Secure Communication in WMNs (WirelessHART) and its Integration with Legacy HART

Shahid Raza
ICSS-2007
sraza@kth.se

March 12, 2009

Acknowledgment

I am very admiring to all the people in KTH, SICS and ABB who were associated with this work and guided me throughout the thesis period, but it is worth mentioning some of the people who were really kind and helpful.

Firstly, I like to express my gratitude to Dr. Thiemo Voigt for giving me chance to work in the SICS Center for Networked Systems at Swedish Institute of Computer Science (SICS) and supporting me all the way from day first. Secondly, I am very thankful to Adriaan Slabbert for his full support, encouragement, and the effort he put to correct, comment, and clarify my work. Thirdly, I am really grateful to my examiner Dr. Morogan Matei Ciobanu at KTH for trusting my abilities and accepting me as thesis student. Last, but not the least; I am obliged to Krister Landernäs from ABB Västerås for his support and valuable comments during the entire thesis period.

I wish to thank all my teachers at Department of Computer and System Sciences (DSV) at KTH especially Dr. Morogan Matei Ciobanu, Prof. Louise Yngström, and Prof. Sead Muftic for their guidance, motivation, and inspiration for the international students.

I would like to dedicate this work to my parents. They are really special to me and I am thankful to them for their love and support.

This thesis has been performed within the SICS Center for Networked Systems funded by VINNOVA, SSF, KKS, ABB, Ericsson, Saab Systems, TeliaSonera and T2Data.

Abstract

The WirelessHART is a new standard for Industrial Process Automation and Control, formally released in September 2007. WirelessHART specifications are very well organized in all aspects except security as there are no separate specifications that document security requirements, the security is limited and spread throughout the WirelessHART specifications, and it is hard to understand the employed security without reading all the core specifications.

This thesis will provide a comprehensive overview of WirelessHART security, the provided security mechanisms will be analyzed against the possible threats and the solutions will be proposed for the identified shortcomings.

The thesis work also comprises of the ways to integrate the WirelessHART network with the legacy HART network. Different integration options are provided and each differs with the kind of legacy HART network already in use. A secure way of integrating HART and WirelessHART is also proposed by enhancing the capabilities of Adapters and connecting them with the HART Masters rather than slave devices.

Finally the architecture of such a Security Manager will be proposed which will be capable of securing the entire WirelessHART network. A comprehensive and secure key management system is proposed which is capable of random key generation, secure key storage and retrieval, secure and automatic key renewal, timely key revocation, and efficient key distribution.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Wireless Mesh Networks (WMNs) is a kind of Wireless Ad hoc Network where almost all nodes are static but all have routing capabilities. There are many applications for WMNs especially in process automation industry where there is need for secure reliable communication with high bandwidth. WirelessHART is the only standardized solution to provide secure, reliable, and scalable communication in process automation industries. WirelessHART is WMN standard in a wireless sensor based environment.

This chapter will give you general overview of the thesis. It will start with some background and then give a formal statement of problem, the thesis goals, and the methodology used in the thesis. Later in the chapter, we will explain the scope of this thesis and its boundaries. The outline of the thesis will be explained at the end.

1.1 Background

With the advent of Highway Addressable Remote Transducer (HART) in mid-1980s and its standardization in 1986, the industrial process automation systems continued to develop and flourish. HART hybrid (analog + digital) functioning and bi-directional operating capabilities at 4-20mA signal have made HART one of the most prevailing industrial protocols. Currently, HART Communication Foundation (HCF) [**?**] is actively governing HART Protocol. Recently, HCF released HART 7 as wireless extension to legacy HART Protocol and formally named it WirelessHART^{TM}.

WirelessHART (HART 7.1) is a brand new Multihop Wireless Mesh Network Standard for Industrial Process Automation and Control, formally released in June 2008. International Electro-technical Commission (IEC) has approved it as an open standard on September 19, 2008. Wireless Mesh Networks (WMN) is an active research area in IT. There were no standards

in WSN until recently when HCF announced WirelessHART. WirelessHART is specifically designed for industrial process automation that can be applied in monitoring and control applications e.g.: Asset management, process and equipment monitoring, diagnostics and maintenance, etc.

WirelessHART specifications are very well organized in all aspects except security as there are no separate specifications that document security requirements, and security is spread throughout the WirelessHART specifications. Furthermore, the security at Application Layer is not specified by the standard. The Key Management (generation, storage, revocation, and renewal) for all the required keys is left unspecified in the standard.

WirelessHART is claimed to be a secure protocol but some of the basic security requirements are unaddressed in the standard, including: complete end-to-end security while integrating WirelessHART with HART; secure communication between WirelessHART devices and Plant Automation Application Hosts; key management; etc. The WirelessHART standard only provides Authentication and limited Confidentiality services at Data-Link Layer and Network Layer level, by using same keys for both Authentication and Confidentiality.

The *motive* of this thesis is to thoroughly analyze the security requirements for WirelessHART and fill the gap between what is available (regarding security), what is incomplete, and what is left for the user to propose and design. Although we will discuss the security issues in WMN, our main focus will be WirelessHART.

1.2 Statement of the Problem

Investigating, analyzing, and specifying the secure communication mechanisms in Multihop Wireless Mesh Networks (WirelessHART) and integrating it with the Legacy HART Protocol and providing all-round Security Manager for key management that meets the requirements of both the wireless and the backend wired network.

1.3 Project Goals

The goal for this project is to investigate the provided security in the WirelessHART standard and securely integrate the wireless (WirelessHART) technology with the wired technology (HART)-that is already in the market since 1980s. Furthermore, the project will design and Implement Security Manager for the WirelessHART. The ultimate goal is to analyze the provided security mechanisms against the standard security services including:

Confidentiality and privacy, Integrity, Authentication, Authorization, and Accounting for an integrated (wireless and wired) network. The concrete goals of the project include:

- Analysis of Security mechanisms in the WirelessHART Standard and identification of loop holes. The security solutions for the identified shortcomings will be proposed *(This in itself is a very enterprising task as we will be the first to do security analysis of WirelessHART).*

- The integration of the secured WirelessHART network with the unsecured wired HART network. Security in WirelessHART is built-in at Data-Link and Network Layer level while HART is not secured at any level.

- The WirelessHART standard does not provide key management mechanisms. So, the major portion of the thesis will include such a key management (key generation, storage, distribution, renewal, revocation, and scalability) system that fulfills the requirements of all the meshes: IEEE 802.15.4-2006 based WirelessHART Networks; IEEE 802.11 and/or IEEE 802.1 Networks for Gateway - Network Manager communication, Gateway - Plant Automation Application Hosts communication, and Security Manager - Network Manager communication; and HART Network.

- Thesis work will also include the implementation of the WirelessHART Security Manager that will fulfill the need of both the wireless and core/wired part of the WirelessHART network.

- The thesis will be a comprehensive document that will address WirelessHART Security at all levels, and it can later be redesigned for inclusion as *Security specifications* in the WirelessHART standard (This is no doubt the desire of HART Communication Foundation and many other organizations that want to implement WirelessHART).

1.4 Scope

This thesis will fulfill the requirements of a Master's ThesisProject at KTH Sweden. The thesis will be carried out at the Swedish Institute of Computer Science (SICS) Stockholm in collaboration with Asea Brown Boveri (ABB) Sweden. This thesis will deal with the secure communication in Wireless Mesh Networks in general and WirelessHART in specific. WirelessHART is the only available standard for Wireless Mesh Networks at the time of conducting this research. The following figure shows that our scope is limited to the technologies inside.

Figure 1.1: Scope is limited to the technologies inside

1.5 Research Method

As the WirelessHART has just entered the market, there are two or three research articles available on this topic, but these articles do not describe the standard as a whole. As far as security of the standard is concerned, we have no research material available yet, and most probably we will be the first one to research the security issues in WirelessHART. The HCF has released the WirelessHART standard as a set of specifications. So we will be exploring and analyzing the standard from the ground up and looking for security loopholes as well as identifying areas for future research.

For this purpose we will start up with the quantitative approach that is inductive in nature as it helps us answer questions such as how much security WirelessHART provides, to what extent and how often? The use of this approach will really help us to identify shortcomings in the WirelessHART, and we can then perform threat analysis of WirelessHART.

After analyzing WirelessHART security using the quantitative approach we will shift to a qualitative approach that is deductive in nature as it helps us answer questions such as why it is important to secure WirelessHART, how can we secure it, and what should we do to provide a comprehensive solution to secure WirelessHART communication at both wireless and wired realms.

The security mechanisms in WirelessHART standard are spread throughout the specifications and there is no single specification that explains the security issues comprehensively. So we will study the whole standard and find the security mechanisms employed. Later on, we will critically analyze the security mechanisms and try to find some shortcoming (if any). The WirelessHART governing body claims that it is a secure standard but at the same time they state that they have employed security in only the wireless part of the standard not in the complete (wired and wireless) system.

1.6 Thesis Constitution

The tentative outlines for the thesis are:

1. Introduction
2. WirelessHART Security
3. WirelessHART Security Analysis
4. Key Management in Multihop Wireless Mesh Networks (WirelessHART)
5. Security in Integrated WirelessHART and HART Protocols
6. Design and Implementation of Security Manager
7. Conclusion and Future Work

The contact persons in SICS and ABB are:

- Adriaan Slabbert (SICS)
  adriaan@sics.se
- Thiemo Voigt (SICS)
  thiemo@sics.se
- Krister Landernas (ABB)
  krister.landernas@se.abb.com
- Tomas Lennvall (ABB)
  Tomas.Lennval@se.abb.com

Chapter 2

WirelessHART Security

This chapter will start with general overview of multi-hop wireless mesh networks; and explain the specific characteristics of mesh networks and the standardization of wireless mesh networks. The specific features of WirelessHART, as being mesh networking standard, and the employed security in the standard will be discussed later in the chapter.

2.1 Multihop Wireless Mesh Networks

Wireless Mesh Networks (WMNs) are gaining attention with the advancement of wireless technologies like smart antennas and Multi-Input Multi-Output systems. WMN is a new wireless network communication architecture that has the following unique features.

- Every network device act as a router, so all nodes can communicate through multi-hopping.
- Almost all radio nodes are static.
- Use novel radio technology like smart antenna and multiple channels
- Also use connecting devices like gateway for communication between devices
- The network is usually a mixture of wireless and wired devices
- WMNs are self-configured and self-organized

WMNs can be considered as one kind of ad hoc networks where nodes are normally static; but WMNs can also be regarded as wireless sensor networks in the sense that nodes usually contain one or more sensors. So the WMNs are a combination of ad hoc and sensor networks where sensor nodes act as router and hence support multi-hopping. Some of the applications of WMNs

include: home and enterprise networks, network management services, reliable broadband services, industrial process control system, etc. WMNs can be developed and deployed using any of the physical interfaces but the usefulness is more in IEEE 802.11 (Wi-Fi), IEEE 802.15 (PAN), and/or IEEE 802.16 (WiMax).

WMN is an active research area and people are working on different physical interfaces in order to find new applications and usages for the mesh networking. The standardization is important for commercial usage and interoperability between different vendors. New specifications for WMNs are under developed by different standardization task groups of the IEEE. IEEE 802.11s task group is working on the standardization of Wi-Fi with multihop and multi-channel capabilities, IEEE 802.15 task group 5 is working on standardization of personal area network with mesh networking capabilities, and the IEEE 802.16 standard was refined with non line-of-sight (NLOS) and mesh networking capabilities in the IEEE 802.16a standard.

HART Communication Foundation took the initiative of standardization of HART protocol with wireless mesh networking capabilities that meets the requirements of process industry. The project was started in early 2004 and the standard was approved in September 2007; the new standard is formally named *WirelessHART*. International Electro-technical Commission (IEC) has approved it as an open standard in September 2008.

The other Wireless Personal Area Network (WPAN) standards such as Bluetooth and ZigBee have tried to enter into industrial automation but were unsuccessful because of some standard inherited limitations [**?**]. Other protocol such as WibRee and ISA100.11.a:2008 are trying to enter in the industrial applications as well. This thesis will cover only the WirelessHART standard, not the other mesh networking standards by IEEE 802 and ISA. WirelessHART uses the same physical interface as used by IEEE 802 PAN (IEEE 802.15), Wi-Fi, Bluetooth, and ZigBee.

2.2 WirelessHART

WirelessHART is the first open standard for process automation industry specified by HART Communication Foundation (HCF) and approved by IEC. Before the standardization of WirelessHART, there was very slow progress in process automation industry regarding the use of advance wireless networking techniques because interoperability among different product by different vendors was almost impossible. Now with the advent of WirelessHART standard, the vendors have shown greater interest in the standard and developing different products bases on WirelessHART protocol. The

users are also eager to use the new products; and the overall environment and trends in the process automation industry are changing. This change has brought the interest in the wireless network researches and organization to delve deeper in the standard and investigate the feasibility of implementing it for real environments.

After reviewing the standard, we have found some unique features that are very promising to implement it in real world applications. These features are explained in the following sections.

2.2.1 Network Topology

WirelessHART uses wireless mesh networking technologies for communication between devices. In WMNs, every device acts like a router that in turn provides multiple network paths for communication. According to WirelessHART standard ?[2], for each wireless device there should be at least two connected neighbors that can route traffic using graph routing. Mesh topology provides more reliability, have low installation cost, wide coverage, and dynamic network connectivity. The use of mesh networking topology makes WirelessHART more reliable to use in sensitive applications like industrial process automation and control. The following figure shows the WirelessHART network.

Figure 2.1: WirelessHART Network

WirelessHART comprises of five core devices:

- *Field Device (FD)*: A wireless sensor device connected to the actual process.
- *Gateway*: An Access Point that connects wireless network with the plant automation network.
- *Adapters*: It is used to connect wired HART devices with WirelessHART network.
- *Network Manager*: An application for configuring and scheduling for network.
- *Handheld*: Host application residing on the portable device; this device can be connected with any field device. It is normally used for device/network monitoring and/or writing Join key (see section 4.2.1).

Other devices that are the part of complete WirelessHART standard are:

- *Security Manager (SM)*: The Network Manager uses the SM for key management, but the SM can also be used for secure communication in the wired part of the WirelessHART network. Chapter 6 will give the design and implementation of the SM for WirelessHART.
- *Plant Automation Host (PAH)*: These are the applications that reside on some host(s) that use the output of the processes, sensed by the sensor attached to the field devices.
- *Router:* In a mesh network, if a field device has no or less neighboring devices for routing messages then routers can be added in the network for path redundancy. Routers are not sensors like field devices and hence are not attached to the processes.
- *Access Point (AP)*: Normally APs are built into the gateway but they can exist as separate devices. APs connect a gateway to the wireless devices. AP is the entry point to the wireless network from the core network, and it is an entry point to the core network from the wireless network.

2.2.2 Protocol Stack

WirelessHART protocol stack is more or less the same OSI seven layers stack with some extensions for more security and reliability. Security Sub-Layer is add beneath Network Layer for enhanced security and MAC sub layer is added for reliable communication through channel hopping. Like HART protocol, WirelessHART is command oriented; this means that all WirelessHART messages are the combination of commands that flow through the network. Transport PDU is constituted [**?**] by combining transport byte, device status, and one and more commands at the Transport layer and sends

to the Network layer for delivery. Network Layer provides routing and data security. Data link layer is responsible for wireless signaling, security, and reliability. Physical layer finally converts bits into wireless signals and sends them to neighbors at 2.4 GHz frequency (the same used by Bluetooth and ZigBee).

Figure 2.2: WirelessHART Protocol Stack

2.2.3 Legacy support

One of the features that makes WirelessHART a more ready-to-use standard is the provision for legacy HART devices. WirelessHART specifications list Adapters as one of the WirelessHART devices that are used for integrating/connecting the HART devices with WirelessHART network. Depending upon the design of Adapters, one or more HART devices can be connected with the WirelessHART network; but Adapters are not meant for connecting the whole Token passing based HART network with the mesh topology based WirelessHART network. The integration of HART and WirelessHART networks will be discussed in detail in chapter 5.

2.2.4 Security and Reliability

HCF claims WirelessHART to be a secure protocol. Security in WirelessHART is enforced at Network layer and Data-link layer. Data-link layer provides hop-to-hop security between two neighboring devices using Network key; and Network layer enforces end-to-end security between source and destination using session key(s) and/or join key. Section 2.3 will discuss WirelessHART Security in detail.

WirelessHART is considered a reliable protocol. WirelessHART uses 2.4 GHz frequency band which is a free unlicensed portion of the spectrum; the adaptation of this frequency band leads to the interference which is avoided by using Channel Hopping: shuffling frequency channels and using the one which has the least interference. Channel Hopping clearly enhances the reliability of WirelessHART network. Also, WirelessHART uses the concept of Blacklisting i.e. if some frequency band frequently suffers from interference then it can be blacklisted (banned) permanently by an administrator. Reliability is further enhanced by providing multiple paths from source to destination using mesh networking technology.

2.2.5 Intelligent Devices

WirelessHART is a self healing and self organizing wireless protocol, meaning that the devices are able to find neighbors and establish paths with the neighbors by getting channel hopping and synchronization information and measuring signal strength. This device intelligence is a source of long term network performance and expansion.

The wireless nature of WirelessHART makes it easy and feasible to deploy, especially is manufacturing industry where use of cables drastically increases cost. Installation cost of WirelessHART is far less than in case of the legacy HART protocol. In spite of all these advances, WirelessHART is prone to attacks because of its wireless communication medium. The next section will discuss specified WirelessHART security in detail and the next chapter will critically analyze the provided security and try to find any shortcomings.

2.3 WirelessHART Security

Primarily, WirelessHART is based on the mesh networking technology but at the same time it also inherits the features of wireless sensor networks as all the field devices are equipped with one or more sensors. Sensors investigate the actual process. So, the security requirements for the WirelessHART network amalgamate the security requirements for both the mesh network

and the wireless sensor network.

WirelessHART is an IEC-approved standard for industrial process automation and control and is comparatively secure and reliable protocol for the process automation. The field devices collect data about processes and securely send it, as an input, to the other field devices. PAHs can also collect data from the field devices on a secure channel. The routing information, security keys, and the timing information are sent to the devices in a secure way. In short, all data in the WirelessHART network travel in the form of commands and the confidentiality, integrity, and the authenticity of the commands are ensured, while the data travels through the wireless part of the WirelessHART network but not in wired part.

The WirelessHART standard strongly recommends that the data communication in the wired part of the network should be conducted on a secure channel but does not enforce and specify any means to provide security and reliability in a wired network. We will discuss the ways to secure wired part of the WirelessHART network in upcoming chapters; here we will focus on wireless portion security and see how WirelessHART enforces secure communication between the devices.

As we have seen before, the WirelessHART protocol stack is based on the OSI seven layers architecture, but only from network layer onwards, the data (WirelessHART Commands) is protected. The data from the transport to the application layer is clear with no cryptographic protection, but still it fulfills the requirements for the secure and reliable communication in the wireless network.

The figure 4 shows OSI seven layer enabled WirelessHART protocol stack with the security (and reliability) features at different layers.

Figure 2.3: Security at different OSI based layers of WirelessHART

Figure 4 shows that the network and data-link layer are collectively used to provide core security services: Confidentiality, Data Integrity, Source Integrity (Authenticity), and Availability. In the following section we will inspect these security services in details.

2.3.1 Source-to-Destination end-to-end security

The Network Layer is used to provide end-to-end security between the source and destination devices; it also provides routing and transport services. The Network Layer either gets the Transport PDU (TPDU) from Transport layer and sends it toward the destination by enforcing security and providing intermediate routing information, or gets Data-link PDU (DLPDU) from the

data-link layer and processes it accordingly. If the DLPDU is intended for the current device, it will send it to the transport layer for further processing, but if data is destined for another device it will send it back to the Data-link layer. Now, any data that travels from the network layer to the data-link layer is enciphered (except for the NPDU header) and only the destination device is able to decipher it.

All data from the source field device to the destination field device always travel through the gateway because two field devices cannot create sessions between them. Sessions are only created between the wireless devices[1] and gateway, and between wireless devices and the network manager. So, if a field device (source) wants to send data to another field device (destination), it will encrypt the data with the unique symmetric session key and send it to the destination via gateway; the gateway will decrypt the source device's data and encrypt it again with the destination device's session key and send it towards destination as gateway has session with all the field devices.

Any wireless device that is the part of WirelessHART network has four session keys, one Join key, and the Network key. A Handheld device also needs a Handheld Key[2]. Normally, the network layer requires four session keys to create sessions between:

i. Gateway and single wireless device (unicast)

ii. Network Manager and single wireless device (unicast)

iii. Gateway to all wireless devices (broadcast)

iv. Network Manager to all wireless devices (broadcast)

A peer-peer session (direct one-to-one) can also be created between the handheld device and the field device using the Handheld key (see sub-section 2.3.3).

The management and distribution of keys will be discussed in next chapter. Here we will discuss the ways the network layer enforces end-to-end security using these keys. WirelessHART Network Layer PDU (NPDU) is shown is the following table;

The Transport Layer PDU (TPDU)[3] in the table above is an NPDU payload which is always encrypted using Advanced Encryption Standard

[1]Wireless device can be: Field Device, Adapter, and Handheld. Routers are also wireless devices used to enhance reliability by routing traffic to the next hop (only).

[2]Handheld key is use to communicate with a single device using a special high speed superframe [**?**].

[3]TPDU is the actual HART/WirelessHART data consists of Transport Byte, Device status or Device extended device status, and aggregated commands.

Header	SCB	Counter	MIC	NPDU Payload (Encrypted)

Table 2.1: WirelessHART Network Layer PDU

(AES) with a 128 bit key. The Message Integrity Code (MIC), Counter, and Security Control Byte (SCB) collectively form Security Sub-layer for the WirelessHART protocol stack (See table 2.1). Other fields in NPDU are needed for routing of data; for details about these fields please consult Network Management Specification by HCF (HCF-SPEC-85). The three fields in the security sub-layer are used as follows:

i. *Security Control Byte (SCB):* It is used for defining the type of the security employed. First four bits are reserved for future security enhancement and the next four bits define the key type. Till HART 7.1, only three key types are identified. See the figure below for details.

Figure 2.4: Security Control Byte

ii. *Counter* A four-byte nonce counter that is used to create nonce.

iii. *MIC:* It is used for data integrity and source integrity (authentication) between source and destination. The MIC is calculated on the whole NPDU by setting the TTL, counter, and MIC to zero. Four byte-strings are needed to calculate MIC, including:

- NPDU header (a): from control byte to MIC.
- NPDU payload (m): the encrypted TPDU.
- The Nonce: It is 13-byte long and provides defense against reply attacks. The first byte is either all ones (for join response message only) or all zeros. The next 4 bytes makeup the nonce counter; and the remaining 8 bytes form the source address. For detail about constructing this counter please refer to page 51-53 of Network management Specification by HCF (HCF-SPEC-085). The counter field in the security sub-layer is populated with this nonce counter before sending the message.

- AES key: A 128 bit key is needed for calculating MIC; this is the same key which is used for the encryption of NPDU payload.

Network Layer in WirelessHART protocol stack provides three security services: Confidentiality, Integrity, and Authentication. AES in Counter with CBC-MAC (CCM) mode is used to calculate MIC (to provide authentication and data integrity) and encrypting (to provide confidentiality) NPDU payload. Same session key is used for both encryption and MIC.

CCM mode is the combination of counter mode and Cipher Block Chaining-Message Authentication Code (CBC-MAC) mode. The two methods are highlighted below:

i. *AES-CCM CBC-MAC mode:* CBC-MAC mode is used to calculate MIC. CBC-MAC can be used for both plaintext and cipher text as in WirelessHART, and this mode needs exact number of blocks (padding can be used to equalize the last block). Only Encryption is used for calculating and verifying MIC. The four parameters (discussed above in point 3 under MIC) are used to calculate MIC. A formatting function is applied on Unencrypted NPUD header, encrypted NDPU payload, and on Nonce to produce the blocks B0, B1, B2 ... Bi; for details about this formatting function and combination please refer to ?[6]. The following figure shows the working of CBC-MAC mode.

Figure 2.5: AES-CCM CBC-MAC mode for calculating MIC

ii. *AES-CCM in Counter Mode:* Counter mode is used for the encryption/decryption of WirelessHART NPDU payload. Here too, the message blocks are created in the same fashion as above, but no padding is required and blocks can be manipulated in parallel. The counter mode is shown in the figure below.

Till now, we have seen that security sub-layer (under network layer) allows confidential and correct end-to-end communication between the WirelessHART devices, but WirelessHART also provides ways to secure wireless the signal that flows between the two neighboring wireless devices.

Figure 2.6: AES-CCM Counter mode for enciphering NPDU payload

2.3.2 Per-Hop Security

The Data link-layer is used to provide per-hop security between the two neighboring wireless devices using Network key. The Network key is known to all the authenticated devices in the WirelessHART network. Consider the Data Link-layer PDU (DLPDU) below.

0x41	Address Specifier	SN	Network ID	Destination Address	Source Address	DLPDU Specifier	DLPDU Payload	MIC	CRC

Table 2.2: WirelessHART Data-link Layer PDU

The MIC is calculated on the entire PDU (from field 0x41 to DPPDU Payload) using AES-CCM mode (For details see section 2.3.1). The four parameters for the AES CCM mode are:

m: It is the encrypted message; but as the DLPDU is not encrypted so the length of this byte-string is zero.

a: DLPDU from 0x41 to DLPDU payload (shown as shaded portion in the figure above).

N: It is a 13 bytes byte-string that is formed by concatenating the Absolute Slot Number (ASN) [4] and source address. Following table shows its construction.

K: 128 bit Network Key

[4] ASN is the total slots that occurred since network is formed and it is always incremented and must never be reset.

13 Byte-strings	Value	Nonce (N)
First 5 bytes	5-byte ASN	N[0] - N[4] (MSB to LSB)
Next 8 bytes	EUI-64 Source Address	N[5] - N[12][5]
	2-bytes Nickname + zeros	N[11]-N[12] is Nickname, N[5]-N[10] are zeros

Table 2.3: Nonce for DLPDU MIC

DLPDU ensures source integrity (authentication) of the message that flows between the two neighboring devices. The receiving device gets the DLPDU and verifies the MIC; if the calculated MIC is not equal to the MIC in the DLPDU, the packet is discarded.

DLPDU also offers data integrity (not as standard security service against active attacks) using Cyclic Redundancy Check (CRC). CRC is not a cryptographic way to enforce integrity; rather it is just a way to check communication errors as no secret key is used to calculate the CRC. WirelessHART standard uses the 16-bits ITU-T polynomial [**?**] to calculate CRC.

During the joining process, the device has only the Join key but no Network key. The join request is secured with the Join key (shared between the wireless device and the network manager) at network layer level. To be able to communicate with the neighboring devices the WirelessHART device must have a Network key, but as the joining device is not a part of network it needs some known key in order to calculate the MIC. WirelessHART standard specifies a well-known network key (777 772E 6861 7274 636F 6D6D 2E6F 7267) for per-hop communication during the join process (and also for advertising join packets). The bit 3 in the DLPDU Specifier (see figure 8 above) is used to species the key type being used to authenticate the DLPDU. If this bit 3 is set (i.e. 1), the Network key is used to used to authenticate the DLPDU; otherwise, the well-known key will be used.

2.3.3 Peer-Peer Security

All traffic in the WirelessHART network flows through the gateway, but handheld devices can create a direct one-to-one wireless connection[6] with the field device using the Handheld key. In order to establish this connection with the field device, the handheld device first has to join the WirelessHART network using its join key. When the handheld device is a part of the

[6]Handheld can also have direct wired connection with the field device using device's maintenance port but the communication on this connection does not use TDMS based WirelessHART protocol. This type of connection is normally used to write the Join key in wireless devices.

WirelessHART network, it can get the Handheld key (for the specific device) from the Network Manager. The received handheld is used to create a one-to-one direct session with the field device. This session is normally used for device maintenance.

Chapter 3

WirelessHART Security Analysis

Although WirelessHART standard provides recommended (by NIST USA) ways to secure the communication between the wireless devices, the security of an industrial process automation system depends on the complete protection of wireless medium as well as the wired medium. The lack of security at the wired portion of the complete WirelessHART network leads to the new challenges and threats. In this chapter we will evaluate the security and reliability of the complete WirelessHART network by doing threat analysis. Both wireless network and the wired network threats will be discussed. Also, the threats and challenges we can face at the point of integration of the wireless and the wired networks will be discussed.

3.1 Wireless Threats

A threat is an indication of a potential undesirable event [**?**]. The mandatory properties of threats include: Asset under attack, Actor what/who breaches the security, and Outcome of security breach. Optionally, Motive (intentional/unintentional) can be one of the properties of threat. In case of WirelessHART, the asset is either the data stored in one of the devices or the information which flows through the network. Outcome of the security breach is leak or modification of information, or disruption of smooth network traffic.

Now we will enlist the possible threats against WirelessHART and try to find which threats are addressed by WirelessHART and which threats need to be addressed. The threats which are not addressed in WirelessHART lead to the potential vulnerabilities in the standard. The potential threats and their effect on WirelessHART network are discussed below:

3.1.1 Interference

It is an unintentional disruption of radio signal; a signal with same frequency and modulation technique can override the actual signal at the receiver. WirelessHART operates at 2450 (2400-2483.5) MHz frequency band spectrum and has 16 channels and each channel's bandwidth is 5 MHz. This spectrum is shared with IEEE 802.11b/g commonly called Wi-Fi, Bluetooth, and ZigBee. However, the use of Frequency Hopping Spread Spectrum (FHSS) [**?**] (frequency diversity), time diversity, and path diversity almost eliminates the chances of interference but still the strict and sensitive nature of a process automation system requires fail proof[1] reliability of the wireless medium. Failing to provide 100% reliability may lead to catastrophic outcomes. The growth of Wi-Fi, WibRee, ZigBee, Bluetooth etc. devices can make WirelessHART 2.4 MHz frequency band vulnerable to interference in future.

3.1.2 Jamming

It is normally considered an intentional interruption of radio signal when purposely introducing noise or signal with same frequency and modulation technique as used in the target network. WirelessHART is more vulnerable to jamming attacks than interference; the attacker can deliberately introduce radio signals using commonly used Bluetooth devices like cell phone and laptops. In the automation industry, unintentional jamming can also occur as the operating machines can produce sufficient noise that can jam some of the channels.

WirelessHART introduces the concept of channel Blacklisting. If some frequency channel is jammed or is a continuous source of interference, then it can be omitted and channel hopping is restricted to other available channels. In WirelessHART channel Blacklisting is network-wide and is done manually by a network administrator. Blacklisting enhances the reliability of the WirelessHART network but at the same time it limits the number of channels the device can use to send/receive traffic.

In spite of FHSS and 15 available channels, the active attacker can jam the WirelessHART network. The switching of channels in the FHSS is based on pseudorandom sequence. Now if,

a An attacker has knowledge of pseudorandom sequence which may help in calculating actual channel.
(ActualChannel = (ChannelOffset + ASN) % NumChannels) [**?**]

[1] The chances of failure are 0%.

b And has sufficient number of 2.4 GHz (Bluetooth or ZigBee) based devices in WirelessHART range (normally cheap)

c The manufacturing plant has legally deployed Wi-Fi networks in and around WirelessHART network

d The Manufacturing Plant produces sufficient amount of noise signals (which is very common there)

e Some of the channels are already blacklisted

then the active attacker can jam the WirelessHART network. This jamming of the whole or a part of WirelessHART network can block or even damage the manufacturing machinery.

3.1.3 Sybil Attack

This is a classical form of attack which is more common in Network and Data-link layer (DDL), but its base is the Physical layer. In this type of attack, an antagonist can introduce an adverse entity (a node or piece of software) into a WirelessHART network. WirelessHART is a more prone to Sybil attacks at the Physical and Data-link layersl than at the Network layer. WirelessHART uses Network key to authenticate the source of the message at DLL; the Network key is shared between all the WirelessHART devices and it is comparatively easy to find a Network key as compared to device-specific session keys used at Network layer.

An attacker can get the Network key by capturing and cloning any of the WirelessHART devices (as all devices have same Network key); other attributes like network ID, etc. are not considered secrets and an active attacker can easily find them. Once the Network key is exposed to the attacker, it is very easy to launch Sybil attack. A new node (fake WirelessHART device) can be placed in the range of WirelessHART network and this node can send messages to the other devices and can receive messages from them. The success of Sybil attack can lead to the other attacks like tampering, wormhole, Selective Forwarding Attack, Masquerading, DOS etc (discusses below).

Sybil attack at Network Layer is difficult to perform as each device has separate session key to encrypt/decrypt and authenticate Network PDU.

3.1.4 Tampering

The success of Sybil attack at DDL can lead to the tempering of DLPDU. As DLPDU is unencrypted, the attacker can route the packet to its desired direction by inspecting and changing the destination address. This attack is

more effective if the attacker changes the destination address to the source address and sends the packet back to its source. In short, having knowledge of Network key and unencrypted DLPDU, an adversary can seriously damage the normal operations of the WirelessHART network by tampering with the DLPDU and calculating the MIC again to make it authentic.

3.1.5 Collusion

WirelessHART protocol uses CRC to avoid collusion but the changing of few bits will result in discard of packet. WirelessHART uses 16-bits ITU-T polynomial (aka CRC-16) to compute CRC which might not be able to detect insertion attack (see security consideration in [**?**]). This attack can be avoided by better implementation and active coordination between the Physical and Data-link layer especially when the physical layer connection state changes. Also, the concept of time diversity (TDMA based dynamic time slot management) minimizes the collusion in the WirelessHART network. However, multiple hops can increase the chance of collusion in the WirelessHART network.

3.1.6 Exhaustion

Any device that supports the WirelessHART protocol stack and has knowledge of unsecure WirelessHART network parameters (network ID etc.) can send messages to WirelessHART devices using the well-known network key(see section 2.3.2). The fake device can use the well-known key for calculating the MIC over the DLPDU; and can use the Join key (fake) to encrypt and authenticate the NPDU. Although this message will be discarded when received by the Network Manager it consumes network resources along the route from the field device to the Network Manager. If a series of such join attempts are initiated by an active attacker then it can give rise to a serious DOS effect/risk.

3.1.7 Spoofing

Field devices use well-known network key for not only joining the network but also for the advertisements[2]. The adversary can spoof the new joining device by sending fake advertisements and on receipt of the join request it can simply discard it. If the spoofing device is more close to the joining device then the new device will not be able to join the network. If the fake device has access to the valid Network key then the spoofing attack will be more effective and can result in a serious blockage of network traffic.

[2]WirelessHART devices have Advertisement slot that are reserved for the joining devices who want to join the network.

3.1.8 DOS

Denial-of-Service (DOS) is the simple common attack but it is still very effective to interrupt the normal operation of the WirelessHART network. DOS attack against the normal operation of the WirelessHART network can be launched by:

- Flooding the network with the join requests.
- By sending the fake Advertisements to the neighbors.
- By replacing the DLPDU and re-computing the CRC. If DLPDU and corresponding CRC are replaced then the WirelessHART has to verify the message integrity by calculating the MIC. WirelessHART protocol uses AES in CCM for calculating MIC; this is an expensive task which requires strict timing (TsTxAckDelay =1ms [**?**]) requirements to verify the MIC. The unverified packet will be discarded, which results in the retransmission of the packet and consumption of network resources.
- A DOS attack can also be launched by jamming the radio signal (see jamming above).

3.1.9 Traffic Analysis

The NPDU header and DLPDU are un-encrypted and the adversary can easily analyze the WirelessHART traffic. The NPDU header fields e.g. source/Destination addresses, Security Control byte, ANS snippet, and Nonce counter are all sent in clear; also, the DLPDU fields e.g. Address Specifier, Addresses, and DLPDU Specifier are sent in clear. These fields provide enough information to the rival to allow analysis of the network: finding new devices (using join requests), work peak hours, device usage (that can help to make other attacks more effective) etc.

3.1.10 Wormhole

It is one of the most famous attacks in ad hoc networking. WMNs like WirelessHART are also prone to theses attacks. In a wormhole attack, the adversary creates a tunnel between two legitimate devices by connecting them through the stronger wireless link or wired link. The potential WirelessHART devices that the attacker can use to launch wormhole attack are HART devices connected to WirelessHART network through Adapters; the adversary can create a tunnel by connecting two field devices by using their maintenance port (WirelessHART protects this by restricting network access in this mode). A tunnel can also be created by the wireless connection if the Network key (shared between all the devices) and session keys are compromised.

WirelessHART is subjected to wormhole attack if it is using Graph Routing (that supports redundant paths), but if Source Routing is used then the device must use device-by-device route from source to destination. Source Routing provides defense against wormhole attacks but is not reliable, since if any of the intermediate links fail the packet will be lost.

WirelessHART protocol does not provide direct defense mechanisms to fight against wormhole attack. One good solution to this shortcoming is packet leaching [**?**].

3.1.11 Selective Forwarding Attack

The success of Sybil attack can give rise to selective routing attack. Here the compromised node will not forward all packets and selectively drops packets. The worst form is when the node does not forward any packet and creates a black hole, but normally the node selectively discards packets so that it is considered as legitimate and could not be detected by the recovering mechanisms. The Selective Forward attack is more effective if it is backed by proper traffic analysis.

3.1.12 De-synchronization

WirelessHART network has strict timing requirements, and Timer is one of the primary modules in the WirelessHART. The timer module has to meet the timing requirements and keep the time slots (10ms) in synchronization. The MAC sub-layer is responsible for time slotting. Each time a node receives an ACK from its time source, it adjusts its clock. The timing source for a node can be a sender [**?**]; and if the sender is compromised it can disrupt the timing between two nodes and the participating nodes are compelled to waste their resources in synchronization.

Although WirelessHART Standard provides strong security defenses to protect wireless devices, the poor administration or weak implementation of the WirelessHART protocols can put it under attack. Also, the physical protection of the assets in a WirelessHART network is very important.

3.2 Wired/Core network Threats

The wireless medium in WirelessHART protocol in considered secure and reliable and security is not optional and all messages flowing in the wireless portion must adhere to these security requirements. However, the security in the wired medium is neither specified nor enforced. Although the WirelessHART standard specifies that connection between the wired or core network device should be secure, the security is optional in wired portion and the WirelessHART protocol still works without securing the wired medium. This lack of security in the wired portion makes it more vulnerable to attacks. Some of the attacks are discussed below.

3.2.1 Weak or Partial security solutions

The security in the core/wired portion of the WirelessHART standard is optional i.e. the protocol will work without secure links between the wired devices. Even if the security in wired network is enforced, the weak design will put the whole WirelessHART system at risk. Unlike wireless devices, wired devices are not resource constrained and strong security solutions (using asymmetric cryptography) should be provided to protect the wired network. Also the security in the wired network should be enforced among all the devices, not just between Gateway and Network Manager or between Network Manager and Security Manager. The partial security will certainly put the whole system under attack.

3.2.2 Spoofing and Impersonation

This attack is very easy to perform in the absence of security in the core wired network. Even if the wired or core network is secured, the absence of uniformity in the security protocols in wireless and wired medium will make the whole system less defensive against attacks.

The interface between the Gateway and the Network Manager is not specified in the WirelessHART standard. The poor design of this interface can make the whole WirelessHART network vulnerable to attacks. The ultimate point of attack for a smart attacker is the Gateway. The Gateway separates the wireless and wired network, and all WirelessHART network traffic passes through the Gateway.

The Gateway maintains sessions with the wireless devices based on session keys; and wireless devices can access the Gateway through Access Points (APs). Now if the fake gateway (through access points) is able to spoof the nearby wireless devices that *I am the Gateway* then all the traffic from wireless devices will be directed to this gateway. This fake gateway can implement its own fake network manager (if the link between the Gateway and Network Manager is strongly protected), which leads to further attacks against the whole system.

The above attack is possible because one of the shortcomings in the WirelessHART is the lacking of two-way authentication, i.e. Network Manager checks the authenticity of the wireless devices (based on join key), but the wireless devices cannot check the authenticity of the Network Manager. The fake Network Manager can spoof the devices.
The fake gateway and the network manager can collectively spoof the other legitimate devices and gain control of the WirelessHART network. The spoofing results in impersonation or masquerading, i.e. the wireless devices will assume that they are communicating with the legitimate gateway but the gateway is masqueraded.

3.2.3 DOS

In the WirelessHART network, the wired/core[3] portion is more prone to DOS than the wireless part. The wireless part has multiple links, multiple channels, and multiple time slots. On the other hand wired/core network devices normally have just one link. If the link between the core network devices is wireless like Wi-Fi then this is even more prone to DOS attacks, e.g. the failure of Wi-Fi link between the Gateway and the Network Manager will stop the functioning of the whole system.

The reliability of the core portion is a serious concern while designing WirelessHART network. The delivery of the message can be verified by acknowledgement (ACK), but the path redundancy is not available in the core network portion. DOS attacks can easily be performed by flooding or jamming the Wi-Fi link between the core network devices. Main threats and their defense mechasims, in the core/wired part of the WirelessHART network, are shown in the table below:

As the security in the core network is undefined we cannot precisely enlist threats, but it can be concluded that, in the absence of security in the core wired network, wireless network cannot function in a secure way. In order to provide secure and reliable communication in the wired network

[3]The link between the wired/core network devices can be wired or wireless. So by wired network we mean the core network from Gateway onward (Network Manager, PAH, Security Manager, and other specific application like Assets Manager)

we will design a Security Manager. The last chapter shows the design and implementation of Security Manager that will enforce security in the core network along with meeting the requirements of the wireless network.

3.3 Main Shortcoming in WirelessHART Security

Some of the clear-cut shortcomings in WirelessHART standard are:

1. Security of the connection between the Gateway and the Network Manager is optional, i.e. WirelessHART standard does not enforce or specify security mechanisms for the protection of the link between the Gateway and Network Manager; but it highly recommends that this connection should be secured. Security at network layer by protecting the NPDU is enforced at this link.

2. WirelessHART does not enforce and specify security mechanisms to protect the link between the Security Manager and Network Manager, neither the link nor the data; but recommends that this link should be secured.

3. Also no security mechanisms are enforced to protect the connection between the Gateway and the host application.

4. The integration between the WirelessHART network (secure) to the HART network (unsecure) is not specified.

5. One-way authentication

6. No path redundancy in the core/wired network

7. One of the notable shortcomings in the WirelessHART standard is the lacking of key management. Although it specifies that Network Manager will get security keys from the Security Manage and distribute them accordingly but it does not specify the ways to generate, renew revoke, store, and vet keys.

8. The design and functions of the Security Manager are not comprehensive in the WirelessHART standard. It simply specifies that Security Manager is used to generate key for WirelessHART.

9. WirelessHART standard provides Confidentiality, Integrity, and Authentication security services for the wireless part but there are no security mechanisms in the standard to provide Authorization (Access Control), Accounting, and Non-repudiation security services for the WirelessHART network.

10. The security mechanisms to protect the WirelessHART network are not specified in the form of a comprehensive document: these mechanisms are spread in all the WirelessHART specifications. It is very hard for the designers and developers to implement the security services without exploring the entire WirelessHART specifications.

11. Last, but not least, WirelessHART standard does not specify the ways to securely integrate the HART and WirelessHART network. However, it provides the ways to add HART devices to the WirelessHART network using Adapters.

3.4 Overcoming Security Shortcomings

In section 2.3, we have seen that WirelessHART standard enforces security at different levels by using strong cryptographic techniques like AES. Due to the sensitive requirements of the industrial process automation and control systems, WirelessHART standard has to enforce security with fail proof reliability from the field devices to the host applications. Unfortunately the WirelessHART standard only provides the mechanisms for the security and the reliability of wireless part and does not specify the ways for secure and reliable communication among the wired or core network devices, not even between the main WirelessHART devices like Gateway to Network Manager and Network Manager to Security Manager. The WirelessHART standard only recommends that the communication in the wired network should be secured, but the level of security is neither specified not enforced.

In this chapter we have analyzed WirelessHART security and identified the shortcomings. In coming chapters we will provide the ways to overcome these shortcomings. The next Chapter will elaborate the key management in the standard and highlight the limitations of the WirelessHART regarding key management. Chapter 5 will provide ways to securely integrate HART and WirelessHART networks. The Last chapter will provide solutions to the rest of the shortcoming by designing and developing the Security Manager for the WirelessHART.

OSI Layer	**Security Threat**	**General/WirelessHART Defense Mechanism**
Physical	Interference	Channel hopping and Blacklisting.
	Jamming	Channel hopping and Blacklisting.
	Sybil	Physical Protection of WirelessHART devices.
	Tampering	Protection and Changing of Network key.
Data-Link	Collusion	CRC and Time diversity.
	Exhaustion	Protection of Network ID and other information that is required to joining device.
	Spoofing	Use different path for re-sending the message.
	Sybil	Regularly changing of Network key.
	De-Synchronization	Using different neighbors for time synchronization.
	Traffic Analysis	Sending of dummy packet in quite hours; and regular monitoring WirelessHART network using Handhelds etc.
	Eavesdropping	Network Key protects DLPDU from Eavesdropper.
Network	Wormhole	Physical monitoring of Field devices and regular monitoring of network using Source Routing. Monitoring system may use Packet Leash techniques [**?**].
	Selective forwarding attack	Regular network monitoring using Source Routing.
	DOS	Protection of network specific data like Network ID etc. Physical protection and inspection of network.
	Sybil	Resetting of devices and changing of session keys.
	Traffic Analysis	Sending of dummy packet in quite hours; and regular monitoring WirelessHART network using Handhelds etc.
	Eavesdropping	Session keys protect NPDU from Eavesdroppers.

Table 3.1: Attacks on Wireless portion of WirelessHART

Security Threat	**Defense Mechanism**
Spoofing	Implementation of security in core network and excellent architecture of gateway.
Masquerading	Use of PKI in the core network will eliminate this issue if carefully implemented.
DOS	Eliminating illegal access to the legal network, proper monitoring and administration of network. (There is no definite solution against DOS attacks)
Interference/ Jamming	Better to use Wired medium between Network Manager and Gateway (but wireless link can be provided for redundancy and hence reliability). The redundant device can minimize this problem.
Eavesdropping	Physical protection of wires (OR Wi-Fi using WPA/RSN).
Social Engineering	Protection of device and network secrets such as passwords through education and reminders.

Table 3.2: Attacks on Core/Wired portion of WirelessHART

Bibliography

[1] *HART Communication Foundation.* `http://www.hartcomm2.org/index.html` (2008-10-15)

[2] Tomas Lennvall, Stefan Svensson, Fredrik Heklan, *A Comparison of WirelessHART and ZigBee for Industrial Applications.* IEEE International Workshop on Factory Communication Systems, 2008. WFCS 2008 (ISBN: 978-1-4244-2349-1), Pages 85-88

[3] *Network Management Specification.* HCF-SPEC-085, Revision 1.1, page 55

[4] *WirelessHART Device Specification.* HCF-SPEC-290, Revision 1.1

[5] W. Simpson, *PPP in HDLC Framing.* Network Working Group, Request for Comments (RFC): 1549; December 1993

[6] Christopher Alberts, at al., *Managing Information Security Risks: The OCTAVE Approach.*Addison Wesley July 09, 2002 (ISBN: 0-321-11886-3)

[7] *Frequency Hopping Spread Spectrum* (FHSS). `http://en.wikipedia.org/wiki/Frequency-hopping_spread_spectrum(2008-10-01)`

[8] *TDMA Data Link Layer Specification*, HCF-SPEC-075, Revision 1.1, page 48

[9] Yih-Chun Hu, et al., *Wormhole Attacks in Wireless Networks.* IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 2, FEBRUARY 2006.

[10] Jianping Song, et al., *WirelessHART: Applying Wireless Technology in Real-Time Industrial Process Control.* IEEE Real-Time and Embedded Technology and Applications Symposium, DOI 10.1109/RTAS.2008.15

[11] *Safe as Milk.* Captain Beefheart, Zoot Horn Rollo, Winged Eel Fingerling, Alex Snouffler, John French. Budda Records 1969.

[12] *Title of document*. List of authors in the order they appear in the document Name of publisher, or other remark and year of publication. Document number or version number is good to include.