ISSN 2277-3061

Security service for Wireless Sensor Network

S. Vivek Saravanan[1] and A. Solairaju[2]

[1] Final year B.E. Department of Electrical and Electronics Engineering, SRM Easwasri Engineering College, Ramapuram, Chennai, Tamilnadu, India, email: vivekcst2048@gmail.com

[2] Associate Professor of Mathematics, Jamal Mohamed College, Tiruchirappalli, Tamilnadu, India, email: solairama@yahoo.co.in

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. To examine both of these perspectives, we select and survey relevant WSN technologies dedicated to industrial automation. We determine to 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 some research issues.

Keywords: Wireless Sensor Networks; Industrial Automation; State-of-the-art; WirelessHART;Zeebeg PRO;

Council for Innovative Research

Peer Review Research Publishing System

Journal: INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY

Vol 11, No. 6

editor@cirworld.com

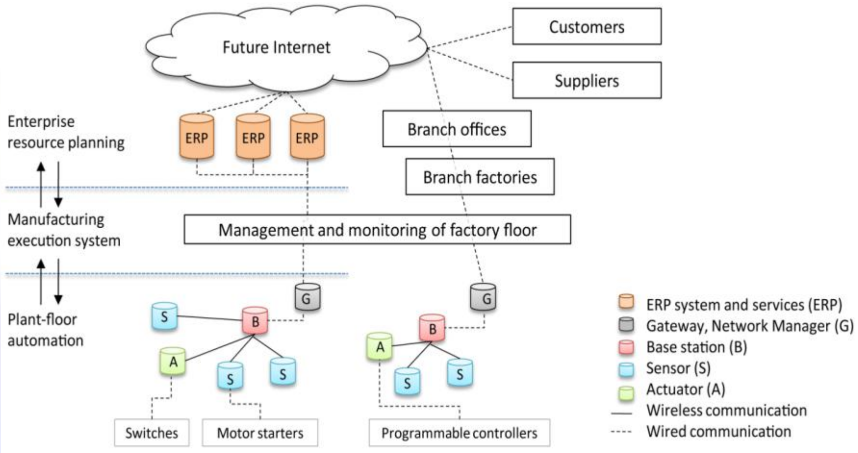
www.cirworld.com, member.cirworld.com

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: 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.

SECTION 1: PLANT - FLOOR AUTOMATION: 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.

Figure 1. From the sensors to the customers.



The WSNs are part of this layer and can be used for multiple purposes, such as monitoring synchronous or synchronous events that require periodic data collection or detecting exceptional events, respectively. 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.

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 issues.

SECTION 2: SELECTED WIRELESS SENSOR NETWORKS STANDARDS

2.1 Wireless communication in industrial automation: It is mostly based on standardized technologies, such as IEEE 802.15 standard families [2], 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 802.15.4 -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 802.15.4 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 and IEEE 802.15.4 standard.

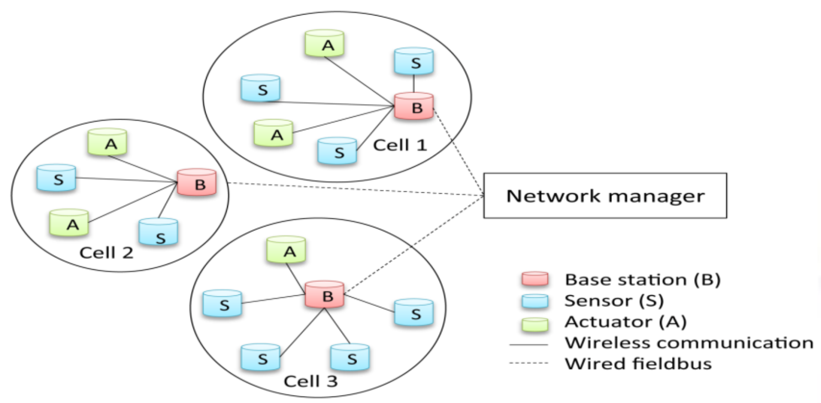
2.2 IEEE 802.15.1-based Standards: The IEEE 802.15.1 standardcan be classified to fall between the IEEE 802.11 and IEEE 802.15.4 standards in terms of energy consumption and data rates. With medium data rates and lower energy consumption than IEEE 802.15.1 offers an interesting compromise between energy 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.

2.3 Wireless Interface for Sensor and Actuators (WISA): Released by ABB and presented in [3], 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.

2.4Network Elements and Architecture

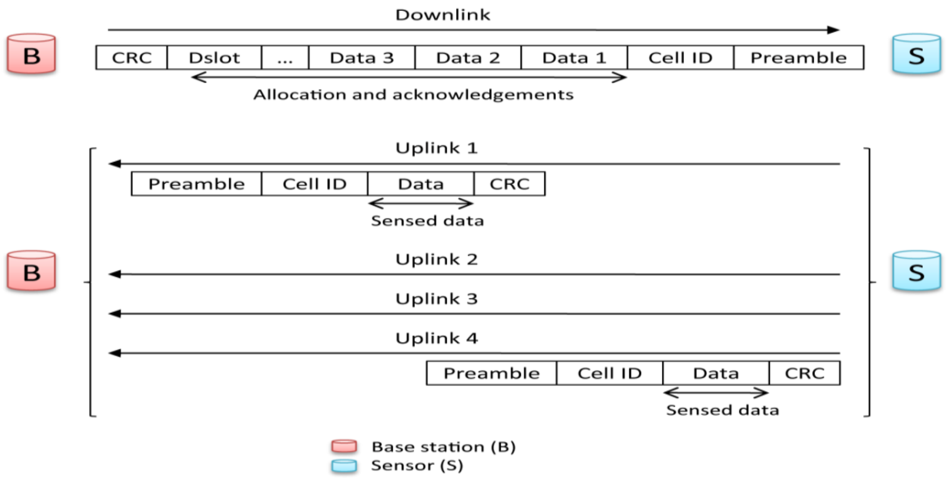
WISA networks can be deployed in cellular topology with up to three cells (Fig. 2).

Figure 2. WISA network elements.



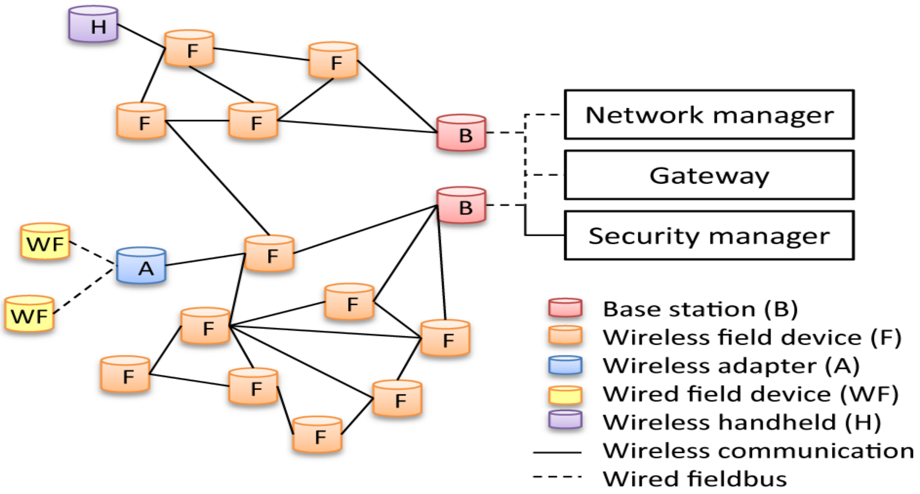
Each cell uses a different transmission frequency, and is composed of a base station and up to 120 end devices including sensors and/or actuators organized in a star topology. The WISA architecture is limited to the physical and MAC layers, as sensors and actuators communicate exclusively with a central base station in a star topology within each cell. 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).

Figure 3.WISA superframe structure



2.5 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^{TM} standard in 2007, considered as the only released open wireless standard suitable for process measurement and control applications. WirelessHART networks are composed of different devices as illustrated in (Fig. 4), including field devices, gateways, network and security managers.

Figure 4. WirelessHART network elements .

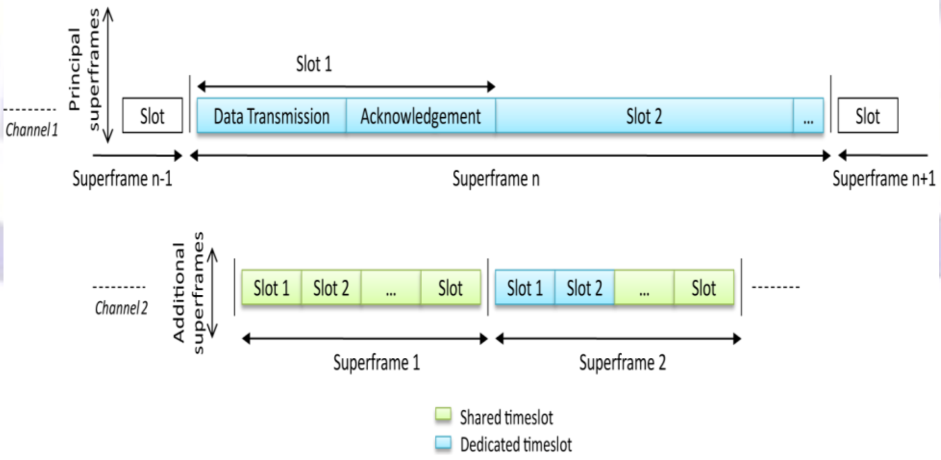


2.6 Network Elements and Architecture

The gateway is a bridge between the field device network and the host application. The gateway is configuredby 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.

At the data link layer, the WirelessHART standard coordinates and manages each device's transmission time by using TDMA with timeslots of 10ms. 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. 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.

Figure 5. WirelessHART superframes



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 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.

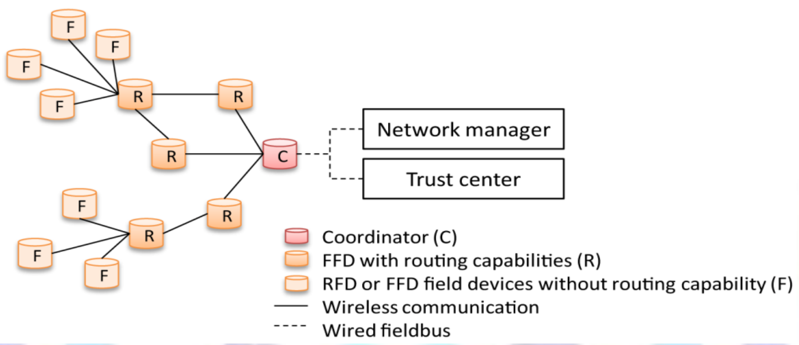
SECTION 3: ZIGBEE AND ZIGBEE PRO

The ZigBeestandard, described in [4], 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.

3.1Network 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.6).

Figure 6. ZigBee network elements

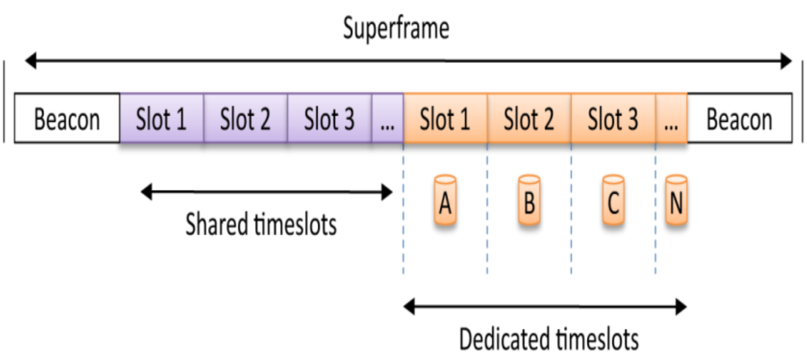


A unique FFD ZigBee coordinator manages the network by supervising the net-work formation as well as information storage, and bridges it with others ZigBee networks. The ZigBee routers are complementary to the network manager and also FFD devices with additional routing capa-bilities, responsible for 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. 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.

3.2 Zigbee superframe: 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 (Figure 7).

Figure 7. ZigBee superframe.



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 ofnew 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 tocomplete 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.

The ZigBee application layer proposes a framework for distributed application development and communication [4]. 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.

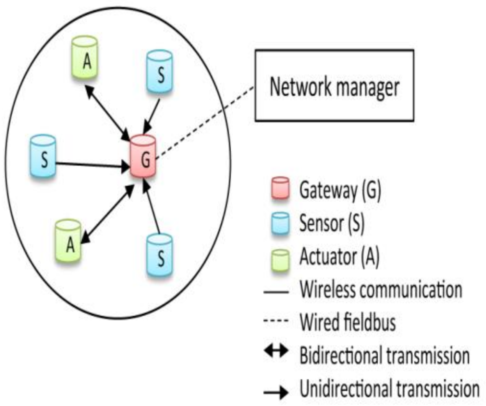
3.3: Network, Architecture and 802.15.4e Factory Automation MAC Layer

The IEEE 802.15 Task Group 4e is currently developing a MAC layer 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 [Figures 8, and 9].

The network is composed of sensors and actuators organized in star topology around a gateway (Figure 8). 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.

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. The gateway supports three main transmission modes: discovery mode, configuration mode and online mode

Figure 8. 802.15.4e Factory Automation MAC Layer network elements.



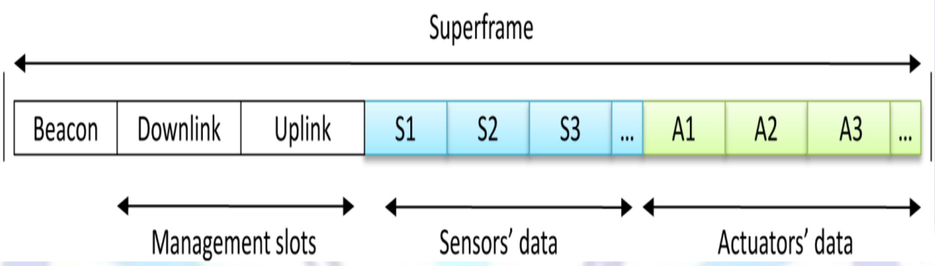
The discovery mode takes place during either network setup or joining procedure. The gateway sends superframes with beacons to indicate the discovery mode. When a device wanting to join the network receives such a beacon, it tries to access the transmission medium to send a Discover Response frame to 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 (Figure 9) 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 transmission 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.

Figure 9. 802.15.4e FA MAC superframe structure



SECTION 4: SECURITY OF SERVICE IN WSN

In addition to the quality of service (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 [1] 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.

4.1Threat 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. 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).

4.2 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 [5]. However, an attack directed against the data sink can be very efficient, as the entire data set may be damaged or lost.

4.3 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.

4.4Authenticity 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 and node replication 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 or black hole attacks, where the attackers are able to disconnect part of the network or make it totally inoperable.

4.5 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.

4.6Evaluation 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.

4.7 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 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 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 ex-ample, 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. An eavesdropper can therefore discover the crucial information, such as source and destination addresses that are contained in the net-work header, and perform traffic analysis easily afterwards. Nonetheless, the traffic analysis attack can also be performed without any message decryption [5].

4.8 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.

4.9 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. 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. 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.

4.10 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.

4.11 Summary:(1) Eavesdropping is made difficult or even impossible, but confidentiality is not addressed at all layers; (2) Traffic analysis is still possible; (3) The information integrity is sufficiently ensured; (4) the probability of successful Sybil and node replication attacks are limited; (5) The frequency diversity and agility is sufficient to protect the network against intermittent jamming; (6) 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.

4.12Conclusions:

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 IEEE 802.15.4e standard family, which has been adapted to industrial applications in need of short-range communication with high data rate, and energy-aware applications requiring larger cover-age, respectively. We have selected the WirelessHART, 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.

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 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 security over heterogeneous network segments, need further research.

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

References

1. Baronti, P., Pillai, P., Chook, V.W., Chessa, S., Gotta, A., and Hu, Y.F., 2007,Wireless Sensor Networks:A Survey on the State of the Art and the 802.15.4 and ZigBee Standards. Computer Communications 30, 1655-1695.

2. Scheible, G.; Dzung, D.; Endresen, J.; Frey, J.E., 2007Unplugged but Connected - Design and Implementation of a Truly Wireless Real-time Sensor/Actuator Interface.IEEE Industrial Electronics Magazine, 1, 25-34.

3. Walters, J.; Liang, Z.; Shi, W.; Chaudhary, V., 2007,Wireless Sensor Network Security: A Survey. Security in Distributed, Grid, Mobile, and Pervasive Computing, 367-405.

4. Willig, A., 2008, Recent and Emerging Topics in Wireless Industrial Communications: A Selection. IEEE Transactions on Industrial Informatics, 4, 102-124.

5. Willig, A.; Matheus, K.; Wolisz, A., 2005, Wireless Technology in Industrial Networks. Proceedings of the IEEE, 93, 1130-1151.

Authors:

1S. Vivek Saravanan is doing Final B.E. (Electrical and Electronics Emgineering), Eawasri Engineering College, Ramapuram, Chennai, Tamilnadu, India.

2A. Solairaju is working as an “Associate Professor of Mathematics”, Jamal Mohamed College, Tiruchirappalli-620020, Tamilnadu, India. He wrote five books on Engineering Mathematics. He has published 150 research papers in National and International Journals. 10 students in Mathematics one student in Computer Science are awarded Ph.D. degree under this guidance. He is an editor in some National and International Journals.