UNIVERSITY OF VAASA

SCHOOL OF TECHNOLOGY AND INNOVATION

COMMUNICATION AND SYSTEM ENGINEERING

Eshun Frederick Abeku

WirelessHART: Wireless System for Process Automation

Master`s thesis for the degree of Master of Science in Technology submitted for inspection, Vaasa, 19 April 2019.

Supervisor Professor Mohammed Elmusrati

Instructors Professor Mohammed Elmusrati

ACKNOWLEDGEMENT

I would like to express my deepest gratitude to Professor Mohammed Elmusrati who supervised this thesis work, for his time and encouragement throughout this thesis work and my education in University of Vaasa.

I wish to thank all the teaching staff of the department for the impact each of you have had on my studies.

I am very grateful to my wife Sarah Bennett-Lartey and daughter Naana Eshun for all the support and encouragement I received during my studies.

Lastly, I would thank my parents Mr. Anthony Eshun and Mrs. Ernestina Eshun and my siblings Frank, Naana, Rita, and Michael, thank you all for the support and encouragement throughout my studies.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

3DES	Triple Data Encryption Standard
AES	Advance Encryption Standard
AL	Application Layer
AP	Access Point
APDU	Application Protocol Data Unit
ASCII	American Standard Code for Information Interchange
BGWK	Broadcast Gateway Key
BNMK	Broadcast Network Manager Key
CRC	Cyclic Redundancy Check
DES	Data Encryption Standard
DLPDU	Data-Link Protocol Data Unit
DLL	Data-Link Layer
DoS	Denial of Service
DSSS	Direct-Sequence Spread Spectrum
FD	Field Device
FHSS	Frequency Hopping Spread Spectrum
FSK	Frequency Shifting Key
GF	Galois Field
HART	Highway Addressable Remote Transducer
IEC	International Electrotechnical Commission
MAC	Medium Access Control

NK	Network Key
NL	Network Layer
NM	Network Manager
NPDU	Network Protocol Data Unit
OSI	Open System Interconnection
PL	Physical Layer
PKI	Public Key Infrastructure
PPDU	Physical Protocol Data Unit
PSK	Phase Shift Key
QPSK	Quadrature Phase Shift Key
SM	Security Manager
TDMA	Time Division Multiple Access
TL	Transport Layer
TPDU	Transport Protocol Data Unit
UGWK	Unicast Gateway Key
UNKM	Unicast Network Manager Key
WMN	wireless Mesh Network
WSN	Wireless Sensor Network

UNIVERSITY OF VAASA

School of Technology and Innovation

Author:	Eshun Frederick Abeku
Topic of the thesis:	WirelessHART (Wireless communication for automation)
Department:	Department of Computer Science
Degree:	Master of Science in Technology
Master's Programme:	Communication and Systems Engineering
Supervisor:	Professor Mohammed Elmusrati
Instructors:	Professor Mohammed Elmusrati
Year of entering the University:	2013
Year of completing the thesis:	2019
Number of pages:	70

ABSTRACT

WirelessHART is a wireless communication protocol for process automation applications. WirelessHART was first introduce in September 2007 by the HART Communication Foundation, and the main aim was to add wireless capabilities to the already existing HART technology.

WirelessHART has five main components namely Gateway, Field device, Network manager, adapter, Security Manager, and Router. The WirelessHART protocol was built based on the Open System Interconnection (OSI) of seven layers, but the WirelessHART has five layers; Physical, Data-Link, Network, Transport, and Application Layer. It employs many processes to ensure data; Confidentiality, Authenticity, Integrity, Availability, and Data freshness.

Key Management is very critical in securing the WirelessHART network. The Security manager is responsible for the key management in the network. The Network Manager is responsible for assigning and allocating the keys in the network.

The WirelessHART is not different from attack on any other wireless technologies. Attacks like Interference, Jamming, Tampering, Sybil, Collusion, Spoofing, Exhaustion, Wormhole, De-synchronization, Selective Forwarding, Traffic analysis, Misdirection, Hello flooding and Sinkhole.

WirelessHART uses the Advance Encryption Standard (AES) to secure the network against attackers. The AES is made up of three parts, Cipher, Inverse cipher and key expansion.

KEYWORDS: WirelessHART, HART, Communication, Open system Interconnection,

Key management, Security, Encryption, Decryption

CHAPTER 1

1.1 Introduction

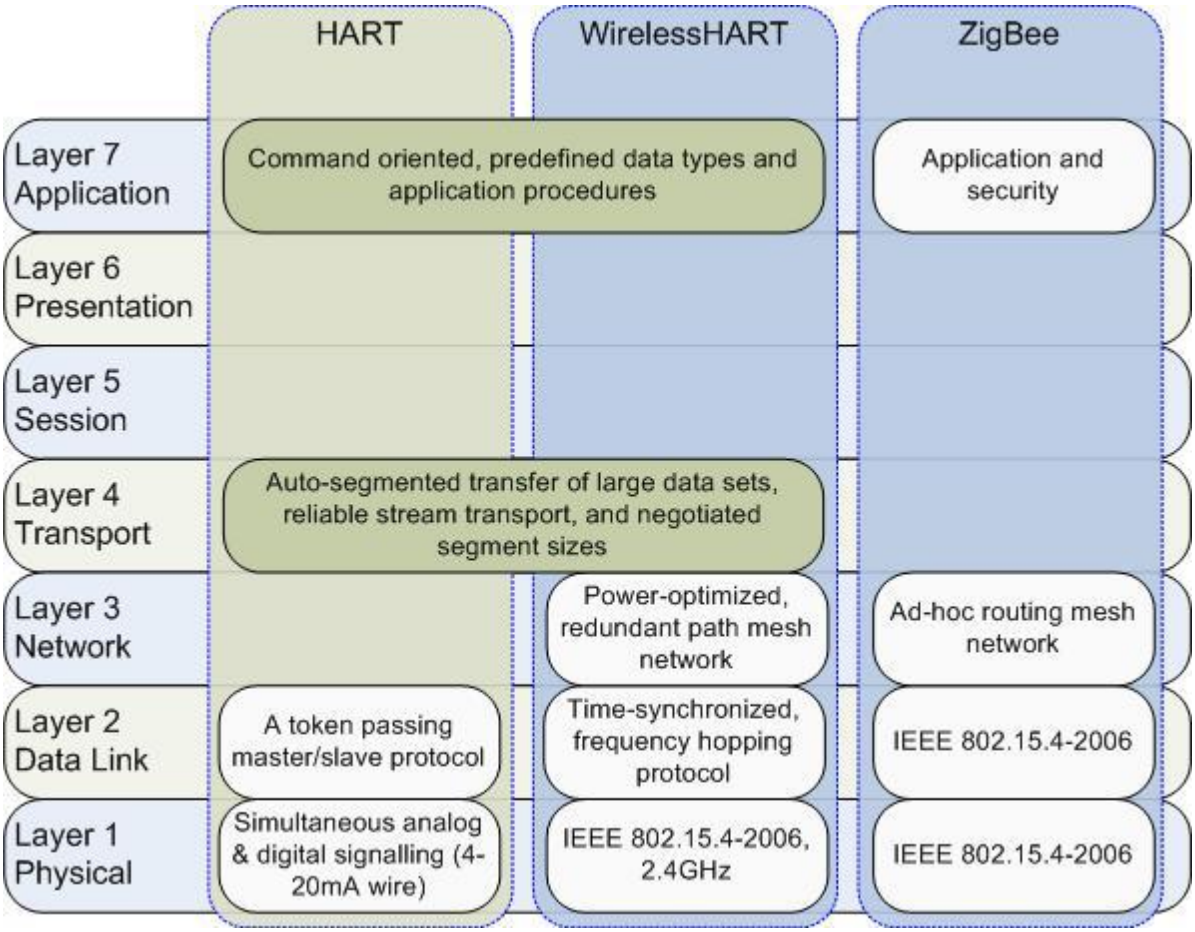
WirelessHART is a HART Communication protocol for automation applications (Raza & Voigt 2010). The WirelessHART give very strong wireless competences to HART technology and upholds compatibility with current HART devices, commands and tools. WirelessHART was primarily planned to use mesh network technology, in a mesh network a device can functions as a router for messages from the other device. WirelessHART uses IEEE 802.15.4 2.4GHz broadband for data transmitting (Raza S. , 2010).

The WirelessHART application targets sensor and actuators, rotating equipment such as kiln dryers, environmental health and safety applications like safety showers, condition monitoring, and flexible manufacturing where parts of the plants can be reconfigured for specific product (Mark Nixon, 2012).

WirelessHART also can group extension to the core HART protocol, thus guaranteeing new devices such as vibration monitoring would be fully supported (Mark Nixon, 2012). WirelessHART offers protected, dependable and competent communication in process automation industries. WirelessHART is a wireless Mesh Networks (WMNs) standard in a wireless sensor environment (Raza S. , 2010).

Before the HART communication released the WirelessHART technology, there were technologies like ZigBee and Bluetooth were used in office and manufacturing automation (Mark Nixon, 2012). These technologies could not meet the strict requirements of industrial control. Both ZigBee and Bluetooth cannot be depending on when it comes to end-to-end wireless communication delay (Mark Nixon, 2012). ZigBee and Bluetooth do not support frequency hopping. ZigBee network works on the same motionless channel throughout its entire lifetime. The use of stationary channel in ZigBee networks makes it more helpless to noise and interference, thus making it impossible for ZigBee to be viewed as strong enough for a harsh radio frequency environment that frequently occurs in industrial applications. ZigBee has low transmission rate, low power wireless with no built-in channel hopping technique, while Bluetooth also assumes a quash static network which is not accessible enough to be used in a very huge control system (Mark Nixon, 2012).

The figure below is the protocol stack of HART, WirelessHART, and ZigBee. The protocol stack comprises of seven layers and these are: Physical, Data link, Network, Transport, Session, Presentation, and application layer



(Lennvall, Svensson, & Hekland, 2008)

Figure 1 HART, WirelessHART, and ZigBee protocol stack

1.2 ISA100.11a

Another communication standard that is same as the WirelessHART is the ISA100.11a (Petersen & Carlsen, 2011). The ISA100.11a was released in 2008. The main goal of the ISA100.11a is to provide protected and a more dependable wireless communication for static, portable and moving devices for non-critical monitoring and control applications (Mark Nixon, 2012).

What differentiate between the ISA100 and WirelessHART lies in the application layers (Petersen & Carlsen, 2011). The ISA100 was intended to take care of handling, in addition to HART commands also Fieldbus foundation, Profibus, and Modbus. ISA100 standard possess a management role that support management in five areas within the network and across all the architecture. Accounting, Configuration, fault, performance, and security are the five management areas. The management

service consists of a device management application process that resides on all ISA100.11a and on one or more system manager application that resides on a small subset of devices. The design criteria of ISA 100 include the following (Mark Nixon, 2012):

- Flexibility
- Multiple protocol support
- Use of open standards
- Multiple Application support
- Dependability (error detection, Channel hopping)
- Determinism (TDMA, QOS support)
- Security

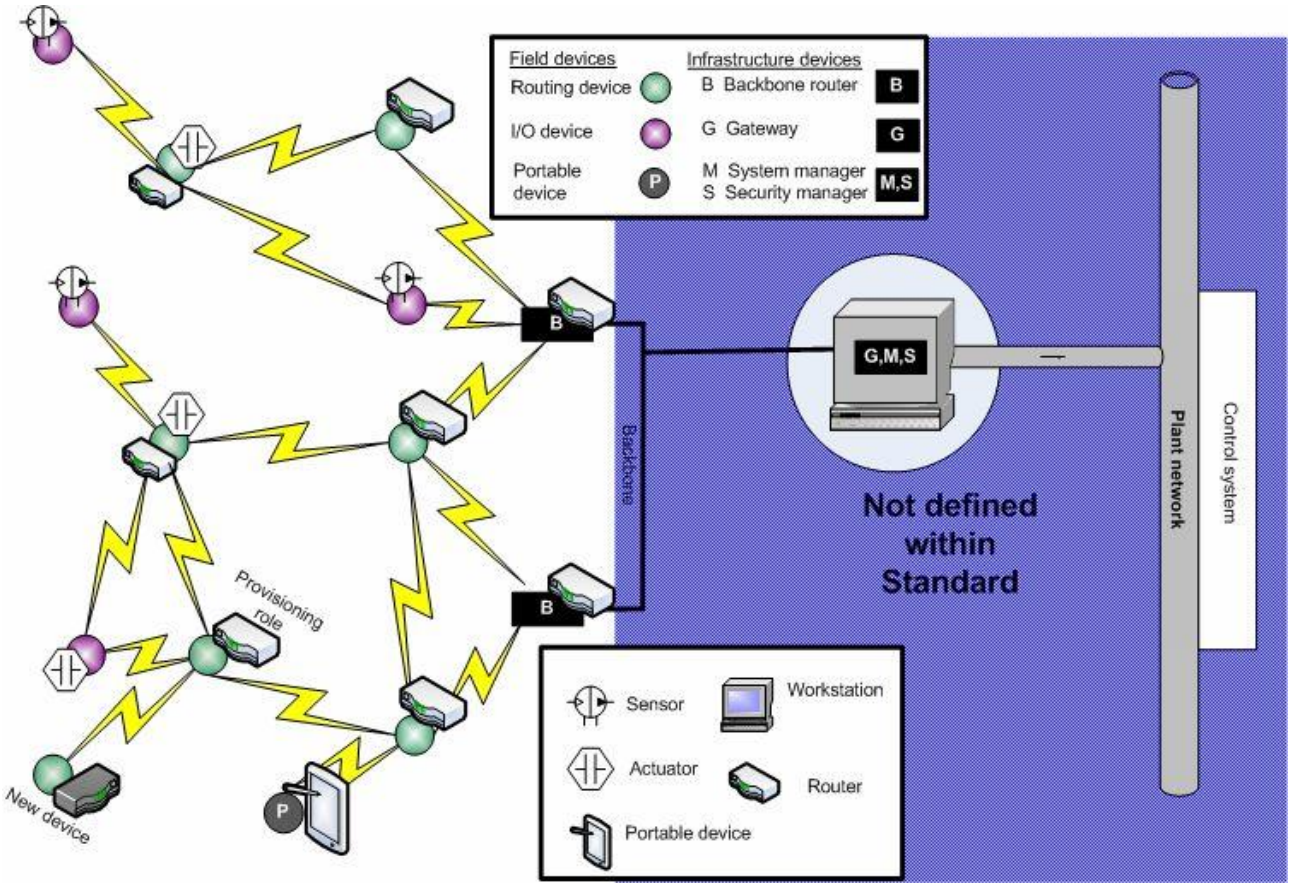


Figure 2 ISA100.11a architecture (Mark Nixon, 2012)

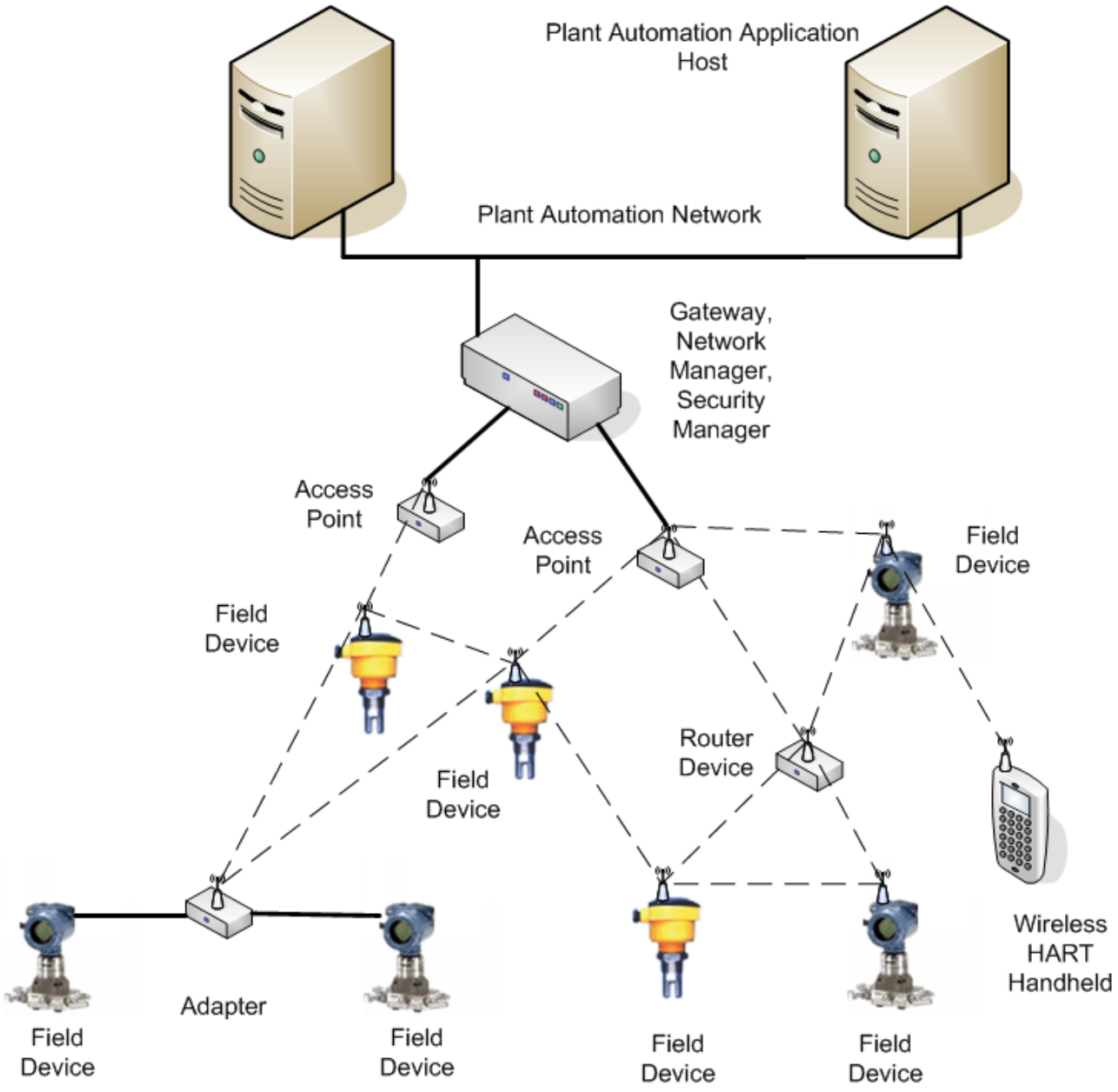


Figure 3 WirelessHART Architecture *(Mark Nixon, 2012)*

1.3 Purpose of the Thesis

The main objective of this thesis work to comprehensively analyze the WirelessHART technology and why it is better than other wireless technologies.

1.4 Outline of the Thesis work

An outline of this thesis is given in details as presented below

Chapter 1 contains the introduction of the thesis work and the purpose of the whole thesis.

Chapter 2 gives briefs discussion on the Open system Interconnection. In the same chapter the HART and WirelessHART technologies are discussed.

Chapter 3 Key management of the WirelessHART is discussed.

Chapter 4 discuss all the security concerns of the WirelessHART.

Chapter 5 present the WirelessHART threat/ attack, where all the security threats are discussed into details

Chapter 6 talks about the cryptographic solution

2 CHAPTER 2

2.1 Open System Interconnection (OSI) Model

The Open System Interconnection (OSI) model was established in 1940s by the International Organization for Standardization (IOS) (Forouzan, 2007). The function of the OSI is to demonstrate how to launch communication between different systems without fluctuations to the logic of the underlying hardware and software. The Open System Interconnection (OSI), is known not to be a protocol, but it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable (Forouzan, 2007). The OSI consist of seven layers namely Physical, Data link, Network, Transport, Session, Presentation, and Application layers as shown in the figure below.

Application
Presentation
Session
Transport
Network
Data link
Physical

Table 1 OSI model *(Forouzan, 2007)*

HART and WirelessHART

2.2 Highway Addressable Remote Transducers (HART)

The highway Addressable Remote Transducer (HART) is a product of the FieldComm group, which was first introduced in the 1990s and it has gone on to become an IEC standard (FieldComm Group, 2018).

According to the HART Communication Foundation group HART is said to be the biggest digital communication technology used in the process industries with more than 400 million field instruments supporting the HART technology installed. HART is a global standard for sending and receiving digital communication across the 4-20mA analog loop that bridges most of the field instruments to the distributed control system (Raza & Voigt, 2010).

HART is a two-way communication protocol that allows data access between an intelligent field and a host system. A host system can be in the form of a software application from handheld device, or computer to a plant process control, asset management, and safety and from systems that uses control platforms.

2.2.1 Structure of HART protocol

The HART communication protocol was build based on the Open System Interconnection (OSI) (Forouzan, 2007). Unlike the OSI which is made up of seven different layers namely physical, data-link, network, transport, session, presentation and the application layers, the HART communication has all the layers except for the session and the presentation layers (Madduri & Jonnalagadda, 2012).

OSI LAYERS	HART Layers
Application	HART commands
Presentation	
Session	
Transport	End-to-end communication
Network	Routing
Data link	HART protocol rules. Master-slave protocol
Physical	Bell 202, AFSK-bus

Table 2 HART Communication protocol *(Madduri & Jonnalagadda, 2012)*

2.2.2.1 ***Physical Layer (PL)***

The physical layer of the HART communication protocol adopts the frequency shifting key (FSK) process to interact with other devices. Analog and digital signals are supported at the same time without interference (Madduri & Jonnalagadda, 2012).

2.2.2.2 ***Data-Link layer (DLL)***

Data-link layer of the HART communication protocol is in-charge of communications that place between devices in the system. In the data-link layer there can be one or two master's in systems that interact with the field device to undertake different task (Madduri & Jonnalagadda, 2012). The Data-link layer is between the physical and network layers. The Data-link layer transfer frames from physical layer to the network layer and vice versa.

2.2.2.3 ***Network Layer (NL)***

The network layer of the HART communication protocol is the one that is responsible for the routing, data transfer, and for security purposes. This layer also takes care of the source to destination of a packet between two systems on the same network (Madduri & Jonnalagadda, 2012).

2.2.2.4 ***Transport Layer (TL)***

HART protocol transport layer is the one responsible for data transporting from one device to another. The transport layer makes sure to check the status of the transporting data to make sure they arrived at its destination safely and intact (Madduri & Jonnalagadda, 2012).

2.2.2.5 ***Application Layer (AL)***

The application layer is responsible for command oriented (read and write), predefined data type, and the application procedures. Users get access to service through the application layer. These commands are classified as Universal, Common practice, Device specific, and, Device family commands (Madduri & Jonnalagadda, 2012).

Universal command	Common Practice Commands	Device Specific Commands
• Read manufacturer and device type • Read Primary Variable (PV) and unit • Read Current output and percentage of range • Read up to four pre-defined dynamic variables • Read or write eight-character tag, 16-character descriptor date • Read or write 32-character message • Read device range values, units and damping time constant • Read or write final assembly number • Write polling address	• Read selection of up to four dynamic variables • Write damping time constant • Write device range values • Calibrate (set zero, set span) • Set fixed output current • Perform self-test • Perform master reset • Trim PV zero • Write PV unit • Trim DAC zero and gain • Write transfer function (square root/linear) • Write sensor serial number • Read or write dynamic variable assignment	• Read or write low-flow cut-off • Start, stop, or clear totalizer • Read or write density calibration factor • Choose PV (mass, flow, or density) • Read or write material or construction information • Trim sensor calibration • PID enable • Write PID set point • Valve characterization • Valve set point • Travel limits • User units • Local display information

Table 3 HART commands *(FieldComm Group, 2018)*

2.3 HART Packet Structure

Preamble	StartByte	Address	Command	ByteCount	Status	Payload	Checksum

Table 4 HART Packet structure *(Lorente, 2015)*

Preamble: 5-20 bytes with the value of 0xFF (Lorente, 2015).

StartByte: The type of message determines the value of the StartByte. It can be master to slave. Slave to master, it also has the address format, either short or long frame depending on the HART revision (Lorente, 2015).

Address: Two frame types, short and long. For short frame its only one byte and one bit to differentiate between the two masters and another bit to point to burst mode packets. With long frame format it contains 5bytes and the field device is 38 bits (Lorente, 2015).

Command: The command field is a 1byte numeric value which encode the master commands. These commands are Universal, Common-Practice and the Device-Specific (Lorente, 2015).

Byte Count: This field tells the length of the message. The receiver can differentiate the payload from the checksum. Sum of the status and the payload byte determines the byte amount (Lorente, 2015).

Status: Bytes are included in responses from the slaves and it's also have health status. These bytes tell if the communication was a success or failure. If the response is positive these bytes a zeroed on the slaves. The masters are not obliged to use these 2 status bytes (Lorente, 2015).

Payload: Data associated with command. This can also be insignificant depending on the command (Lorente, 2015).

Checksum: It is an XOR of all byte from the start byte to the last byte of the data. It is also known as parity (Lorente, 2015).

Attributes	HART	WirelessHART
Physical layer	4-20mA wiring	IEEE 802.15.4-2006
Data-link Layer	Token passing	TDMA & FHSS
Network Layer	Undefined	Defined
Application Layer	Legacy HART	Legacy HART
Security	No	Mandatory

Table 5 Comparison between HART and WirelessHART *(Raza & Voigt, 2010)*

Field Name	Length (Bytes)	Purpose
Preamble	5-20	Synchronization and carrier detection
Start Byte	1	Master Number
Address	1-5	Slave, Master and Burst Mode
Command	1	Numerical value of the command to be executed
Byte Count	1	Data field size
Status	Master (0) Slave (2)	Execution and Health reply
Payload	0-253	Command data
Checksum	1	XOR of all bytes from start Byte to the last byte of data

Table 6 Dissection of a HART packet (Lorente, 2015)

2.4 WirelessHART

WirelessHART is a wireless communication protocol for process automation applications (Konovalov, Neander, Gidlund, Österlind, & Voigt, 2011) .

WirelessHART communication was first introduced by the HART Communication Foundation in September 2007 (Song, et al., 2008). WirelessHART add wireless abilities to the HART technology and at the same time preserving compatibility with already HART devices, commands, and tools (Chen, Nixon, Han, Mok, & Zhu, 2014).

The WirelessHART was built to use mesh network technology. A device can be used as a router to receive or send message from other devices (FieldComm Group, 2018). WirelessHART has five main components namely Gateway, field device, network manager, adapter, security manager, and a router.

2.4.1 **Field Device (FD)**

The field device is a sensing device that is used for sensing functions. These devices which are movable devices for example phone, laptops and any other communication has in them an in-built WirelessHART communication features making it possible for devices to interconnect with each other (Petersen & Carlsen, 2011).

2.4.2 **Access Point (AP)**

When the gateway wants to have communication with the wireless devices it must seek access permission from the access point (Petersen & Carlsen, 2011).

2.4.3 **Gateway**

The gateways give communication access to the devices and the host applications. It is an access point where the WirelessHART network and the automation network are connected and allowing data to be transferred between them (Petersen & Carlsen, 2011).

2.4.4 **Adapter**

The main responsibilities of the adapters are to connect the already wired HART devices to the WirelessHART devices (Madduri & Jonnalagadda, 2012).

2.4.5 **Network Manager (NM**)

The network manager of the WirelessHART is the one responsible for managing all the network configurations, scheduling the communications between devices, managing the messages routes and checking the network health. The network manager can be an in-built into the gateway, host application or the automation controller (FieldComm Group, 2018).

2.4.6 **Security Manager**

The security manager is responsible for making sure they give strong security and protection communication to the wired part in the WirelessHART network against attackers (Raza S. , 2010).

2.4.7 **Routers**

The routers give all the devices the capabilities to routes in the WirelessHART (Mark Nixon, 2012).

2.4.8 **Handheld**

They are WirelessHART devices which plant engineers and other field workers used on the field, which are connected to field devices. Sometimes they serve as monitoring devices or writing join key, configuration, diagnostic, and calibration (Mark Nixon, 2012).

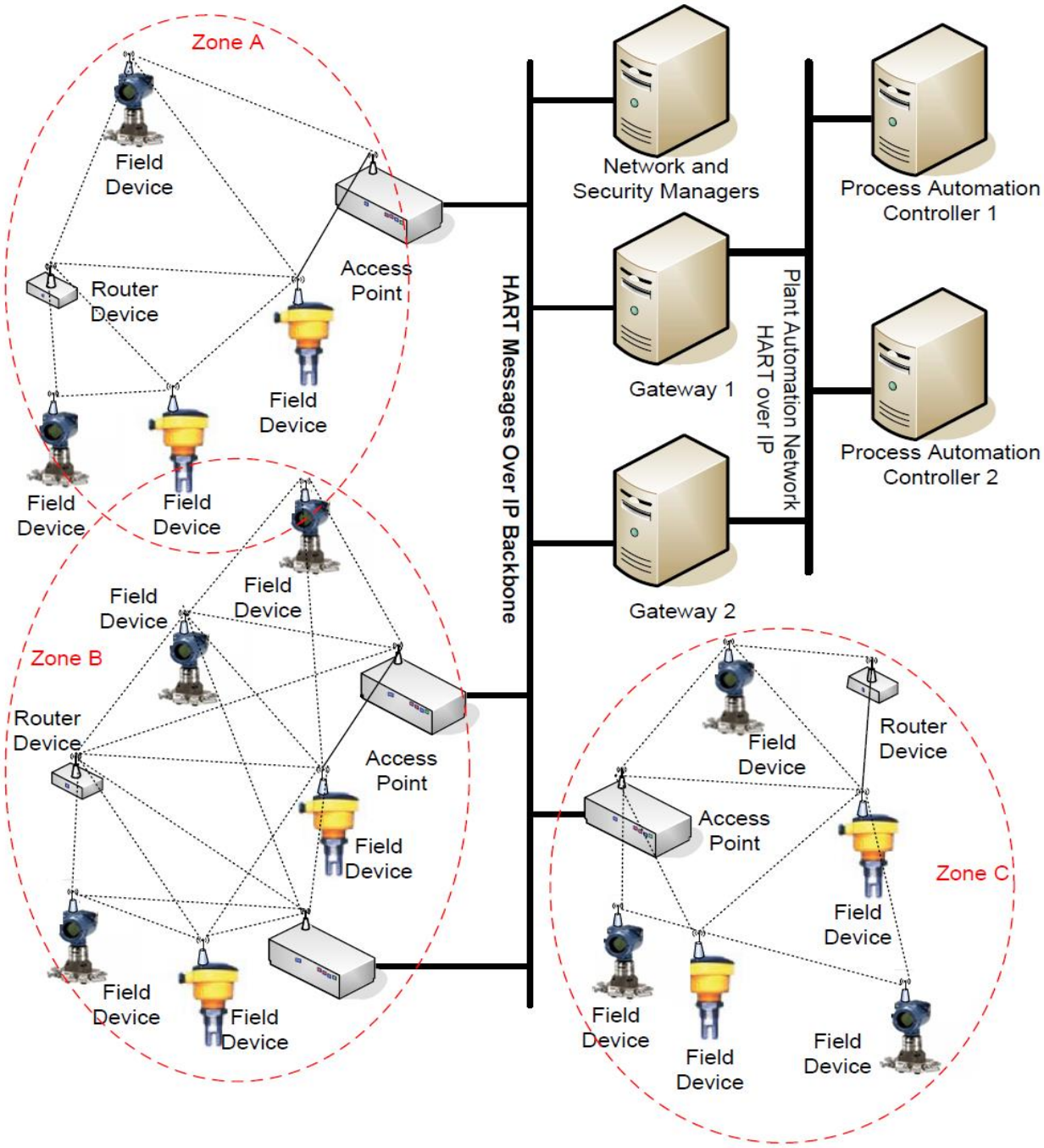


Figure 4 connected WirelessHART devices *(Mark Nixon, 2012)*

2.5 Structure of WirelessHART Protocol

The table below shows the architecture of the WirelessHART protocol. The WirelessHART protocol is like that of the HART protocol was build based on the Open System interconnection (OSI) of seven layers. The fig below shows the WirelessHART protocol stack with five layers namely physical, data-link, network, transport, and the application layers.

Application Layers
Transport Layers
Network Layers
Data-Link Layer
Physical Layer

Table 7 WirelessHART communication protocol *(Forouzan, 2007)*

2.5.1 **Physical Layers**

The physical layer of the WirelessHART was build based on the IEEE802.15.4-2006 2.4GHz DSSS physical layers. Radio characteristics like signaling methods, signaling strength and device sensitivity are define on this layer (Madduri & Jonnalagadda, 2012). Quadrature Phase shift key (QPSK) is the modulation used by the physical layer of the WirelessHART. Bits are modified into wireless signals and sends to other layers at 2.4GHz frequency (Raza S. , 2010).

2.5.2 **Data-Link Layers (DLL**)

The WirelessHART Data-Link Layer (DLL) is also based on IEEE802.15.4-2006 MAC. The DLL prolong the working of the MAC by defining a fixed 10ms time slot. This time slots are well managed by what is known as super frames, that groups a sequence of successive time slots. A super frame is known to be periodic. In WirelessHART network all super frames begins with absolution slot number (ASN) 0; which represent the time when the first network was created (Mark Nixon, 2012). The main function of the Data-link layer of WirelessHART for radio synchronization (Petersen & Carlsen, 2011). It also functions as the one that send and receive frames with other radio devices. The Data-Link Layer (DLL) is divided into two, Logical link control (LLC) and Medium access control (MAC). The data-link layer is in-charge of secure, more reliable, and error free communication of data between HART compatible devices (Madduri & Jonnalagadda, 2012).

2.5.3 **Network Layer (NL)**

The network layer of the WirelessHART has many functions, but the most important of them are routing and security. In the Data link layer (DLL) packet are moved between devices, where as in the network layer packets are moved end-to-end within the wireless network. The network layer has features like route table and time table. The route table is for route communication along a graph whiles the time table for assigning communication bandwidth to some service like publishing data and transmitting block of data (Mark Nixon, 2012). The layer takes care of routing packet from the

initial source to their destination (Petersen & Carlsen, 2011). There are two types of routing supported here, the graph and the source routing and all devices must support both routing. A graph is made up of path that are connected to network nodes. These paths are created by the network manager and then downloaded to the individual devices. For packet to be send successfully the source device must write a specific graph ID in the network header (Madduri & Jonnalagadda, 2012).

2.5.4 **Transport Layer (TL)**

The transport layer (TL) of the WirelessHART main function is the block data transfer mechanism. The transport layer set up communication between the host application and the field device (Kim, Hekland, Petersen, & Doyle, 2008). The layer also provides end-to-end acknowledgment communication. HART command is used by the host application for configuring the slave device, by opening a port on board of the device. Another function of the transport layer is to constantly check the neighboring devices. These devices listen for new neighbors and give information if they come across a new neighbor. The devices keep information on communication with other devices like received signal level and packet count (Madduri & Jonnalagadda, 2012).

2.5.5 **Application Layer (AL)**

In the WirelessHART, the application layer is said to be the highest of all the layers in the architecture. The WirelessHART uses the same standard as the HART application layer which is a command based (Madduri & Jonnalagadda, 2012). The application layer also describes various commands, responses, data type, and status reporting (Song, et al., 2008).

In the application layer all communication between devices are through a set of define commands, which are divided into groups namely universal commands, common practice commands, device families' commands, and device specific commands (Petersen & Carlsen, 2011). The main function of the Application layer is for analyzing the message content, extracting the command number executing the specified command and generating responses (Song, et al., 2008).

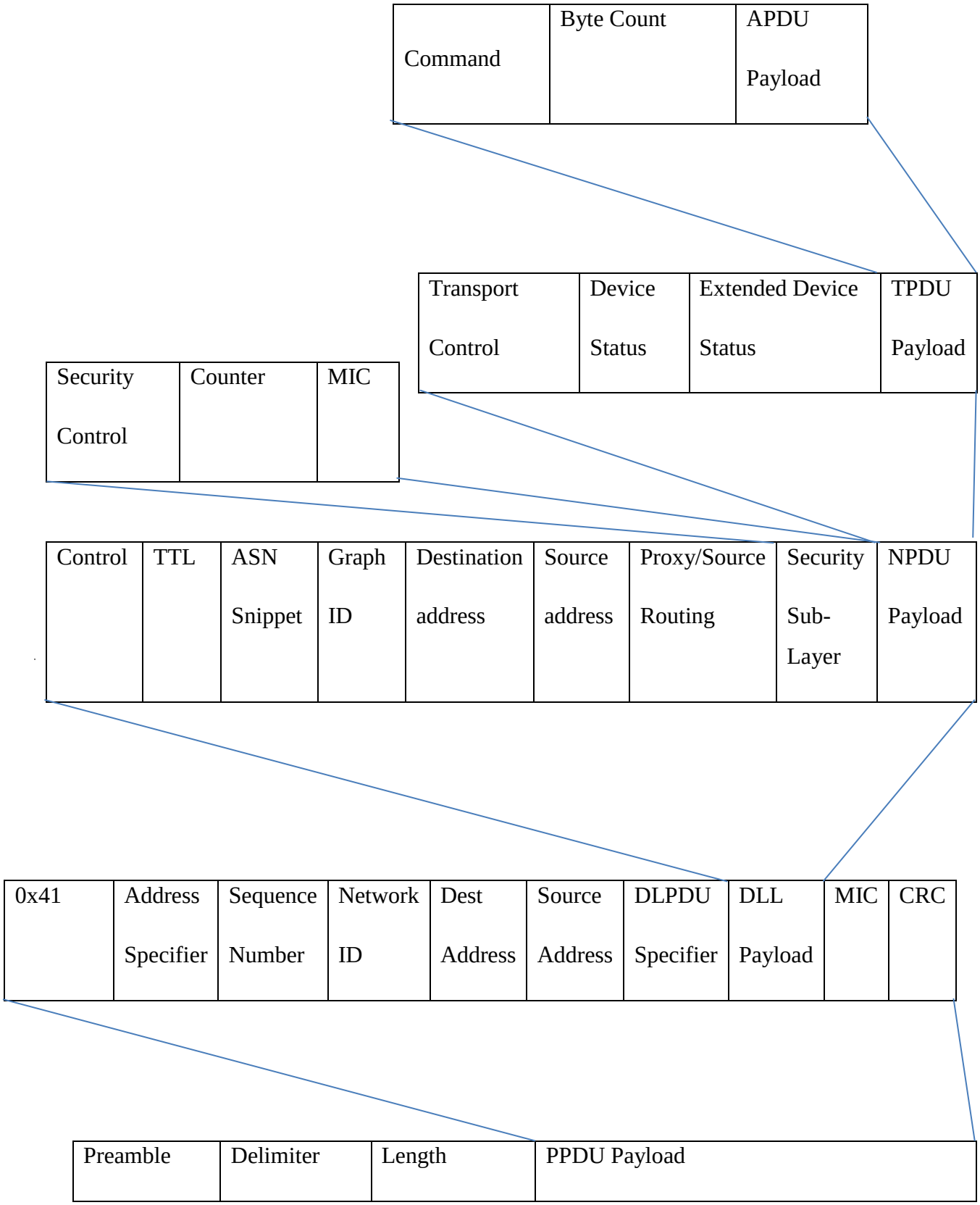


Figure 5 Dissection of a WirelessHART packet at different layers *(Lorente, 2015)*

3 CHAPTER 3

3.1 Key Management in Wireless HART

In every communication network keying management plays very important role when it comes to security. Due to power limited device of public key infrastructure (PKI) are not used (Lorente, 2015).

When it comes to protection of WirelessHART network, it is required that both wireless and wired devices are very important.

3.1.1 **Join key**

In wireless HART join key is regarded as the most important key. This join key is an unknown and phase shifting key (PSK) is used to authenticate with the network manager (Lorente, 2015). This is a key which is put into a device by a handheld device which is connected to the network. The join key is also said to act as a password that the device used to verify it to the network manager (Raza S. , Voigt, Slabbert, & Landernas, 2009). The join key (JK) provides an end-to-end security between a device and the network manager (NM) (Madduri & Jonnalagadda, 2012). The join key is used only when the joining process and both the join request and response are encrypted with such key at the network layer (Lorente, 2015). At the network layer level, the join key function as a tool to encrypt the payload and calculate the MIC (Raza, Voigt & Landernas (2009). The network manager (NM) has the mandate to verify the device by its join key and then write back the network key and the session key into the device, when the device is being connected for the first time (Madduri & Jonnalagadda 2012). The network manager can change the join key of the device immediately they are found to become part of the network. According to the HART Communication foundation;

- The join key serves as authentication to the security manager that the device belongs to this network
- The join key treated separately from the other keys to enhance security.
- Join keys can either be unique to each device, or be common to a given WirelessHART network based on the user security policies
- Join keys can be changed after the device join the network to further increase security

3.1.2 **Session Key**

The session keys are used by the network layer to provide end-to-end communication between two devices on a network (Petersen & Carlsen 2011). In this session four session keys needs to be established and these keys are as follows:

- Unicast Network Manager Key (UNMK)

- Unicast Gateway Key (UGWK)
- Broadcast Network Manager Key (BNMK)
- Broadcast Gateway Key (BGWK)

Unicast Network Manager Key (UNKM)

The unicast network manager key is used to provide an end-to-end encryption between the network manager and the wireless nodes in the network (Lorente, 2015). The network manager and the wireless nodes uses this key to interact in the network. This key is used by the network manager for device management, example asking about device health information, time slots allocation and renewing the join key when needed

Unicast Gateway Key (UGWK)

The unicast gateway key provides a very secured end-to-end interaction between the gateway and the field device or between two field devices (Lorente, 2015). The Gateway has session with all the field devices, and two field devices should communicate through it. The UGWK also function as securing the NPDU payload and calculate the MIC at the network layer.

Broadcast Network Manager Key (BNMK)

This key is used for sending global secure messages into the wireless network between the network manager, wireless devices and the Gateway. Some of these messages includes routing information, scheduling in network, and many others. This key can also be used to change the network key (Raza S. , Voigt, Slabbert, & Landernas, 2009).

Broadcast Gateway Key (BGWK)

The BGWK is the key used to send broadcast messages from the gateway to the field devices for examples notifications or timing amongst others (Lorente, 2015).

3.1.3 **Network Key (NK)**

The network key is the key that is initiated by the security manager and after some time disseminate to all the devices in the wireless sensor network (WSN) by the network manager. The Datalink layer (DLL) uses this key to validate messages on a one-hop basis (Petersen & Carlsen, 2011). This key is rotated from time to time because of the security arrangement of the process automation plant. The network key also provide security against attacks from outsiders. The network key is used to calculate the keyed MIC to secure the datalink PDU. The network key is used by two devices to authenticate each other at the datalink layer, and by making sure the calculated MIC is verified using AES-128

CBC-MAC (Lorente, 2015). The network key is used by the network manager for broadcast session and key renewal. This key is also known is some papers as “Link key”.

3.1.4 **Handheld Key**

Handheld key is used for peer-to peer wireless communication between a handheld device connected to a field device without the use of the gateway. Before a handheld device connected to a field device get connected to the network and its devices, it must make use of the join key (Madduri & Jonnalagadda 2012). After making sure it has been validated by the network manager, using the join key, a handheld device can move on to request for a handheld key. The network manager accepts this request and then grant both the hand-held device and field device the key (Raza S. , Voigt, Slabbert, & Landernas, 2009).

For the handheld device to establish connection with the field devices an AFSK modem needs to be used. The handheld key is used to provide security to the NPDU.

3.1.5 **Well-Known Key**

The well-known key is a coded key in the WirelessHART, which is the same always. This key is given to a device upon joining the network without a network key and in other to protect the datalink layer PDU. The well-known key (WKK) 777 772E 6861 7274 636F 6D6D 2E6F 7267 which happens to be the ASCII translation of: “ www.hartcomm.org” (Lorente, 2015). This well-known key is used to calculate the MIC for the join request and response messages (Madduri & Jonnalagadda, 2012).

3.2 Key Management

In WirelessHART network, keys are very important since they provide the needed security to the network. The security manager in the WirelessHART network are responsible for the key management in the network. The network manager in-charge of assigning and allocating the keys in the network.

3.2.1 **Key Generation**

In WirelessHART network key generation does not follow any required format. The security manager is the one in-charge of the generation of the keys and the network manager on the other hands is responsible for providing the needed password that needs to be authenticated. AES is used for the key generation and the logic for generating various keys depends on the security (Madduri & Jonnalagadda 2012).

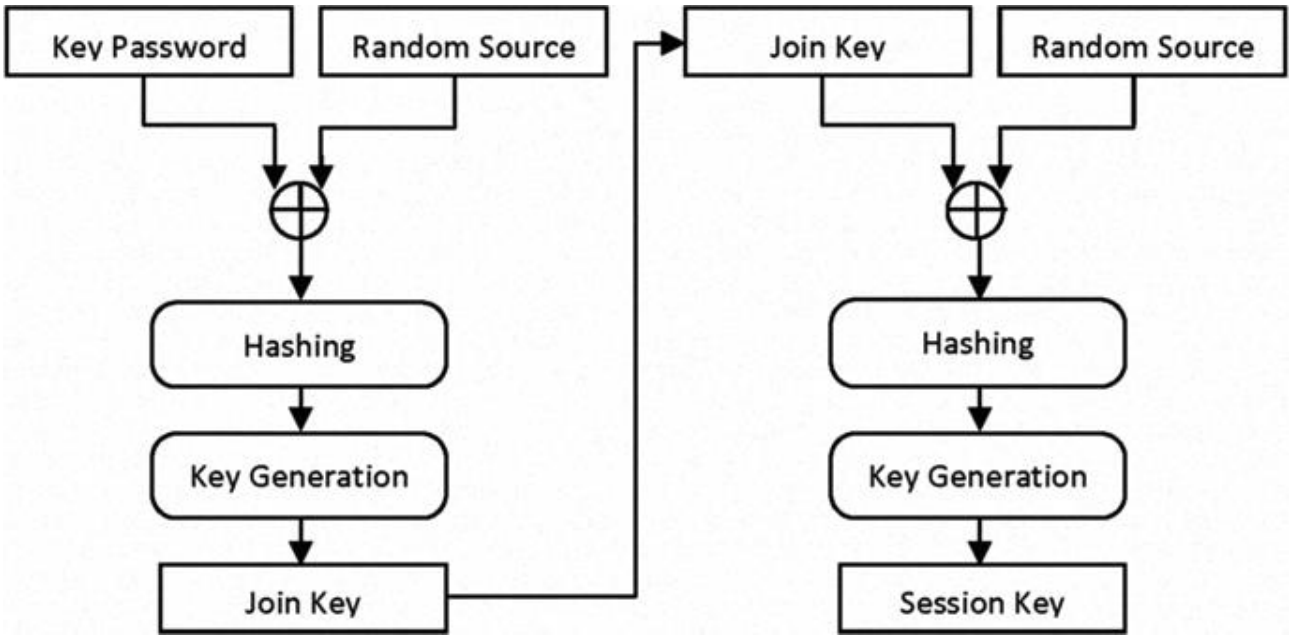


Figure 6 Key Generation Process *(Raza S. , 2010)*

3.2.2 **Key Request**

In the key request process the Network Manager (NM) depends on the Security manager for all the key but not the Well-Known key. The Network Manager needs Unicast and Broadcast session keys to decrypt the Network Protocol Data Unit (NPDU) message from both devices and Gateway (Raza S. , 2010). The key request process starts with the Network manager sending request message to the Security Manager. The security manager grants this request by releasing Handheld, Network, and Gateway sessions and are later spread to the appropriate devices to empower wireless communication (Madduri & Jonnalagadda, 2012). The key request process is explained in the figure below.

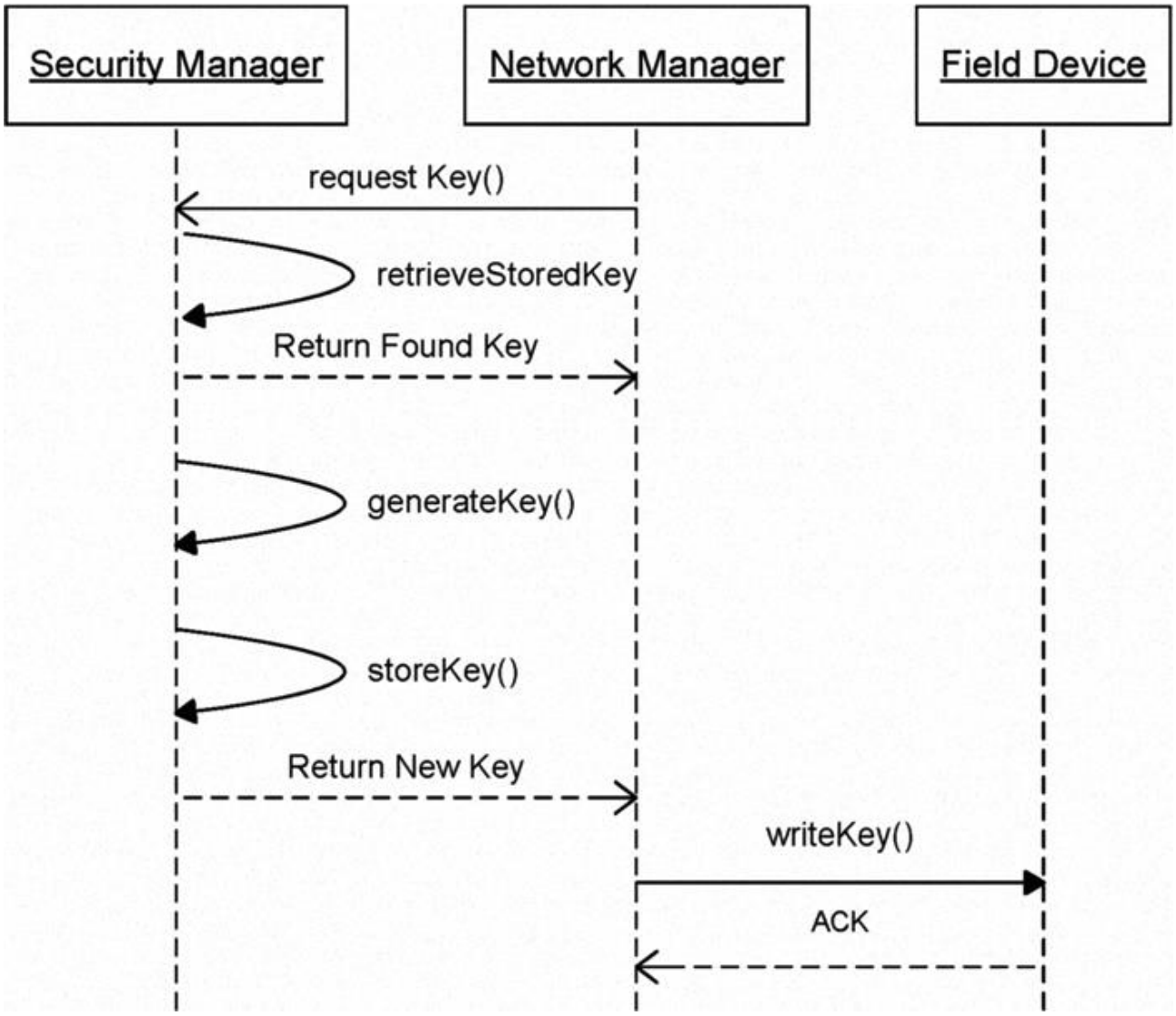


Figure 7 Key request process (Raza 2010)

3.2.3 **Key Storage**

The security manager is the one in-charge of making sure all the keys are safely stored in the network. All the keys are placed in a safe storage which has a security password. These passwords are kept safe by the security administrator. The network manager or the security manager are the ones responsible for managing the password in the storage. In the key database all the generated keys are stored by the security managers and its key related information like Network ID, Nickname, Device address, Device identity, key type, Status, Generation date, and Expiry date. All information in the database are stored as plain text but at the same time the database can be secured with password.

Network ID

Network ID is very important and thus WirelessHART network are identified by a unique ID. A security manager can serve more than one WirelessHART network and therefore it's very important to know which network has been served at a time, hence the importance of the Network ID in identifying them.

Nickname

A nickname is given to all device that join the network by the network manager. This network manager gives nickname to all the verified WirelessHART devices. All key request except the join key contains this parameter (Raza S. , Voigt, Slabbert, & Landernas, 2009)

Key Type

The key type is the name of the key requested at a time. The key type can be Join key, Unicast-Gateway key, Unicast network key, Broadcast Gateway key, Broadcast network manager key, Handheld key, and Network key (Raza S. , Voigt, Slabbert, & Landernas, 2009).

Device Address

When a device joins the network and has no Nickname it is regarded as not been part of the network. The network manager then assigns it an address, which is used to identify this device (Madduri & Jonnalagadda, 2012).

Device Identity

The device identity is the response to WirelessHART command 0 (read unique identifier) or command 20 (Read long tag). When the device successfully joins the network this device identity is used to authenticate it (Madduri & Jonnalagadda, 2012).

Status: The status indicates if a device is still part of the network or not part of the network.

3.2.4 **Key Distribution**

This is a process where the network manager distributes the keys to the device on the network and the key to the wireless network. The table below represents the commands used in management of the Keys.

WirelessHART Keys	Commands
Session key	Command 963 (Write session)
Network Key	Command 961 (Write network key)
Hand-held key	Command 823(Request session)
Join Key	Command 768 (Write join Key)

Table 8 Key distribution Commands *(Madduri & Jonnalagadda, 2012)*

3.2.5 **Key Renewal**

Key renewal in WirelessHART is done often because of the possible security breached or brute – force attack. In the WirelessHART network all keys are subjected to renewal except for the Well-known key (Raza S. , 2010). The system administrator (SA) is the one who request for the key renewal (only for the join key), security manager (SM) for key expiration or by the network manager (NM). When the system administrator or the system manager make request for key renewal the Network manager is made aware of such request. Without a renewal request from the network manager, the system manager will not change the key. The system manager will go on to change the key only it receives information from the network manager. The network manager on the other hand must write the change into the main device since the system manager is not in the position to make session with the field device and the Gateway (Raza S. , 2010). When the network manager gets a key renewal request or need to change keys itself, it asks the system manager to change the key. The system manager makes sure this request is authentic and if it verifies it is genuine, then it goes ahead to make the changes to the key and then sends back the new key to the network manager and the network manager sends it to the wireless device or the gateway (Raza S. , Voigt, Slabbert, & Landernas, 2009).

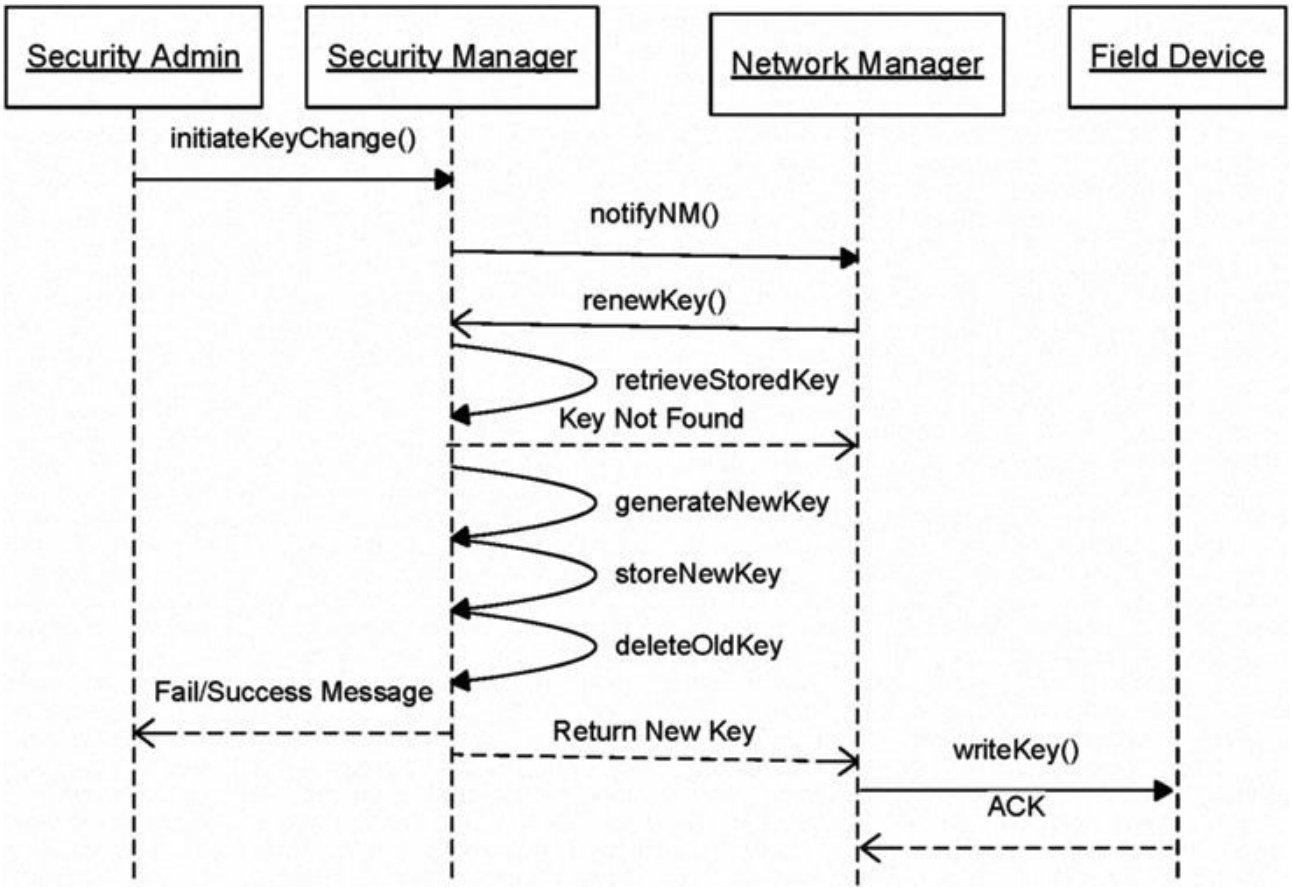


Figure 8 Key 8 renewal process (Raza 2010)

3.2.6 **Key Revocation**

Key revocation is the process of deactivating or deleting a key from the secure storage and other related information from the key database (Raza S. , 2010). When a device is no longer part of the network the network manager initiates the key revocation process for it to be deactivated or deleted from the secure storage. In the key revocation process parameters like Network ID, Nickname, and key types are deleted (Madduri & Jonnalagadda, 2012). The security manager deletes the keys and sends a feedback message if it was successful or failure. If a device leaves the network, all related features to it are deleted, but when Hand-held-to-field device (peer-to-peer) session expires only the Hand-held key is deactivated (Raza S. , 2010).

3.2.7 **Key Vetting**

Key vetting is the process to make sure the keys are verified and authenticated to be part of the network. In this process the device status is checked, and information sent to the main control system (Raza S. , 2010).

3.3 WirelessHART key Management challenges

Key Management in wireless network comes with lot of challenges. WirelessHART key management also has shortcomings. The table below shows the key management in the wireless devices.

Key Management	WirelessHART Solution	Comments
Key Generation	No	Not defined
Key Storage	No	Not defined
Key Distribution	Limited	Key distribution from the Network Manager (NM) to the devices is defined but the key distribution from the Security Manager to the Network Manager not defined. Join Key distribution not defined
Key Renewal	Limited	Though solutions to how key renewals are provided by WirelessHART, no information is given on how the key are renewed in the security manager.
Key Revoking	No	Not defined
Key Vetting	No	Not defined

Table 9 Key Management in Wireless part of WirelessHART (Raza S. , 2010).

4 CHAPTER 4

4.1 WirelessHART Security

WirelessHART was built on the mesh networking technology and at the same time possess some features of wireless sensor networks as all the field devices are enable with one or more sensors. WirelessHART security requirement s are combination of both mesh network and the wireless sensor network. WirelessHART uses very strong security measures to protect the network and secure data at all times. WirelessHART implement many processes to ensure data confidentiality, authenticity and integrity in both hop-by-hop and end-to-end transmissions (Bayou, Espes, Cuppens-Boulahia, & Cuppens, 2016). IEC has approved WirelessHART standard for industrial process automation and control. WirelessHART is a secure and reliable protocol for the process automation. According to the HART Communication Foundation security automatically protects valuable information (FieldComm Group, 2018):

- Robust, multi-tiered, always-on security
- Industry standard 128-bit AES encryption
- Unique encryption key for each message
- Data integrity and device authentication
- Rotate encryption keys used to join the network automatic or on-demand

Protect Wireless Network (FieldComm Group, 2018):

- Channel hopping for security protection and co-existence
- Multiple levels of security keys for access
- Indication of failed access attempts, perhaps by rogue demands
- Reports message integrity and authentication failures
- Safe from Wi-Fi type internet attacks

Security Requirements

For any network to be successfully secured against attacks, some certain security features must be met before. For WirelessHART to be successfully secured from attacks all these features must be met. Some of these security features to be discussed in this thesis work includes Authentication, confidentiality, integrity, availability, data freshness and time synchronization.

- **Authentication**: Authentication is a state where all nodes within the WirelessHART network are verified and their identities known to all. Authentication helps in identifying the source of data and then reassures other participants on the network that data being received or transmitted is sent from or delivered to the right target (Messai, 2014).
- **Confidentiality**: Confidentiality is very important when it comes to data security. Wireless data transmission has a high risk of been attacked because of their mode of transmission. Wireless information can easily be captured by people with highly sophisticated equipment when the confidentiality agreement is breached (Messai, 2014). Confidentiality of any message within the WirelessHART network is not guaranteed without security. Confidentiality protect the privacy and integrity of the information being transferred over the network.
- **Integrity**: Integrity determines the originality of data sent or received. Integrity of data ensures that data transmitted between communicating nodes within a network remains the same, (Murty et al. 2010). Some area of application of WirelessHART sensor network deals with financial institutions, health organizations, military intelligence etc., so the integrity of data sent and received on the network very importance (Messai, 2014). Any changes in such data could result in bad consequence.
- **Availability**: Availability, deals with maintain the functionality of the network in a situation of internal or external attacks (intentional or unintentional). The main duties of the WirelessHART sensor network (WSN) is to collect and transmit data wirelessly to it target destination (Messai, 2014). When there is no data available to be transmitted this purpose comes to an end. Another important application that uses WSN is collection of data for successful prediction of change that could have an impact on the health of an individual. An example is the collection of data for a disease outbreak, if data availability were to be tempered with within the network it could lead to wrong medication administered which could lead deformity or loss of lives
- **Data freshness**: Data freshness deals with data that are current. One of the requirements of the WSN is its ability to provide the network a fresh data. When an attacker attacks the network and decides to circulate old data within the network, which could be mistaken as currently received data at the collection center. Situation like this create difficult situation for data analyst whose judgement on the received data could be different from the current situation at the physical location.

4.2 Security policy and why the need for it

A good security policy is a way of building a very strong and successful implementation of security related issues in the future; this is without doubt the first step that must be taken to reduce the risk of unwanted use of any of the company's information resources (. The first step in making sure company's security issues are kept intact is to introduce security policies, give training to staff on the various aspect of their responsibilities, general use of the company resources and explains how staff can handle sensitive company information (Brotby, 2006). The policy will also describe in detail in the meaning of acceptable use, as well as listing unaccepted events. A WirelessHART Security Policy is a well-defined and documented set of guidelines that describes how an organization manages, protects its information assets and makes future decisions about its information systems security infrastructure (Bowen, Hash, & Wilson, 2007). The development (and the proper implementation) of a security policy is highly beneficial as it will not only turn all your staff into participants in the company's effort to secure its communications but also help reduce the risk of a potential security breach through "human-factor" mistakes. There are usually issues such as revealing information to unknown (or unauthorized sources), the insecure or improper use of the Internet and many other dangerous activities. Additionally, the building process of a security policy will also help define a company's critical assets, the ways they must be protected and will also serve as a centralized document, as far as protecting Information Security assets is concerned (Bowen, Hash, & Wilson, 2007).

4.2.1 **Purpose of Security Policy**

- To launch a general method to information security
- To notice and envision the compromise of information security such as misuse of data, network, computer systems and applications.
- To protect the reputation of the company with respect to its ethical and legal responsibilities.
- How to properly maintain your ID(s) and password(s), as well as any other accounting data
- How to responds to a potentially security incident, intrusion attempt.
- How to properly use the corporate e-mail system
- How to use work station and internet connectivity in a secure manner

4.3 Risk Management

An effective risk management procedure is a vital component of a successful information security program (Bowen, Hash, & Wilson, 2007). The main objective of an organization's risk management procedure is to protect the organization and its capacity to accomplish its mission, not just its information assets. Therefore, the risk management procedure should not be treated mainly as function carried out by the security experts who operate and manage the security system, but as an important management function of the organization that is firmly interlaced into the system development life cycle (Bowen, Hash, & Wilson, 2007). Because risk cannot be eliminated entirely, the risk management process allows security program managers to balance the operational and economic cost of protective measures and achieve gains in mission capability. To manage and mitigate risk and reduce potential impacts on information assets to an acceptable level, consider the following goals:

- Account for and protect all IT assets
- Create and reduce the possibility and influence of IT security risk
- Do systematic risk assessment with senior managers and key staff members.
- Permit access to critical and sensitive data only to authorized users
- Safeguard serious and confidential information is withheld from those who should not have access to it
- Identify, monitor and report security weaknesses and incidents
- Develop IT continuity plans that can be implemented and are tested and maintained

4.4 Risk Assessment

According to the Hart Communication foundation to be a credible threat, an attacker must require access, technical know-how and motivation to attack (FieldComm Group, 2018). The goal of risk assessment process is to identify and assess to a given environment (Bowen, Hash, & Wilson, 2007). The depth of the risk assessment performed can vary greatly and is determined by the critically and sensitivity of the system, as applied to confidentiality, integrity, and availability (Bowen, Hash, & Wilson, 2007). According to the HART Communication Foundation the WirelessHART security architecture helps users to address three very important areas (FieldComm Group, 2018):

- Minimize, control and audit access
- Need high level of technical proficiency to disrupt
- Reduce the span and duration of any individual security breach

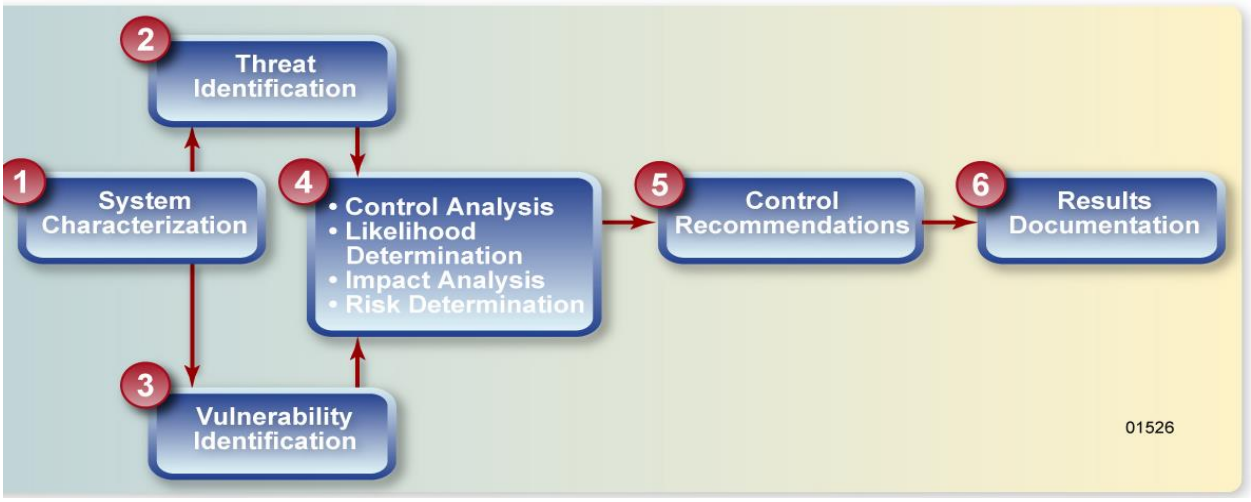


Figure 9 Risk assessment process *(Bowen, Hash, & Wilson, 2007)*

4.5 Risk Mitigation

Another phase of risk management is the risk mitigation. Studies have revealed that it is impossible to abolish risk from WirelessHART network system. Risk mitigation objectives at prioritizing, evaluating and implementing the needed risk reducing control policies. System and organizational managers may use numerous possibilities to reduce the risk to a system (Bowen, Hash, & Wilson, 2007). These options are risk assumption; risk avoidance; risk limitation; risk planning, research, and acknowledgement; and risk transference.

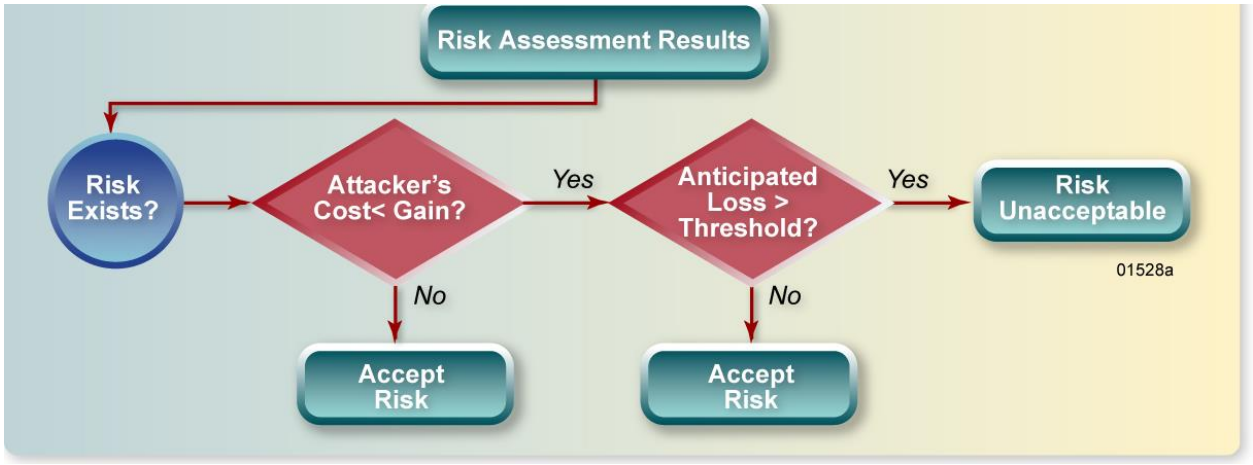


Figure 10 Risk Mitigation strategy *(Bowen, Hash, & Wilson, 2007)*

4.6 Data Security

The main reason for security features associated with privacy is to minimize eavesdropping by an unsolicited device inside or outside the network. A WirelessHART sensor network (WSN) employs end-to end CCM mode 128-bit AES encryption at both network and transport layers for every message in the network (FieldComm Group, 2018). A common network key is distributed among all devices on a network for broadcast activity. Encryption keys can be rotated as dictated

by plant security policy to offer an even higher level of protection. During the joining process a 128-bit join encryption key is applied to keep data sent and received private. Data security features associated with integrity ensures data sent and received over the wireless sensor network is the same and has not been changed. Data integrity ensures packets received has been authenticated and from the correct source.

- WirelessHART uses two Message Integrity Check (MIC) Fields that are added to each packet
- At the session layer, the receiving device uses the session MIC along with the protected data to confirm that the content of the packet has not been tampered.
- At the link layer a separate MIC protect network routing information to prevent attacks that attempt to change the packet´s network/transport layer information.

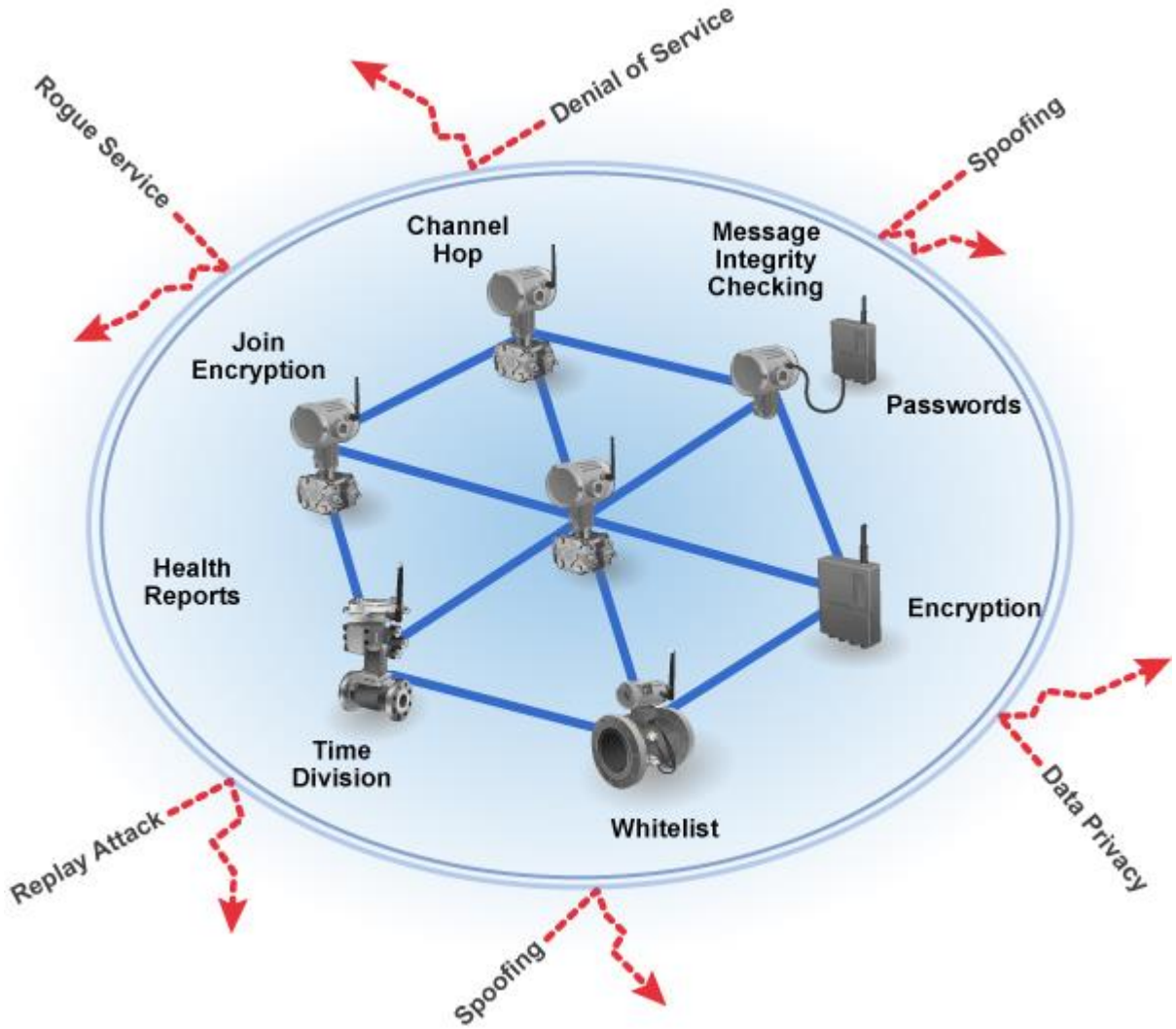


Figure 11 Data Security of WirelessHART *(FieldComm Group, 2018)*

4.7 Network Security

Network security is very important in WirelessHART sensor network. Many attackers within and from outside will try to attack the network. These attackers will try as much as possible to attack the network by inserting trojan horse devices, impersonating network to get vital information from devices and causing the network to function properly as expected leading to denying of important services. An attacker attacking the network can be from insider example an employee and from external. Good network security depends on techniques that support authentication, authorization, and threat sensing. According to the HART Communication Foundation these three points are crucial when it comes to network security in WirelessHART:

- Before the network, the WirelessHART Gateway and the wireless sensors needs to be configured to control which devices are allowed permission to the network
- For proper network security to be achieved all the devices in the wireless network should maintain their security status
- WirelessHART Gateway has a secure validation procedure which it uses to negotiate with all joining devices to ensure they are authentic. As with all other network communications, all join negotiation traffic is encrypted end-to end.

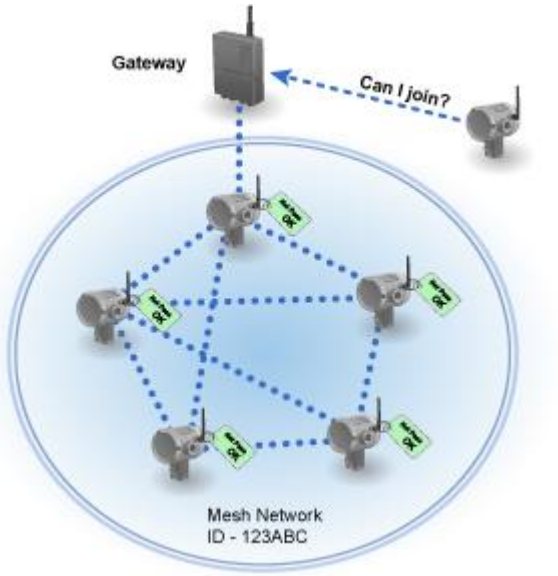


Figure 12 Network Security of WirelessHART *(FieldComm Group, 2018)*

4.8 Types of Attackers

There are different types of attacker who may try to attack a network at a time. These attackers are grouped according to the types of attackers and the damages they cause to network and the

kind tools with which they attack. The attacker could be a passive, or an active and in some cases both.

Passive Attacker: The passive attacker is the who does not cause serious damage to the network. They keep tracking of the network and tries to eavesdrop on the network but do not really make any changes to data or dropping any of the transmitted data.

The key goals and effect of this attacker includes (FieldComm Group, 2018):

- Eavesdropping
- Gather and stealing information
- Change privacy and confidentiality requirements
- Make sure the WSN does not work well
- Network partition by non-cooperate operations
- Storing energy by selfish node and avoid from cooperation

Active Attacker: These attackers takes actively part of the attack and in the end cause serious damages in the form of changing and modifying data. This can also change communication protocols and thereby introduce latency within the network, where it can have serious effect on area of application where WSNs are used. The active attacker always tries to insert faulty data into the network, impersonating, data modification, creating a hole in the security protocols (Mohammadi & Jadidoleslamy, 2011).

The main goals and effects of this attacker includes:

- Make sure the WSN is malfunctioning
- Make sure WSN performance is degraded
- Sensor nodes destruction
- Data modification or changes
- Preventing the operation or cut off certain nodes from their neighbours

Insider attacker: An insider attacker has little or no knowledge about the network. They apply brute force to get information about the network and d its architecture.

The main goals of this attackers include (Mohammadi & Jadidoleslamy, 2011):

- Make sure they get access to cryptography keys or other codes
- Make sure secrete keys opens to public
- Partial, total degradation or disruption
- To make sure the system functionality and efficiency is attacked

Outsider Attacker: This attacker most cases have all information about the network they attack. They normally have access to some or all part of the network. Based on the level of access or information partial or fully, they obtain knowledge about the network.

The main goals of this attacker include (Mohammadi & Jadidoleslamy, 2011):

- Jamming the whole communication of the WSN
- Triggering Denial of Service (DoS) attacks
- WSN resources consumption

Mote class: This kind of attacker uses devices that look like common sensor nodes. This attacker in this case has access to nodes or motes that look just as the nodes in the WSN and maybe used to compromise one of the network nodes. These attackers execute malicious codes or programs to the WirelessHART network (Mohammadi & Jadidoleslamy, 2011).

The main goals of Mote-class attacker include (Mohammadi & Jadidoleslamy, 2011):

- They are responsible for jamming the radio link
- Stealing and getting access to the cryptography keys

Laptop Class Attacker: This attacker is like the mote class attacker. This attacker uses the laptop to attack the network. Because of the nature of powerful devices, they use they have access to high bandwidth and low-latency communication channel. These enemy creates traffic jam on the network and attempts to substitute genuine nodes with illegal ones (Mohammadi & Jadidoleslamy, 2011).

The main goal of Laptop-class attacker includes:

- Jamming the radio links on the network
- Creating more serious attack on the network causing more damages to the network
- Getting access to high bandwidth and low-latency communication channel

Attack category/ Features	Type	Damage level	Ease of identify	Attacker presence
Based on damage level	Active attacker	High	Easy	Explicit
	Passive attacker	Low	Hard	Implicit
Based on attacker location	External(outsider)	Low	Medium	Implicit
	Internal(insider)	High	Hard	Implicit
Based on attacking devices	Mote-class attacker	Low	Hard	Implicit
	Laptop-class attacker	High	Easy	Explicit
Based on attack function	Secrecy	High	Hard	Implicit
	Availability	High	Hard	Both
	Stealthy	High	Hard	Implicit

Table 10. Threat model of WSNs *(Mohammadi & Jadidoleslamy, 2011).*

5 CHAPTER 5

5.1 WirelessHART THREAT/ATTACKS

There are different kinds of threat the WirelessHART sensor network must deal with due to the nature of network. The threat can be attributed to the size of communication nodes on the network. A threat happens when an attacker tries to get very important information from the wireless network. When an attacker attacks a network there some essentials properties that includes (Mohammadi & Jadidoleslamy, 2011): Asset under attack, Actor (what or who breaches security), product of the security attack, and motive (intentional or unintentional). The asset of a WirelessHART sensor network can be data stored in a device or information that run through the network. The main aim of an attacker on it prey is to leak very important information, data modifications, and disruption of smooth network traffic (Raza S. , 2010). The attack on the network has been grouped based on the network layers they exist. The network layers include the Physical layer (PHY), Data link layer (DLL) and the network (routing) layer.

5.2 PHY Layer Threat

The physical layer threat is attributed to the wireless nature of communication inside the WSN. An attacker with the right equipment can easily eavesdrop and tries to get some secrete information from the network. Some of the physical layer attacks includes Denial of Service (DoS), Jamming, Physical tampering, Interference, Sybil.

5.3 Denial of Service (DoS)

In this attack the attacker tries to use all possible mean to prevent the nodes from properly functioning well, (Murty, Namboothiri, & Sivalingam, 2010). They try to block or jammed all resources such as frequency being used for transmission. This attack occurs when the attacker finds security lapses in software design. They make nodes are required to function to their outmost level and to keep the network working are made useless.

5.4 Jamming

Jamming is a situation where the attacker tries to obstruct the network by transmitting on the same wavelength used by the WirelessHART sensor network the same time the nodes within the network are transmitting, (Murty, Namboothiri, & Sivalingam, 2010). When network uses the same frequency for transmission it causes disturbances or disruption to the network. When some of the routing protocols for WSNs, uses frequency hopping, the attacker just needs to know the hopping sequence of the protocol. This threat can be corrected applying spread-spectrum for transmission within the network. This type of attack aims to disturb the network by transmitting on the same frequency being used by WSN at the same time the nodes within the network are transmitting, (Murty, Namboothiri, & Sivalingam, 2010). It is also known to be an intentional interruption of radio signal when intentionally introducing noise or signals with same frequency and modulation technique as used in the target network (Raza S. , 2010). Disruption within the network is easily achieved if the network uses a single frequency for transmission. WirelessHART is more vulnerable to jamming attacks then interference; the attacker only needs to introduce radio signals using Bluetooth devices like cell phones and laptops. WirelessHART introduces the concept of channel Blacklisting. In WirelessHART channel Blacklisting is network-wide and is done by a network administrator manually. Blacklisting improves the reliability of the WirelessHART network and same time limits the number of channels the device can use to send or receive traffic. If frequency hopping is used in the WirelessHART, then the attacker only needs to learn the hopping sequence of the protocol.

Despite Frequency-hopping spread spectrum and 15 available channels, the active attacker can jam the WirelessHART network. A possible solution used in this situation is to employs the services of spread-spectrum for transmission within the network.

5.5 Tampering

Tampering is because of the isolation of nodes in the WSNs. Tampering is very serious as the isolated nodes comes under intense pressure from the attacker to the point of been compromised and in some cases destroyed totally. The focus of the attacker in this case is to make some changes to the hardware and get access to sensitive information like cryptography keys. To make sure this kind of threat is eradicated security measures that make sure the nodes are tamper-proof are implemented. Another is to ensure that on probation, nodes can self-erase (Raza S. , 2010).

5.6 Interference

Interference is an unintentional disturbance of radio signal. WirelessHART operates at 2450 (2400-2483.5) MHz frequency band spectrum and has 16 channels and each channel´s bandwidth is 5 MHz.

WirelessHART share same spectrum with Wi-Fi, Bluetooth, and ZigBee. Applying Frequency Hopping Spread Spectrum (FHSS), time diversity, and path diversity helps in eradicating interference. Process automation system requires fail proof (100%) reliability of the wireless medium, failure may produce very bad results (Raza S. , 2010).

5.7 Sybil Attack

In this attack the attacker can hold different identities. The main objectives of this attacker are to obtain the identity of any of the nodes to be used within the network. The attacker could also create an identity for the nodes to be used within the network (Messai, 2014). Because there is no trusted central authority in the traditional wireless ad hoc and sensor network, the chances of the attacker to have multiple identities is high (Raza S. , 2010). This attack is so possible if the attacker is an insider, since the attacker already has full knowledge about the network. The attacker creates different kinds of identities with the intention of using them to create virtual nodes known as Sybil nodes (Yang, Tarng, Hsieh, & Chen, 2010). After creating these virtual nodes, the attacker then uses it to perform any kinds of attack on the network. In this situation the attacker makes it possible for all the identities created to communicate within the network at the same time, (Murty, Namboothiri, & Sivalingam, 2010). In cases like Data fragmentation and replication mechanisms employs as security some WSN ineffective as Sybil nodes has the identities of the original nodes within the network. For this attack to be prevented the Network Manager in the WirelessHART allocate a unique Nickname to all the devices connected to the network, and a unique ID which is unique for the device globally. The Gateway and the Network Manager maintains the list of Unique IDs and Nicknames respectively in the WirelessHART network. The wireless devices use these Unique IDs and the Nicknames to maintain sessions with the Gateway and Network manager respectively. With all these in place sybil attack in the WirelessHART network in unsuccessful (Raza S. , 2010).

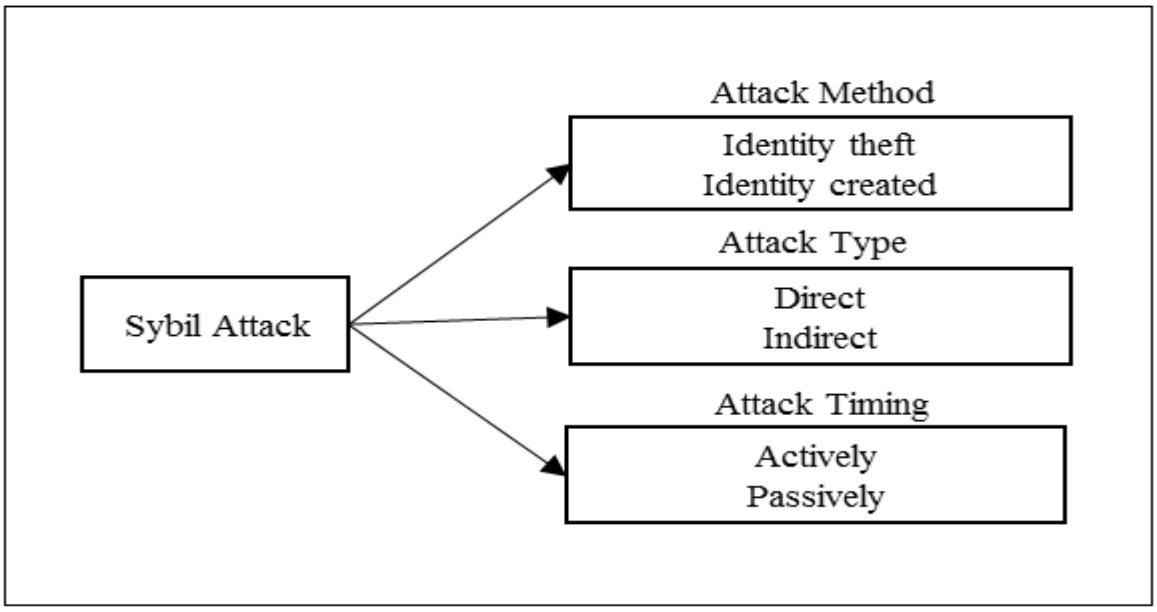


Figure 13Sybil Attack Process *(Raza S. , 2010)*

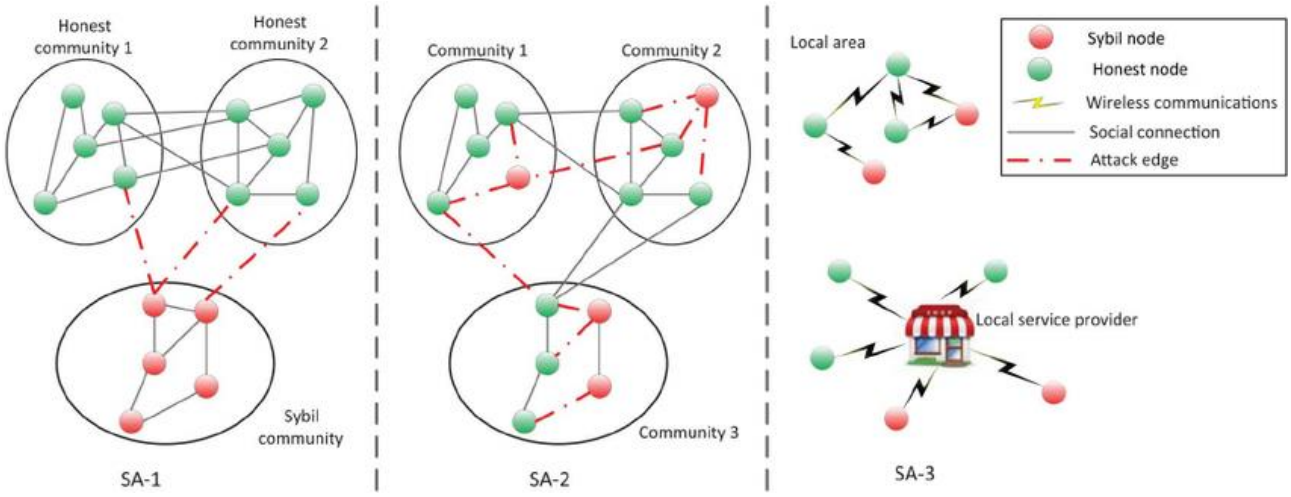


Figure 14 Sybil attack *(Yang, Tarng, Hsieh, & Chen, 2010)*

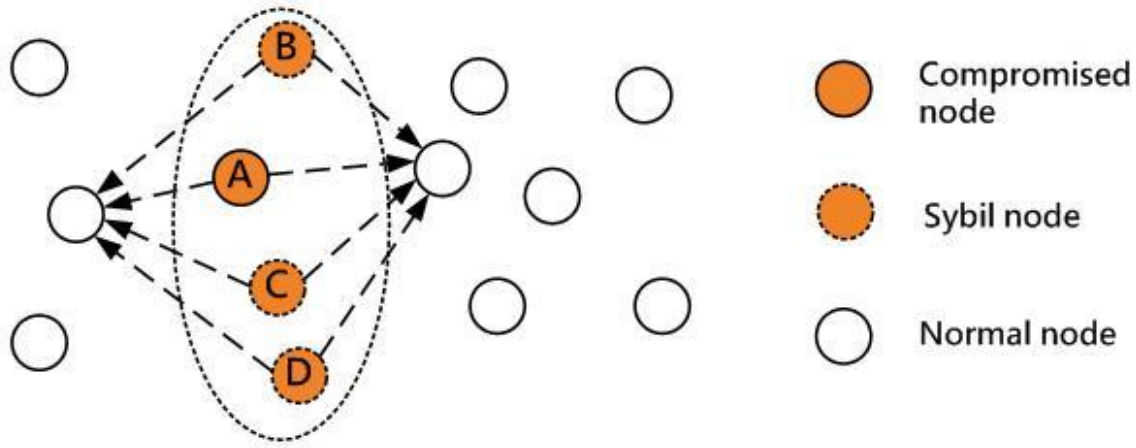


Figure 15 Sybil attack (Yang, Tarng, Hsieh, & Chen, 2010)

5.8 Collusion

Wireless collusion is because of two or more devices trying to access the same frequency at the same time. In situation like this it could be a planned or unplanned. Collusion can be minimized by merging of time and frequency diversity and CRC-16 is used to detect the collusion in the WirelessHART network. Schedule data transmission based on time slotting is very in the WirelessHART protocol to reduce the possibility of collusion. Time Division Multiple Access (TDMA) and channel hopping used to control access to the network. Cyclic redundancy check (CRC) is used in detecting collusion based on ITU-T polynomial. The CRC-16 is not always guaranteed to have knowledge about the insertion attack. This attack can be totally eradicated or prevented by application and active coordination between the physical and Data-link layer (Raza S. , 2010).

5.9 Spoofing

In communication network all the devices are required to use a well-known key. This key is not only for joining the network but also for the advertisement. The attacker can spoof the new join by dispatching wrong advertisement and upon receiving the join request it can simply ignore it. The new device cannot join the network because if the spoofing device is closer to the device joining the network. In spoofing attack, the attacker alters or replayed routing information, in this situation when a routing protocols are not in used fall prey in this type of attack. When the attacker has the possibility of performing alteration, and replaying routing information then the attacker could create routing loops, attract or repel network traffic, change source roots, create false error messages, increase latency and more (Murty, Namboothiri, & Sivalingam, 2010) (Karlof & Wagner, 2003). If the lookalike device possesses a valid network key, then spoofing attack will be more dangerous and can lead to serious blockage of network traffic.

5.10 Exhaustion

Exhaustion is a situation where the attacker consumes all the resources energy of the victim node, by trying to do calculations or receiving data or sometimes transmitting data (Messai, 2014).

With devices that supports the WirelessHART protocol stack and has information about unsecure WirelessHART network parameters can send messages to the WirelessHART devices using a well-known key. Fake devices that have join the network uses the well-known key to calculate the MIC over the DLPDU and use the fake join key they have acquired to encrypted and validate the NPDU. Even though the messages that are sent are neglected by the Network Manager it drains network resources along the route from the field device to the network Manager (Raza S. , 2010).

5.11 Wormhole Attack

In the Wormhole attack the attacker tries to establish a tunnel between two genuine devices by making them communicate through a stronger wireless link or wired link (Messai, 2014). The HART devices that are connected to the WirelessHART network through adapters are the most subjected to wormhole attack by the attacker. By using the maintenance port of the two field devices, the attack creates a tunnel between these devices. When the Network key and the session key are compromised then a tunnel is established. In this attack multi-hop protocols, which are built-in the WirelessHART architectures, is the reason that makes this attack possible. In this attack the attacker usually uses two compromised nodes, these nodes seem to have the shortest hop route to the destination which is always the base station or the master node (Messai, 2014). These two nodes are far from each other in the network and data sent through this route may be dropped on the node receiving the data. If the WirelessHART employs graph routing technique then it has a high risk of been subjected to wormhole attack, but if Source routing is employed the device must use device-by-device route from source to destination. With regards to the source routing when any of the intermediate links fail the packet will be lost making it provide little defence against wormhole but not reliable one. Packet leaching is the best defence mechanism to wormhole attack (Raza S. , 2010).

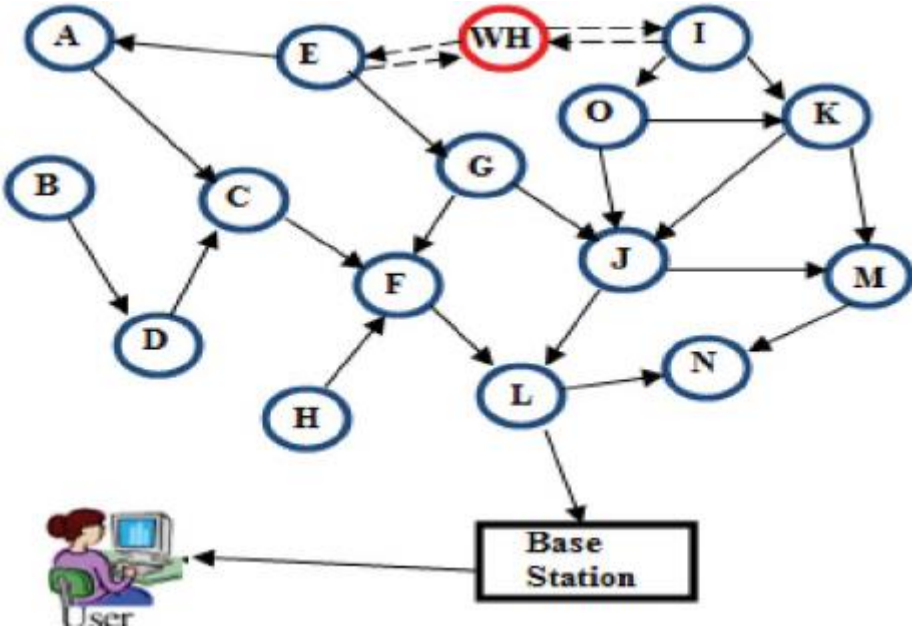


Figure 16 Wormhole attack *(Ould Amara, Beghdad, & Oussalah, 2013)*

From the figure above shows the attacker (WH) builds a tunnel between E and I.

5.12 De-synchronization

De-synchronization attack is a situation where the attacker can interrupt the exchange of information between two nodes by introducing distorted timing information in the network and making the devices to waste their resources in time synchronization (Raza et al. 2010). Timing is an essential requirement when it comes to WirelessHART network and the Timer is known to be one of the important modules in the WirelessHART. The timer module in the WirelessHART network is required to meet timing requirement to keep the time slots (10ms) in synchronization. Time slotting is the responsibility of the Medium access control (MAC) sub-layers. Anytime a node gets an acknowledgement message from its time source, it modifies its clock. A sender can be a timing source for a node and if the sender corrupted it can interrupt the timing between the two nodes and the nodes taking active role are forced to waste their resources in synchronization (Raza S. , 2010).

5.13 Selective Forwarding Attack

Selective forwarding attack is because of the attacker taking advantage of the weakness of the multi-hop technique of forwarding packet within the WirelessHART network. The corrupted node in the network will not forward all packets and some packets will be selectively dropped (Messai, 2014). Packet dropped in this situation are haphazardly chosen based on the inclination of the attacker attacking the network. The attacker's inclination in this situation is based on what is contain in the

packets, the address of the forwarding node, or some random algorithm. In this attack when the node is not sending any packet and create a black hole, but usually the node selectively ignores packets so that it regarded as valid which could not be recognized by the recovering procedures. This attack is more intense if it supported by a proper traffic analysis (Raza S. , 2010).

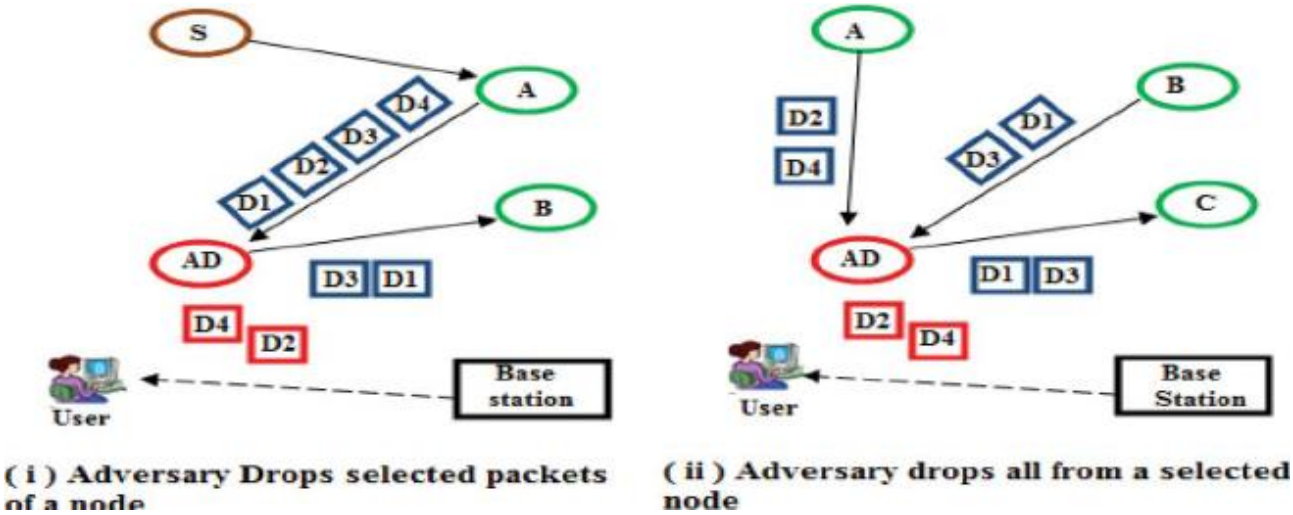


Figure 17 Selective Forwarding *(Ould Amara, Beghdad, & Oussalah, 2013)*

From the fig above in the (i) situation S which is the source node forwards data packets D1, D2, D3, D4 to node A, and when A received these packet forwards them to node B. The attacker in this case node AD the selectively sends packets D1, and D3 to node B and drops D2, and D4. In the (ii) case the attacker AD can decide to selectively drop packet from one source and then forward packet of others. Selective forwarding attack can be prevented by adopting multiple-path to send data and get information about mischievous node or suspect that it has failed and then look for another path (Ould Amara, Beghdad, & Oussalah, 2013).

5.14 Traffic Analysis

The Network Layer Protocol Data Unit (NPDU) header and the Data-Link layer Protocol Data Unit (DLPDU) are not protected and the attacker can easily get information on the WirelessHART traffic. The NPDU header fields which is made up of source address, destination address, security control byte, ANS snippet, and Nonce counter are all sent in clear. The DLPDU fields which are made up of fields like Address Specifier, Address, and DLPDU Specifier are sent in clear. These fields give other competing for same objectives enough information to allow analysis of the network (Raza S. , 2010).

5.15 Misdirection Attack

In this attack the attacker's main target for attack is the number of hops. In the network design, those with the shortest path are favoured because it reduces latency in the network to the lowest. In this attack tries to compromise a node on the network and then uses the node to change the path of any packet that are to be sent to another node that is far away from the intended destination. This situation brings about inactivity in the network and tries to stop packet from ever getting to the destination. The more nodes a network contain the more vulnerable they are to this attack.

5.16 HELLO flood Attack

In this form of attack protocols make sure that nodes sent HELLO packets to all other nodes in the network to start all interaction among the communicating nodes. Laptop class attacker is one of the uses the HELLO flood attack (Karlof & Wagner, 2003). Protocols that use the hello packets are made to believe that receiving those packets show the sender is in close radio range, and therefore they are meant to believe they are neighbours. Uses of a highly developed powered transmitter by the attacker to deceive wide area of nodes that they are neighbours of that transmitting node. These deceived nodes are made to send information to the attacker rather than the base station. In the figure below AD the attacker's node sends a hello packet deceiving the nodes in the network that they are its neighbours (Messai, 2014). The (AD) makes I, H, F which are far from it are deceived into believing that they are closer and neighbours and try to send packets through it and in the process losing date and wasting energy too. To prevent this attack from occurring, a mechanism known as authentication by third node is employed.

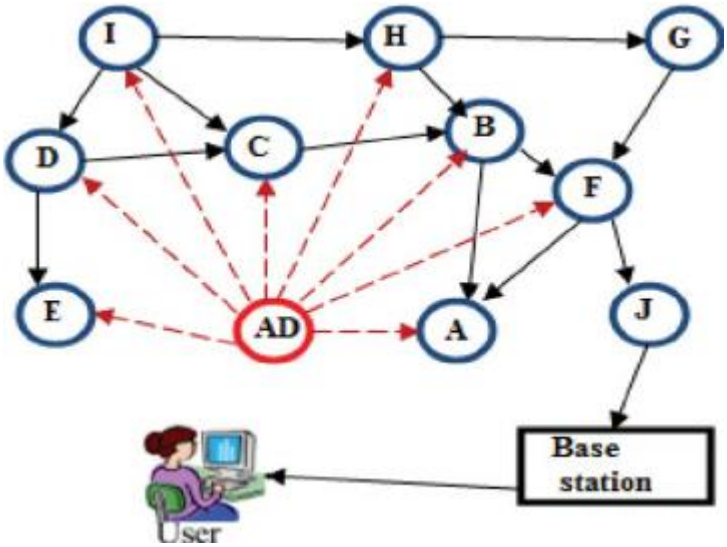


Figure 18 HELLO flood attack *(Ould Amara, Beghdad, & Oussalah, 2013)*

5.17 Sinkhole Attack

In this form of attack, the attacker makes sure compromised nodes looks beautiful to nodes around by forging routing information. The nodes around are more likely to choose the compromised nodes as the next node to route their packet through. Sinkhole attack is an upgrade of blackhole attack. With regards to the blackhole attack, the attacker compromise nodes inside the network and drops all data that are routed through it. This compromised node is unnoticed because it keeps transmitting packet it has generated by itself to the next hop, (Murty et al. 2010). The network administrator is deceived into believing that nodes that used the compromised node as the next hop are unresponsive. The sinkhole attacker takes advantage of this situation by advertising to be the shortest path to the master node or base station. The sinkhole attack drops large amount of data compared to the blackhole attack. The sinkhole attack makes selective forwarding easier, since all traffic from big area in the network passes through the attacker´s node (Ould Amara, Beghdad, & Oussalah, 2013). The figure below is an example of Sinkhole attack.

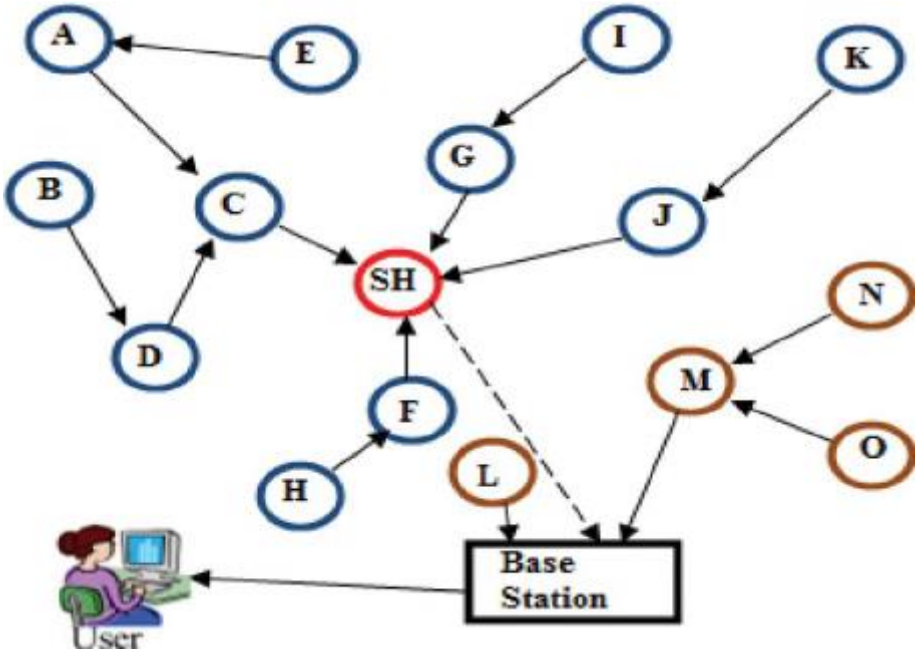


Figure 19 Sinkhole Attack *(Ould Amara, Beghdad, & Oussalah, 2013)*

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 required to joining device
	Spoofing	Use different path for re-sending the message
	Sybil	Regularly changing of Network key
	De-Synchronization	Using different neighbours 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 Technique
	Selective forward	Regular network checking using Source Routing
	DOS	Protection of Network specific data like Network ID etc. Physical protection and checking of network
	Sybil	Resetting of devices and changing session key
	Traffic Analysis	Sending of dummy packet in quite hours; and regularly checking WirelessHART network using Handhelds etc
	Eavesdropping	Session key protect NPDU from Eavesdroppers

Table 11 Attacks on wireless portion of Wireless of WirelessHART *(Raza S. , 2010)*

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
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
DOS	Eliminating illegal access to the legal network, proper monitoring and administration of network (There is no definite solution against DOS attack)
Eavesdropping	Physical protection of wires (OR Wi-Fi using WPA/RSN)
Social Engineering	Protection of device and network secrets such as password through education and reminders.

Table 12 Attack on Core/wired portion of WirelessHART *(Raza S. , 2010)*

6 CHAPTER 6

6.1 CRYTOGHRAPIC SOLUTION

The method used in protecting or secure a wireless or wired communication from an attacker is called Cryptography. In this process is in two forms; firstly plain text which is the original set of text that are to be changed in a way that the attacker is not able to understand are converted in to cipher text known as encryption and then from cipher text which is the end-product of any changes made to the plain text, this is made up of the characters on the plain text, but totally different because of some algorithm the sender and receiver have put in place which is changed back to plain text is known as decryption. This method of securing the communication protocol is made up of two type; the symmetric encryption and asymmetric or public key cryptography (PKC).

6.2 Symmetric Encryption

In the symmetric encryption method, the sender and receiver employ the use of shared secret key or encryption or decryption algorithm in their communication for encryption and decryption.

Symmetric encryption methods

- Data Encryption Standard (DES)
- Triple DES (3DES).
- Advanced Encryption Standard (AES).

The Data Encryption Standard was the cryptosystem been used until it was broken in July 1998 using DES cracker (Stallings, 2011). This led into the introduction of the Triple DES, that is implementing the DES three times. In 2001 the National Institute of Standard and Technology approved the Advanced Encryption Standard (AES) (Stallings, 2011).

Asymmetric Encryption Method (PKC)

- Rivest Shamir Adleman (RSA).
- Elliptic Curve Cryptography (ECC).
- ElGamal Cryptosystem.

With key sharing now becoming not very secured the idea of PKC was brought in a way to secure the system from attack. The keys used must always has to be private and the distribution of these keys must be secret can be complex when taking into consideration the types of attacks on the system. According to Stalling William RSA is widely used PKC system (Stallings, 2011).

6.3 Advanced Encryption Standard (AES)

According to Stalling the advanced Encryption Standard (AES) is a block cipher that employ the use of 128-bit block size and 128, 192, or 256 bits of key (Stallings, 2011). The algorithm of the AES works in Number of Rounds (Nr), and the design of one round consist of two different data-paths, namely the decryption data-path and inverse key scheduling data-path (Madduri & Jonnalagadda, 2012).

AES algorithm is made of three main parts; Cipher, Inverse cipher and key expansion. Cipher changes data into cryptic form known as ciphertext, whiles inverse cipher convert data back into its main form called plain text. The key expansion is the one responsible for generating key for scheduling that are used in cipher and inverse cipher (Madduri & Jonnalagadda, 2012). In the AES, a single round is made up of four different functions which are byte substitution, permutation, arithmetic operation over a finite field and XOR operation with a key. AES operations are done using 8-bit bytes. Arithmetic operations of addition, multiplication and division are all done using finite field known as Galois Field GF (2^8). The AES algorithm uses ten rounds which is made of four different stages.

- Substitute bytes
- Shift Rows
- Mixed Columns
- Add Round Key

6.4 Encryption Process

This process is made up of four different stages namely sub byte, shift row, mix column and add round key. These stages are applied consecutively over the data block bits, in a fixed number of iterations called rounds. In the encryption process the length of the key determines the number of rounds. From table 12 below its shows that when the user uses 128-bit key the number of rounds are 10. In 192-bit, the number of rounds is 12 and if the key length is 256-bit, then the number of rounds is 14 (Vanishreeprasad & Pushpalatha, 2015).

.

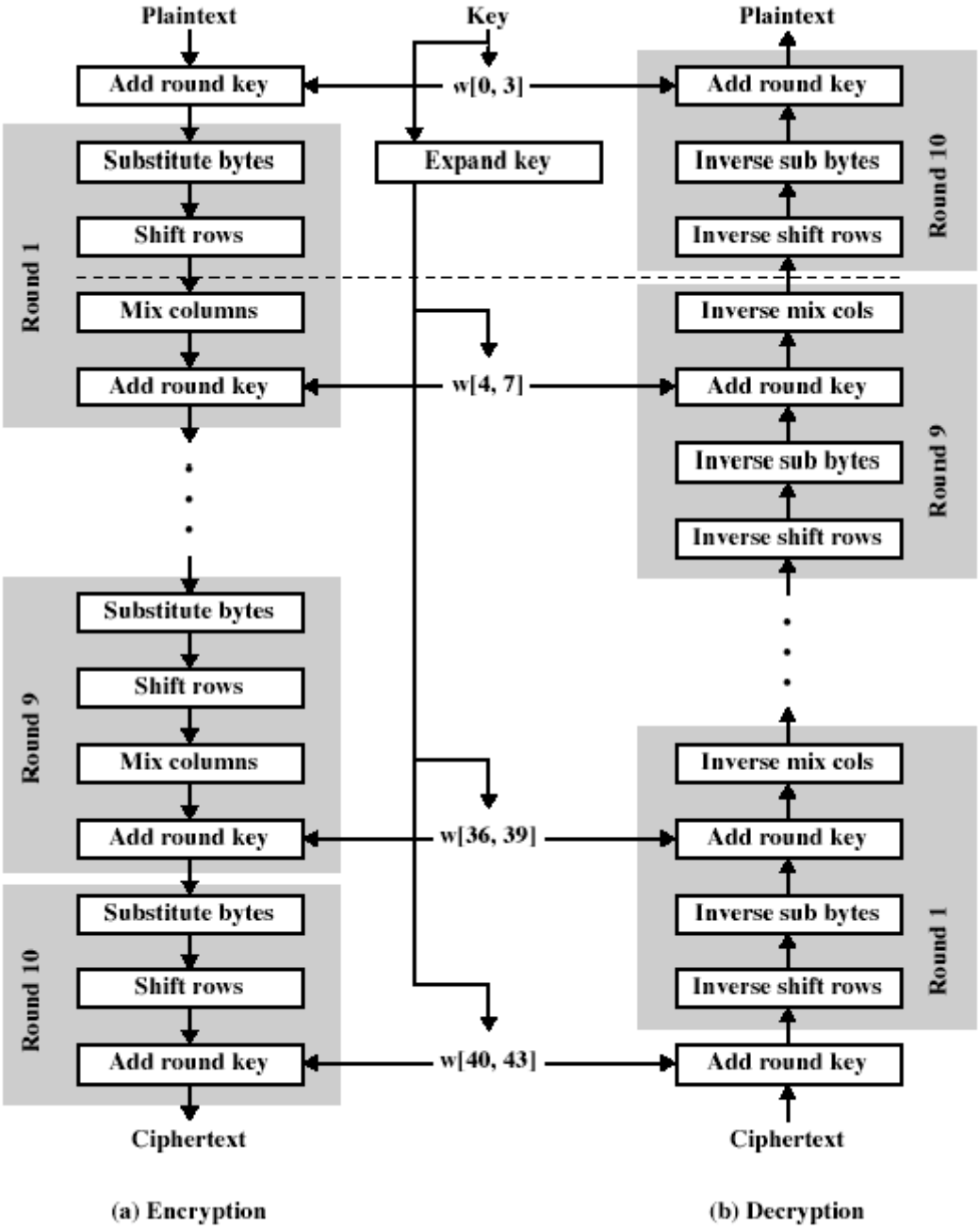


Figure 20 Encryption and Decryption Process *(Stallings, 2011)*

6.4.1 Sub Byte

In the substitute bytes process the use of an S-box to undergo byte to byte substitution of the block. Byte in the matrix are substituted with a sub byte using data from the Rijndael S-box (Vanishreeprasad & Pushpalatha, 2015). The process is much explained in the figure below.

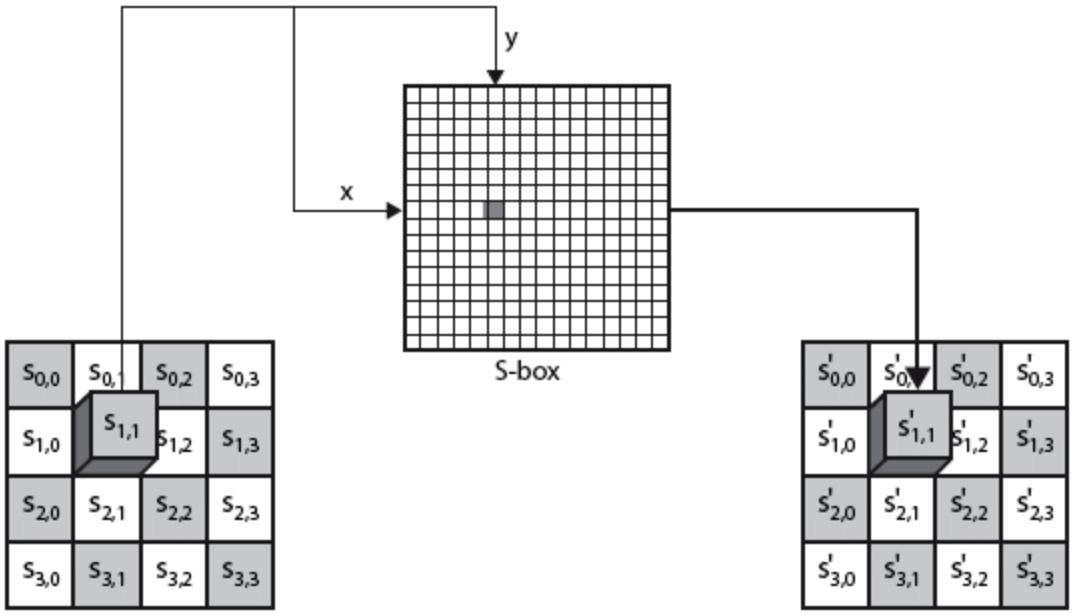


Figure 21 Sub-byte *(Vanishreeprasad & Pushpalatha, 2015)*

6.4.2 Shift Row

The shift Row process is the only process where permutation is done in the AES. In this process a periodic shift of the bytes in each row by certain offset to the left. For AES, there is no change on the first row. On the second row each byte is moved by one to the left. On the third is moved by two and on the fourth row is moved by three (Vanishreeprasad & Pushpalatha, 2015).

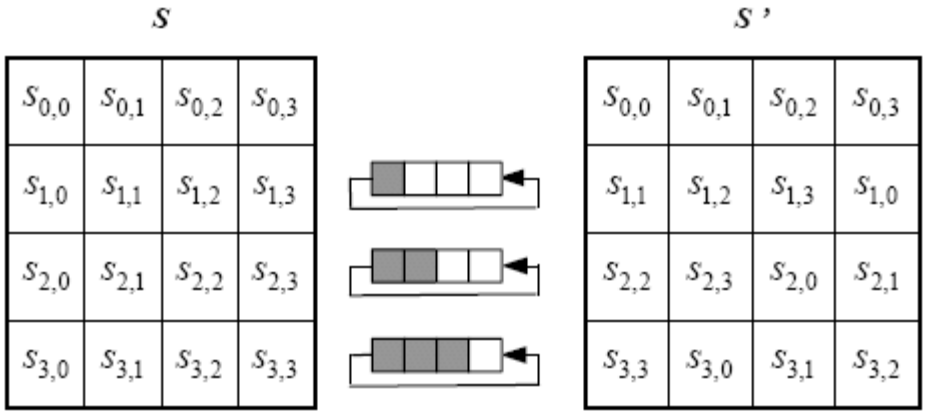


Figure 22 Shift Row (Madduri & Jonnalagadda, 2012)

6.4.3 Mix Column

This is a process of substitution that uses arithmetic of GF (2^8). In this process each column is performed separately. Individual byte of column is mapped into a new value that will be function of all four bytes in the column. The sum of products of elements of one row and one column

becomes the product matrix. The addition and multiplication in this process are done by using the Galois Field (2^8) (Vanishreeprasad & Pushpalatha, 2015).

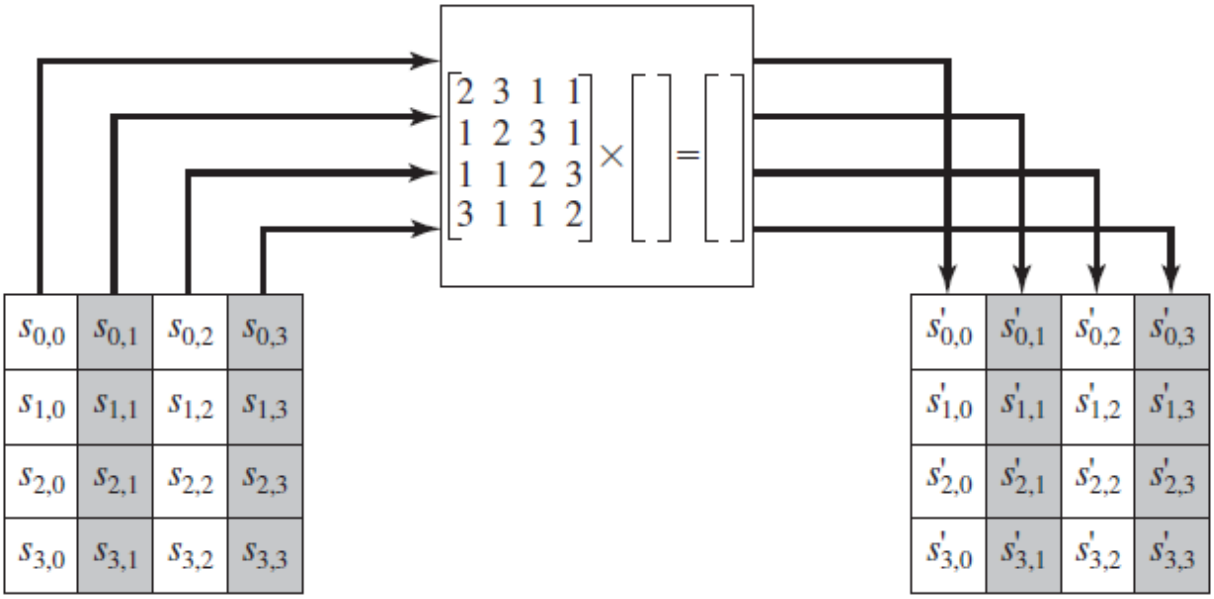


Figure 23 Mix Column (Vanishreeprasad & Pushpalatha, 2015)

6.4.4 Add Round Key

This is a bitwise XOR of the current block with a portion of the key which has been expanded before. In this process the XOR operation is done between the output from the Mix column and the Round Key (Vanishreeprasad & Pushpalatha, 2015)

	Block size (Nb) Words	Key length (Nk) Words	Number of Rounds (Nr)
AES-128 Bits key	4	4	10
AES- 192 Bits key	4	6	12
AES- 256 bits key	4	8	14

Table 13 Types of Key Sizes (Madduri & Jonnalagadda, 2012)

The table shown above, shows that the number of rounds depends on the size of the AES key. 128-bit key is divided into 4X4 matrix which individual element contains 8 bits. When it comes to 192-

bit size, it is split into 6X6 matrix with individual element of 8bits. For the 256-bit size it is split into 8X8 with individual element of 8bits.

6.5 Decryption Process

The decryption process is the direct opposite of the encryption process. In this process all the four stages in the encryption process are inversely applied to this process. In this process the last rounds values of the encryption process become the first-round inputs values for the Decryption process. The four stages of the Decryption process namely Inverse sub byte transformation, Inverse Shift Row Transformation, Inverse Mix Column Transformation, and Inverse Add round Key Transformation will be discussed in detail.

6.5.1 Inverse Sub Byte Transformation

The inverse Sub Byte transformation is the direct opposite of the Sub byte in the encryption process. In this process each byte in the cipher matrix is changed with a corresponding inverse sub byte (Madduri & Jonnalagadda, 2012).

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
	1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
	2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
	3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
	4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
	5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
	6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
	7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
	8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
	9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
	a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
	b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
	c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
	d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
	e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
	f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Figure 24 AES Specified Inverse Substitution Matrix *(Madduri & Jonnalagadda, 2012)*

6.5.2 Inverse Shift Row Transformation

In this process bytes are shifted in same mode as in the encryption process but to the right. The first row remains unchanged. Byte in the second row is shifted by one to the right, third row is shifted by two, and fourth row is shifted by three (Vanishreeprasad & Pushpalatha, 2015).

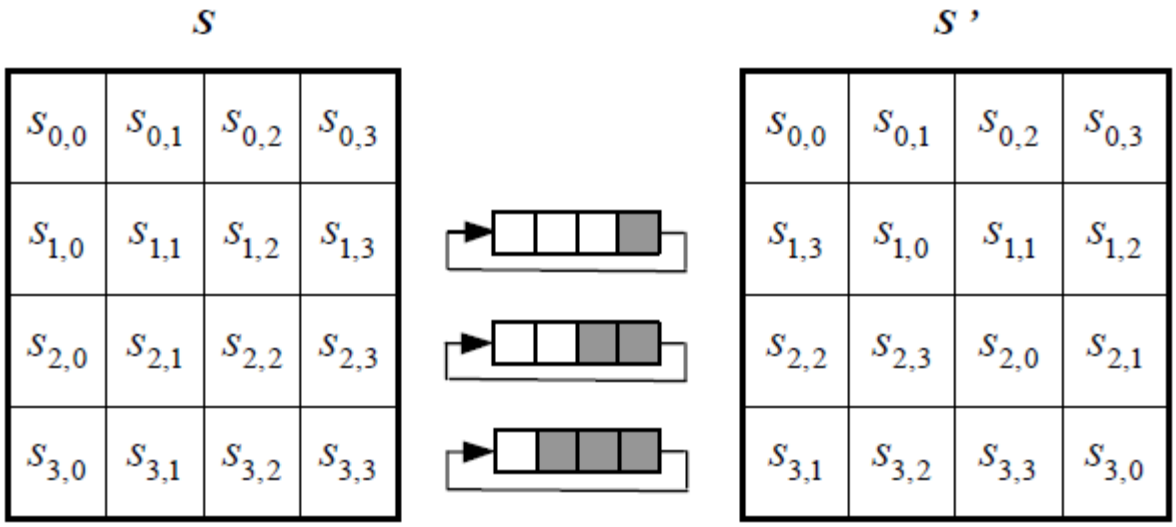


Figure 25 Inverse Shift Row Transformation *(Madduri & Jonnalagadda, 2012).*

6.5.3 Inverse Mix Column Transformation

The Inverse Mix Column transformation in the decryption process is the inverse of the mix column in the encryption process. Though this process is done same way as the Mix column but with different values in the matrix.

$$\begin{pmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{pmatrix} \begin{pmatrix} S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\ S_{1,0} & S_{1,1} & S_{1,2} & S_{1,3} \\ S_{2,0} & S_{2,1} & S_{2,2} & S_{2,3} \\ S_{3,0} & S_{3,1} & S_{3,2} & S_{3,3} \end{pmatrix} = \begin{pmatrix} \acute{S}_{0,0} & \acute{S}_{0,1} & \acute{S}_{0,2} & \acute{S}_{0,3} \\ \acute{S}_{1,0} & \acute{S}_{1,1} & \acute{S}_{1,2} & \acute{S}_{1,3} \\ \acute{S}_{2,0} & \acute{S}_{2,1} & \acute{S}_{2,2} & \acute{S}_{2,3} \\ \acute{S}_{3,0} & \acute{S}_{3,1} & \acute{S}_{3,2} & \acute{S}_{3,3} \end{pmatrix}$$

Figure 26 Inverse Mix Column Transformation *(Madduri & Jonnalagadda, 2012).*

6.5.4 Inverse Add Round Key Transformation

The inverse Add Round Key Transformation is the inverse of the Add Round Key in the encryption process.

7 CONCLUSION

In concluding my thesis work on WirelessHART compared to other wireless technologies. WirelessHART has a wide range of advantages over other wireless technologies ranging from power consumption, cost effective, data security, network security, reliability, fault finding and diagnose, time saving, easy to use, real time update, wide reach and availability and environmentally friendly.

Security: When it comes to security the WirelessHART provides end-to end, per-hop, and peer- to-peer security. WirelessHART uses Advanced Encryption Standard (AES) for encryption and decryption to secure the communication network against inside and outside attackers.

Cost: WirelessHART is said to be less expensive as compared to the wire HART. The cost involve in WirelessHART installation is cheaper than that of wired HART. With wired HART cable installation is either underground or overhead which requires more funding and time.

Installation: WirelessHART installation is simple, time saving and less expensive.

Fault finding and diagnoses: Fault finding in WirelessHART can easily be detected and diagnose by network manager or technician.

Time saving: Because installation in WirelessHART is simple and fast it saves lot of time.

Reliability: WirelessHART is more reliable than other wireless technologies due to redundant of communication path.

Mobility: WirelessHART is mobile as its work in the entire wireless network coverage area.

During my thesis work I came across few shortcomings in WirelessHART security as discuss below:

a. There is no definite public key cryptography
b. There is no path redundancy in the wired part of the network
c. There is no clear connection between the Gateway and the Network manager.

d. WirelessHART does not administer and stipulate security mechanisms to protect the link between the security Manager and Network manager.
e. The network integration between the WirelessHART and the HART is not definite.
f. There is no existing security protection between the Gateway and host application
g. Broadcast communication between field devices is not reinforced.

8 REFERENCES

Bayou, L., Espes, D., Cuppens-Boulahia, N., & Cuppens, F. (2016, October). WirelessHART communication scheme. In International Symposium on Foundations and Practice of Security. 223-238.

Bowen, P., Hash, J., & Wilson, M. (2007). Information security handbook: a guide for managers. . *In NIST SPECIAL PUBLICATION 800-100,*.

Brotby, W. K. (2006). Information security governance: guidance for boards of directors and executive management.

Chen, D., Nixon, M., Han, S., Mok, A. K., & Zhu, X. (2014, February). WirelessHART and IEEE 802.15.4e. 760-765.

FieldComm Group. (2018, December 16). *wirelesshart-security*. Retrieved January 16, 2019, from fieldcommgroup.org: https://fieldcommgroup.org/wirelesshart-security

Forouzan, A. B. (2007). *Data communications & networking*. Tata McGraw-Hill Education.

Karlof, C., & Wagner, D. (2003, May). Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. *Proceedings of the First IEEE International Workshop on Sensor Network Protocol and Applications*, 113-127.

Kim, A. N., Hekland, F., Petersen, S., & Doyle, P. (2008, September). When HART goes wireless: Understanding and implementing the WirelessHART standard. In Emerging Technologies and Factory Automation. pp. 899-907.

Konovalov, I., Neander, J., Gidlund, M., Österlind, F., & Voigt, T. (2011). Evaluation of WirelessHART enabled devices in a controlled simulation environment. *2011 IEEE International Symposium on Industrial Electronics*, 2009-2014.

Lennvall, T., Svensson, S., & Hekland, F. (2008, May). A comparison of WirelessHART and ZigBee for industrial applications. 85-88.

Lorente, E. P. (2015, August). Reverse Engineering WirelessHART Hardware (Masters). 103.

Madduri, K., & Jonnalagadda, P. R. (2012). Decryption of security system for a data link layer in WirelessHART. 1-59.

Mark Nixon. (2012). A Comparison of WirelessHARTTM and ISA100.11a. *whitepaper, Emerson Process Management* , 1-36.

Messai, M. L. (2014). Classification of attacks in wireless sensor networks. , 1-6.

Mohammadi, S., & Jadidoleslamy, H. (2011). A comparison of physical attacks on wireless sensor networks. *International Journal of Peer to Peer Networks , 2(2)*, 24-42.

Murty, S. A., Namboothiri, G. P., & Sivalingam, K. M. (2010). Security Trends and Challenges in Wireless Sensor Networks. *In Handbook On Sensor Network*, 357-397.

Ould Amara, S., Beghdad, R., & Oussalah, M. (2013). Securing wireless sensor networks: a survey EDPACS, 47(2). 6-29.

Petersen, S., & Carlsen, S. (2011). . "WirelessHART vs. ISA100. 11a:"The Format War Hits the Factory Floor. *IEEE INDUSTRIAL ELECTRONICS MAGAZINE*, 25-33. Retrieved 04 17, 2019, from https://brage.bibsys.no/xmlui/bitstream/handle/11250/2430391/SINTEF%2bS18047.pdf?sequence=2&isAllowed=y

Raza, S. (2010). Secure Communication in WirelessHART and its Integration with Legacy HART. 1-103.

Raza, S., & Voigt, T. (2010, June). *Interconnecting WirelessHART and legacy HART networks*, 1-8.

Raza, S., & Voigt, T. (2010, June). Interconnecting WirelessHART and legacy HART networks. 1-8.

Raza, S., Voigt, T., Slabbert, A., & Landernas, K. (2009). Design and implementation of a security manager for WirelessHART networks. In Mobile Adhoc and Sensor Systems. 995-1004.

Song, J., Han, S., Mok, A., Chen, D., Lucas, M., Nixon, M., & Pratt, W. (2008, April). WirelessHART: Applying wireless technology in real-time industrial process control. In IEEE real-time and embedded technology and applications symposium. I., (pp. 377-386).

Stallings, W. (2011). Cryptography and Network Security: Principles and Practice. 31-60.

Vanishreeprasad, S., & Pushpalatha, K. N. (2015). Design and Implementation of Hybrid Cryptosystem using AES and Hash function. . *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE), 10(3).*, 18-24.

Yang, C. L., Tarng, W., Hsieh, K. R., & Chen, M. (2010, December). A security mechanism for clustered wireless sensor networks based on elliptic curve cryptography. *In IEEE international conference on systems, man, and cybernetics (IEEE SMC).*