Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Environments

Draft

April 2007

Author

Ken Masica
Lawrence Livermore National Laboratory

Homeland Security

Control Systems Security Program

LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

Recommended Practices Guide

Securing ZigBee Wireless Networks in Process Control System Environments

(DRAFT)

Ken Masica

Vulnerability & Risk Assessment Program (VRAP)
Lawrence Livermore National Laboratory (LLNL)

for
DHS US CERT
Control Systems Security Program (CSSP)

April 2007

This work was performed under the auspices of the U.S. Department of Energy by University of California, Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

UCRL-TR-xxyyzz

Table of Contents

Section A: Introduction 1
Section B: Technology Overview 2
Section C: The IEEE 802.15.4 Standard 3
Section D: The ZigBee Standard 6
Section E: ZigBee Security Features.. 9
Section F: Security Design Principles 10
Section G: Security Best Practice Recommendations 13
Section H: Considerations for Industrial Environments 16
Section I: Conclusion 19
Section J: Technical References 20

Table-1: LR-WPAN Frequencies, Data Rates, and Modulation 4
Table-2: IEEE 802.15.4 Security Suites 5

Figure-1: The ZigBee Layered Model 3
Figure-2: The Star Network Topology 7
Figure-3: The Mesh Network Topology.. 8
Figure-4: The Cluster-Tree Network Topology.. 8
Figure-5: ZigBee Networks Deployed in an Industrial Enterprise Environment........... 12

A. Introduction

This paper addresses design principles and best practices regarding the secure implementation and operation of ZigBee wireless networks. ZigBee is a protocol specification and industry standard for a type of wireless communications technology generically known as *Low-Rate Wireless Personal Area Networks* (LR-WPAN). LR-WPAN technology is characterized by low-cost, low-power wireless devices that self-organize into a short-range wireless communication network to support relatively low throughput applications such as distributed sensing and monitoring. Networks can range from simple single-hop star topologies to more complex multi-hop mesh networks. The emergence of LR-WPAN technology and ZigBee standardization is appealing because of its potential for relatively fast, low cost, and simplified implementations compared to more traditional wired network installations used for industrial and process automation applications. The ZigBee specification provides a standardized set of protocols, services, and interfaces for vendors to create LR-WPAN hardware platforms and software applications that will enable customers to deploy complete, interoperable low-power mesh networking systems for monitoring and control.

The focus of this paper is on the secure deployment of ZigBee networks in industrial environments, such as manufacturing and process automation facilities. ZigBee is the name given to a specific protocol standard being developed by the ZigBee Alliance, the industry group overseeing its development and the process for certifying and branding compliant products. The term LR-WPAN, on the other hand, is a generic reference to the type of technology that is being standardized by groups such as the ZigBee Alliance. LR-WPAN is the term used by the IEEE, which has standardized the lowest layers of the technology but stopped short of developing the higher layers of the protocol stack needed to achieve fully functional and interoperable networks and applications. It should be noted that other industry groups are also engaged in the development of LR-WPAN standards, such as the ISASP100 and Wireless HART efforts.

This document will begin with a conceptual overview of LR-WPAN technology and the role that the ZigBee protocol plays in the development and standardization process. A section on the IEEE 802.15.4 specification upon which ZigBee is based is then presented, followed by a description of the ZigBee standard and its various components. A following section will describe ZigBee the security architecture, services, and features. Next, a section on secure LR-WPAN network design principles is presented, followed by a list of specific recommended security best practices that can be used as a guideline for organizations considering the deployment of ZigBee networks. Finally, a section on technical issues and special considerations for installations of LR-WPAN networks in industrial environments is presented. A concluding section summarizes key points and is followed by a list of technical references related to the topics presented in this document.

B. Technology Overview

ZigBee is the name for a short-range, low-power, low-cost, low-data-rate wireless multi-hop networking technology standard. The features of ZigBee networks include self-organization, support for multi-hop routed networking topologies, interoperable application profiles, and security based on the Advanced Encryption Standard (AES). As noted in the introduction, ZigBee is a type of LR-WPAN technology and is built upon the lower layers of the IEEE 802.15.4 LR-WPAN standard. While the 802.15.4 standard defines the lower-level Physical (PHY) and Media Access Control (MAC) layers, the ZigBee standard defines the higher-level Network and Application layers as well as the security services. The top layer in the system model is where the customer application resides. In terms of general functionality, the Physical Layer provides the basic radio communication capabilities, the MAC Layer provides reliable single-hop transmission, the Network Layer provides routing and multi-hop transmission for creating more complex topologies, the Application Layer provides device and network management functions as well as message formats, and the Security Services Provider establishes the trust infrastructure of the network and provides essential security services such as cryptographic key management and admission control for nodes joining a network. **Figure-1** depicts the ZigBee layered model.

The 802.15.4 lower layers provide the basic capabilities for LR-WPAN devices such as ZigBee nodes to join a network and send data to a neighboring device, but they do not provide the enhanced functionality for creating more complex multi-hop routed network topologies, nor the device and network management services needed for developing higher-level applications. The role of the ZigBee standard is to define the higher-layer network and application services that build upon the 802.15.4 wireless transmission capabilities to enable the development of complete LR-WPAN systems.

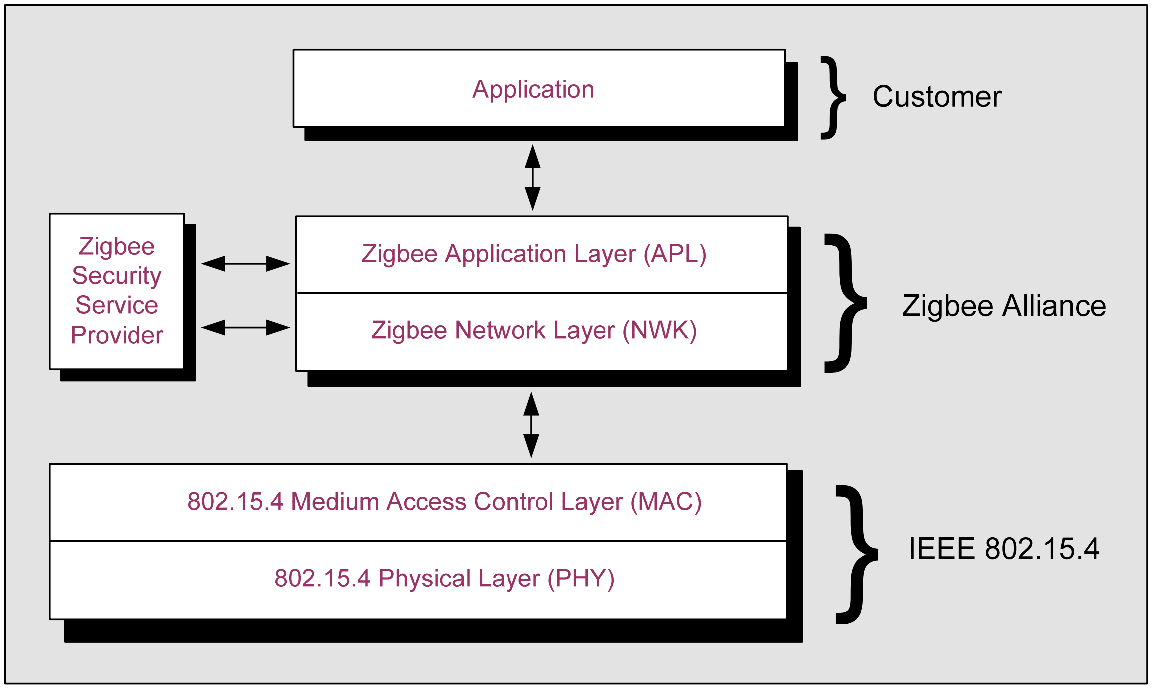
Application
Customer
Zigbee Security Service Provider
Zigbee Application Layer (APL)
Zigbee Network Layer (NWK)
Zigbee Alliance
802.15.4 Medium Access Control Layer (MAC)
802.15.4 Physical Layer (PHY)
IEEE 802.15.4

Figure-1: *The ZigBee Layered Model.*

C. The IEEE 802.15.4 Standard

As noted previously, the ZigBee standard is built on the lower layers defined by the IEEE 802.15.4 standard. The initial version of the standard was ratified in 2003 and is referred to as the *802.15.4-2003* standard. (See link provided in reference #2 in **Section J** Technical References of this document.) A subsequent revision of the standard was ratified by IEEE Task Group 4b and is referred to as *802.15.4-2006*. (See link provided in reference #3.) The 2006 version supersedes the 2003 version, but it is important to note that the current ZigBee standard (*ZigBee-2006*) is based on the *802.15.4-2003* version.

The functionality of the two lower layers defined by 802.15.4 are:

1) The Physical Layer (PHY): The PHY layer provides the basic communication capabilities of the radio and is responsible for the wireless transmission and reception of MAC frames. It performs such functions as radio control, energy detection, clear channel assessment, channel selection, data modulation, signal spreading, and the transmission and reception of bits onto the physical medium. The unit of transmission at this layer is the PHY frame.

2) The Medium Access Control Layer (MAC): The MAC layer establishes reliable and secure single-hop communication links between devices. It provides the basic functions of monitoring and accessing the wireless communications medium to coordinate the transmission of data from the higher layers. The MAC layer handles network association and dissociation functions and uses unique 64-bit MAC hardware addresses assigned by the manufacturer. The MAC layer also provides optional

security services including frame encryption, integrity, and access control. The unit of transmission at this layer is the MAC frame.

A slight departure from previous IEEE Layer-2 definitions is that the 802.15.4 MAC comprises the entire Data Link Layer (LLC) and is not a sub-layer. The standard DLL layer in the IEEE model normally consists of two sub-layers, a MAC sub-layer and a Logical Link Control (LLC) sub-layer. The LLC sub-layer normally specified is the IEEE 802.2 standard. Both the wired ethernet network standard (802.3) and the wireless ethernet standard (802.11) utilize the standard 802.2 sub-layer. However, the 802.15.4 standard does not utilize a separate 802.2 LLC sub-layer, but instead incorporates its functionality into an enhanced MAC sub-layer. Therefore, the 802.15.4 standard consists of just two layers, the PHY and the MAC. Such an approach provides for simplicity in operation and implementation, which is important for LR-WPAN node design where low cost and low processing overhead are essential due to limited power, memory, and processing capabilities. Because of the enhanced functionality of the 802.15.4 MAC layer, the ZigBee Network Layer can interface directly with it.

Devices based on the 802.15.4 standard operate in the unlicensed portion of the *Industrial, Scientific, and Medical* (ISM) frequency spectrum. (The ISM bands are ranges of frequencies set aside for unlicensed, low-power RF operation as defined by FCC Part 15.) See **Table-1** below for a list of the frequencies and data rates defined by the IEEE 802.15.4 standard.

Frequency Band	Frequency Spectrum	Number Channels	Maximum Data Rate	Modulation Type	Availability & Usage
868 MHz	868-868.6 MHz	1	20 Kbps	DSSS with BPSK	Most Europe Countries
915 MHz	902-923 MHz	10	40 Kbps	DSSS with BPSK	N. America, S. America, Australia, NZ
2.4 GHz	2.4-2.4835 GHz	16	250 Kbps	DSSS with O-QPSK	Most Countries Worldwide

Table-1: *Frequency Band, Number of Channels, Data Rate, Modulation, and Geographic Availability of the IEEE 802.15.4 bands of operation*

Note: For the purposes of the 802.15.4 standard, the IEEE considers the 868 MHz and 915 MHz bands to be a single, contiguous band and vendors that choose to support either band must support both.

The 802.15.4 standard includes the definition of *security services* provided by the MAC layer. There are four basic security services defined:

1) *Access Control*: This security service enables the MAC to select the devices with which it is willing to communicate based on the MAC address of the received frame.

2) *Data Encryption*: This security service is based on the use of symmetric key cryptography to encrypt the MAC frame for data privacy protection.

3) *Frame Integrity*: This service enables a receiving device to detect the modification of a message (deliberate or inadvertent) using a cryptographic message integrity code (MIC). The MAC layer generates a MIC and appends it to the MAC frame.

4) *Sequential Freshness*: This security service appends an ordered sequence of values to the MAC frame in order to prevent replay attacks in which an old message is captured by an attacker without the cryptographic key and then re-sent later. The freshness code is five octets (bytes) in length.

The above MAC layer services are used in various combinations based on one of three supported security modes of 802.15.4:

1) Unsecured Mode

In this mode, no security services are provided. MAC frames are sent in clear text and have no data privacy, integrity checking, or access control filtering enabled.

2) Access Control List (ACL) Mode

In ACL mode, the MAC maintains a list of hardware device addresses with which it will communicate.

3) Secured Mode

In this mode, the device may have any of the four security services enabled, depending on the security suite implemented. The 802.15.4 standard defines seven suites based on the *Advanced Encryption Standard* (AES). **Table-2** below outlines the security suites supported in the 802.15.4-2003 standard.

Security Suite	Integrity Bits	Access Protection	Frame Encryption	Frame Integrity	Sequential Freshness
AES-CTR	0	Yes	Yes	No	Optional
AES-CCM-128	128	Yes	Yes	Yes	Optional
AES-CCM-64	64	Yes	Yes	Yes	Optional
AES-CCM-32	32	Yes	Yes	Yes	Optional
AES-CBC-MAC-128	128	Yes	No	Yes	No
AES-CBC-MAC-64	64	Yes	No	Yes	No
AES-CBC-MAC-32	32	Yes	No	Yes	No

Table-2: *IEEE 802.15.4 Security Suites*

(Source: See #7 ***Section J Technical References****)*

The ZigBee standard uses the security services specified in 802.15.4 in order to secure MAC layer frames. (There are some minor changes the ZigBee standard specifies with regard to MAC layer security, which will be discussed in the section on ZigBee security.) In addition, ZigBee defines its own security model and set of security services at the Network and Application Layers of the stack in order to provide a comprehensive network security infrastructure. This is needed because the 802.15.4 standard stops short of defining essential security services such as cryptographic key management, leaving the definition of such functions to the higher layers. The ZigBee security model will be discussed below in **Section E *ZigBee Security Features*** of this document.

D. The ZigBee Protocol

The ZigBee protocol is a product of the ZigBee Alliance, an industry group that oversees the development of the standard. Formed in 2002, the ZigBee Alliance is focused on the standardization of LR-WPAN technology for applications in the industrial, building automation, and consumer markets. In addition to the development of the standard, the Alliance also certifies products and brands compliant products with the ZigBee label. The Alliance defines the upper layers of a protocol stack that builds upon the IEEE 802.15.4 lower layers with the goal of creating secure, multi-hop LR-WPAN networks and interoperable applications.

This section will provide an overview of ZigBee networking concepts in order to create the foundation for the discussion on ZigBee security. Readers who would like more detail are encouraged to obtain further background information on ZigBee by accessing the online references provided in **Section J *Technical References*** of this document.

The two types of generic 802.15.4 LR-WPAN nodes upon which ZigBee devices are based consist of the following:

1) *Reduced Function Devices* (RFD): These are reduced complexity nodes with relatively limited memory, processing, and power capabilities. They can only serve as End Devices in a network and cannot perform the more complex roles of Router or Coordinator.

2) *Full Function Devices* (FFD)*:* These devices have the resources to perform more complex task such as Coordinator or Router but can also be an End Device in a network.

The primary components that comprise a ZigBee LR-WPAN network are

1) *ZigBee Coordinator:* Also referred to more generically as the PAN Coordinator, this device is responsible for performing critical functions such as starting a PAN network, assigning device addresses, and controlling the PAN formation and operation. There can be only one Coordinator per ZigBee network, and the Coordinator must be an FFD.

2) *ZigBee Router:* A Router has the resources to execute routing algorithms and forward message to and from ZigBee devices. It is capable of establishing and maintaining multiple connections to children and parent nodes. A Router must be an FFD.

3) *ZigBee Trust Center* (ZTC*):* The ZTC is the central component in the ZigBee security architecture and is trusted by all other ZigBee devices. It provides the vital services of trust management, device management, and network management.

4) *ZigBee End Device (*ZED*):* An End Device can be an RFD or an FFD but is a leaf node in the network and does not perform any of the other ZigBee device functions of Router, Coordinator, Trust Center, or Gateway.

5) *ZigBee Gateway:* A gateway node serves as a bridge between a ZigBee network and another network (such as a wired Ethernet network) and performs protocol conversion as necessary.

The number and type of each device in a ZigBee network will vary depending on the size, complexity, and type of applications supported. Since security, interconnection to other networks, and more sophisticated multi-hop routed topologies are not mandatory, the least complex network configuration (and minimum required) would consist of one FFD to serve as the PAN Coordinator and one FFD or RFD to serve as a second End Device. In reality, however, applications in the industrial domain are likely to be larger and more complex in nature with interconnection to other legacy or enterprise networks. Although ZigBee networks can be implemented without any security enabled, ZigBee networks deployed in industrial environments should employ the security services and trust management infrastructure specified in the protocol.

The ZigBee Network Layer supports the formation of both star and peer-to-peer topologies. Shown in the figures below are three common topologies supported by ZigBee (one star and two peer-to-peer). **Figure-2** depicts the simplest topology, the star network. The ZigBee Coordinator is at the center of the star, and either FFD or RFD devices form the End Devices.

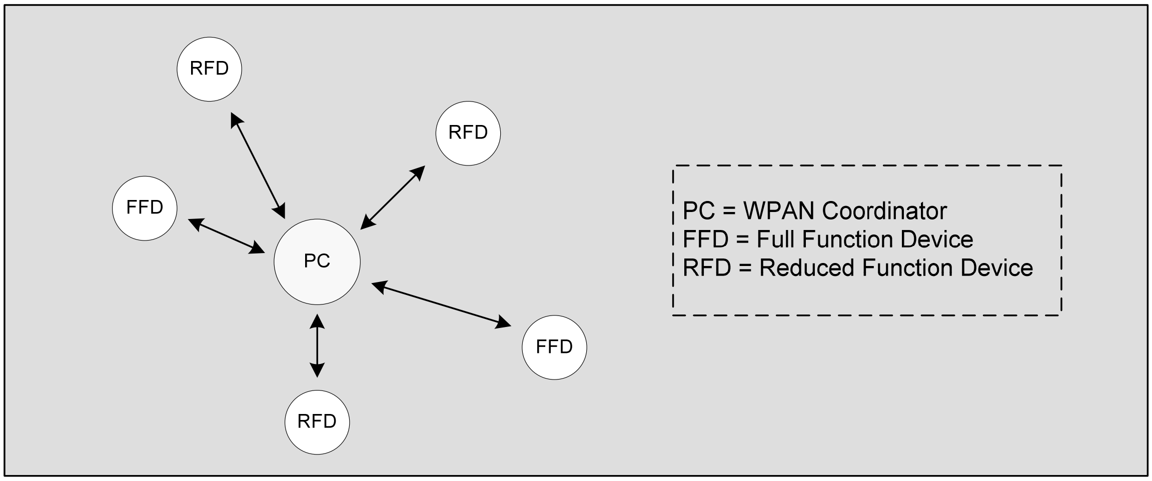

Figure-2: *The Star Network Topology*

Figure-3 below shows a more complex peer-to-peer topology referred to as a mesh network. FFD devices perform the ZigBee Router functions in this type of network and either FFD or RFD devices comprise the End Devices.

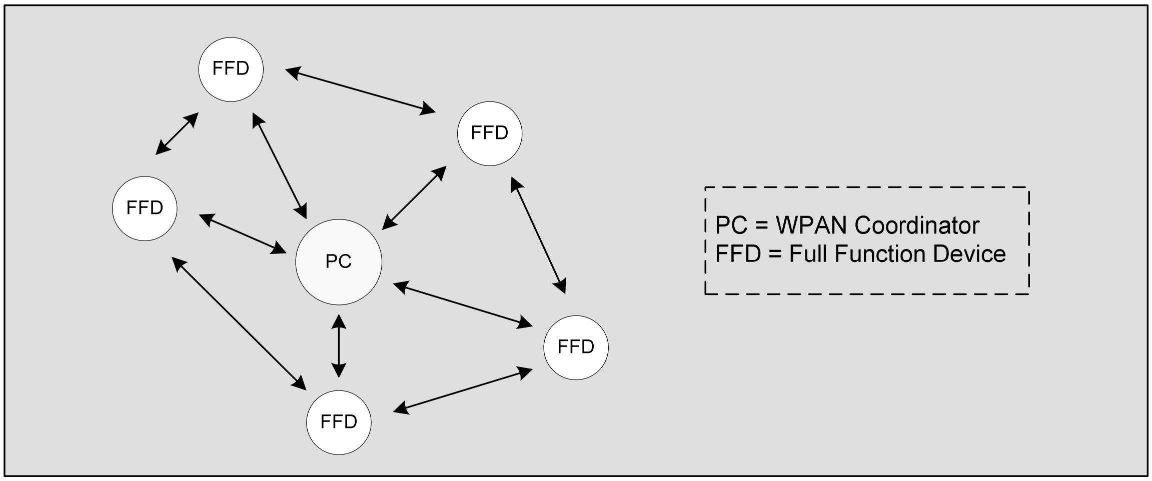

Figure-3: *The Mesh Network Topology*

Finally, **Figure-4** illustrates another type of popular peer-to-peer topology called a cluster-tree network. In this topology, only ZigBee Routers forward packets in a simplified routing scheme among their parent and child nodes.

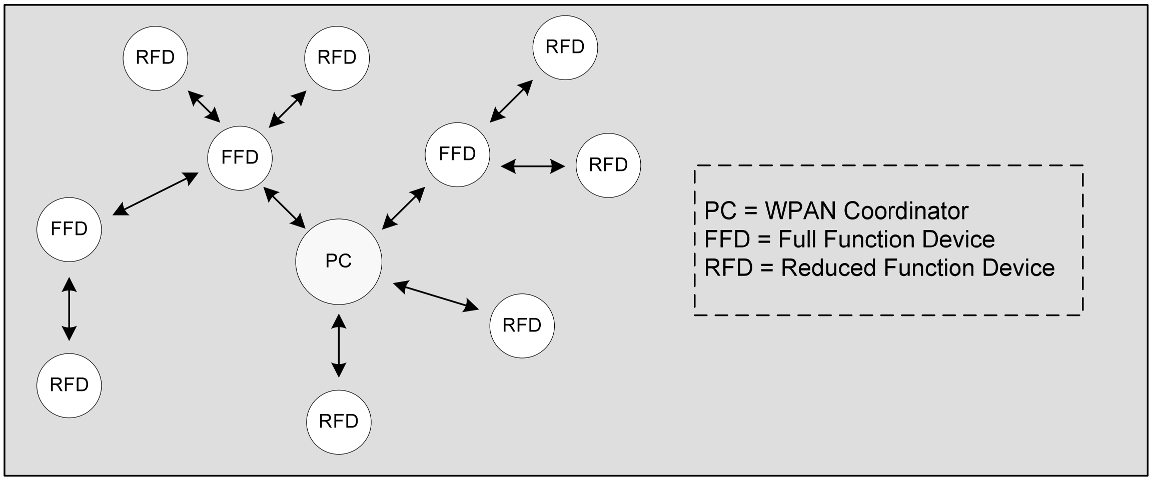

Figure-4: *The Cluster-Tree Topology*

In terms of device addressing, *long addresses* are implemented at the MAC layer by the manufacturer and are 64-bits in length. *Short addresses*, on the other hand, are dynamically assigned and are 16-bits in length. Short addressing is used for simplicity and to reduce the memory storage requirements of the hardware platform.

A central concept of the ZigBee Application Layer is the *Application Profile*. Profiles are the key to communicating between devices on a ZigBee network. Application Profiles define the devices, messages, and processing actions that comprise an application running among ZigBee End Devices in a given environment in order to ensure compatibility and interoperable functionality between them. There is a *Profile Identifier* field in the Application Layer frame that is 16-bits in length and specifies the profile. Of potential interest to the industrial and process automation industry is the *Industrial Process Monitoring* (IPM) profile, which is under development by the ZigBee Alliance and will provide an interoperable set of device descriptions and message formats related to monitoring and control of industrial equipment (e.g. pressure and temperature sensor devices and their respective parameters and output values).

E. ZigBee Security Features

The ZigBee protocol defines methods for implementing security services such as cryptographic key establishment, key transport, frame protection, and device management. The ZigBee security architecture includes security mechanisms at three layers of the protocol stack - MAC, Network, and Application. Each layer has services defined for the secure transport of their respective frames.

The MAC layer is responsible for its own security processing, but the upper layers determine which security level to use. Note that when MAC layer integrity protection is employed, the entire MAC frame is protected, including the MAC header that contains the hardware source and destination addresses. By enabling MAC frame integrity, the MAC layer source address can be authenticated. This measure can counter address spoofing attacks and allow a device to more effectively process and compare a received MAC frame against an Access Control List (ACL).

Cryptography within the ZigBee specification is based on the use of 128-bit keys and the AES encryption standard. Encryption, integrity, and authentication can be applied at the Application, Network, and MAC layers to secure the frames at each of those levels. In terms of key types, ZigBee specifies the use of Master, Link, and Network keys to secure transmitted frames. A Network Key is a common key shared among all nodes in a ZigBee network. The standard also specifies an Alternate Network Key as a form of key rotation that may be employed for key update purposes. At a minimum, a ZigBee network should be secured with the use of a Network Key used by all the devices to protect all network frames (routing messages, network join requests, etc.) and prevent the unauthorized joining and use of the ZigBee network by illegitimate devices. Link Keys, on the other hand, are secret session keys used between two communicating ZigBee devices and are unique to those devices. Devices use their Master Key to generate the Link Key. The manner in which Master, Link and Network Keys are generated, stored, processed, and delivered to ZigBee devices determines the effectiveness and degree of security of the overall ZigBee network implementation. **Section G *Security Best Practice Recommendations*** of this document outlines measures for how to securely deploy and manage encryption keys as well as other measures for achieving secure ZigBee implementations.

ZigBee uses the AES-based CCM* security suite, which is based on the security suite specified in the 802.15.4 standard and summarized in **Table-2**. CCM* is a minor modification of the CCM modes in the 802.15.4 standard and offers encryption-only and integrity-only capabilities. According to the ZigBee specification, the extra capabilities in CCM* simplify security by eliminating the need for the CTR and CBC-MAC modes in the 802.15.4 suite and also allow the use of a single key for each security level within the protocol. With CCM*, the MAC, Network, and Application layers within the ZigBee stack can optionally reuse the same key for more efficient implementation based on limited storage and processing resources within the ZigBee device.

The central component of the ZigBee security architecture is the ZigBee Trust Center (ZTC). All devices within a ZigBee network recognize and trust exactly one ZTC. The ZTC stores and distributes keys to ZigBee devices. (However, for maximum security, it is a recommended best practice to pre-load the keys into the ZigBee devices directly.) The functions performed by the ZTC are trust management, network management, and configuration management.

It is important to note that different applications running on the same ZigBee device are not logically separated (due to cost and complexity constraints). Therefore, different applications are not cryptographically separated either, and one must assume that the applications trust each other because they are using the same keying material. ZigBee refers to this as an *open trust model* in which different layers of the communication stack and all applications running on a single device trust each other. The implication for use of this model is that all devices and applications within a given ZigBee network trust each other and that security is realized on a device-to-device basis. Layer-to-layer or application-to-application security is not possible under the current standard.

F. Security Design Principles

This section describes the principles involved in architecting and designing a secure LR-WPAN solution based on the ZigBee standard. These principles should be employed in the planning and design of a ZigBee network. The subsequent section will list specific best practice guidelines for the implementation of a ZigBee network.

The following are design principles for developing a secure architecture:

1) Principle: *Apply a Defense-in-Depth approach.*

   This concept of secure design involves implementing multiple layers of security measures to control access to mission-critical systems and networks. These are often the targets that an attacker attempts to gain unauthorized access to by compromising a wireless network and using it as an attack path or vector in to an organizational network such as a plant network where the target systems reside. In order to defend the target environment, multiple security measures should be implemented so that if one measure is defeated by an attacker, additional measures and layers of security remain to protect the target environment. Measures such as separation of wireless and wired network segments, strong device and user authentication methods, filtering of traffic based on addresses and protocols, securing end-points/stations from unauthorized access, and monitoring and intrusion detection on the wireless and wired segments are examples of multiple layers of defense that can be employed to achieve a defense-in-depth design.

2) Principle: *Analyze and harden all components of the system.*

This principle of security design entails looking at the entire application that is being deployed or expanded, not just the ZigBee wireless component. This is especially critical if the ZigBee network will be integrated into an existing enterprise environment. Other components might include existing wired and wireless networks, storage servers, processing or transaction servers, log servers, end devices, and application software. Each element should be analyzed for ways to harden it against security attacks or configuration failures. For example, a ZigBee network may interconnect to an existing factory ethernet LAN through a gateway device and record data onto a server that is running a software package for performance analysis. Each of these components should be examined for ways to strengthen security. A good starting point is to review the documentation that comes with the product to see if security features exist and can be enabled. Conversely, a review of product manuals can reveal features or capabilities that are not needed and can be disabled. For interconnection points between the ZigBee network and the enterprise network, the gateway device should be hardened as well as the perimeter interconnection point. Servers with which the ZigBee network communicates should be hardened by disabling unnecessary services, applying current OS patches, removing unused accounts, etc.

3) Principle: *Separate and segment the ZigBee network from other networks.*

ZigBee networks and wired networks should not be directly connected if possible. For example, a ZigBee wireless environmental sensing LR-WPAN or equipment monitoring LR-WPAN network should not have direct connectivity to the wired plant network, but instead be separated by a device such as a firewall, bastion host, or security gateway to establish a security perimeter that can more effectively isolate, segment, and control traffic flows between them.

4) Principle: *Restrict traffic in and out of the ZigBee network.*

If the ZigBee network must be interconnected to other existing networks, filter the traffic by source and destination address and service port number to the minimum required to achieve the desired functionality and requirements. For example, if a ZigBee environmental monitoring network is deployed in a factory and the data must be collected and stored on a server, then the ingress point to the server (a wired network or connection to a dedicated port on the server) should be configured to receive traffic only from the ZigBee gateway address and destined for the server address and application/service port required.

5) Principle: *Enable 802.15.4-defined security features at the lower layers of the stack.*

As noted previously, the ZigBee Alliance defines the upper layer standards and the IEEE defines the lower layer standards. Both standards have security services defined in their specifications. In addition to utilizing the ZigBee security services as outlined in this document, consideration should also be given to leveraging the security available at the MAC layer as defined in the IEEE 802.15.4 standard. Having security defined at both the higher and lower layers of the protocol stack creates a stronger security solution and should be adopted if supported by the ZigBee vendor.

6) Principle: *Enable ZigBee-defined security features at the higher layers of the stack.*

As described previously in this document, ZigBee defines security services for use in the Network and Application layers of the standard. These services include encryption, authentication, and integrity. They should be utilized to ensure the highest level of protection appropriate for the given application and operational environment. When evaluating ZigBee vendors and products, support for security services at the Network and Application layers should be part of the evaluation and selection criteria.

7) Principle: *Develop a security architecture based on maximizing protection of the Trust Center.*

A strong set of policies, procedures, and technical control measures should be implemented to secure the Trust Center (TC) component of the ZigBee network. The TC is a device within the network that all ZigBee nodes trust and that is responsible for the distribution of cryptographic keys for network and end-to-end application configuration management. It is the core component within the ZigBee security architecture and therefore its compromise would undermine the entire trust model.

Shown below in **Figure-5** is a conceptual example of an industrial enterprise environment employing some of the design principles presented. It shows several ZigBee networks that are segmented from each other and from the plant network using dedicated ports on a multi-port firewall. Each network should be authenticating source MAC addresses and filtering access based on those addresses against Access Control Lists. A separate network segment for security management is shown to emphasize the importance of isolating and controlling platforms for performing network and device configuration. An Intrusion Detection System (IDS) on the wired network is used to monitor suspicious activity and alert on potential attacks.

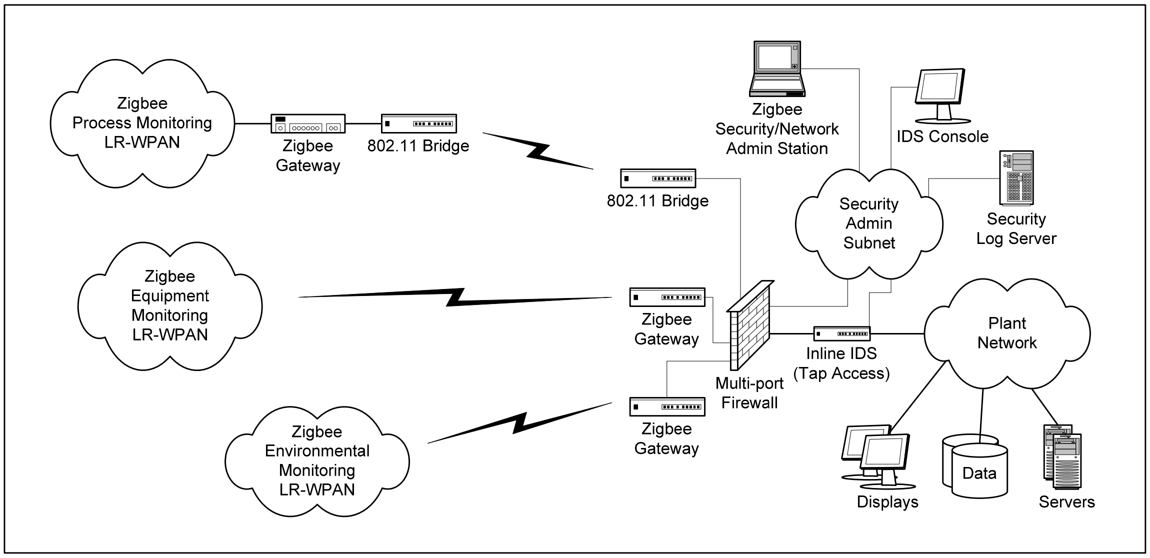

Figure-5: *Example of ZigBee Networks Deployed in an Industrial Enterprise Environment*

G. Security Best Practice Recommendations

The following are recommended practices that should be considered when implementing a ZigBee LR-WPAN network:

1) Recommendation: *Create a LR-WPAN security policy and set of procedures to govern the implementation, management, and operation of ZigBee networks*.

   The organization should develop a general LR-WPAN technology security policy, which can be an addendum to an existing IT or wireless security policy. In high-level non-technical language, the policy document should authorize the use of LR-WPAN networks within the organization and specify the roles and responsibilities of personnel to ensure their safe and secure operation. A corresponding security plan containing more specific procedures should provide details on the security measures required for the design, implementation, management, and use of specific LR-WPAN networks such as ZigBee applications deployed within the facility. For example, the policy may require a security plan for each Zigbee network implementation, while the set of procedures within the security plan may mandate the physical inventory and tracking of ZigBee devices, configuration management procedures, and change control measures.

2) Recommendation: *Protect the ZigBee network infrastructure with a Network Key.*

   One type of cryptographic key specified in the ZigBee standard is the Network Key. A Network Key is shared among all nodes in a ZigBee network, including End Devices, Routers, and Gateways. Ideally, all nodes should be required to possess a valid Network Key in order to utilize the ZigBee network for transmitting and receiving data. Nodes without a valid Network Key should not be able to join (associate) or utilize a ZigBee network for transport. Routing nodes should validate ZigBee packets based on the Network Key before processing and forwarding the packet.

3) Recommendation: *Employ address filtering at the MAC layer.*

   This is a low-level security mechanism that is defined within the IEEE 802.15.4 standard and is referred to as *Access Control List* (ACL) mode. If the ZigBee vendor supports this feature, it should be utilized by all nodes within the network to only accept received MAC frames from authorized nodes listed in the ACL for the device.

4) Recommendation: *Utilize the ZigBee encryption security service.*

   As discussed previously, the ZigBee standard provides data privacy protection mechanisms based on the AES encryption standard. This security service should be used to protect the transmitted data.

5) Recommendation: *Implement source node authentication.*

   If the ZigBee vendor supports it, source node authentication should be implemented in order to cryptographically verify the identity of a transmitting node. Although a shared ZigBee Network Key will provide a security check for packets utilizing the

ZigBee network, source node authentication can be used by the destination ZigBee device to verify the identity of the source device. In order to authenticate a source device, a ZigBee *Link Key* (end-to-end crypto key) must be generated and used. This key is unique to a pair of devices that are communicating with each other and is derived from their respective *Master Keys*. (This is equivalent to the concept of a shared secret or unique session key that is derived between two entities in order secure data transmitted between them.)

6) Recommendation: *Designate a ZigBee Coordinator.*

The ZigBee standard supports the automatic formation and self-organization of a LR-WPAN network. One node, however, must function as the WPAN Coordinator and initiate the formation of the network as well as perform other essential functions such as sending beacon transmissions and setting the security level of the network. In the ZigBee standard, this node is referred to as the *ZigBee Coordinator*. The underlying IEEE 802.15.4 protocol mechanisms that govern self-organization allow any Full Function Device (FFD) to assume the role of WPAN Coordinator, provided that a Coordinator for the network has not already been established. From a security and network management perspective, however, such flexibility and potential uncertainty regarding which node assumes this critical function may be undesirable. (This is especially true if every device in the ZigBee network is an FFD.

Therefore, it is recommended that a particular FFD node be designated as the dedicated ZigBee Coordinator for each ZigBee network implementation in order to ensure maximum control over the formation and operation of the WPAN network. All other nodes should be disabled, if possible, from assuming the role of WPAN Coordinator with the possible exception of a ZigBee node specifically designated to function as a backup Coordinator (see next recommendation).

7) Recommendation: *If supported, designate a backup ZigBee Coordinator.*

If supported by the ZigBee vendor, a backup or secondary WPAN Coordinator should be designated to function as the Coordinator in the event that the primary Coordinator fails. As with the primary Coordinator, the secondary Coordinator should be a dedicated node within the network that performs this vital function, and all other nodes should be configured to not assume the role of Coordinator dynamically. This will prevent other nodes from taking over the role of an existing Coordinator if it fails or attempting to establish a new, separate LR-WPAN network on their own.

8) Recommendation: *Pre-assign a PAN Identifier and restrict node connectivity.*

In addition to configuring a dedicated ZigBee Coordinator for the network, a predetermined PAN Identifier should be used by the Coordinator. ZigBee nodes should be limited to joining only the network with the pre-assigned PAN Identifier. Also, the ZigBee network policy can be configured to use the *permit join* access control to restrict device connectivity. (Note that a degree of coordination and control of PAN Identifiers is necessary if multiple ZigBee networks will be operating in a given environment in order to prevent potential conflicts. Also, if supported by the vendor, ZigBee Coordinators should be configured to conduct active channel scans at startup to detect conflicts.)

9) <u>Recommendation</u>: *Choose an out-of-band key loading method if possible.*

If the ZigBee vendor supports it, use an out-of-band method of loading the cryptographic key(s) onto the ZigBee devices. The methods for key management (generation, distribution, updating, revoking, etc.) will vary among ZigBee vendors. Generally, the initial generation and loading of cryptographic keys (e.g. the Master key) will be possible in three ways:

a) *Out-of-band*: This method entails loading the key into the ZigBee device using a mechanism other than through the normal wireless communication channels used for network operation. An example would be a serial port on the device through which a key could be loaded with a cable attachment to the key generation device (such as a laptop or the Trust Center host).

b) *In-band*: This method delivers keys over-the-air through the normal wireless communication channels used for network operation. This is a less secure method of key delivery because the transmission of the key to a device joining the network that has not been pre-configured is unprotected (creating a potential short period of vulnerability).

c) *Factory pre-loaded:* This method of key deliver consists of the vendor generating and loading the key(s) into the ZigBee devices at the manufacturing location prior to deliver to the customer. Key values must subsequently be conveyed to the customer when they receive the ZigBee equipment. This approach is the least secure because the vendor has knowledge of the key values and must also successfully convey the information to the customer in a secure manner.

From a security standpoint, the preferred method (if supported by the ZigBee vendor) is to have the customer generate and load keys out-of-band. If that is not supported, then an in-band delivery method for loading keying material under controlled conditions (e.g. the ZigBee devices are in a central location within the facility prior to deployment) would be the second most secure method. The factory generated and pre-loaded key option is likely to be the least secure method and should be used only if the two other key loading methods are not supported.

10) <u>Recommendation</u>: *Enable Layer-2 security mechanisms supported in the IEEE 802.15.4 lower layer MAC if supported by the vendor.*

As discussed previously, the ZigBee protocol is built on the lower layer IEEE 802.15.4 protocol and uses the MAC layer security features defined in the standard but with the CCM* cipher suite. These security features should be utilized if supported by the vendor, especially the frame integrity capability since it protects the MAC header that contains the source and destination hardware address fields.

It should be noted that presently the ZigBee-2006 standard does not address the use of 802.15.4-2003 MAC Layer security services, so customers interested in this capability will need to inquire with vendors regarding support and whether inclusion of the option will impact ZigBee compliance.

11) Recommendation: *Implement secure network admission control.*

The ZigBee protocol specifies a method for devices to join a WPAN network by first *associating* to the network and then *authenticating* to it. The ZigBee Trust Center (ZTC) is responsible authenticating nodes requesting admission and deciding whether to permit the node to join. By securely pre-loading a common network security key in all ZigBee devices prior to deployment, only *secure joins* by authorized ZigBee nodes possessing the correct Network Key should be permitted by the security policy specified in the ZTC. A secure join will avoid the situation where a ZigBee node without a Network Key first associates to the ZigBee Coordinator or ZigBee Router using an unsecured request.

12) Recommendation: *Pre-configure nodes with the Trust Center address.*

The Trust Center (TC) is the central element in the ZigBee security architecture and is trusted by all devices in the network. There is exactly one TC in a ZigBee network. If possible, the address of the TC should be pre-loaded into the ZigBee node. (The pre-loading of the TC address can be combined with pre-loading of the crypto keys as recommended previously.)

H. Considerations for Industrial Environments

This final section discusses issues specific to implementing and securing ZigBee networks in industrial environments.

1) *Interference*: Industrial environments can produce a significant amount of electromagnetic noise from machinery such as pumps, motors, fans, and various actuator devices. The resulting EMI (Electro Magnetic Interference) can interfere with the operation of LR-WPAN networks by increasing the white noise floor and reducing the signal-to-noise quality of transmissions. The MAC layer of 802.15.4 is based on the CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) channel access method in which a station will first listen for an open channel before transmitting. This is done by sensing the energy level in the frequency band corresponding to the channel. In an environment with significant levels of EMI, the noise floor in the operating frequency ranges of 802.15.4 networks can prevent stations from transmitting because the RF energy threshold level for an open channel has been exceeded. Essentially, the LR-WPAN devices conclude that all of the channels are in use by other stations and hold off on transmissions. This can create performance problems for LR-WPAN networks operating in high EMI environments and should be taken into consideration.

Possible mitigations include:

a) Choosing the least susceptible 802.15.4 frequency band (900MHz or 2.4GHz) for a given industrial environment.

b) Configuring the ZigBee devices to use a particular channel within the selected frequency band that is least affected by the EMI.

c) Increasing the transmit power level of the ZigBee devices by selecting a product that supports higher power levels or using a higher-gain antenna.

d) Deploying a mesh topology to allow a ZigBee device to have multiple next-hop neighbors to communicate with and therefore *spatial diversity* in terms of multiple transmission paths. Higher node density will also permit shorter distances between ZigBee devices and can result in increased received signal strength and improved signal-to-noise ratios.

e) Using a Frequency Hopping (FH) radio with configurable hopping channels and patterns. This type of temporal and frequency diversity approach can improve EMI immunity in an industrial environment as well as provide an additional measure of security if a non-default hopping pattern is used and also changed on a periodic basis. (Note, however, that a FH Physical Layer implementation will be proprietary in nature from the vendor and not compatible with the current 802.15.4 and ZigBee standards, which are based on a Direct Sequence Spread Spectrum method.)

In addition to EMI, issues regarding Radio Frequency Interference (RFI) generated by transmitting ZigBee devices should be considered. Depending on the type of equipment installed, the frequencies used may interfere with industrial control and monitoring equipment. This effect tends to be somewhat mitigated by the typically low power and low duty cycle of ZigBee End Devices (i.e. devices sleep the majority of the time and only wake periodically to transmit or receive messages at relatively low power levels). However, high duty cycle (and potentially higher powered) devices such as the ZigBee Coordinator and ZigBee Routers can produce more RFI. The RFI generated may also interfere with other wireless communication systems that may be deployed in the plant (e.g. 802.11 WLAN networks using the same 2.4GHz ISM spectrum). Again, however, the low power and duty cycle of ZigBee devices is less likely to be a source of interference to other wireless systems. More likely is the negative interference effects of higher power 802.11 WLAN networks on 802.15.4 networks.

Possible mitigations for RFI include:

a) Selecting the frequency band that generates the least interference (900MHz or 2.4 GHz).

b) Configuring the ZigBee devices to use a particular fixed channel that produces the least interference with other industrial equipment or wireless systems in the plant.

c) Increasing node density in order to reduce required transmitter power and enable shorter link distances.

d) Placing ZigBee devices away from susceptible industrial equipment and other wireless transmitters and creating a topology that avoids them if possible (e.g. cluster-tree or linear hopping patterns).

e) Using a Frequency Hopping (FH) radio with configurable hopping channels and patterns.

2) *Reliability*: Consideration should be given to the types of applications that operate over LR-WPAN networks deployed in industrial environments. RF transmission quality and reliability are affected by many factors in the operating environment, many of which are dynamic in nature. As mentioned above, EMI from factory or process machinery can cause degradation of LR-WPAN performance, and objects in the path of the receiver can cause reflections resulting in attenuated multi-path reception issues. In factory environments with an abundance of machinery and metal objects that are both static and dynamic in nature (conveyors, cranes, robotic devices, etc.), reliable wireless communication may present a challenge, especially for low-power devices such as ZigBee networks. Therefore the types of applications and their criticality, performance, and reliability requirements should be analyzed and tested before deployment over LR-WPAN networks.

   Note: The ISA-SPA100.11a Working Group has developed a set of *usage classes* that categorize inter-device industrial wireless communications based on such factors as importance of message delivery timeliness, the function of the application, and the type of system (safety, control, monitoring). This can serve as a useful starting point for assessing the criticality and performance requirements of an application before deployment over a LR-WPAN network such as ZigBee.

   Considerations for addressing reliability and performance when deploying ZigBee networks include the choice of network topology and the use of Guaranteed Time Slot (GTS) transmission:

   a) *Topology*: The star is the least complex of the topologies supported by the ZigBee standard. All nodes communicate over a single hop to the ZigBee Coordinator. Because of the simplified communication patterns and the lack routing support needed by the nodes, the reduced complexity can improve the reliability and manageability of the ZigBee network. Additionally, the single-hop path to the ZigBee Coordinator and the maximum two-hop path to other devices can reduce end-to-end latency and improve performance for applications that require it. However, the single path nature of star topologies can introduce single points of failure in the network and reduce reliability of the RF link to the ZigBee Coordinator should it experience degradation due to path loss or interference. Various forms of peer-to-peer topologies that include multiple paths to the ZigBee Coordinator and between ZigBee End Devices can improve reliability in such scenarios. However, multiple node paths can increase latency and therefore reduce end-to-end data throughput rates. Therefore, choice of topology will require analysis of application requirements in terms of reliability versus throughput.

   b) *Guaranteed Transmission*: The 802.15.4 standard supports an optional Guaranteed Time Slot (GTS) transmission mode. Normally, an LR-WPAN network operates in a *contention-based* mode in which the CSMA/CA channel access protocol is used by devices to contend for the wireless transmission medium whenever a message is ready for delivery. A device in this mode will listen for an available channel based on the RF energy detected and then transmit if it concludes the channel is unused. GTS mode, however, is a *contention-free* method for accessing the wireless medium based on regular time slots assigned to devices by the LR-WPAN Coordinator. GTS mode can be employed to ensure that devices with critical data to transmit are guaranteed the opportunity to send during a specified time interval without risking a collision with other devices transmitting at the same time. (Note that successful reception of the frame at the destination is not guaranteed, only the transmission.) It should be noted that presently the ZigBee-2006 standard does not address the use of GTS, so customers interested in this capability for their application will need to inquire with vendors regarding support and whether inclusion of the option will impact ZigBee compliance.

3) *Security*: Related to the issue of reliability is security. This paper has discussed the security design principles and recommended practices for securing ZigBee networks. By applying these principles and practices, the security risks of deploying and operating a LR-WPAN network can be mitigated. As with any network implementation, security is only as effective as the controls implemented and the practices followed by those who use and manage it. Furthermore, because of the unbounded nature of RF propagation, the perimeter of a wireless network cannot be contained and controlled to the degree possible with a wired network. Signals will reflect off objects and find their way out of buildings. Motivated attackers can attempt to detect these stray signals, however low-strength they may be, and attempt to interfere with the LR-WPAN if they are in physical proximity of the facility. Attackers can passively capture traffic and attempt to penetrate the network and reach other connected enterprise networks. Both RF attacks based on frequency jamming and protocol attacks based on crafted packets can create denial-of-service (DOS) situations that interfere with the operation of the LR-WPAN network. The security design principles and best practices presented in this paper can mitigate these risks to acceptable levels but not completely eliminate them.

I. Conclusion

Although the ZigBee Alliance was formed in 2002, only recently have certified platforms become available for designers to create real-world applications and embedded product offerings. LR-WPAN technology has been evolving rapidly, with the ZigBee specification having undergone its most recent revision in December of 2006. However, as more certified chip sets, OEM modules, and ZigBee-enabled devices become available, industrial users will have the opportunity evaluate the technology and consider deployment within their enterprise environments. This paper has provided an overview of the ZigBee protocol standard and the LR-WPAN technology on which it is built. The primary focus has been on describing the security features in the ZigBee standard and making recommendations regarding the secure implementation of this type of wireless communications technology within industrial environments.

The ZigBee standard defines a comprehensive security architecture and trust management model, including frame encryption, authentication, and integrity at each layer of the ZigBee protocol stack. ZigBee also defines a Trust Center that provides the essential security functions of key management, network management, and device configuration. These security capabilities will enable application designers to create policy-based security features into their product offerings and allow customers to deploy secure LR-WPAN networks. The recommendations provided in this report are intended to assist industrial users in understanding ZigBee security features in order to evaluate product offerings as they become available and plan and choose solutions that can provide the security required by their industrial enterprise environments and specific applications.

As industrial users begin considering deployments or pilot implementations based on emerging ZigBee technology, they should employ basic network security design principles during the planning stage. These include creating a set of policies and procedures to govern the security and operational aspects of the deployment, employing a defense-in-depth approach to analyzing and hardening all elements of the system, segmenting the ZigBee network(s) from the existing plant network as well as restricting and monitoring traffic flows between them, utilizing ZigBee frame protection services at multiple layers within the protocol stack, and finally maximizing protection around the critical ZigBee Trust Center component responsible for centralized security and network management. Once a secure architecture has been developed, the specific security measures and hardening techniques outlined in the security best practices section of this report should be considered during the implementation of the ZigBee network(s). The best practice recommendations can also be used to evaluate ZigBee vendor product offerings for support of security features required or preferred by the industrial user.

Lastly, industrial users should consider the type of monitoring and/or control applications that are suitable for LR-WPAN technology such as ZigBee. Reliability, security, and performance are potential challenges when designing and deploying wireless technologies in general, and factors such as EMI/RFI and multi-path fading in industrial environments can be specific issues to consider. The choice of ZigBee network topology, the use of guaranteed time slotting, and the application of the security measures presented in this paper are some options to consider when addressing these issues.

J. Technical References

Below are references related to the topics discussed in this paper.

1) *The ZigBee Alliance homepage*:

   http://www.ZigBee.org

2) *Information on the IEEE 802.15.4-2003 standard*:

   http://grouper.ieee.org/groups/802/15/pub/TG4.html

3) *Information on the IEEE 802.15-2006 revised standard*:

   http://grouper.ieee.org/groups/802/15/pub/TG4b.html

4) *The ISA Working Group SP100 is developing standards for LR-WPAN industrial wireless technology and has created a set of application classes based on criticality/consequence for in-plant wireless systems*:

http://www.isa.org

5) *Paper on performance of IEEE 802.15.4 transceivers in factory environments*:

http://www.cs.utexas.edu/~cdj/wia_files/submissions/008Final.pdf

6) *White paper entitled “Understanding 802.15.4 and ZigBee Networking” by Daintree Networks Inc. that provides a good overview of ZigBee networking, routing, and application message interchange*:

http://www.daintree.net

7) Paperback book entitled “*Low-Rate Wireless Personal Area Networks: Enabling Wireless Sensors with IEEE 802.15.4*”. IEEE Press, 2004. ISN 0-7381-3557-7.