]. An eavesdropper can therefore discover the crucial information, such as source and destination addresses that are contained in the network header, and perform traffic analysis easily afterwards. Nonetheless, the traffic analysis attack can also be performed without any message decryption [39].

Integrity of Information

The selected industrial standards benefit from the security mechanisms included in the IEEE 802.15.4 standard that ensure data integrity at data link layer. An additional *Message Integrity Code* (MIC) is inserted at the queue of the data to protect. The data are signed and the receiver is able to determine whether the data have been tampered with or not. Data integrity protection can be provided in complement with encryption by using the *enhanced combined encryption and authentication block cipher mode* (CCM*). Depending on the desired security level, the length of the MIC can be set to 32, 64 or 128 bits. The longer the code is, the higher the integrity protection is, but also the greater the overhead is. The length should therefore be selected carefully.

[8] The security issues are not addressed in the current proposal of the 802.15.4e FA MAC standard as well as in the publicly available information about the WISA technology.

Message and Device Authenticity

In addition to provide hop-to-hop data integrity, the MIC allows to authenticate the packets by using secret symmetric keys known by both sender and receiver. For example, the shared network key and the unique session key are used in WirelessHART to authenticate the messages at data link and network layers respectively [45]. The authenticated packets are thus recognized as originated by authorized members of the network. However, before message authentication can be performed, each device must be first authenticated during the join procedure. Even if the name of the keys may vary between the standards, their functions are similar. Devices willing to participate to the network exchange *join requests* and *join responses* with the network manager and use public key and asymmetric private key kept inside the joining devices. These keys are used for computing the data link and network MICs respectively and may be either preloaded in the devices at the factory or distributed by a unique trusted center, which maintains and updates the security keys. In WirelessHART, an additional join key is used to encrypt the *join request*. Once the device is recognized as authorized member, it can exchange authenticated data with the other members. As each standard is based on a central entity responsible for the network management and keeping tracks of the participating devices, the probability is very low that the attacks such as Sybil and node replication attacks may be performed successfully. For example, in WirelessHART, the network manager links each device with a unique identity [45]. The identification is completed by a list of unique IDs maintained at the gateways. The network manager identifier and the gateway ID are used conjointly with the session key to maintain sessions between the device and the network manager as well as the gateway respectively. Devices claiming the same identity as an existing one or sharing multiple identities would be immediately discovered, as these would already be listed.

Availability of Information

The last threat to be evaluated is the availability of information. First of all, the information availability can be threatened by jamming according to different patterns. In case of continuous jamming with one or several jammed frequencies, channel blacklisting provides an efficient solution, as the jammed channels are eliminated from the set of communication frequencies. In case of intermittent jamming, frequency hopping provides good results and allows keeping sufficient levels of information availability. With both frequency hopping and channel blacklisting features, the WirelessHART and ISA100.11a standards provide therefore a better protection against jamming than the ZigBee PRO standard that only offers frequency agility. At network layer, attacks modifying the routing scheme can be avoided by the authentication mechanisms, as devices would only be able to route packets, if they have been previously identified as reliable and authorized to take part to the WSN. Nonetheless, the selected standards do not provide dedicated mechanisms to avoid the generation of collisions by a malicious source transmitting continuously data, as well as solutions against flooding of connection requests at transport layer.

To summarize, we have shown that:

- Eavesdropping is made difficult or even impossible, but confidentiality is not addressed at all layers.

- Traffic analysis is still possible.
- The information integrity is sufficiently ensured.
- The probability of successful Sybil and node replication attacks are limited.
- The frequency diversity and agility is sufficient to protect the network against intermittent jamming.
- The current mechanisms do not provide protection means against malicious sources transmitting continuously or performing higher layer attacks such as flooding of connection requests at transport layer.

4.3. Open Issues

The selected standards are resistant against most of the considered attacks except for continuous jamming at all frequencies, collision and flooding attacks as well as traffic analysis. However, solutions against such particular kind of jamming and collision attacks are particularly difficult to find because the data transmission is made impossible in both cases. The only solution would necessitate human interventions to eliminate the interference source(s), as soon as a long-term communication breakdown is detected. Flooding of *connection request* is more delicate to solve, as regular nodes must still be able to send such request in order to join the network and authenticate themselves. Filtering the connection requests by a list of devices susceptible to join the network would not solve the problem, as the network manager would have to receive the requests in order to determine the sender identity. A solution remains therefore to be found. Even if payload encryption provides a partial solution to traffic analysis, it is not sufficient. Indeed, an analysis of the routing paths can be sufficient to determine the traffic scheme. Countermeasures to this analysis could be to insert fake packets and/or randomly distribute the traffic. However, the routing would not be optimized and the network performances including end-to-end delay would be degraded. Moreover, insertion of additional packets would drag the energy budget of the nodes down.

The existing security mechanisms are theoretically sufficient to cover the main attacks. However, the standards only provide specifications and leave design and implementation to the users. For example, the roles of each security key are described, but their management scheme has to be developed by the users, according to their requirements and respecting the standard specifications. To the best of our knowledge, Raza *et al.* are the first to have proposed a design and an implementation of a security manager adapted to the WirelessHART standard in [47]. The investigation of similar proof of concept for additional standards e.g. the promising ISA100.11a may be an interesting track to follow in order to provide already evaluated implementations that the users can tune to meet their requirements.

5. Conclusions

Within the scope of this article, we have provided a detailed survey on WSN standards dedicated to industrial automation networks. The standardization efforts are ongoing and targeting different application areas such as factory automation or process automation. We have focused on the IEEE 802.15.1

and IEEE 802.15.4 standard families, which have been adapted to industrial applications in need of short-range communication with high data rate, and energy-aware applications requiring larger coverage, respectively. We have selected the WirelessHART, ISA100.11a, ZigBee and 802.15.4e Factory Automation MAC standards among the IEEE 802.15.4 standard families and the WISA specification among the IEEE 802.15.1-based standards. Except for the WISA and 802.15.4e Factory Automation MAC, all the selected standards target mainly process automation applications. An overview of each standard has been provided with particular focus on the network elements and the features of the protocol stack.

In the next step, we have identified several QoS requirements posed by industrial applications, such as support of real-time communications as well as highly reliable communications. The selected standards have been evaluated to determine how real-time and reliability requirements are supported. The results have revealed that no officially released and open standard is currently able to fulfill the strong real-time requirements of the factory automation domain. Moreover, the questions of QoS provisioning over heterogeneous networks as well as over multi-hop routes in homogeneous networks have been raised.

We have then focused on security issues of the surveyed standards by identifying potential attacks that could threaten the industrial WSNs and affect their operation. The standards have also been evaluated to determine if the proposed security mechanisms are sufficient to protect the WSNs against the derived threats. The evaluation has shown that the standards are resistant against most of the investigated threats, except for continuous jamming at all frequencies, collision attacks and flooding of connection requests. Moreover, we have pointed out that the design and the implementation of the security managers are left to the users or implementers of the standard. Here, the detailed operation of such security and network managers and the corresponding protocol mechanisms are an interesting area for further research.

We conclude that the selected standards fulfill almost completely the identified QoS and security requirements as long as they operate in single-hop mode. However, some aspects that are of high interest for the domain of industrial automation, including multi-hop operation and support of QoS and security over heterogeneous network segments, need further research.

Acknowledgements

This work was supported by CASED (www.cased.de) and Siemens AG Corporate Technology. The authors would like to thank the anonymous reviewers for their valuable comments.

References

1. Geng, H. *Manufacturing Engineering Handbook*; McGraw-Hill Professional: New York, NY, USA, 2004.
2. Shell, R.L.; Hall, E.L. *Handbook of Industrial Automation*; Marcel Dekker: New York, NY, USA, 2000.
3. Low, K.S.; Win, W.N.N.; Er, M.J. Wireless Sensor Networks for Industrial Environments. In Proceedings of the International Conference on Computational Intelligence for Modelling, Control and Automation and International Conference on Intelligent Agents, Web Technologies and Internet Commerce (CIMCA-IAWTIC), Vienna, Austria, November 2005.

4. Mukhopadhyay, S.C.; Huang, Y.M. *Sensors: Advancements in Modeling, Design Issues, Fabrication and Practical Applications*; Springer-Verlag: Heidelberg, Germany, 2008.
5. IEEE Computer Society. IEEE Standard for Information Technology, Telecommunications and Information Exchange between Systems, Local and Metropolitan Area Networks, Specific Requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2007.
6. Willig, A.; Matheus, K.; Wolisz, A. Wireless Technology in Industrial Networks. *Proceedings of the IEEE* **2005**, *93*, 1130–1151.
7. IEEE Computer Society. IEEE Standard for Information Technology, Telecommunications and Information Exchange between Systems, Local and Metropolitan Area Networks, Specific Requirements, Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANS), 2002.
8. IEEE Computer Society. IEEE Standard for Information Technology, Telecommunications and Information Exchange between Systems, Local and Metropolitan Area Networks, Specific Requirements, Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs), 2007.
9. Scheible, G.; Dzung, D.; Endresen, J.; Frey, J.E. Unplugged but Connected - Design and Implementation of a Truly Wireless Real-time Sensor/Actuator Interface. *IEEE Industrial Electronics Magazine* **2007**, *1*, 25–34.
10. ABB. Reliable Factory Automation: Wireless Automation with WISA. http://www.abb.com (accessed on November 2009).
11. Steigmann, R.; Endresen, J. Introduction to WISA and WPS. http://www.abb.com (accessed on November 2009).
12. Willig, A. Recent and Emerging Topics in Wireless Industrial Communications: A Selection. *IEEE Transactions on Industrial Informatics* **2008**, *4*, 102–124.
13. ODVA. The DeviceNet Specification, Common Industrial Protocol (CIP) Specification. http://www.odva.org (accessed on November 2009).
14. Modbus Organization. Modbus Application Protocol Specification. http://www.modbus.org (accessed on November 2009).
15. Dzung, D.; Apneseth, C.; Endresen, J.; Frey, J.E. Design and Implementation of a Real-time Wireless Sensor/Actuator Communication System. In Proceedings of the IEEE Conference on Emerging Technologies and Factory Automation (ETFA), Catania, Italy, September 2005.
16. IEEE 802.15.1 Standard. http://www.ieee802.org/15/pub/TG1.html (accessed on December 2009).
17. De Biasi, M.; Snickars, C.; Landerns, K.; Isaksson, A.J. Simulation of Process Control with WirelessHART Networks Subject to Packet Losses. In Proceedings of the Conference on Automation Science and Engineering (CASE), Washington, DC, USA, August 2008.
18. Lennvall, T.; Svensson, S.; Hekland, F. A Comparison of WirelessHART and ZigBee for Industrial Applications. In Proceedings of the IEEE International Workshop on Factory Communication Systems (WFCS), Dresden, Germany, May 2008.
19. Griessmann, J.L. WirelessHART, an Overview. http://www.hartcomm.org (accessed on December 2009).

20. HART Communication Foundation. WirelessHART Technical Data Sheet. http://www.hartcomm.org (accessed on December 2009).
21. HART Communication Foundation. TDMA Data Link Layer Specification. http://www.hartcomm.org (accessed on December 2009).
22. Song, J.; Han, S.; Mok, A.K.; Chen, D.; Lucas, M.; Nixon, M. WirelessHART: Applying Wireless Technology in Real-Time Industrial Process Control. In Proceedings of the IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS), St. Louis, MO, USA, April 2008.
23. Tanenbaum, A.S. *Computer Networks*; Prentice-Hall: Upper Saddle River, NJ, USA, 2002.
24. International Society of Automation. ISA-100.11a-2009, Wireless Systems for Industrial Automation: Process Control and Related Applications. http://www.isa.org (accessed on November 2009).
25. International Society of Automation. ISA100.11a Status. http://www.isa.org (accessed on December 2009).
26. Montenegro, G.; Kushalnagar, N.; Hui, J.; Culler, D. RFC 4944: Transmission of IPv6 Packets over IEEE 802.15.4 Networks. http://www.ietf.org/rfc/rfc4944.txt (accessed on November 2009).
27. Baronti, P.; Pillai, P.; Chook, V.W.; Chessa, S.; Gotta, A.; Hu, Y.F. Wireless Sensor Networks: A Survey on the State of the Art and the 802.15.4 and ZigBee Standards. *Computer Communications* **2007**, *30*, 1655–1695.
28. Galeev, M. Home Networking with ZigBee. http://www.media.mit.edu (accessed on December 2009).
29. Winkel, L.; Bahr, M.; Vicari, N. 15-08-0572-00-004e Proposal for Factory Automation. http://www.ieee802.org/15/pub/TG4e.html (accessed on December 2009).
30. International Telecommunication Union. E.800 - Terms and Definition Related to Quality of Service and Network Performance Including Dependability. http://www.itu.int (accessed on November 2009).
31. Schmitt, J. *Heterogeneous Network Quality of Service Systems*; Kluwer Academic Publishers: Norwell, MA, USA, 2001.
32. Mathiesen, M.; Thonet, G.; Aakwaag, N. Wireless Ad-hoc Networks for Industrial Automation: Current Trends and Future Prospects. In Proceedings of the IFAC World Congress, Prague, Czech Republic, July 2005.
33. DiStefano, J.J.; Stubberud, A.R.; Williams, I.J. *Schaum's Outline of Feedback and Control Systems*; McGraw-Hill Professional: New York, NY, USA, 1994.
34. Liu, X.; Goldsmith, A. Wireless Communication Tradeoffs in Distributed Control. In Proceedings of the IEEE Conference on Decision and Control (CDC), Maui, HI, USA, December 2003.
35. Neumann, P. Communication in Industrial Automation: What is going on?. *Control Engineering Practice* **2007**, *15*, 1332–1347.
36. Kim, A.N.; Hekland, F.; Petersen, S.; Doyle, P. When HART goes Wireless: Understanding and Implementing the WirelessHART Standard. In Proceedings of the IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Hamburg, Germany, September 2008.
37. HART Communication Foundation. Why WirelessHART? The Right Standard at the Right Time. http://www.hartcomm.org (accessed on December 2009).

38. Sereiko, P. The ISA100 Standard: Characteristics and Benefits of the Standard, Latest Developments and Progress. http://www.isa.org (accessed on December 2009).
39. Walters, J.; Liang, Z.; Shi, W.; Chaudhary, V. Wireless Sensor Network Security: A Survey. *Security in Distributed, Grid, Mobile, and Pervasive Computing* **2007**, 367–405.
40. Newsome, J.; Shi, E.; Song, D.; Perrig, A. The Sybil Attack in Sensor Networks: Analysis & Defenses. In Proceedings of the International Symposium on Information Processing in Sensor Networks (IPSN), Berkeley, CA, USA, April 2004.
41. Parno, B.; Perrig, A.; Gligor, V. Distributed Detection of Node Replication Attacks in Sensor Networks. In Proceedings of the IEEE Symposium on Security and Privacy (S&P), Oakland, CA, USA, May 2005.
42. Hu, Y.; Perrig, A.; Johnson, D. Packet Leashes: a Defense against Wormhole Attacks in Wireless Networks. In Proceedings of the IEEE Conference on Computer Communications (INFOCOM), San Francisco, CA, April 2003.
43. Karlof, C.; Wagner, D. Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. *Ad Hoc Networks* **2003**, *1*, 293–315.
44. Schneier, B. *Applied Cryptography*, 2nd ed.; John Wiley & Sons: Hoboken, NJ, USA, 1996.
45. Raza, S.; Slabbert, A.; Voigt, T.; Landerns, K. Security Considerations for the WirelessHART Protocol. In Proceedings of the IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Mallorca, Spain, September, 2009.
46. Phan, R. Impossible Differential Cryptanalysis of 7-round Advanced Encryption Standard (AES). *Information Processing Letters* **2004**, *91*, 33–38.
47. Raza, S.; Voigt, T.; Slabbert, A.; Landerns, K. Design and Implementation of a Security Manager for WirelessHART Networks. In Proceedings of the IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS), Macau, China, October 2009.