CHALMERS

Comparison and Evaluation of Industrial Wireless Sensor Network Standards ISA100.11a and *Wireless*HART

Master of Science Thesis, Communication Engineering

GENGYUN WANG

Department of Signals and Systems

CHALMERS UNIVERSITY OF TECHNOLOGY

Gothenburg, Sweden, 2011

Report No. EX036/2011

Abstract

For the reason of ever-growing interest on the utilization of wireless technologies in industrial automation applications, a series of wireless standards that highlight robustness, power efficiency and security, keep struggling with each other. For instance, *Wireless*HART [8] and ISA-100.11a-2009[1], which are two competing wireless standards in process automation industry, both build on the same IEEE STD 802.15.4-2006 radio [2] and aim at the same objectives. In this report, we will present the significant differences that we have found between ISA100.11a and *Wireless*HART, regarding network architectures, functionalities of protocol layers and network operation. For instance, compared with *Wireless*HART ISA100.11a includes comprehensive design of Security Manager, defines three variations of channel hopping schemes, supports legacy protocol tunneling (*Wireless*HART only supports HART protocol tunneling) to highlight interoperability and etc. An evaluation report about different provisioning schemes in ISA100.11a and *Wireless*HART is embedded in the report. Moreover, I will also provide a general view about the possibility of convergence for these two opponents.

Acknowledgements

This master thesis has been advised and performed in the Automation Network Group of Industrial Communication and Embedded System Department at ABB Corporate Research Center. Hence I would like to thank my main supervisors: Mikael Gidlund and Tomas Lennvall, for their guidance and enlightening discussions. Additionally, I want to say thanks to my examiner at CHALMERS, Erik Ström, for his thoughtful advice and helpful comments.

I genuinely express my deepest appreciation to my family, and without their support I would never have been able to keep my faith so as to stand up right on a place far away from home. In addition, many of my special thanks go to Jacques Salaün, Janus Delahaye and Yu Kan for being my wingman and cheering me up from frustration.

Everyone, who has ever directly or indirectly offered their help to the completion of this thesis, is gratefully acknowledged here.

TABLE OF CONTENTS

Definitions, acronyms and abbreviations

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CCM	Counter with Cipher block chaining Message Authentication Code
AL	Application Layer
TL	Transport Layer
NL	Network Layer
DL	Data link Layer
PHY	Physical Layer
DPO	Device Provisioning Object
DBP	Device to Be Provisioned
DPSO	Device Provisioning Service Object
PD	Provisioning Device
ISA	International Society of Automation
OOB	Out Of Band
OTA	Over The Air
EUI	Extended Unique Identifier
HFC	HART Communication Foundation
CA	Certificate Authority
HMI	Human Machine Interface
DM	Device Manufacturer
PKI	Public Key Infrastructure
MAC	Message Authentication Code
6LoWPAN	IPv6 over Low power Wireless Area Networks
CTR	Counter Mode
DPDU	Data Link Layer Protocol Data Unit
ECC	Elliptic Curve Cryptography
MMIC	MAC Layer Message Integration Code
IEC	International Electrotechnical Commission

BBR	Backbone Router
MEMS	Micro-Electro-Mechanical Systems

1 INTRODUCTION

1.1 Industrial Wireless Sensor Network

Wireless technologies have been widely adopted and integrated into almost every part of our every-day life. The result of introducing wireless sensor network to industrial process automation by some organizations [3] [4] [5] [25] proves to have great benefits. Reliability, flexibility and cost-effectiveness of automation solutions and cost reduction, ease of maintenance of industrial plant are all significant merits brought along-side by adapting automation systems in a wireless way.

1.1.1 Wireless Sensor Network

The basic functionality of wireless sensor network is to corporately sensor, gather, process and publish data in the surrounding environment. Sensor nodes could be designed in the form of small devices with low power consumption, limited memory for calculating and communication for the purpose of the convenience of installation in remote area. They are required to have capabilities of routing, dynamically searching, positioning and self-recovery in order to enable flexible topology of the network against harsh and unpredictable environment.

As depicted in figure 1, wireless sensor network consists of groups of sensor nodes that communicate measurements collected in their vicinity to their host sink. Multiple communication paths between intermediate nodes could be adopted flexibly as the network is implemented in an ad-hoc way that each node can route packets independently to the final destination. When data is forwarded on the way to the final sink between arbitrary nodes, extracting useful data out of redundancy needs to be performed.

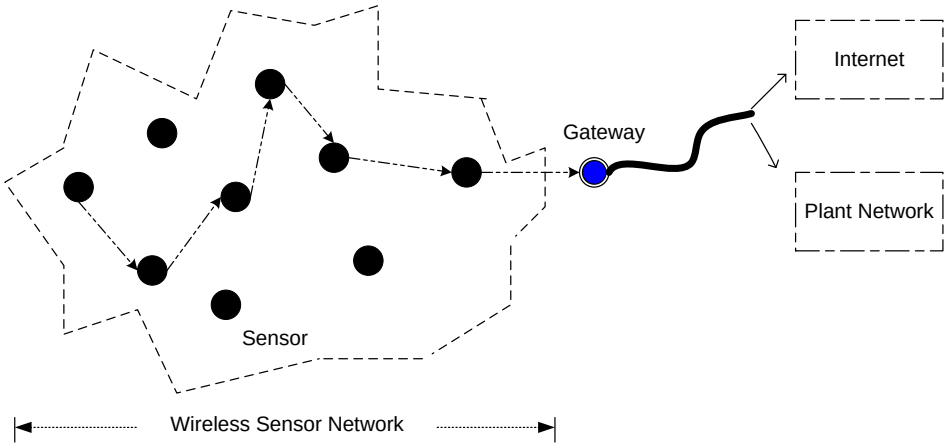

Figure 1, Architecture of Wireless Sensor Network

1.1.2 Industrial Automation in Wireless Sensor Network

The Industrial Automation consists of process automation and factory automation, and the gap between them is shrinking [9]. The process automation is a computer technology-involved continuous process and its plant produces gas, chemical, petroleum, electricity, steel and etc. With the presence of process automation, operational efficiency and safety are achieved as maintenance and monitoring can be simplified with the help of information collected by sensor nodes instead of manpower. Human to machine interfaces, supervisory and control systems are placed at its higher level for processing data and configuration. The lower level, field network where sensor nodes are installed might be in a remote place with harsh environment. Hence the issue of high reliability and safety of communication of sensor-to-sensor (within the field network) and sensor-to-host (between field network and plant network) are very crucial. Compared with wired sensor network in industrial environment, wireless sensor network avoids the costly cable installation and difficult cable maintenance (e.g. cable is long-termly exposed to the chemicals). There exist several designing goals (e.g. stringent timing synchronization, resource efficiency, interoperability with legacy protocol such as FIELDBUS) need to be fulfilled to achieve optimized design of industrial WSN design that meets process automation requirements [10]. But development of MEMS, network and wireless communication technology as well as standardization efforts have enabled industrial WSN to bring connectivity and intelligence by means of a wide range of sensor applications to the industries of advanced monitoring, automation and control solutions. The emergence of Industrial WSN will enable opportunities for increased plant agility, decreased raw material costs, reduced consumption of energy, and lessened negative impact of environment via ongoing improvements of related technologies.

1.2 Thesis Motivation

With the advent of wireless sensor networks, thousands of industrial WSN deployments are currently under development in progress. The fact to apply wireless sensor network to industrial processes wherein communication take place in a hostile environment completely changes the way of the industrial communication procedure, such as reduces extremely expensive cost of maintenance and configuration for wired systems consisting of almost uncountable numbers of sensor nodes in harsh environments and remote areas. Correspondingly, wireless industrial process standards are booming prosperously. ISA100.11a and *Wireless*HART are both wireless communication standards that aim at wireless technology adoption in real-time process control industry with the guarantee of high reliability and robustness. The purpose of this thesis is to gather all information necessary to further dig into two industrial wireless process standards and find out the differences between the two rivals.

1.3 Thesis Organization

This thesis is organized in the following structure.

Chapter 1 Introduction, this chapter gives a brief introduction of industrial WSN, and describes the purpose and scope for this thesis as well as the scientific contribution of mine.

Chapter 2 Background, this chapter reviews the development of industrial WSN standards and provides an overview of *Wireless*HART and ISA100.11a regarding their architecture (e.g. devices and protocol layers).

Chapter 3 Related research work on ISA100.11a, comparison of industrial WSN standards and etc.

Chapter 4 Comparison, this chapter elaborates differences that I have found between two standards from the perspective of Architecture-level, protocol layer-level and network operation-level.

Chapter 5 Evaluation, this chapter is embedded with a comparison and evaluation report with respect to provisioning schemes defined in ISA100.11a and described in a proprietary report of *Wireless*HART from ABB, respectively.

Chapter 6 Conclusion and future work.

Chapter 7 References specifies source material and further reading.

1.4 Thesis Contribution

This thesis acts as an essential summary of ISA100.11a with regard to almost every concerned aspect. Officially, ISA100.12 subcommittee is chartered with convergence work of two standards, but their numerous tasks [36] are yet to be published. This thesis then identifies the in-depth differences between ISA100.11a and *Wireless*HART, which are two competing industrial WSN standards now and in a considerable future. Relevant comparison items, tables and time sequences are originally written and drawn by me to make clear presentation of differences.

2 INDUSTRIAL WIRELESS SENSOR NETWORK STANDARDS

In this chapter, the background information of industrial WSN standards are provided, such as the development trend of industrial process automation standards, the overview of two major opponent standards: ISA100.11a and *Wireless*HART, and their related work.

2.1 The Development of Industrial WSN Standards

As technologies of WSN are developed rapidly, there is a trend to adopt low power, cost and rate standards for ambient intelligence of industrial automation application. Zigbee [5], with the upper layer specification built upon IEEE STD 802.15.4 which is a major standard of low-rate wireless personal area network operating in the 868/915MHz and 2.4 GHz ISM bands, comes out as one of few low-power/cost, monitoring and control based wireless standards together with Bluetooth [6]. However, [7] showed that Zigbee is not suitable for industrial application because it cannot meet the stringent requirements of industrial control regarding deterministic delay and high reliability. Industrial applications demand secure and reliable communication, however, these cannot be achieved by Zigbee as it only has one static channel (no channel hopping scheme is available) and vulnerable to interference in harsh industrial environments. From the timing point of view, neither of Zigbee and Bluetooth can guarantee the end-to-end delay required by monitoring applications that are demanded to communicate with sensor nodes within a second. Therefore two new industrial wireless standards, *Wireless*HART and ISA100.11a, have both emerged and highlighted strict latency and high reliability for the availability of process automation and manufacturing. Additionally, an industrial wireless standard called Wireless Network for Industrial Automation – Process Automation (WIA-PA) [26] is proposed by China and gets approved by IEC with features of HART compatibility, datagram aggregation and so on.

2.2 WirelessHART

*Wireless*HART that was officially released by the HART Communication Foundation in September 2007 is the first open wireless communication standard for process control and related applications [3]. It could be summarized as a TDMA-based wireless mesh networking technology operating in the unrestricted 2.4GHz ISM radio band with stringent timing and security requirements of industrial automation process. And those factors are always major concerns for traditional wired and wireless systems for manufacturing automation applications.

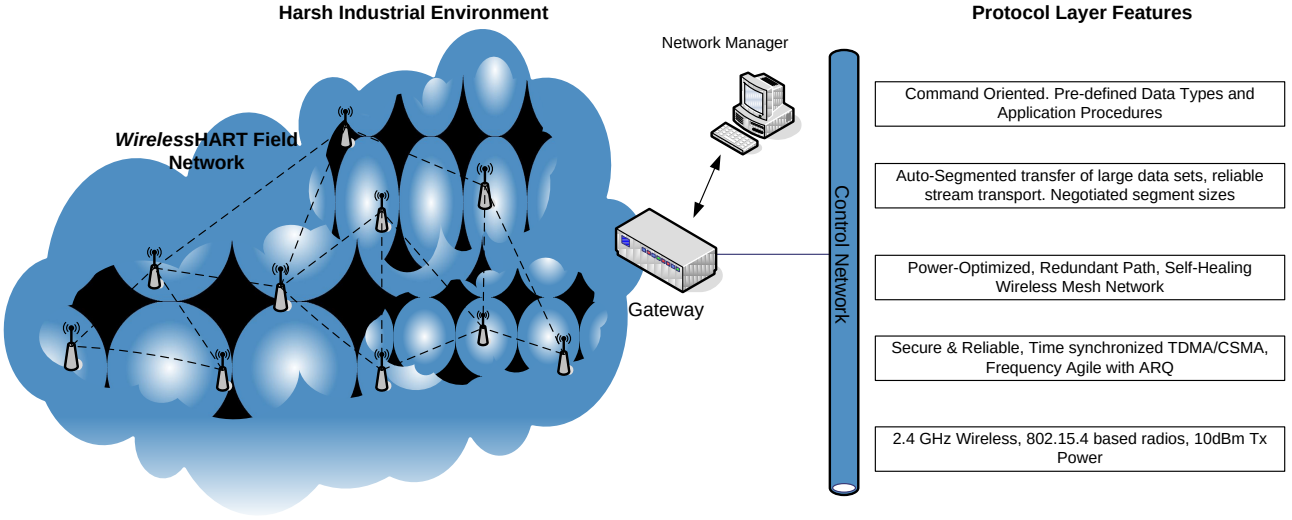

Figure 2, WirelessHART Overview [8]

Six different types of *Wireless*HART devices are involved in the formation of a typical *Wireless*HART network [8].

- Field Device
- Adapter
- Gateway
- Network Manager
- Security Manager
- Handheld

Field devices with routing capabilities installed all over the plant for collecting necessary information and transmitting it back to the plant network for the purpose of process monitoring and control. Generally speaking, they could be viewed as a series of devices with the combined roles of data producer, consumer and router on behalf of routing other devices' messages to their destination. Adapters are specially utilized for converting from a wired fieldbus protocol to a wireless fieldbus protocol, for instance, connecting HART compatible devices that want to communicate via *Wireless*HART network. The gateway acts as an active interface between the Plant Automation network and *Wireless*HART network via one or more Access Points as they are responsible for the communication between host applications and field devices, Network Manager and field devices in the form of protocol translation, tunneling, etc. The Network Manager acts as a commander and controller of the whole network by building and maintaining wireless mesh network. It is also responsible for identifying the best paths and managing distributing resources, scheduling communication for every device in *Wireless*HART Network. The dataflow between Network Manager and

field devices needs to pass through gateway as specified in the standard. Hence a secure communication channel between gateway and Network Manager is a must. Security Manager is in charge of all security-related operations within the network. The last but not the least, a portable handheld operated by plant personnel is used for the installation, configuration and maintenance of field devices. This handheld can be connected to the network either to be a *Wireless*HART device for viewing network diagnostics or a maintenance tool for provisioning, configuring field devices.

According to figure 2, the architecture of *Wireless*HART protocol stack is depicted based on OSI layers, which are Physical Layer, Data Link Layer, Network Layer, Transport Layer and Application Layer. Its Physical Layer adopts IEEE STD 802.15.4 DSSS radios [2], which has 16 different channels with a 5MHz gap between two neighbour channels. The so-called TDMA Data Link Layer is built upon IEEE STD 802.15.4 Physical Layer for mesh network communication and responsible for the collision free, deterministic communication between HART compatible devices. [8] It also defines fixed timeslot of 10ms, network wide time synchronization, channel hopping scheme, channel blacklisting and industry-standard AES-128 block ciphers and related keys. The Network Layer and Transport Layer cooperate together to provide secure and reliable end-to-end communication by means of source routing or graph routing, acknowledged and un-acknowledged transactions to ensure successful delivery against interference. They support varieties of topologies such as self-organizing and self-healing mesh, so as to ensure the robust transfer of data packets to their final destination. In addition to error free transmission, Network Layer utilizes sessions to secure end-to-end communication for confidentiality and integrity of data transferred between *Wireless*HART devices. Only the device on the other end of session processes the same session key that is used to decipher data packet. All devices must have at least two sessions with Network Manager and two sessions with gateway, respectively: one for pair-wise communication and one for network broadcast communication from Network Manager and gateway [8]. The Application Layer of *Wireless*HART protocol architecture is command-oriented with well-defined commands. Moreover, Device-specific commands can be developed by manufactures for device-specific needs as well. The focus of Application Layer is the core payload of messages, such as command definition and data interpretation.

By the end of year 2009, several companies such as Siemens, ABB, Emerson [29] [30] and etc. have already begun to ship interoperable *Wireless*HART automation products including smart wireless adapters that can upgrade existing HART instruments that are installed worldwide to enhance process improvements that are previously unavailable. Some published research and development about *Wireless*HART are available, such as a prototype implementation of the *Wireless*HART has been developed by Song et al.[28] , threats, vulnerabilities and their countermeasures of *Wireless*HART are pointed out and a comprehensive Security Manager design is proposed by Raza et al.[33], regarding the lack of specification of Security Manager in *Wireless*HART. To ensure the HART compatibility, a test suite is designed by Song et al. [34] for the compliance verification and assessment of

*Wireless*HART devices. In addition, being one of many applications that are developed based on *Wireless*HART, a software- based location determination application is implemented and evaluated by Zhu et al.[35] for locating mobile device (e.g. maintenance personnel) using received signal strength in *Wireless*HART network.

2.3 ISA100.11a

ISA-100.11a, approved by ISA standards & Practices Board as an official ISA standard in September 2009, is a wireless mesh networking standard that is targeted to provide reliable and secure wireless communication and operation for process control and related application. The focus of ISA SP100 committee [4] is ISA100 Standard that is a family of industrial wireless standards covering different applications such as process applications, asset tracking and identification, and so on. ISA100.11a is the first standard of ISA100 family with the specification for process automation including the management and security coverage.

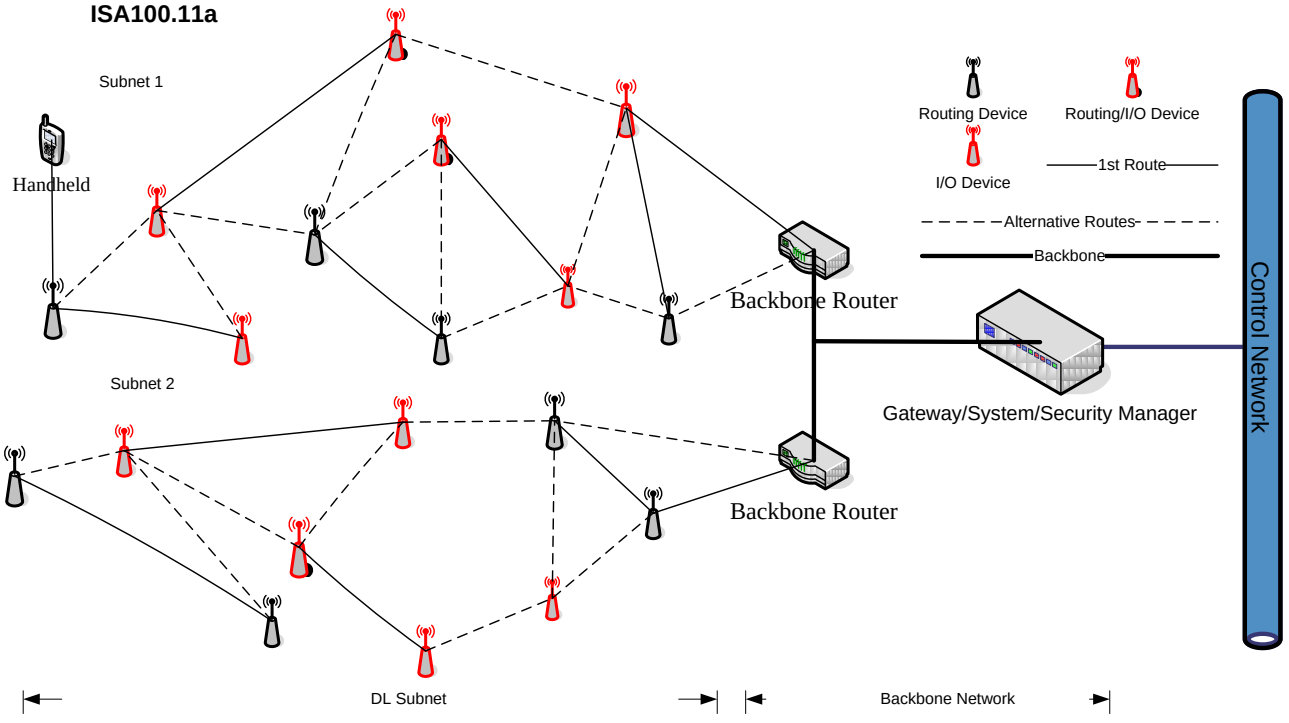

Figure 3, ISA100.11a Network [1]

According to figure 3 the components in an ISA100.11a network consists of field devices, backbone routers, gateway, System Manager and Security Manager. Moreover, ISA100.11a defines different role profiles that represent various functions and capabilities of devices, such as I/O devices (sensors and actuators), router, provisioning device, backbone router,

System Manager, Security Manager, gateway. Each device's capabilities are reported to the System Manager upon joining the network and should be implemented at least one role.

- The I/O device (sensor and actuator) that provides or/and consumes data, which is the basic role to be implemented so as to participate in the network.
- The router role shall be implemented for devices that are responsible for routing data packet from the source to its destination and propagating clock information. In addition, a router role can also enable a device to act as a proxy for the new device to join the network as well as adding path redundancy for mesh.
- A device with provisioning role is responsible for pre-configuring device with necessary information that is used to join a specific network (will be discussed in 4.1.1.3).
- Backbone router can route data packet from one subnet over the backbone network to its destination (e.g. another subnet connecting to the backbone). The backbone shall be implemented with both ISA100.11a wireless network interface (router role) and backbone interface.
- The gateway compliant to this standard is ought to be implemented with a protocol translator and high side interface (GSAP, refer to 4.6.6) at the Application Layer based on existing protocol suite of the device. It acts as an interface between ISA100.11a field network and plant network or probably host applications in the control system and integrates ISA100.11a field network and its device with them.
- The device of System Manager role that is the administrator of the ISA100.11a wireless network shall be implemented with a System Management Application Process (SMAP). System Manager monitors the whole network and is in charge of system management, device management, network run-time control, and communication configuration (resource and scheduling) as well as time related services.
- The Security Manager (refer to 4.1.3) takes active part in providing security services based on security policies defined in this standard, performs security keys management, and guarantee secure system operation. Security manager cooperates with System Manager to participate in system operation internally and externally. It is functionally hidden behind the System Manager. Hence it can only directly communicate with System Manager that implements a Proxy Security Management Object (PSMO) to enable services for forwarding the security message between devices and Security Manager.

As the specified network architecture in figure 3, gateway and System Manager also need to be implemented with backbone router role to get access to the backbone network. The ISA100.11a follows the same OSI layer description methodology as *Wireless*HART does, however many of its protocol suite specifications appear to vary from those of *Wireless*HART's. Chapter 4 of this thesis will elaborate those differences from different layers' point of view.

ISA100.11a is developed to have a broader coverage of process automation (supports factory automation in the future release) networks than those are dominated by HART devices and aimed at converging existing networks and assimilate devices communicating in different protocols. The convergence of *Wireless*HART and ISA100.11a has always been a heated attention paid by both vendors and users. Therefore, ISA100.12 subcommittee [4] has been founded to work under the mission of long-term convergence of the *Wireless*HART and ISA100.11a.

3 RELATED WORK

There is not very much work available on the research and development of the ISA100.11a. But with respect to its security issue, Zhang et al.[18] did develop ISA100.11a-2009 based sensor node platform with implemented security measures and test the security performance of ISA100.11a based network such as computation cost, communication cost and storage capabilities. Other than this, their paper also proposed a brief summary of security protocol suite defined by ISA100.11a. Additionally, an in-depth security analysis for IWSN standards including Zigbee Pro, *Wireless*HART and ISA100.11a has been done recently by Cristina Alcaraz and Javier Lopez [11]. In their paper, the security implementations of the three ISWN standards have been generally reviewed and a set of threats, vulnerabilities and their corresponding countermeasures regarding confidentiality, integrity and availability are presented. Finally the paper proposes some recommendations to enhance those standards' defense capability against certain attacks based on their countermeasures, wherein ISA100.11a has better countermeasures on Sybil attack and sniffing attack than *Wireless*HART does. In contrast to their work, the security part of my thesis is mainly focusing on elaborating differences of security implementations between *Wireless*HART and ISA100.11a regarding:

- Different security levels and cryptographic algorithms available in two standards;
- distinct security operations performed during provisioning and join process (key agreement and key distribution schemes) ;
- summarization of the function of different keys involved in security mechanism;
- and then the functionality of security manager;

Since my thesis does not only concentrate on the security threats and their countermeasures, the aforementioned papers are really worthwhile of digging further into for readers with great interest of security analysis and performance.

Hayashi et al. [32] talk about standardization activities of industrial wireless including Zigbee, *Wireless*HART and ISA100.11a A very brief and general comparison between *Wireless*HART and ISA100.11a is made. The authors highlight that the prospect of ISA100.11a is rising as the end user's expectation and attention have made effort to its standardization. Compared with the comparison made by Hayashi et al., my thesis has proposed a considerably detail comparisons in terms of differences of system architecture, protocol suite, concrete layer operations and so on.

Ishii [31] has used ISA100.11a as a reference system and IPv6 as a backbone to present the effectiveness and functionality of multiple backbone routers adoption. Based on both theoretical analysis and experimental proof, he proves that the spatial diversity that is introduced by multiple backbone routers helps improve the reliability of industrial wireless system.

In [7], Lennvall et al. present *Wireless*HART and compare it with Zigbee regarding issues such as robustness, coexistence and security, proving that *Wireless*HART outweighs Zigbee in many aspects for the industrial applications. In this paper, the authors express the impression of *Wireless*HART and Zigbee on behalf of ABB that has vast experience of industrial applications and their standardization.

4 ISA100.11A VS *WIRELESS*HART

The fact that there are two existing peer standards ISA100.11a and *Wireless*HART both targeting the same industrial automation result from the free-market. Unlike from *Wireless*HART which is an extension to the well-established and well-supported HART Communication Protocol Standard, ISA100.11a developed by ISA SP-100 standards committee aims at a completely new communication standards including management and security design. Hence, this chapter will penetrate and magnify several most significant differences in a broad perspective in two wireless communication standards.

Table 1 summarizes all the differences that are going to be discussed in this thesis. The detail of the difference comparisons and considerations can be found in the corresponding chapters. Please note that these differences shown in the table do not cover every difference in two standards, and only some of them that are to our great interest are going to be elaborated.

	ISA100.11a	***Wireless*HART**
Architecture-level Difference	Backbone device; Provisioning device; Well-defined security manager; Subnet definition; Contract provides QoS for device communication;	Network Access Points; Peer-to-peer communication with potential security risks;
Digital Link Layer	Three channel hopping schemes; Active and passive neighbor discovery; Subnet routing; Configurable length of timeslot;	One channel hopping scheme; Passive neighbor discovery; Fixed timeslot;
Network Layer	Three header specifications; Fragmentation and assembly; Based on IPv6 addressing; Compatible with 6LoWPAN;	Only one header specification; End-to-end session security; Based on HART addressing;
Transport Layer	Connectionless service (UDP); End-to-end session security; Compatibility of 6LoWPAN;	TCP-like reliable communication service;
Application Layer	Object-Orientation; Standard management objects, industry-dependent/independent objects, and ASL services; Three communication interaction models; Support legacy protocol tunneling;	Command-orientation; Predefined data types; Support HART protocol;
Join Process	Symmetric and asymmetric methods; Symmetric and asymmetric key agreement during the key distribution scheme;	Only symmetric method;
Provisioning Process	OTA symmetric and asymmetric methods; Out-of-Band methods;	Cable connection to the maintenance port using Handheld;

Table 1, Differences Preview

4.1 Architecture-level Differences

In the Architecture-level Differences sub-clause, new device and role types (backbone device and provisioning device) in ISA100.11a are described, subnet architecture is discussed, differences in system management suites are presented and security elements (Security Manager, methods, and security keys) of two standards are given.

4.1.1 Network Architecture

As mentioned in chapter 2.2 and 2.3 of this thesis, the basic constructive components of wireless field network in two standards appear to be similar such as field devices, adapters, but with several different implementations.

4.1.1.1 Routing Capability of Devices

The routing capability is inherent in all devices conforming to *Wireless*HART, and every device is required not only to source and sink data but also to forward data packets to their destinations on behalf of other devices. While in ISA100.11a, devices and role profiles are defined, which enable flexible design of devices with multiple role profiles for specific functionalities such as field devices with or without routing capability. The field device (implemented with I/O device role) compliant to ISA100.11a may be implemented with a router role to improve wireless mesh, but this role can also be switched off by the System Manager from the energy saving's perspective. In the harsh environment, the energy-reliability of a field device may surpass its contribution to the system's path redundancy. Likewise, in a low-power-device friendly power plant, the device complexity may compromise with the throughput of the network by switching on the router role.

4.1.1.2 Backbone devices (router) vs Network Access Points

As stringent timing accuracy and high reliability is crucially demanded by industrial process systems, according to the standard of ISA100.11a, it is allowed to configure a field backbone into the network for the purpose of latency minimization, additional bandwidth and higher QoS. In figure 4 the backbone router that acts as an interface between field network and backbone network (probably connecting to the gateway of the field network) encapsulate network layer messages and carry them through protocol stack (PHY, DL, NL) of backbone to the destination, which could be gateway for the host application or another I/O device placed in another end of the backbone (see 4.1.1.3 description of subnet in ISA100.11a).

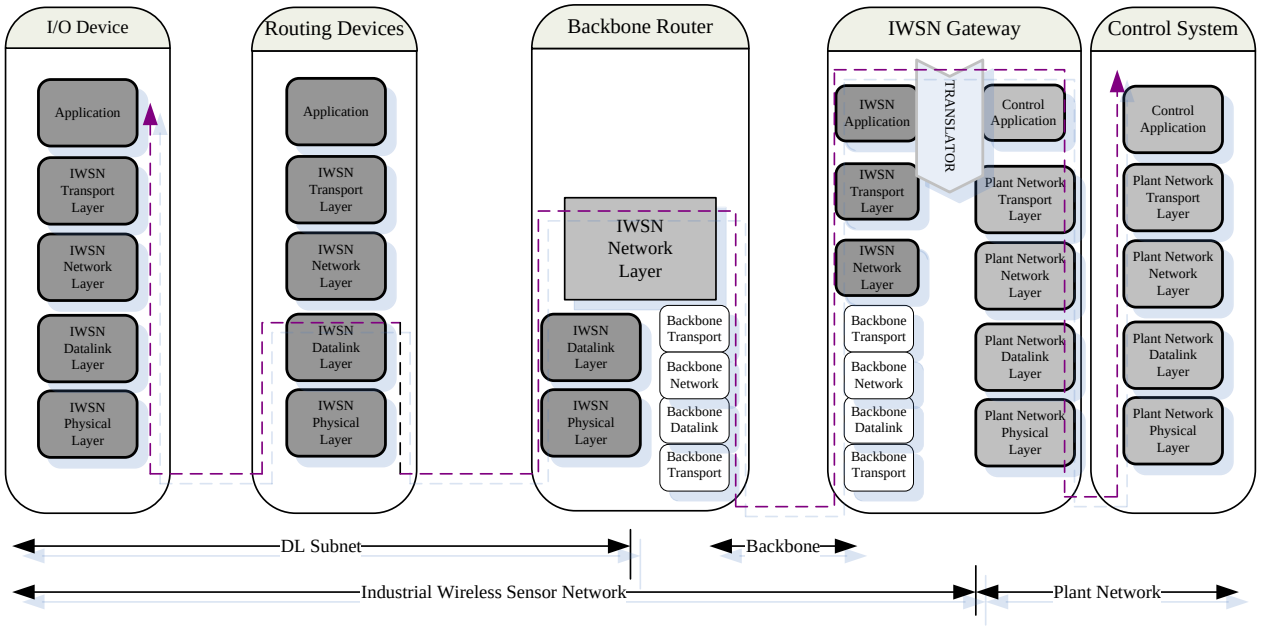

Figure 4, Data Flows through Backbone Router [1]

In *Wireless*HART, no backbone network and devices are defined. But it describes Network Access Points [8] (in figure 5) that can directly connect gateways into the network. They are often referred as virtual gateway and multiple access points and could help increase the efficiency of throughput and improve overall reliability of the network such as what backbone routers do in ISA100.11a. But in *Wireless*HART, the external connection of Network Access Points (the opposite direction of field network side) is not specified. In this way, we could possibly imagine it to be any sort of networks including any commercial backbones considerations in the future release. However, experts working on ISA100.11a have already been considerate enough to make configuration of backbone devices and their interactions with other devices specified into the standard. Moreover, the desired characteristics of backbone network have been summed up in the standard of ISA100.11a in terms of level of throughput, QOS, reliability, security and traffic supported.

Multiple Backbone routers may mitigate the traffic congestion, avoid burst errors and finally enhance the reliability of the industrial wireless network [31].

The inclusions of backbone router enable the usage of higher performance, additional bandwidth and longer range networks. As coin has its reverse side, potential drawbacks of the introduced backbone may also be brought along. For instance, if IP backbone is adopted, corresponding anti-hacking measures (such as restricted access control of backbone routers) need to be performed.

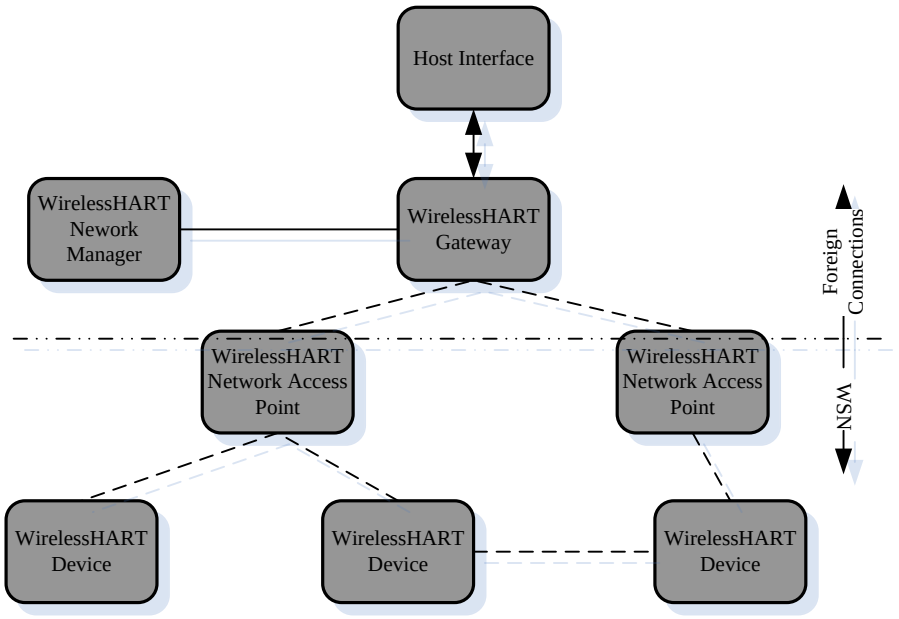

Figure 5, Network Access Points [8]

4.1.1.3 Provisioning Device

Provisioning is the mandatory step before the device over-the-air joins the target field network in both ISA100.11a and *Wireless*HART. The provisioning device will provision new devices arrived from factory default with enough credentials that are going to be verified by authority of target network upon the receipt of join request from the new device. In *Wireless*HART, the handheld terminal is responsible for commissioning secrets to *Wireless*HART field devices [8], while in ISA100.11a, a specialized provisioning device with implementation of Device Provisioning Service Object (DPSO) are in charge of the provisioning process with devices compliant to this standard. The differences and comparisons are elaborated in detail in chapter 5.

4.1.1.4 Subnet

According to the figure 3, subnets are defined as a subset of the full field network. The definition of subnet highlights the scalability of ISA100.11a as there can be up to 2^{16} devices participating in the same subnet and an ISA100.11a can have multiple subnets. From a technical point of view, no limitation is set to the size of a wireless system in this standard, which can differ from of a simple, mini network (small machine shop) to a large integrated field system with the range of kilometers.

Devices participating in the same DL subnets have a share of system manager (refer to 4.1.2.2), backbone, time sources and a specific series of DL configuration such as specific

superframes, links, etc. The addressing scheme is a local matter within a certain subnet, so that a 16-bit local-unique address is assigned to every device in the same subnet by System Manager (a 128-bit address is used globally and EUI-64 is equipped to the device at factory site).

While in the standard of *Wireless*HART, no such term as subnet is used. As it can be seen from the figure 2, a typical *Wireless*HART network only has a single net that consists of all devices in the field without explicit subordinate-network boundaries. In addition, devices compliant to this standard are identified by their EUI-64 (long) addresses and 16-bit nickname assigned by Network Manager for efficiency. Another significant difference between two standards introduced by the term of subnet lies in the distinction of routing levels (refer to chapter 4.4 for detail comparison). Routing of messages are performed both at local (subnet) level using 16-bit short address and NL (global) level using 128-bit long address in ISA100.11a, however, routing only exists at NL level in *Wireless*HART system. Hence, with the inclusion of subnet, ISA100.11a seems to aim at a conveniently scalable and more integrated architecture of wireless system.

4.1.2 System Configuration and Management

4.1.2.1 Protocol Suite

Device Management Application Process (DMAP) that locates on every device is a dedicated application process responsible for the management of the device itself and relevant communication services. As it is known that the Application Layer of ISA100.11a is object-oriented, DMAP certainly has a series of objects that supports device management operations by configuring their attributes and invoking methods via management service access points (SAPs) at corresponding layers. Likewise, System Manager of the network can also access to and perform device configuration remotely via Application Sub-layer Services as shown in the figure 6.

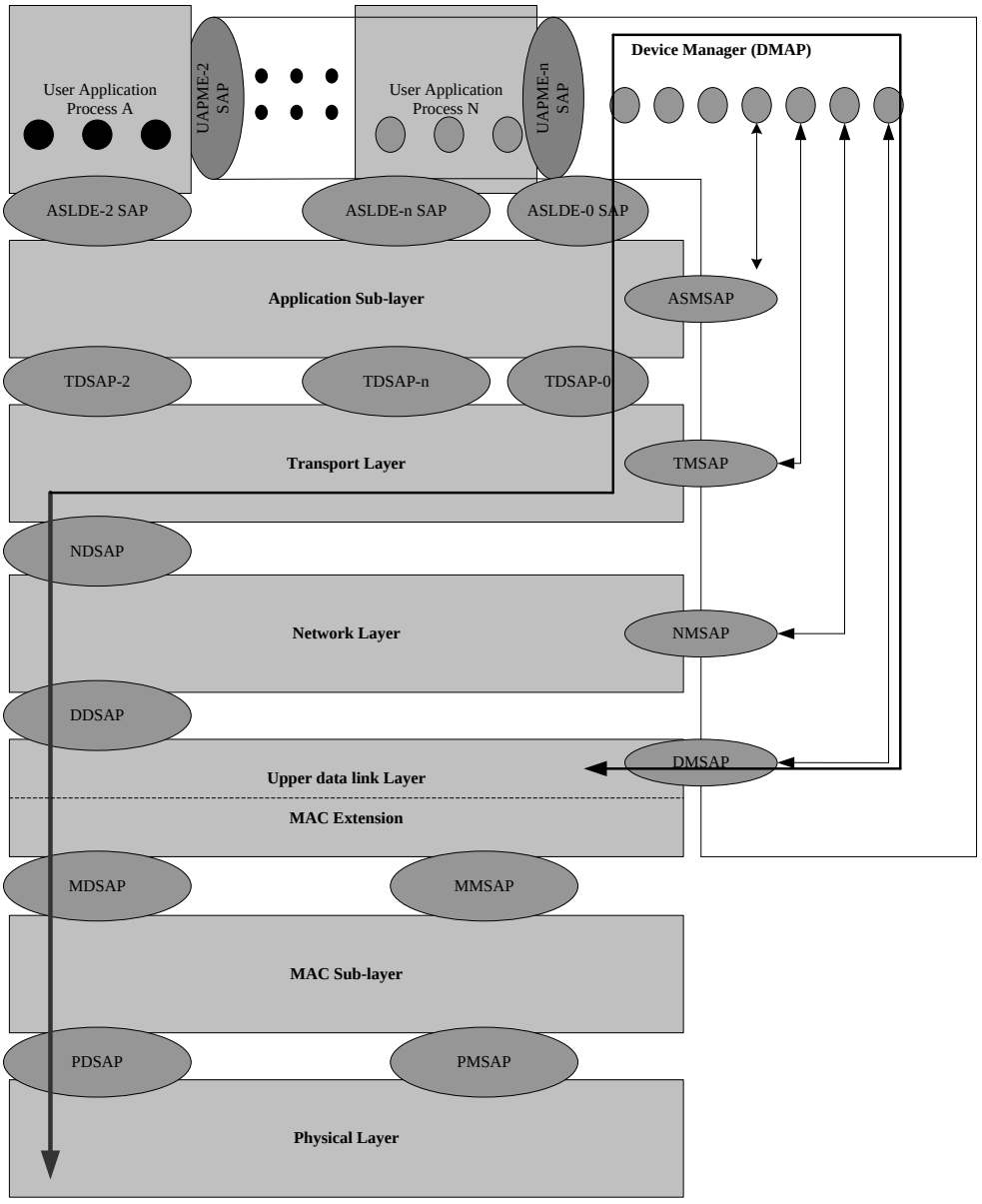

Figure 6, Device Management Dataflow [1]

The arrow on the left side of the figure 6 describes management data flows through protocol suite, wherein the 'XDSAPs' represent the Data Service Access Points of different protocol layers.

The management architecture in ISA100.11a and *Wireless*HART differs widely from each other. According to figure 7, the device compliant to ISA100.11a is viewed as two independent parts that could be configured and managed by different authorities of the system. The DMAP which acts as the manager of the device's communication behaviors

and services is administrated by the System Manager via ASL services over the wireless network. The User Application Processes reside on devices for application-specific purposes, and they are controlled and monitored by host applications (i.e. asset manager) via gateway. The DMAP and UAPs communicate with each other and work together to perform device management.

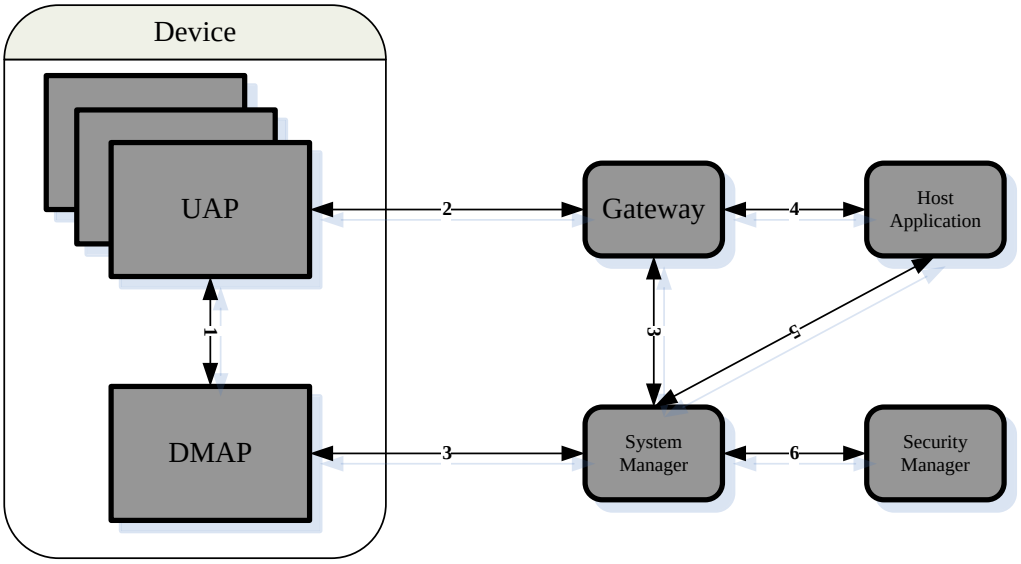

Figure 7 System Management Architecture in ISA100.11a [1]

On the other hand, *Wireless*HART places the gateway as the transport junction of its system management infrastructure as shown in figure 8. Because all device→Network Manager, device→ host applications communication services are passed through gateway that acts as a proxy. Every device in *Wireless*HART network must have two sessions (unicast and broadcast) with gateway to ensure normal participation. Compared with *Wireless*HART, ISA100.11a provides System Manager a direct path to talk to the device for the purpose of system management, while gateway mainly communicates with the UAPs of the device on behalf of the host applications.

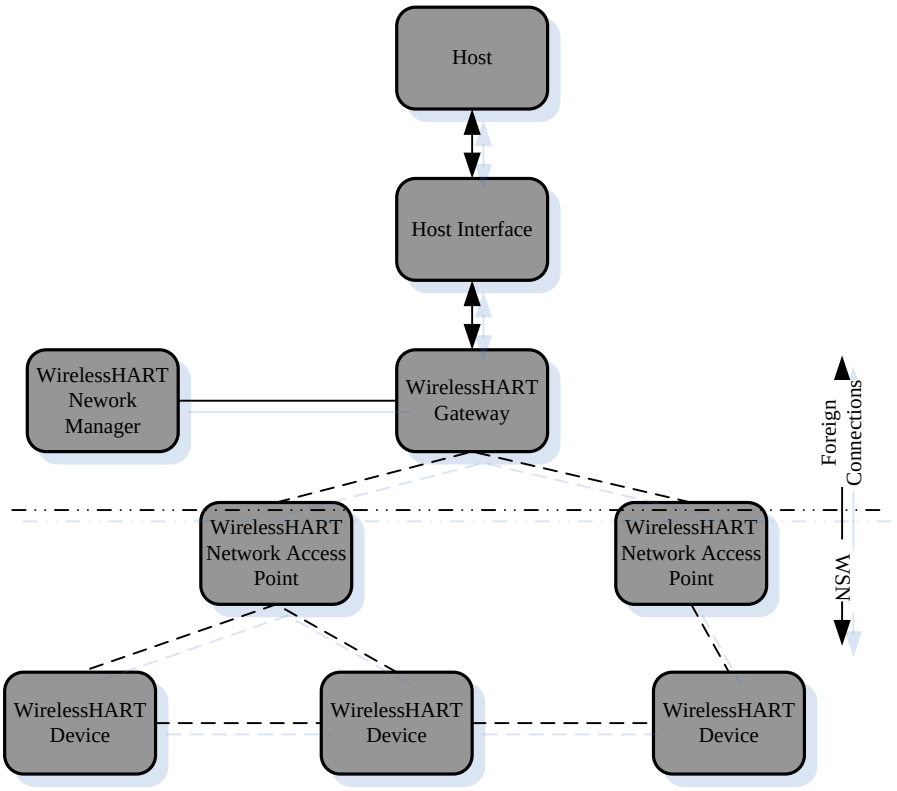

Figure 8, *Wireless*HART Management Architecture [8]

4.1.2.2 System Manager versus Network Manager

System Manager defined in ISA100.11a and Network Manager described in *Wireless*HART performs more or less the same operations regarding the general network management such as, run-time configuration, monitors, scheduling, and optimizations of wireless network as well as support device's joining and leaving in cooperation with Security Manager. Figure 9 and figure 10 show the model of System Manager and Network Manager respectively. Note that the configuration parameters and tables shown in Network Manager model are also all defined in the form of attributes of management objects in the System Management Application Process (SMAP) in ISA100.11a.

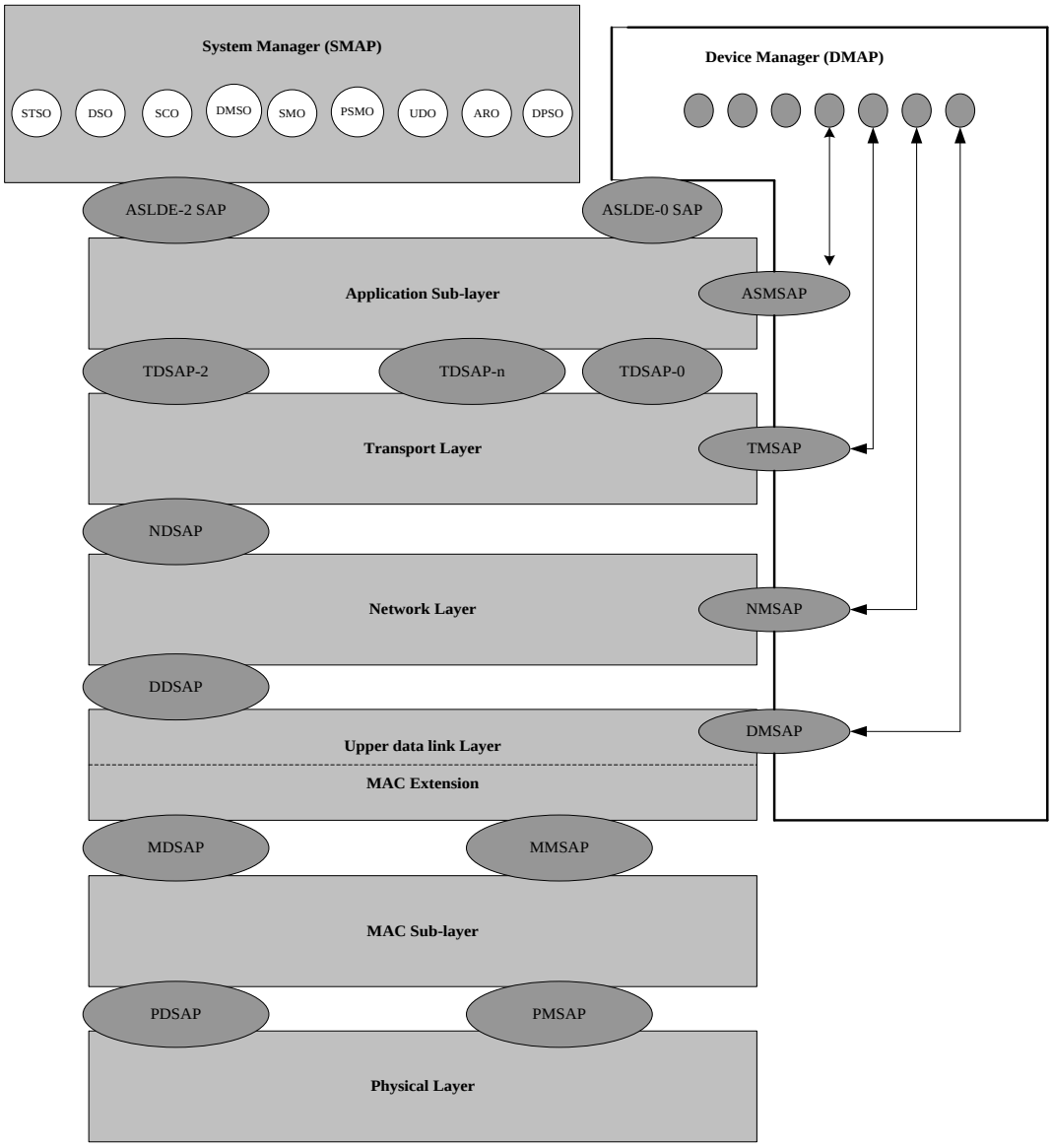

Figure 9, System Management Application Process [1]

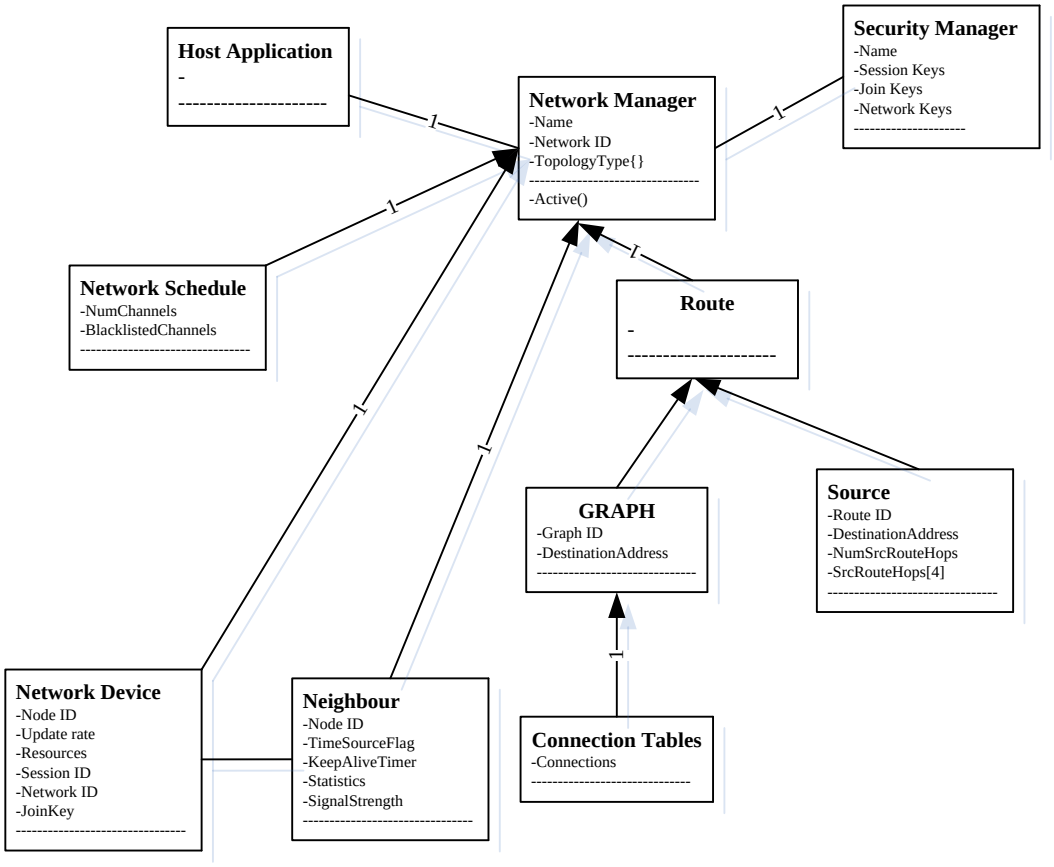

Figure 10, *Wireless*HART Network Manager Management Architecture [8]

4.1.2.2.1 Address Allocation

Device compliant with ISA100.11a shall have EUI-64 as a globally unique identifier, 16-bit locally unique DL address for routing and addressing within a subnet and 128-bit network address in order to enable the device to be accessed by other peers across the network. The latter two addresses of device are both assigned by System Manager while joining the network. Similarly, device in *Wireless*HART network possesses EUI-64 (Unique ID) and a unique 16-bit nickname within its network assigned by Network Manager. In this case, ISA100.11a introduces an additional globally unique address (128-bit) after join process for global addressing (over the backbone), which also dedicates the EUI-64 of device to be utilized for specific uses such as construction of nonce during the security processing. Besides this, System Manager in ISA100.11a can be consulted as a role profile that can be implemented in the form of SMAP on any device in the network without a pre-defined physical address, whereas Network Manager in *Wireless*HART has a fixed well-known (Unique ID and Nickname).

4.1.2.2.2 Peer-to-Peer Communication

Peer-to-peer communication is required in wireless field communication because in some cases it is desirable to keep the control function in field devices and set up direct communication session in between. In ISA100.11a, a contract agreed by System Manager and a device (precisely a certain UAP reside on the device's AL) that wants to communicate with other components in the network, is used to provide system communication configuration. Relevant objects and services are also defined there to formalize the operation of contact establishment, modification and termination. A UAP residing on the device initiates the contract request and sends it to System Manager via its DMAP. Then System Manager determines or negotiates with the device for the allocation of communication resource and configuration required such as time_template, superframes, graph, message priority, etc. A 16-bit contract ID is an important identifier provided to the source device by the System Manager and is the reference to particular configuring information that is needed by the protocol suite of the source (from DL up to AL) and other necessary devices including intermediate and destination. Due to the uni-directionality of contract, the device at the other end of communication path needs to request another contract from the System Manager to run through the pipe as well.

ISA100.11a seems to provide a more direct peer-to-peer communication mechanism. As contract and session (transport layer) are both relevant to a User Application Process (UAP) residing on the device compliant with ISA100.11a. A contract with the peer device includes a shared session key (session is defined at transport layer in ISA100.11a) that secures communication between peer devices. Thus based on already existed contracts, peer devices which want to communicate with each other can set up a secured session with the shared session key obtained from System/Security Manager in a secure way as well as required level of service and management. No contract is defined in *Wireless*HART, but in the latest specification of *Wireless*HART, peer-to-peer communication (arbitrary session) is allowed. Nevertheless, if communication is needed between two arbitrary devices, then the gateway is recommended to be utilized as an intermediate check point in between for monitoring of and protection against malicious traffic as every device in *Wireless*HART network has an existed session (at Network Layer) with gateway. Besides, for maintenance cases such as *Wireless*HART handheld connects field device wirelessly using special superframe [8] and connect field device with cable, direct peer-to-peer communication is always allowed.

4.1.3 System Security

System security is a set of definitions for security terms and building-blocks. Obviously, it contains all crucial aspects for achieving a secure and reliable wireless communication standard. This chapter will elaborate the security features of two standards.

4.1.3.1 Cryptographic Elements in Two Standards

4.1.3.1.1 Symmetric Cryptography

ISA100.11a and *Wireless*HART both adopt “Advance Encryption Standard using 128-bit key in Counter mode with Chained block cipher mode-Message authentication code” (AES128_CCM) as their symmetric cryptography method. Regarding security services, data confidentiality in either standard is provided by AES128 in Counter Mode (CTR) and data integrity, authentication are implemented by AES128 with CBC-MAC (CM). Both encryption and MIC calculation employ the same shared secret key.

AES [13] [14]

The Advanced Encryption Standard (AES) is a symmetric-key encryption standard originating from “Rijndael” that was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen. It consists of three block ciphers, of which the sizes of data are 128, 192 and 256 bits. *Wireless*HART and ISA100.11a both adopt the block cipher of AES-128.

Counter Mode

Counter mode is one of the operation modes defined for block cipher algorithms [15]. According to the figure 11, in counter mode an initialization value (vector) initializes the counter block at the beginning and then the counter block increments itself for each block of plaintext. Afterwards, the algorithm uses the same AES-128 key to encrypt the counter blocks. Finally a XOR operation is performed with corresponding encrypted counter blocks and plaintexts to form the resultant cipher text [15].

As shown in figure 11, data message (plain text) is divided into P1…Pn according to the length of counter (CTR1…CTRn); then the counter is encrypted by AES128 and the XORed with plain text to form cipher text (C1…Cn).

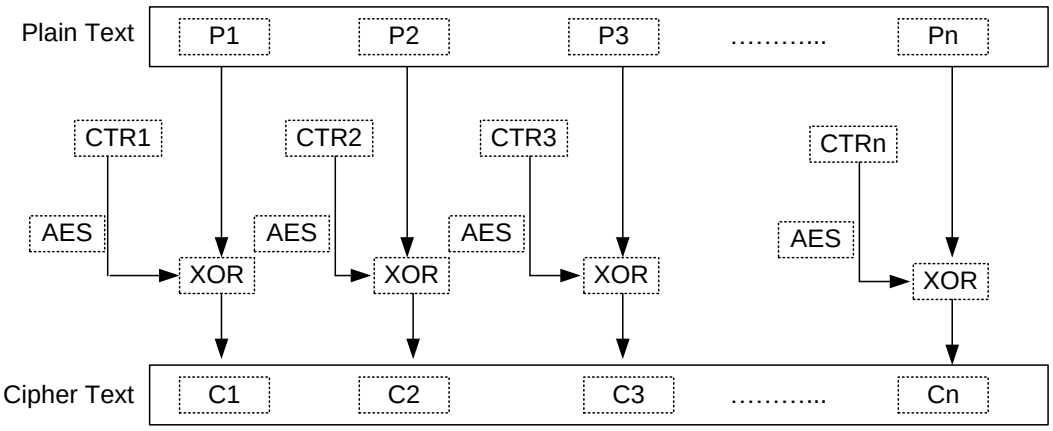

Figure 11, Counter Mode Workflow

CBC-MAC

The CBC-MAC is implemented only for the purpose of data integrity and authentication, wherein MIC is generated by calculation. And both standards make use of the feature that either cipher text or plaintext can be used to generate MIC which can only be verified with the knowledge of shared secret key. According to the figure 12, together with shared secret key, plaintext and initialization vector are used for the calculation of MIC. As the block cipher algorithm needs the exact block size of data to perform processing, the plaintext that is going to be used for MIC computation needs to be grouped into corresponding blocks (where padding might be used). The detail of operation procedure is shown in the figure 12.

The plain text should be divided equally into several blocks according to the length of IV, wherein the zero padding may be performed to fulfill the block size. Then data block (that is formed by the XOR of B1 and IV) is encrypted by AES128. After that, the encrypted data package keeps XORing with B2, and then this result is encrypted by AES128 again. Finally MIC is computed as Bn is XORed with the resultant data from previous operations.

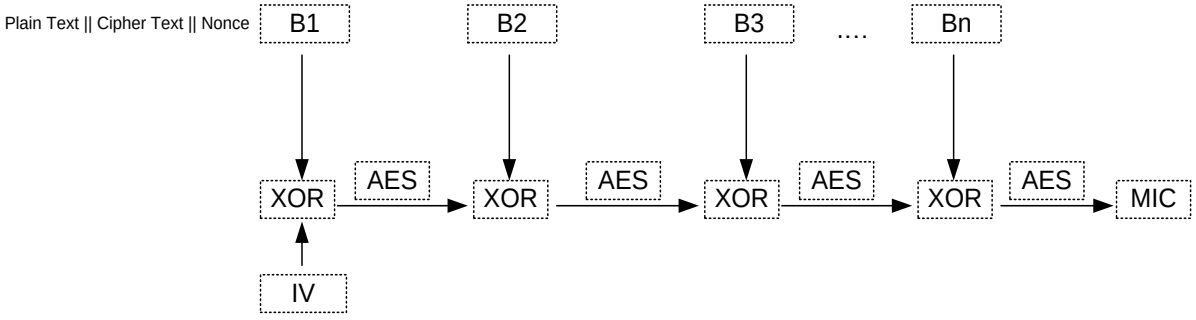

Figure 12, CBC-MAC Workflow

The 13-byte nonce, which adds the freshness factor of messages to prevent replay attacks, is used when generating MIC in both standards. The difference of constructing the nonce in two standards is shown in table 2.

ISA100.11a	**WirelessHART**
DL: Source address EUI-64 (8 bytes) + timestamp (4 bytes) + MHR sequence number (1 byte) TL: Source address EUI-64 (8 bytes) + timestamp (4 bytes) + 0xFF (1 byte)	DL: ASN (5 bytes)+ source address (8 bytes): EUI-64 (8 bytes) or Nickname(2 bytes)+0 (6 bytes) NL: 0 (1 bit) + Nonce Counter (39-bit) + source address (8 bytes): EUI-64 (8 bytes) or Nickname(2 bytes)+'0' (6 bytes)

Table 2, Nonce Construction

4.1.3.2 Differences

Please refer ANNEX H.8 in the standard of ISA100.11a for detail about Security Building Block (data elements and security primitives) for security processing. Herein, only relevant security algorithms and methods mentioned in this thesis are notified.

4.1.3.2.1 Asymmetric Cryptography

ISA100.11a standard uses Elliptic Curve Cryptography (ECC) [23] as its asymmetric cryptographic algorithm during the provisioning and join process. Asymmetric algorithm is optionally used to securely provision security information that is used by devices to join the target network, such as join key and EUI-64 of Security Manager, during the provisioning procedure. And it is also optionally adopted during the join process for first agreement of shared secret that is used to derive the subsequent secret keys. (Key issue, join process and provisioning are going to be discussed later in this thesis.)

In *Wireless*HART, only symmetric cryptography method is supported. But the inclusion of asymmetric cryptography not only introduces more enhanced security strength, but also brings along the computational insensitivity (energy and time) compared with symmetric cryptography.

4.1.3.2.2 Other Cryptographic Methods

HMAC

The default keyed hash function in ISA100.11a is HMAC [16], based on unkeyed hash function Matyas-Meyer-Oseas (MMO) [17].

SKG

The Secret Key Generation (SKG) primitive is used for symmetric key agreement during the symmetric key based join process in ISA100.11a. This SKG primitive provides two communication parties the possibility to agree on the same shared secret when mutual challenges have been exchanged and share the same challenge domain parameters.

4.1.3.3 Security Manager and Security Elements

Generally speaking, Security Manager supervises and controls varieties of operational security aspects of a multi-device network. It cooperates together with System Manager (with which Security Manager can only have direct communication) to ensure security system operation. Due to the fact that Security Manager is functionally hidden behind the System Manager, the System Manager includes a Proxy Security Management Object to manage the security messages (such as messages during join process, and key management and session establishing) that exchanged between devices and Security Manager. However, the interface between System Manager and Security Manager is not specified in this standard. Nevertheless, *Wireless*HART has no description about the design and implementation of Security Manager, only mentioning its Security Manager is responsible for the generation, storage, and management of keying material. While in ISA100.11a, a precise description of Security Manager's functions and definition of security-related objects, methods are given in a formative way.

Security Manager in ISA100.11a	Security Manager in WirelessHART
Support of device provisioning, authorization when joining the system	Be responsible for generation, storage and management of keys, but no normative implementation or design, only support symmetric cryptography
Defined Key management including key generation[1], key storage, key updating, key archiving, key recovery, etc	
Support both asymmetric and symmetric cryptography	
Interaction with system manager and devices via well-defined objects (PSMO and DSMO) and primitives	
Authorization and management of DL and TL communication relationships and security associations	

Table 3, Different Security Manager Design in two Standards

As we can see from the table 3 above, *Wireless*HART has no comprehensively specified requirements of the design or implementation of Security Manager, which also means no methods of key management are specified even though key management plays an extremely important part in the security management of the wireless network standard. Whereas, the specifications for designing System Manager compliant with ISA100.11a is very elaborate (such as well-defined "Delete_key" method overcome the short coming that in *Wireless*HART no command for deleting network key is defined [8]), so that they provide an overall image for the designers to have the convenience for universal implementation.

4.1.3.3.1 Keys

In both standards, data encryption and authentication is achieved by using symmetric keys (128 bit AES keys) with limited lifetime. Unlike from *Wireless*HART, asymmetric keys (public key of a certificate authority and certificate of a certain device) can be used for joining process in ISA100.11a. From the table below, we could have a brief image of the different keys utilized in two standards.

[1] *Please refer to ANNEX H in ISA100.11a*

ISA100.11a	***Wireless*HART**
Join key	Join key
DL key	Network key
Session key	Session key
Master key	No master key is mentioned
K_Global (Global key)	Well-known key
Asymmetric keys	No support for asymmetric cryptography

Table 4 Security Keys defined in two Standards

Join key, namely, is used by the device that wants to join the target network as an authorized password in both standards. In *Wireless*HART, it acts as a session key to ensure the end-to-end security between the device itself and Network Manager during the join process. But in ISA100.11a, UDP checksum is used to protect join message at TL level (session is defined on TL in ISA100.11a). Instead, the join key in ISA100.11a is used to generate message authentication code for application layer data (e.g. EUI-64 of device) in join request (the join process will be discussed later in chapter 4.7 in this thesis). The provisioning process describing how join key is commissioned to the device how provisioning methods differs from each other in two standards will be discussed in chapter 4 of this thesis.

DL key and Network key are actually two different names defined in the two standards but aiming at the same purpose, which is to provide hop by hop security between neighboring devices on the way of data message (generation of MIC at DL level and optional encryption of DPDU payload) to its final destination. The scope of DL key/Network key is different in two standards, which is subnet-level in ISA100.11a and network-level in *Wireless*HART respectively. As the data message may traverse the whole subnet (network in *Wireless*HART), all devices participating in the same subnet/network share the same DL/Network key.

Likewise, the session keys defined in two standards both aim at secured session communication process with the encryption of message's payload and MIC calculation of the entire message. Differently, the sessions described in two standards differ slightly as one is established on the Transport Layer (ISA100.11a) and another one on the network layer (*Wireless*HART). Additionally, a direct peer-to-peer secure session is allowed in ISA100.11a but not in *Wireless*HART as the gateway may act as an intermediate checkpoint.

In *Wireless*HART the distribution of Network key and Session key is accomplished by the command "Write Network Key" and "Write Session" [8] separately. While in ISA100.11a, key distribution of DL key and Session key is performed in a fashionable way with the help of the master key. Master key is the first derived key at the conclusion of key agreement during the symmetric key joining process (this key distribution and key agreement scheme will be

discussed in chapter 4.7 of this thesis). Most importantly, it is the exact key to decrypt data flow from System Manager to obtain DL and Session key. Precisely speaking, this dataflow originates from Security Manager and is redirected by System Manager due to the fact that Security Manager only talks to System Manager directly. Additionally, the master key can be used during the communication between the device and Security Manager, e.g. during the session establishment.

All of Session key, DL/Network key and Master key defined in either standard have limited life-time and need to be updated due to security requirement.

The relationship between Well-known key and Global key is the same as it between Network key and DL key. As they are both published value, they only provide data integrity check and are widely used in the join request message because the device needs to protect DL level message during the join process without receiving DL key from the Security Manager. Additionally in ISA100.11a, Global key has a special application during the provisioning stage, and it will be discussed later in chapter 5.

Asymmetric keys (public/private keys) are used in the asymmetric key based join process and over the air (OTA) provisioning in ISA100.11a. The support for asymmetric cryptographic capabilities is an optional requirement of devices compliant to this standard.

4.1.3.3.2 Security Sub-layer

ISA100.11a defines a specialized security sub-layer that has interfaces to both DL and TL providing transmission security and related aspects required by constructing outgoing DPDU (TPDU) and processing incoming DPDU (TPDU) during session establishment, join process and associated policies. It also provides security services to enable:

- Communication entities authorization (EUI-64 and Join Key);
- Message authenticity and integrity (MIC);
- Data confidentiality; (Encryption with Session key or DL key)
- Replay attack protection (Nonce) ;
- Timing assurance;

For instance, we show a simplified graph here describing the security processing for an outgoing DPDU. As shown in figure 13, security sub-layer in ISA100.11a has a series of interaction with the DL in the way of Automated Teller Machine. The DL inputs freshly constructed DPDU without DL-level protection into the security sub-layer. Then the sub-layer furnishes DPDU with related security information such as building nonce, optional encryption of payload and calculation of MMIC. Similarly, this mechanism applies to all other scenarios such as incoming and outgoing ACK/NACK, and TPDU. Only the primitives and data used by security processing and check differ according to different cases.

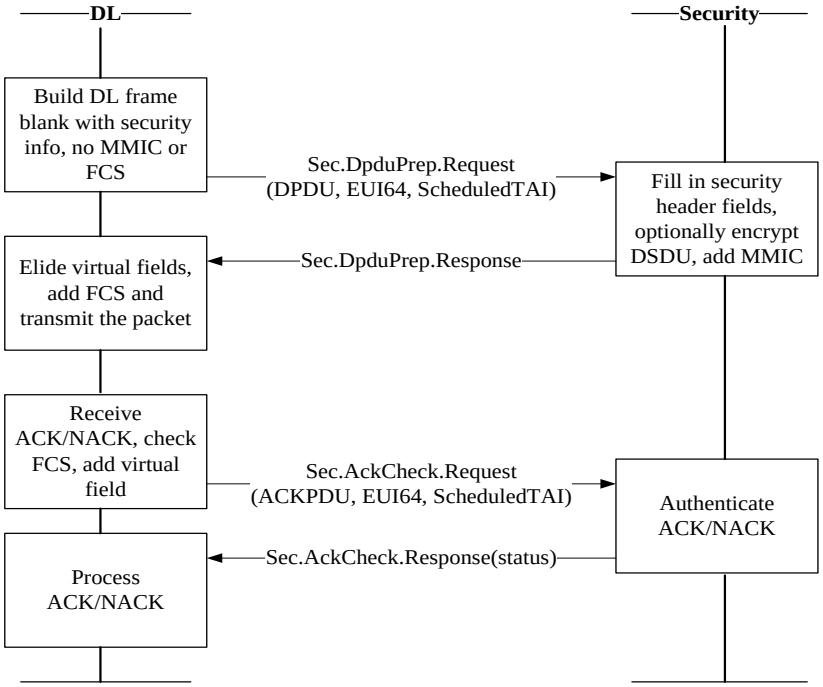

Figure 13, Interaction between Security Sub-layer and DL [1]

In *Wireless*HART, a Logical link control layer is responsible for the security service for used for message integrity and authentication at DL level and a security sub-layer (that is exactly a security sub-header) is defined on the network layer for the secure session communication. According to the security levels, ISA100.11a has a series of levels ranging from default “authentication only with MMIC of 32 bits” to maximum “encryption and MMIC of 128 bits” show in the table 5. But as indicated in the table 6, *Wireless*HART has only one level of 32 bits MIC to protect data integrity which is mentioned on session level.

Security Level Identifier	Security Control Field Bits	Security Attributes
0x00	000	None
0x01	001	MIC-32
0x02	010	MIC-64
0x03	011	MIC-128
0x04	100	ENCRYPTION
0x05	101	ENCRYPTION-MIC-32
0x06	110	ENCRYPTION-MIC-64
0x07	111	ENCRYPTION-MIC-128

Table 5, Security Levels in ISA100.11a [1]

Security Type	Counter Length	MIC Length
Session Keyed	8-bit (LSB of-32 bit Nonce Counter)	32-bit
Join Keyed	32-bit Nonce Counter	32-bit
Handheld Keyed	32-bit Nonce Counter	32-bit

Table 6, Security Type at Session Level in *Wireless*HART [8]

To summarize the security-related aspects (primitives, cryptography building blocks, data structure and so on) in ISA100.11a is well defined and organized. Developers can conveniently adopt the normative design requirement and instructions described in the standard to fulfill a well-qualified security environment. Lacking of a comprehensive description of security mechanism in *Wireless*HART network, *Wireless*HART leads to a diversity of vendor-specific security environments.

4.2 Physical Layer

The Physical Layer of both standards takes the responsibility of modulation method, signal strength, and device sensitivity. The Physical Layer of both ISA100.11a and *Wireless*HART are constructed based on IEEE STD 802.15.4 standard that employs Direct-Sequence Spectrum Spreading and O-QPSK modulation [2] with their own additional requirements and exceptions, respectively. Some of them are much alike for instance, the adoption of 2450

MHz and exclusion of channel 26 (optional in ISA100.11a) [8], and some of them distinct from each other such as transmit power limit. But these similarities and differences are not the major interest of this thesis, and they can be clearly pointed out in the technical data sheet.

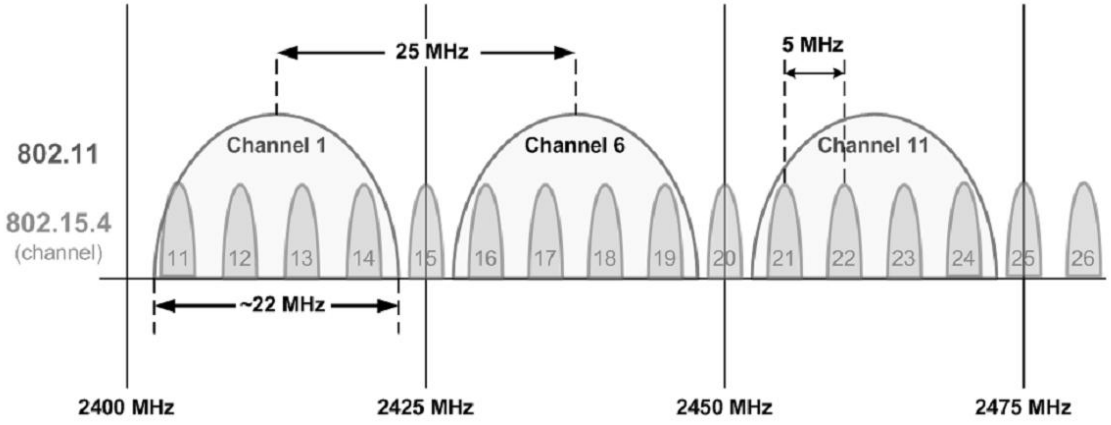

Figure 14, Spectrum Usage and Channels Availability [1]

As we can see from figure 14, Channel 1, 6 and 11 that are assigned for IEEE802.11 such as WIFI, have overlapped with most of channels assigned to IEEE STD 802.15.4. Therefore coexistence among legacy devices will be an important issue and discussed the chapter of Data Link Layer.

4.3 Data link Layer

Generally, the Data Link Layer of both standards are responsible for the secure, reliable and error-free transmission of data packets between devices in the wireless mesh network built on IEEE STD 802.15.4 Physical Layer in harsh industry environment. The DL of both standards also define basic building blocks including timeslots, superframes, links and graphs that can be used by System Manager (Network Manager) to configure the devices' communication alternatives.

4.3.1 Protocol Data Unit Format

The general format of Digital Link Layer protocol data unit in *Wireless*HART is given below in figure 15.

- The Address Specifier is used to specify which type of address is contained in the source and destination field of DPDU, either 16-bit nickname that are assigned by Network Manager or the EUI-64 address.
- The bits in DPDU Specifier indicates the DPDU priority, whether the DPDU is authenticated by Network Key, and the types of DPDU such as Data, Advertise, Keep-Alive, etc.

- The 32-bit MIC is message integrity (authentication) code for the Data Link Layer authentication using Network Key. During the join process, the MIC of DPDU is generated using Well-Known Key.
- The 16-bit CRC that are used for checking random errors, and Physical Layer header format are in accordance to IEEE STD 802.15.4.

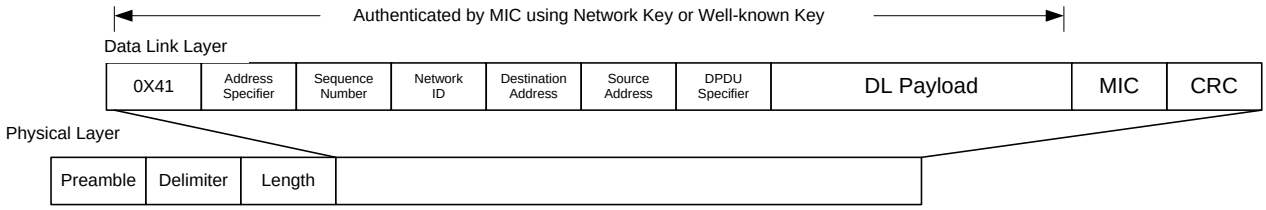

Figure 15, DPDU format in *Wireless*HART

The DPDU in ISA100.11a has a distinct and much more complicated format compared with WirelessHART.

- The PhPDU header, MAC header and Frame Check Sequence are as specified in IEEE STD 802.15.4. The DL of ISA100.11a adopts a subset of IEEE STD 802.15.4 MAC as its Medium Access Control Layer and extends its MAC Layer with other logically MAC functions that are not included by IEEE STD 802.15.4 MAC.
- The DHR in figure 16 consists of a series of sub-headers that abstracts the DL functons e.g. link, mesh, security aspects, etc.
- The Data Link Layer header sub-header (DHDR) has the DL version number and general DL selections such as whether ACK is needed or not by the receipent.
- The Data Link Layer Media Access Control Extension sub-header (DMXHR) contains fields such as security control and key identifier that indicate the security option adopted by security-sub-layer. The MMIC (32-bit, 64-bit or 128-bit according to table 5) that generated by DL key (Global Key during the join process) for data authentication (integrity) should be logically part of the DMXHR. The DMXHR also implement additional fields that are not included by IEEE STD 802.15.4.
- The DHR auxiliary sub-header (DAUX) is only presented in dedicated advertisement or solicitation messages (see 3.3.5 Neighbor Discovery).
- The Routing sub-header (DROUT) provides information for Subnet-level routing (see 4.3.4) in terms of graph ID or source route, DPDU priority, etc.
- The Address sub-header (DADDR) contains Network Layer source and destination addresses as well as Explicit Congestion Control (ECN) [24], Last Hop [LH], Discard Eligible (DE) that are provided via upper layer.

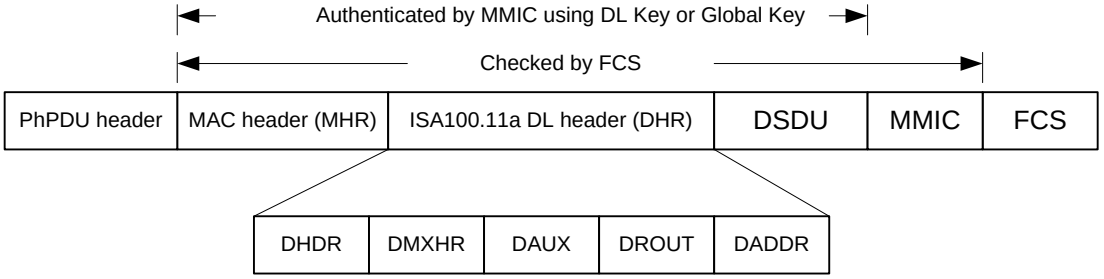

Figure 16, DPDU format in ISA100.11a

The fact that huge differences can be seen from two standards' the DL header specifications has proved that the DL of ISA100.11a aims at a more integrated and flexible wireless link mesh e.g. variations of channel hopping schemes, subnet-level routing, customized security adoption, etc. Some of new features that are introduced by DL of ISA100.11a are going to be discussed in this chapter.

4.3.2 Coexistence Strategies

As the frequency band of 2.4GHz is part of the Industrial, Scientific and Medical (ISM) bands for the intention of unlicensed uses, for reliable and coexistence issues, the DL of both Standards adopt:

- TDMA based time slotted and scheduled operation to minimize the possible collision of transmission within the network (within the subnet in ISA100.11a);
- Channel Hopping scheme to reduce cross-interference or multipath fading;
- Data authentication and integrity (ISA100.11a has an option of data confidentiality on DL but not set as default) provided by security mechanism.
- Limitation for the use of channels that have relatively high interference and error probability, such as channel blacklisting, spectrum management;

The adoption of TDMA technology with precisely network-wide time synchronization give birth to the efficient access to RF medium and time diversity. WirelessHART has a fixed length of timeslot, which is 10ms. Differently, ISA100.11a standard specifies configurable timeslots with the duration between 10 and 12ms on a per-superframe base. Configurable timeslots give birth to optimized coexistence and flexibility as shorter timeslot can make the best utilization of optimized implementations. Furthermore, longer timeslots can be used for extending waiting time for serial ACKs from multiple destinations, accommodating the unpredictable time delay caused by CSMA performed at the start of a certain timeslot, slow hopping (Channel Hopping scheme will be discussed later in this chapter) of extended duration and matching of timing settings with other standards for interaction.

4.3.3 Channel hopping schemes

Based on the availability of multiple channels from IEEE STD 802.15.4 Physical Layer, Channel hopping schemes defined in two standards combine TDMA together to introduce frequency (channel) diversity and time diversity to further reduce the possibility of communication under the relatively high interference. *Wireless*HART describes one channel hopping scheme (slotted hopping) with variation of patterns by changing different channels as shown in Figure 17. The channel hopping order is dependent on the channel offset, absolute slot number (ASN) and the number of channels that are currently alive. The actual channel used for the current communication in its corresponding timeslot can be computed by:

Active Channel = (Channel Offset + Absolute Slot Number) % Number of Active Channels

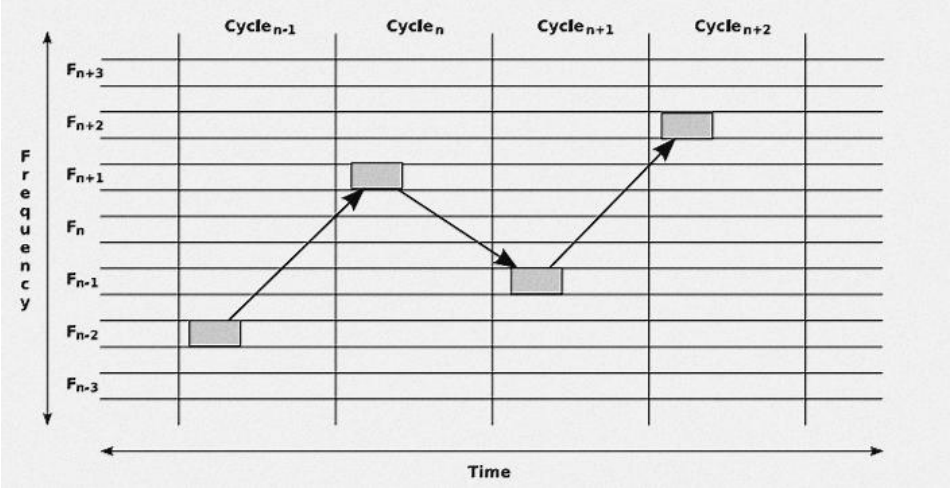

Figure 17, Basic Channel Hopping in WirelessHART

In ISA100.11a, three Channel Hopping schemes, which are slotted hopping, slow hopping and hybrid hopping, are defined to enhance the flexibility and specialty when dealing with different types of communication.

4.3.3.1 Slotted, Slow and Hybrid Hopping Schemes

In **slotted hopping**, each timeslot uses the next successive (different) radio channel in the hopping pattern. The timeslots in slotted hopping shall have the duration and be able to accommodate a single transaction which is DPDU and its ACKs/NACKs. Slotted hopping is used in the communication of which the timeslots are allocated explicitly. Moreover, the slotted hopping scheme is utilized in the communication scenarios where tight synchronization is crucial or transceiver is energy-limited (such as battery-powered).

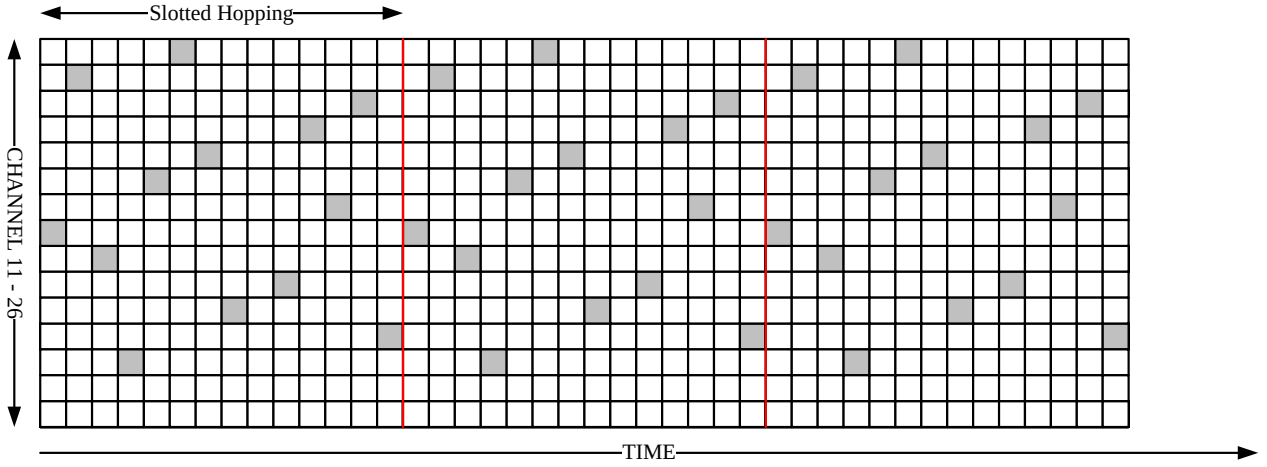

Figure 18, Slotted Hopping [1]

According to figure 19, one channel during **slow hopping** is occupied by successive timeslots, and the slow hopping duration is typically 100-400ms designated by System Manager. Compared with slotted hopping, longer duration of timeslots could support devices with imprecise timing settings or devices that temporarily lost contact with the network. Usually, Channel 15, 20 and 25 are designed as slow hopping channels and may be used for neighbor discovery. Conveniently, the device that wants to join in a certain network could mainly scan field routers on these channels for the advertisement of target network. Besides, slow hopping can be also used when loose requirement of synchronization is required or the energy for running a receiver of the device is enough for a period of time.

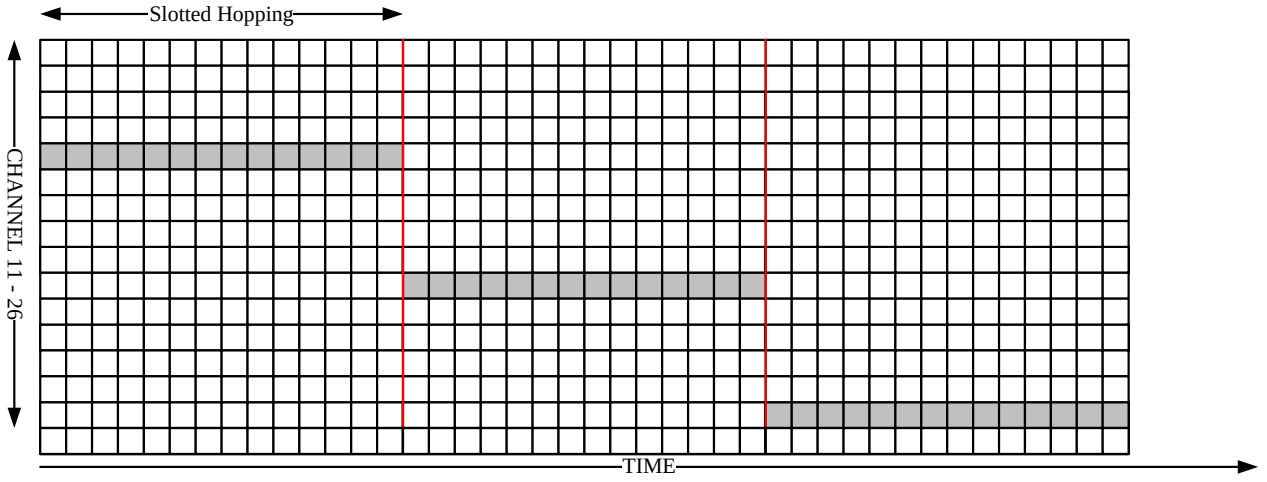

Figure 19, Slow Hopping [1]

Hybrid hopping is actually an adaptive combination of slotted and slow hopping, where slotted hopping accommodates scheduled and periodical messaging, and then slow

hopping less predictable messaging such as alarm and retries. Figure 19 below gives a comprehensive example of hybrid hopping.

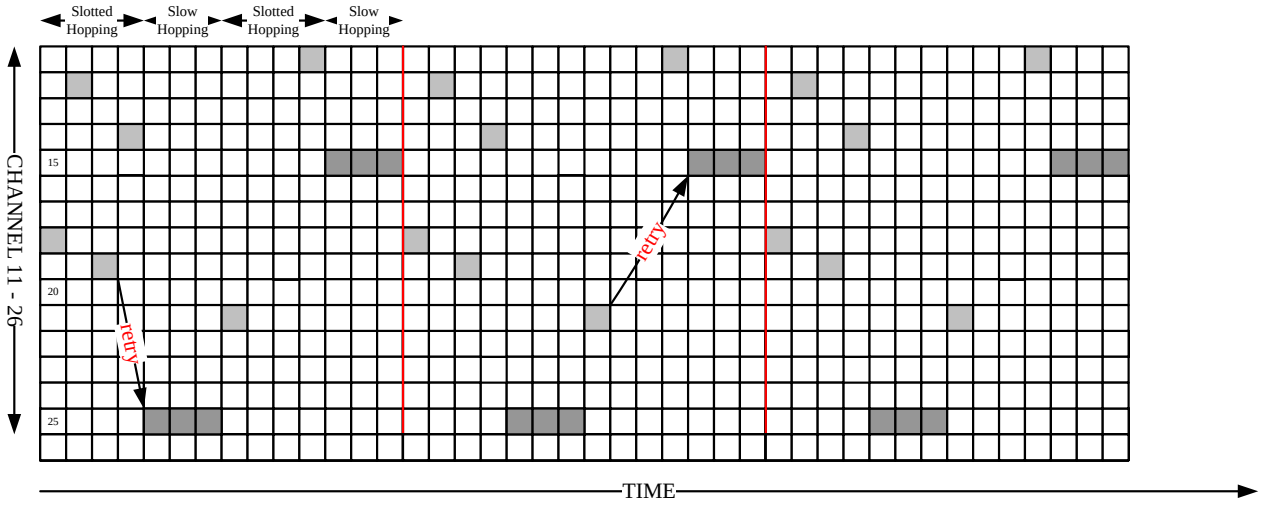

Figure 20, Hybrid Hopping [1]

Five default slotted hopping patterns are pre-defined and supported by every device compliant to this standard. The successive channels organized in the hopping pattern separate each other with 15 MHz or three channels, which reduces the interference and fading Moreover it also ensures retransmission not to be performed on the same IEEE 802.11 channel in figures 14 and 21, due to highly-probable interference from other device operating at the same band. Customized hopping patterns are also supported by ISA100.11a under the administration of System Manager for flexible design.

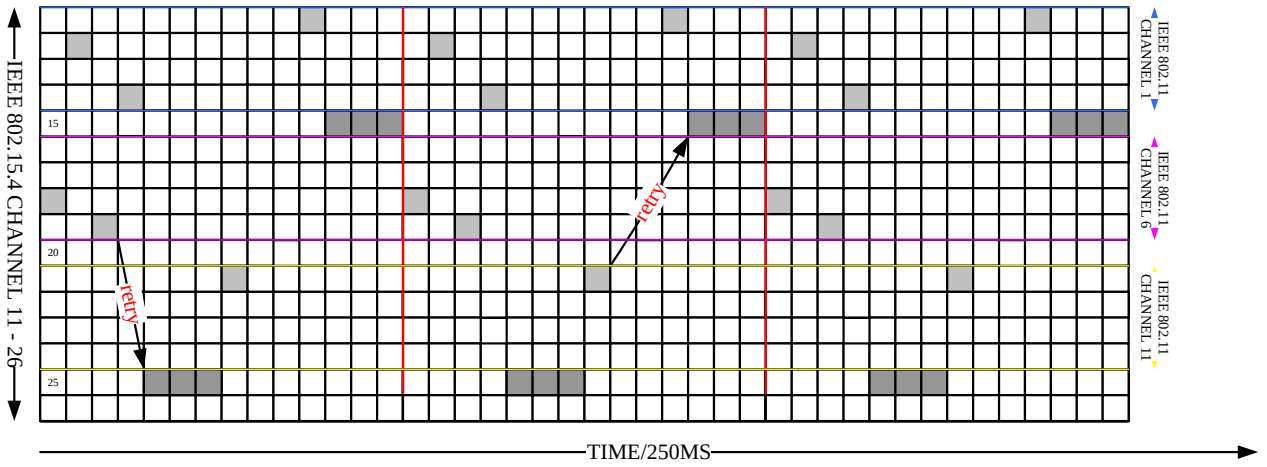

Figure 21, Default Hopping Pattern 1 in ISA100.11a [1]

Multiple choices of channel hopping schemes in ISA100.11a give birth to the communication scenario-specific design. Configurable length of timeslot together with a specific channel hopping scheme assigned for a communication-specific purpose makes the ISA100.11a a versatile communication system.

4.3.4 Data Link Level Routing Scheme

Unlike from *Wireless*HART that only performs routing on its Network Layer, ISA100.11a with the division into subnets also performs its routing at DL level. In the wireless network of ISA100.11a, messages can be traversed through subnet at DL level based on either graph routing or source routing schemes that are configured and designated by System Manager. Figure 22 depicts the routing of DPDU among neighbors within each DL subnet. As soon as the message arrives at the backbone router (endpoint of a subnet), it will be equipped with a network layer header in order to be routed to its final destination across the backbone network.

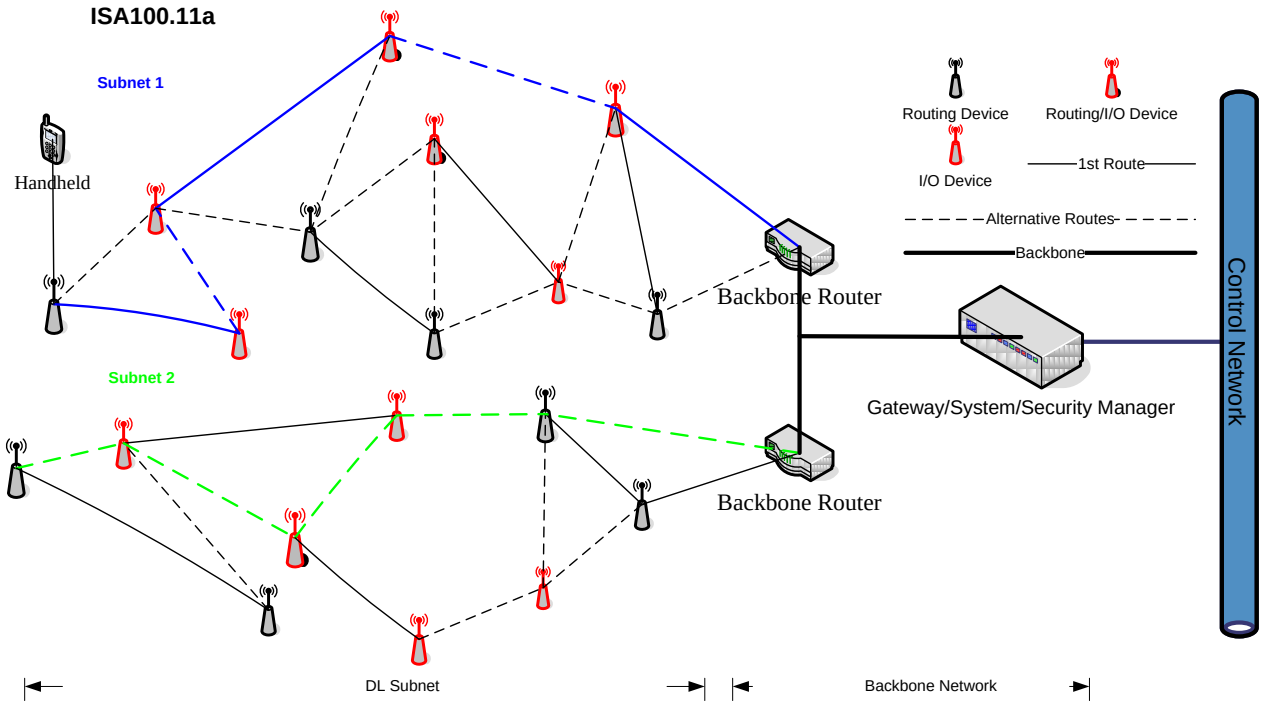

Figure 22, Routing within Subnet [1]

Both graph routing and source routing is supported by devices at DL level. The routing itinerary such as graph ID or source route list is stored in a special section (DROUT-sub header, please refer to ISA100.11a-9.3 for data frame structures) of the DL header. To ensure the feasibility of DL subnet routing, the routing itinerary and related aspects of header are constructed based on the contract ID, destination address or by default route backbone router or other backbone capability-enabled device when the DPDU step into the range of DL subnet. Interestingly, a forwarding limit field in the DL header acts as almost the same function of “hop limit” in IPV6 header. It sets limitation of hops of the DPDU to be routed within the DL subnet. If the forwarding limit field reaches to zero, the corresponding DPDU will be discarded on the next hop. All necessary components involved in routing operation such as table of address lists are defined by this standard.

Resulting from the neighbor discovery (which will be discussed later in this chapter), devices already generate a certain amount of reports that indicates information of current and past connectivity to the surrounding neighbors. Then the System Manager could analyze these references so as to configure the routes needed by devices compliant to this standard. Therefore, the so-called adaptive DL routing that can be conveniently realized as the generation of neighbor discovery reports is an ongoing process, with which the System Manager could optimize the route decisions.

4.3.5 Neighborhood Discovery

Neighbor discovery is a crucial procedure to mesh network operation for the maintenance and optimization of mesh to achieve required communication reliability and efficiency. It is also an ongoing process to be performed throughout the operational cycle of the device, which starts from the unprovisioned states and spreads all over the joined states. Usually, the neighbor discovery consists of two stages:

- Device that wants to join a network discovers and receives advertisement consisting of network information from designated advertising routers or proxies to initialize join request;
- After becoming a part of the network, the device sends out and receives advertisements to/from its neighbors to build internal candidates list so as to help the administrator of network (System Manager in ISA100.11a and Network Manager in *Wireless*HART) to update and finally optimize the network topology and mesh configuration.

In *Wireless*HART, devices that are already parts of the network advertise the network information to new devices with joining attempts and exchanges “Keep-Alive” with neighbor devices in order to provide the update and maintenance of network settings to Network Manager. The main effort that a device’s transceiver spends on scanning either advertisements or “Keep-Alive” messages during the neighbor discovery process is merely listening. Although the device searches the target network to join with two different searching modes (which are active search and passive search) during the joining process, the two modes only differ from the duration for how long the device can run its receiver actively. Hence they are still performing passive actions (listening).

ISA100.11a not only keeps the same passive listening scheme in the neighbor discovery as *Wireless*HART for the benefits of energy issues, but also introduces an active scanning scheme with active solicitations for the advertisements. In active scanning, two roles of scanning interrogator and active scanning host are described. In the case of joining process, scanning interrogators are devices that are in need of advertisements from advertising routers. And they periodically transmit advertisement solicitations to neighbor routers. Upon the receipt of solicitations, the routers that are so-called active scanning hosts will reply the interrogators with advertisements including subnet information for them to initialize join requests. Passive scanning resembles the operations in *Wireless*HART as it also has the active listening period wherein performing on a series of channels at power on, after that it performs passive listening scheme for the purpose of preserving energy. The active scanning hosts in active scanning mode can also be configured to periodically send out advertisements within the network for the convenience of devices that perform passive scanning. The way how devices perform neighbor discovery are scheduled and configured by System Manager of the subnet via management interactions with DL management object and its attributes in DMAP.

Obviously, ISA100.11a creates a way for the devices to take the initiative in acquiring subnet join advertisements and formation advertisements (“Keep-Alive” messages in

*Wireless*HART). However the energy capacity is always an important issue for the selection of neighbor discovery schemes. Active scanning requires devices (e.g. scanning hosts) to have enough energy to run their receiver continuously or at least (for the battery-powered) operate continuously throughout the sensitive periods such as during the network formation. Passive scanning (both in *Wireless*HART and ISA100.11a) can also fulfill the mission by either listening on advertisements channels over a period of time for as many advertisements as possible (active search) or just sampling the channels periodically for handful information. Anyway, active scanning scheme introduced by ISA100.11a probably overcomes the substantial delay that might be brought during the passive scanning and increase the efficiency of operations during the network join/formation process. Furthermore, a filtering scheme can be provided via the mechanism that attaches a subnet ID with the solicitation so that only a preferred set of subnets' advertisements can be heard.

4.3.6 DL Summarization

DL specifications	ISA100.11a	WirelessHART
Routing	Has at subnet level	N/A
Channel hopping	3 variations and pre-defined hopping patterns	Has only one slotted hopping
Neighbor discovery	Active and passive scanning	Passive Listening
Burst advertisement scheme	Has, a series of successive identical ADs transmitted together to provide devices a power-efficient way to use channel sampling techniques for passively listening	N/A
Transaction supported	Unicast, broadcast and duocast	Unicast, broadcast
Configurable timeslots	Has, 10-12ms	N/A, 10ms fixed

Table 7, Summarization of DL Differences

According to the table 7, the DL of ISA100.11a standard covers and extends services that already exist in *Wireless*HART e.g. configurable timeslots, more options of channel hopping schemes to accommodate device with different timing capabilities. Furthermore, it has developed a series of new alternatives that enable more flexible solutions such as DL level subnet routing. All DL behaviors are administrated and maintained by System Manager via interactions with management object (DLMO) and its corresponding attributes defined in DMAP.

4.4 Network Layer

The Network Layer specifications of *Wireless*HART mainly aim at convergence for traditional HART networks and new *Wireless*HART networks [8]. However these features are not the interest and scope of this thesis. In the following paragraphs, we are going to consider and discuss differences such as routing, addressing, etc.

4.4.1 Security

*Wireless*HART's Network Layer provides end-to-end security session for secure communication with correspondent parties. Session key is used for the providing data confidentiality and integrity. Then only the destination device which shares the same session key with the source device is able to decipher the secret messages arriving from the other end of this session. As a part of *Wireless*HART network, the field device compliant to *Wireless*HART should at least have four sessions to ensure normal network operations:

- Unicast session between a field device and Gateway;
- Unicast session between a field device and Network Manager;
- Broadcast session between all field devices and Gateway;
- Broadcast session between all field devices and Network Manager;

The similar session security mechanism (end-to-end) is provided at the Transport Layer in ISA100.11a. Besides, the session in ISA100.11a can be set up arbitrarily with any device (refer to the discussion in chapter 4.1 of this thesis).

4.4.2 Network Layer Functionality

In both ISA100.11a and *Wireless*HART, the Network Layer performs addressing and routing. But it seems that the scope of routing and addressing in *Wireless*HART mainly focuses on a local level, where either nickname or EUI-64 is used. It looks much alike the DL subnet-level routing and addressing performed in ISA100.11a. In ISA100.11a, a broader view of routing and addressing including backbone level and mesh level is described. On the Network Layer of ISA100.11a, IPv6 based backbone level routing and addressing is performed. In addition, it also provides the functionalities for address translation (when mesh-level routing switches to backbone-level routing), header transformation (which will be discussed soon in this chapter), fragmentation and reassembly (for the case when large NPDU ingress to/egress from DL subnet).

Addressing translation is performed by the NL of a DL subnet endpoint such as backbone router attaching to a subnet. As ISA100.11a has routing mechanism at two different levels (mesh-level and backbone level), appropriate address translation between 16-bit DL address and 128-bit backbone address need to be performed when the routing mechanism is switched to another. Devices maintain and update their own address translation table with the help of System Manager that has a database for the DL address and backbone address of each and every single device participating in the DL subnets.

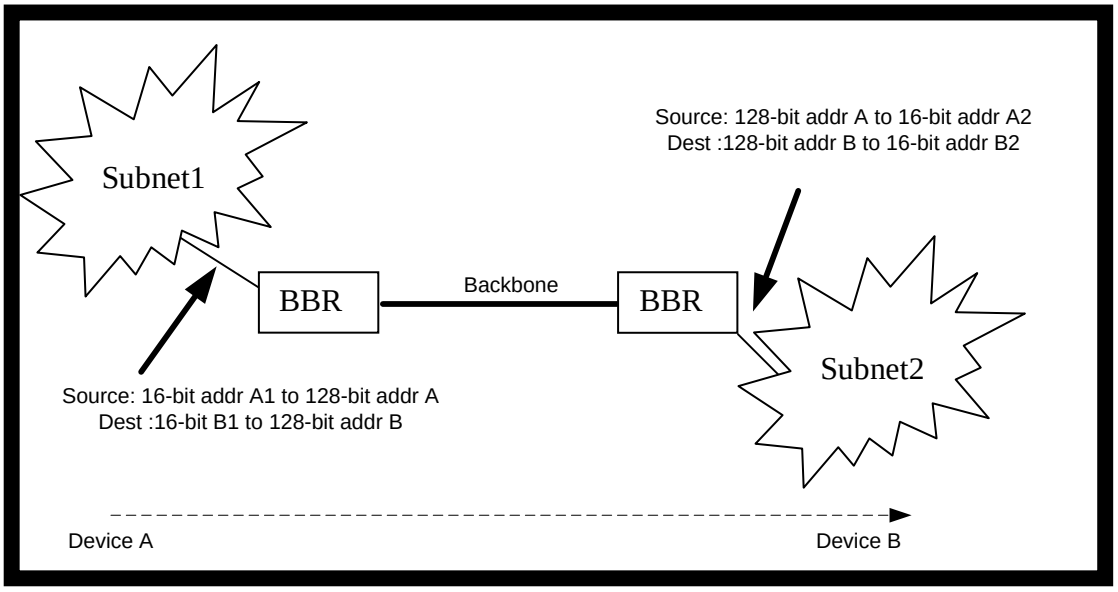

Figure 23, Routing Packets between Different Subnets via Backbone

Fragmentation and reassembly is very possible and practical at the Network Layer, because IP header (NPDU header) is as big as 40 octets [20] and together with the NPDU's payload make it difficult for the DSDU compliant to this standard to accommodate (dlmo11a.MaxDSDUSize indicates the maximum payload for the DL subnet). Hence, the NPDU, of which the size is larger than the maximum DSDU size, shall be divided into fragments with proper size at the point where backbone level routing switches to DL level routing (vice versa for reassembly process).

4.4.3 Header Specification

4.4.3.1 *Wireless*HART

In *Wireless*HART, only one type of header is shown in figure 24 below, with basic addressing and routing information. Besides, the security sub-header in NL header possesses parameters and fields with the specification of security deployment. Thereafter, confidentiality of NPDU payload is achieved as secure end-to-end session is defined at NL level in *Wireless*HART.

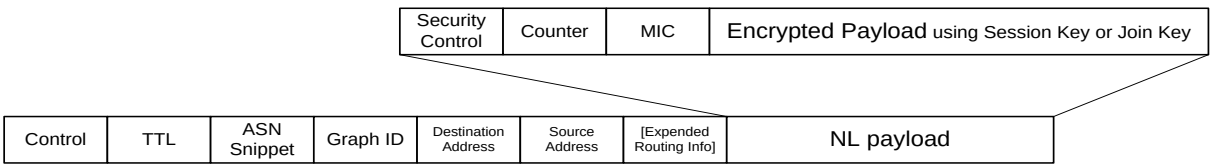

Figure 24, *Wireless*HART NPDU Structure [8]

4.4.3.2 ISA100.11a

A brief overview of 6LoWPAN is presented to echo the information (header specification of Network Layer and Transport Layer of ISA100.11a) as well as three header formats available at its Network Layer.

4.4.3.2.1 6LoWPAN

The Network Layer and Transport Layer of ISA100.11a is 6LoWPAN compatible. 6LoWPAN [12] stands for “IPv6 over Low power Wireless Area Networks” and is also the name of a working group at Internet Engineering Task Force (IETF). Its target aims at the definition of encapsulation and header compression mechanism for transporting IPv6 packets over IEEE STD 802.15.4 low-power wireless area networks, meantime conforming to existing standards. The merits that are brought by IPv6-compatibility will enable convenient and direct communication between such as internet hosts and sensor nodes in WSN, hence add mobility and interoperability.

As IPv6 has a Maximum Transmission Unit (MTU) size of 1280 octets, an IEEE STD 802.15.4 frame will not be able to accommodate such a large portion of data. Hence fragmentation must be performed before the packet enters into lower layer. However only the header size of IPv6 is as large as 40 octets without series of next headers, and in the worst case the payload space of 802.15.4 frame available for upper layer data are 81 octets (after being taken up by maximum frame overhead and maximum Digital link layer security overhead e.g. AES128_CCM*). Thus only 41 octets are available to be populated by Transport Layer and Application Layer data. If UDP (with a header size of 8 octets) is used on Transport Layer, there are merely 33 octets left for application data [19].

The 6LoWPAN hence inserts an adaption layer, wherein header compression and fragmentation are performed, between Digital Link Layer and Network Layer to facilitate the transport of large IPv6 packets over IEEE STD 802.15.4 networks. By doing header compression, fields in IPv6 header that can be reconstructed from DL header should be elided. A dispatch value is utilized as a reference for the reconstruction of original header.

4.4.3.2.2 Three Header Formats for ISA100.11a Network Layer

As we know, ISA100.11a defines subnet-level mesh routing and backbone-level routing, thus different parameters and requirements need to be adopted and fulfilled in different routing scenarios e.g. performing address translation when routing level changes. Also from an energy-efficient point of view, 16-bit address deployment in subnet routing consumes much less energy and bandwidth compared with what it does with 128-bit global address. Based on these considerations, ISA100.11a supports up to 3 different NPDU formats (header) to accommodate different requirements of energy and bandwidth needed in different communication cases. Furthermore, flexible and optimized design is achieved

based on well selected routing, level of service. Header formats are shown together in figure 25.

Basic header

octets	bits							
	7	6	5	4	3	2	1	0
1	Dispatch							
(variable)	Network payload							

Contract-enabled header

octets	bits							
	7	6	5	4	3	2	1	0
1	LOWPAN_IPHC dispatch			LOWPAN_IPHC encoding (bits 8-12)				
2	LOWPAN_IPHC encoding (bits 0-7)							
3 (opt)	Octet alignment				FlowLabel (bits16-19)			
4 (opt)	Flow Label (bits 8-15)							
5 (opt)	Flow Label (bits 0-7)							
6 (opt)	HopLimit							
(variable)	Network payload							

Full IPv6 header

octets	bits							
	7	6	5	4	3	2	1	0
1	Version				TrafficClass (bits 7-4)			
2	TrafficClass (bits 3-0)				FlowLabel (bits 19-16)			
3	FlowLabel (bits 15-8)							
4	FlowLabel (bits 7-0)							
5	PayloadLength (bits 15-8)							
6	PayloadLength (bits 7-0)							
7	NextHeader							
8	HopLimit							
9 -24	Destination address							
25-40	Source address							
(variable)	Network payload							

Figure 25, Three Header Formats Supported by ISA100.11a [1]

Three headers with different formats are supported by the NL of ISA100.11a:

Header type	Size (octets)	Scope	Features
Basic header	**1**	**DL**	**Minimized size solution for the NL header at DL level;** **Routing info of message is known by intermediate routing devices;**
Contract-enabled header	**2-6**	**DL**	**Contract ID is included and provides message routing info guidance to the intermediate router:** **1. Selection of appropriate backbone resource upon egressing from DL;** **2. Selection of appropriate DL resources (such as priority, graph ID) upon ingress into DL;**
Full (IPv6) header	**40**	**Primarily NL**	**1. Expanded from basic either or contract-enabled header upon egressing from DL;** **2. Inclusion of all fields defined in IPv6 header; TrafficClass and FlowLabel may be set to NPDU priority and Contract ID respectively;** **3. 128-bit address of source and destination shall be used instead of their 16-bit address;**

Table 8, Differences in Header Specification

The basic header can essentially be viewed as a one - octet abbreviation and used if only the UDP header is fully compressed. Likewise, the Contract-enabled header can be constructed not only when full UDP compression is done, but also in the case that full UDP header compression is not achieved, for instance, the UDP checksum of messages during join process are not elided for security reason (UDP checksum functions as an integrity check at TL level). Full header is a must for messages to be routed over backbone network, hence the previous two DL-level NL header need to be transformed by subnet endpoint which acts as the interface between DL subnet and backbone network. Although it is not

recommended, this standard does include the case of using full header as a DL-level NL header.

To make it an internet protocol-compatible Network Layer, ISA100.11a defines its NL headers in a compatible way with the IETF 6LoWPAN standard. Its NL headers influenced by 6loWPAN facilitate the compatibility for the potential future use of 6LoWPAN networks as backbone. All fields of full IPv6 header can be elided according to 6LoWPAN format [13]. Besides, basic header and contract-enabled header are both 6LoWPAN-compatible NL headers as well[2].

4.4.4 Routing example (different DL subnets)

Two levels of routing described in ISA100.11a might complicate the normal image of routing in our mind. Here, a simple example summarized from ISA100.11a is given to clear the confusion that might exist. This example will focus at the spot where the routing level is switched. Mesh routing at subnet level is operated in the same way as it does in *Wireless*HART, which is in the forms of graph routing and source routing.

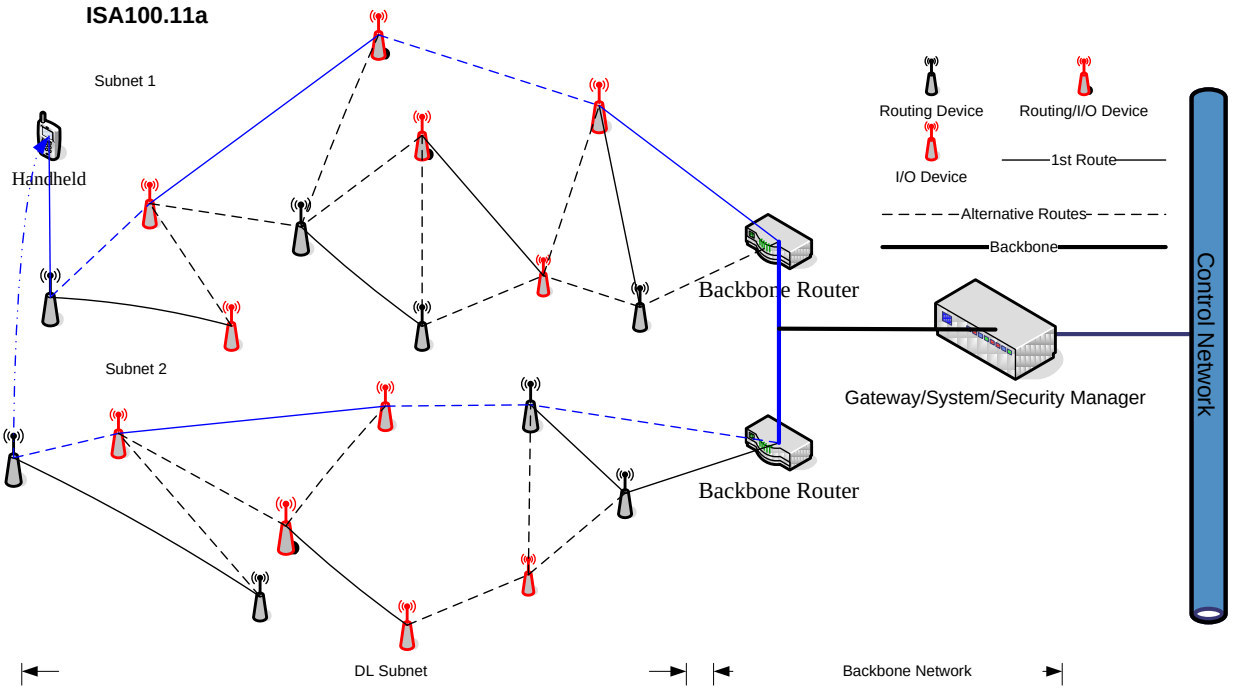

Figure 26, Routing between 2 subnets [1]

[2] *Note that ISA100.11 also defines fragmentation header format for fragments from NPDUs while traversing the DL subnet and its format is entirely based on [19] format.*

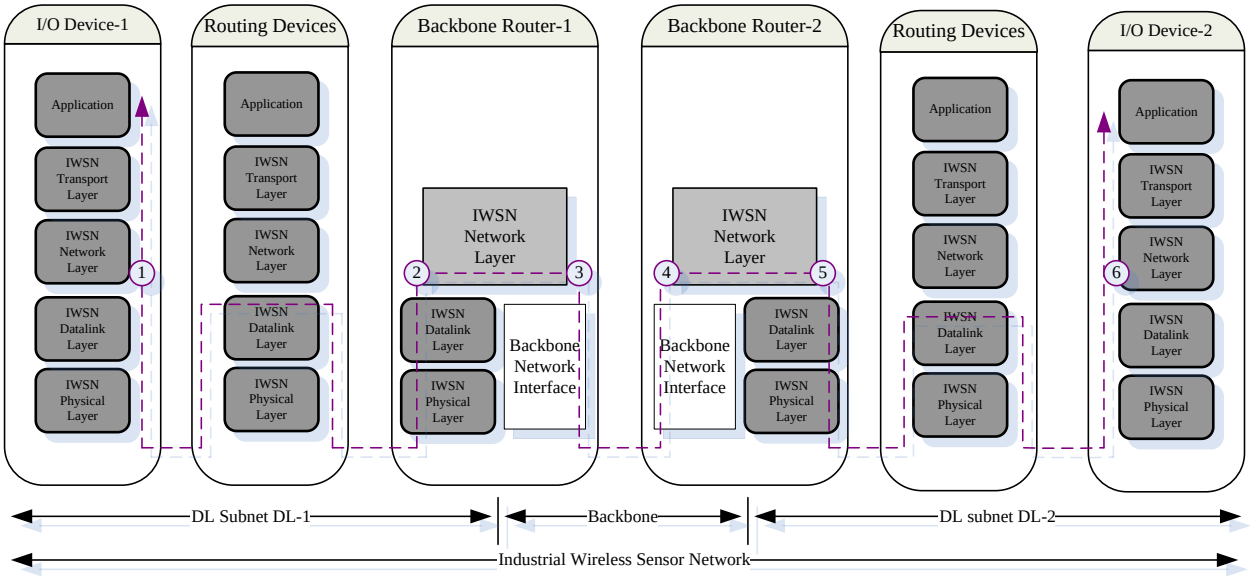

Figure 27, Dataflow through Protocol Suite relevant with Routing between Subnets [1]

I/O device IO-1 wants to communicate with I/O-2 locating in another DL subnet DL-2:

- The NL of I/O-1 originates a NPDU with e.g. a contract-enabled header, and the NPDU is sent down to the protocol suite (DL) together with the source address (16-bit address of I/O-1 in DL-1) and destination address (16-bit address of I/O-2 in DL-1). Whether the contract-enabled header or basic header is used is dependent on the fact if the contract table indicates the Contract ID needs to be included or not. Then fragmentation may be performed according to the size of NPDU. In this case, contract ID is placed in the FlowLabel field of the header and no fragmentation is performed.
- Upon the receipt of NPDU from NL, the DL routes the DPDU to the backbone router in DL-1 via link mesh. After the BBR-1 determines the message's final destination, it replaces the shorter addresses of both source and destination with their 128 bit-addresses according to the address translation table.
- After consulting routing table, the BBR-1 determines the next hop on backbone network to be BBR-2 (using 128-bit address). Then a full IPv6 header is expanded from contract-enabled header, including Contract ID and priority in FlowLable and TrafficClass field respectively.
- Various routing protocols available on backbone network could support the message to be routed to BBR-2. Then BBR-2 checks and confirms the destination range of the NPDU is within subnet DL-2 and whether the assembly should be performed. Next the BBR-2 constructs basic header (if UDP header is fully compressed) for the message so as to efficiently route it over subnet DL-2 without excessive overhead. The address translation is done by using 16-bit addresses of I/O-1 in DL-2 and I/O-2

in DL-2 instead of their longer address. Meanwhile, contract ID and priority are also sent down to the protocol suite for selection criteria of routing resources.

- Upon the receipt of DPDU, I/O-2 first confirms that it itself is the final destination for this DPDU. Then it translate the addresses into 128-bit in its network header and passes the NSDU to its upper layer.

4.4.5 Considerations

This chapter mainly presents the differences between the NLs defined in *Wireless*HART and ISA100.11a. As the new terms such as subnet and backbone are involved in ISA100.11a architecture, it is interesting to see what new functionality is described at NL level brought by these new terms. Thus, we have seen the unique features of NL in ISA100.11a e.g. multiple network header format for energy and bandwidth efficient design, compatibility with 6LoWPAN, and header transformation given by routing examples.

Although the design of NL in ISA100.11a keeps its vast and powerful view compared with *Wireless*HART, there might be some potential questions. For instance, backbone routers functioning as the interface between subnet and backbone network, not only need to fulfill the mission of routing NPDUs on behalf of field devices within subnet over the backbone to their destination, but also have to take the full responsibility of transforming NL header formats of messages during either egress or ingress process. This new feature requires the backbone routers to be able to afford extra workload of header transformation. Hence a number of such powerful and specially-designed backbone routers that are capable of routing and transforming header formats need to be available in the market.

Unlike *Wireless*HART, ISA100.11a defines an internet protocol-compatible NL. Having IP compatibility potentially indicates some merits that may come along with IP connectivity to the wireless system [19]. For example, the simplification and cost reduction of network architecture can be granted because prevalent, mature infrastructure and technologies for IP network already exists. As well as a possibly large need of the address resources and efficient addressing mechanism, IPv6 has sufficient address spaces and capability to accommodate a considerable amount of devices and their addressing needs. The last but not the least, all-IP network is always an ever-going process boosted by the industrial needs, and the fashionable and favorable IP solution are certainly more desired than vendor/organization-specific, proprietary solutions. The inclusion of IP-compatibility extends the future interoperability to be not only within the sensor networks but also between the sensor nodes and internet hosts. However, the IP connectivity indeed brings along some drawbacks such as many mature active IP hacking methods and IP overhead problem. For the solution of IP hacking, countermeasures may be adopted as IP security defense is booming along with endless IP-oriented attacks. In addition, 6LoWPAN compatibility accommodates the large size of IP header at Data Link layer, but it definitely increases the complexity of system design and operation.

4.5 Transport Layer

The Transport Layer defined in either standard has a perspective of edge level, which is end-to-end communication responsibility and endpoints communication operation. The Transport Layer in *Wireless*HART ensures successful communication via mesh topology, and supports either acknowledged transaction for guaranteed message delivery or unacknowledged transaction for specific communication intention such as data publishing.

Differently, the Transport Layer in ISA100.11a provides connectionless services with optional security. They are essentially based on User Datagram Protocol (UDP) with optional security processing using session key. The session which is aimed at providing end-to-end data encryption and authentication for the communication between two parties is defined at TL level in ISA100.11a (at NL level in *Wireless*HART). In addition, the adoption of UDP also extends 6LoWPAN.

4.5.1 Protocol Data Unit Format

As the DL and NL has undertaken most of routing, addressing, and security issues, the TL of *Wireless*HART has a simple specification of Transport Layer Protocol Data Unit (TPDU):

- The different bit fields of Transport Byte specify the type of TL transaction (acknowledged or unacknowledged), type of the message (request or response), the identification of broadcast parent, and the sequence number used to manage packet traffic.
- Device/Extended status is specified in [8].
- Command aggregation will be discussed in 4.6.1 as they are AL level data.

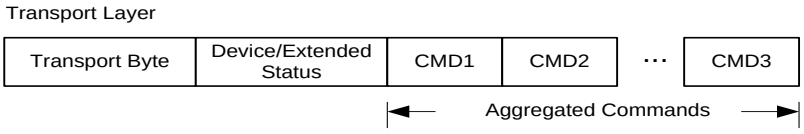

Figure 28, TPDU format in *Wireless*HART

The TL header specification in ISA100.11a has the simliarly straightfoward deployment with an additional security header to support for secure communication at session level.

- At TL level, UDP header should be uncompressed, with the mandatory UDP checksum required by IPv6 [22]. Note that UDP header can be optionally compressed when the TPDU is passing down to NL according to the requirement of extending 6LoWPAN. The detail UDP compression method is described in 11.5.2 of [1].

- The security header contains security control parameters such as security levels (specified in table 3), key_index specifying current session key, and relevant time information.
- The TMIC is generated using session key for data authentication. During the join process, TMIC and security header size are both set to be zero by security sub-layer. Then UDP checksum is respsonsible for the protection of join messages.

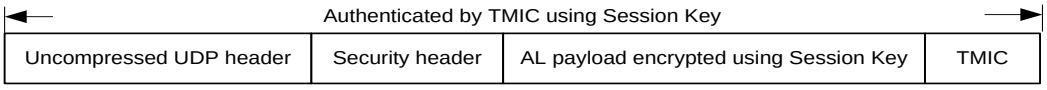

Figure 29, TPDU format in ISA100.11a

4.5.2 UDP and Security

The TL security mechanism in ISA100.11a highlights flexibility, wherein AES128_CCM* and UDP cooperates with each other to provide flexible protection services for different communication purposes and security level required, such as:

UDP checksum is elided for the full header compression required by 6LoWPAN but TL MIC computed by session key takes over the mission of protecting data integrity (authentication).

TL MIC does not function during join process messaging due to the lack of session key but UDP checksum that are not elided in this case ensures end-to-end data integrity, etc.

The cases where UDP checksum should be elided are dependent on authorization of AL or the fact whether TL MIC is provided or not. In the case when backbone router routes data packet into DL and does not know if the TL MIC is turned on or not, the UDP checksum should not be elided during the UDP compression, which means the UDP checksum and TL MIC can both exist in TL header. Whether the data confidentiality, authentication and the level of them should be used for security processing is dependent on the security policy of a particular contract.

4.5.2.1 Contract and Session

Contract that assigned by System Manager is used to support for the communication needs for peer (UAP) communication between two devices. Likewise, the session is established between two TL ports in the source and destination, respectively. It is possible that several contracts that support different needs for communication between the same peer application processes utilize the same session key to secure all the communication pipes between the same TL ports, as a specific port has a one-to-one mapping with a particular application process. The session (session key) should be granted by the System/Security Manager before the contract goes into effect (the data starts to flow). The device uses master key as

a password to request new session (session key), updated session key from System/Security Manager.

4.5.3 Delivery Service

*Wireless*HART defines reliable packet delivery mechanism at TL level, using acknowledged service to create synchronized communication pipe (unidirectional) between two parties. This makes sure the aggregated commands contained in the DPDU payloads go into effect by guaranteed delivery the DPDU to its final destination. Transport table that resides in every device compliant to this standard functions as an attendance record to tracks every entry that represents established acknowledged communication link.

However, the User Datagram Protocol is not a reliable delivery mechanism [22], because it is connectionless-oriented with minimum protocol cost and the packets can be delivered lost, out of order or duplicated. The Application Layer (communication interaction model) in ISA100.11a is in charge of administration and control of network operation because UDP behaves completely transparent to AL.

4.6 Application Layer

The Application Layer of *Wireless*HART extends the standard HART Application Layer, builds on the requirements specified for its Network Layer, and defines commands, responses, data types, procedures and status reporting that are used by the protocol. It is command-oriented with the specification of not only conventional HART commands but also wireless commands, which supports operation, configuration and management of different layers of *Wireless*HART devices [8].

Distinctively, real-industry units are modeled by a series of well-defined software objects at the Application Layer of ISA100.11a. Besides, attributes with pre-defined data structure in the corresponding objects as well as services that enable inter-object communication between different user application processes are also defined in order to support this open, object-oriented Application Layer. The object-oriented design aims at encapsulating information in a manageable way, hiding the complicated implementation from target problems and highlighting the robustness, reusability, feasible maintenance of industrial automation systems [27].

The Application Layer in both standards is targeting at efficient messaging:

- Command Aggregation allows multiple commands transmitted within one transaction in *Wireless*HART;
- Concatenation of hetero/homogeneous application level messaging (refer to 12.17.6 in [1] for additional issues), Publish/subscribe supports assembly and disassembly of multiple values in a single message in ISA100.11a;

These messaging methods give birth to faster configuration uploads, reduced traffic resource and energy-efficient communication. As the battery-life of field devices is a crucial issue in the wireless sensor network, minimized energy consumption during message

processing facilitates the goal of extended battery-life of sensor nodes (field devices). Additionally, nonnative protocol tunneling (tunnel object and interface object are defined at the AL of ISA-100.11a) between legacy host systems and native devices are supported at Application Layer in ISA100.11a when legacy system communicate with the field device in a form of data construction that is not compliant to the standard.

4.6.1 Application Layer Structure

In ISA100.11a, the AL architecture consists of two parts:

- Upper Application Layer (UAL) contains a series of application processes that can be sorted into two categories: User Application Processes (UAPs) that may perform particular function or computation for application-specific use; Management Processes (MPs) such as DMAP, SMAP for management applications.
- Application Sub-layer (ASL) is responsible for providing services to enable object-oriented communication between peer objects in the same UAP or different UAPs (which could be UAPs residing in the same or different physical devices).

4.6.2 Object-orientation

At AL level, objects are the basic units that are contained within UAPs and MPs. They can represent behaviors and states of the real-world thing being modeled using various attributes, and they can also support services and methods to operate and effect certain behaviors and states of each other. We have already talked about the management objects contained in MPs such as DMAP and SMAP in the earlier chapter. This time, an UAP management object (UAPMO) is mandatory in an UAP and it contains attributes such as version, UAP status, number of objects and etc. If self-upgrade is supported by this UAP, it should also contain an UploadDownload object (UDO). Furthermore, other objects can also be implemented within an UAP for application-specific purpose e.g. tunneling object. The AL in ISA100.11a defines standard objects, standard attributes and methods to enable interoperability, and industry-specific standard objects (process industry and factory automation) and vendor-specific standard objects can also be added, so do the attributes and methods.

As various objects are defined at AL level, addressing of objects needs to be performed as well to ensure the accessibility of a certain object. Object identifier is a unique 16-bit ID within a device (TL port number is also required for object addressing because each UAP at the UAL of a device has a one-to-one mapping with their corresponding TL port). UAPMO has a reserved ID = 1 in every UAP and if UDO is presented, ID = 2 is reserved for UDO. The objects defined in this standard may use ASL services to read/write the value of attributes of peer objects as well as to do request of method execution, alert report, data publishing, tunneling and etc.

4.6.3 Communication Interaction Models

Like the acknowledged and unacknowledged transactions defined at DL of *Wireless*HART, the AL in ISA100.11a defines three different communication interaction models, which are

unidirectional buffered communication, queued unidirectional communication and queued bidirectional communication:

- Publish/Subscribe service provided by ASL uses unidirectional buffered communication for unconfirmed scheduled periodical or aperiodical data publishing. (In *Wireless*HART burst messages are used for publishing service.)
- Client/Server service uses queued bidirectional communication for on-demand one-to-one aperiodic communication with retries and flow control.
- Source/Sink messaging uses queued unidirectional communication for unconfirmed, unscheduled alerts reporting without flow or rate control. However, the receipt of alert reporting message can trigger an alert acknowledgment message transmitted back to the alert source. If no alert acknowledgement is received, the alert reporting may be continuously retried[3].

4.6.4 Protocol Data Unit Format

With a command-oriented Application Layer, the APDU format in *Wireless*HART can be viewed as single or aggregated commands, each of which includes 16-bit command number, length and data field. There are some additional requirements and limitations about the aggregation of commands [8].

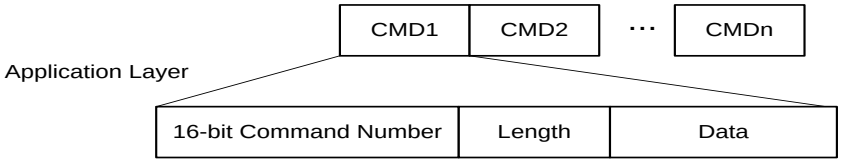

Figure 30, APDU format in *Wireless*HART

As a matter of object-oriented communication, addressing of a particular object in a certain application process needs to be performed at the AL of ISA100.11a. Besides, different service types are provided by ASL in this standard (such as the TL of *Wireless*HART). Hence the header format of an APDU contains information such as object identifier for object addressing, service type identification for indication of a specific service provided by this APDU.

According to the figure 31, object addressing mode give birth to a choice of efficient addressing schemes by saving necessary coding bits of the identifiers of source and destination objects. For application processes with different number of objects, object

[3] *Please refer to 12.12 and 12.17 of [1] for detail*

addressing mode provides coding choice from optimal header compaction to full header representation (both 16-bit source and destination object identifiers).

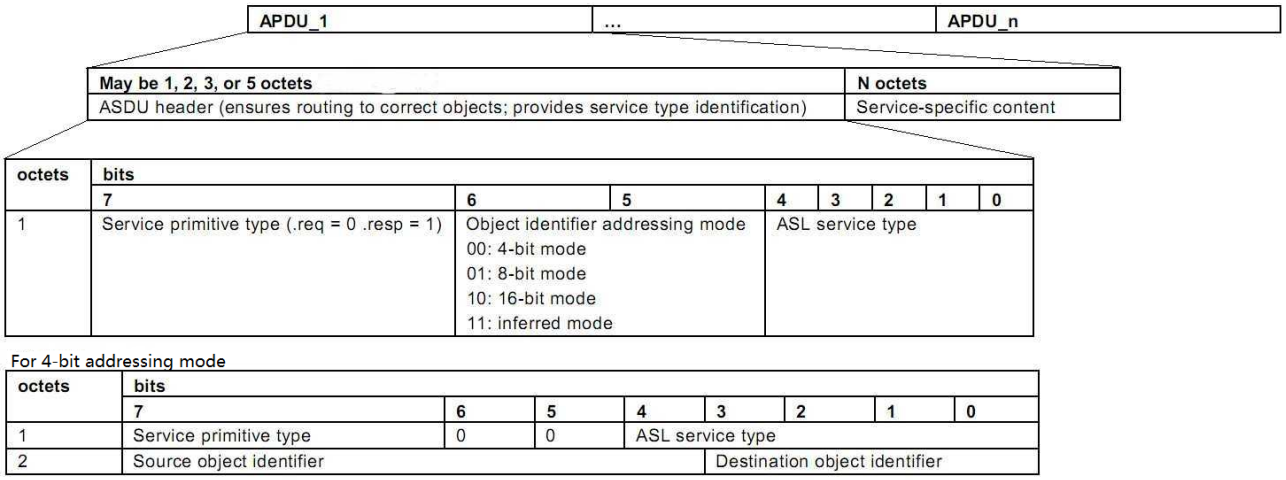

Figure 31, APDU format in ISA100.11a

The inferred addressing mode is used in the case where the APDUs are concatenated together. This mode saves overhead bits in APDUs' headers by referring the source and destination object identifiers of APDUs with the most recently transmitted APDU's source and destination object identifiers within the same concatenation. Moreover, it optimizes the messaging efficiency when concatenated APDUs are given to TL as a single TPDU.

4.6.5 Merits of Object-orientation

ISA100.11a is defined as a universal wireless communication standard instead of being a wireless expansion of an already existing process instrumentation protocol (such as *Wireless*HART). Object-orientation at Application Layer provides ISA100.11a enhanced interoperable capabilities. As standard's management objects, industry-independent/dependent objects are defined in an open and definitive manner, interactions and interoperability with different field devices and legacy systems are achieved as well as uniform system and network management of distributed application processes. Adaption of legacy device communications over the wireless network can be accomplished by mapping relevant aspects onto the attributes of standard objects and the ASL services in between. The promotion of modularity enables add-on capabilities by implementing multiple market (industry/vendor)-specific objects within the same UAP. For example, the process control industry standard objects and data structures are defined in current release of ISA100.11a to enable interoperability among devices and factory automation industry objects are expected to be included in the future release.

4.6.6 Gateway

The role of gateway defined in ISA100.11a has a specialized User Application Process to support gateway functionalities, which is the almost the same as it in *Wireless*HART. The gateways in both standards are aiming at interfacing host-level applications directly to the

wireless field devices or indirectly to wired field devices via adapters by proper protocol translation. The adapter is also used as a protocol translator converting from/to a wireless protocol to/from wired protocol for the field devices. The gateway definition in two standards is similar as they are only defined with supporting functionality for the construction of gateway but without specification of a certain protocol translator or plant network interface.

4.6.6.1 Gateway Service Access Point

A gateway high side service interface called Gateway Service Access Point (GSAP) is defined in the ISA100.11a. GSAP together with relevant AL objects cooperate to provide generic gateway functionalities. Above the GSAP is where the protocol translator resides and it converts the foreign host-level protocols (such as tunneling) to enable communication to the field devices through the wireless field network. The GSAP is also bound to a gateway application process wherein the objects can utilize object-to-object communication provided by ASL services (e.g. client/server) to support gateway functionalities through GSAP. Similarly, the adapter compliant to this standard share the same structure with the gateway as the translation between wired and wireless protocol appears to be in the same manner.

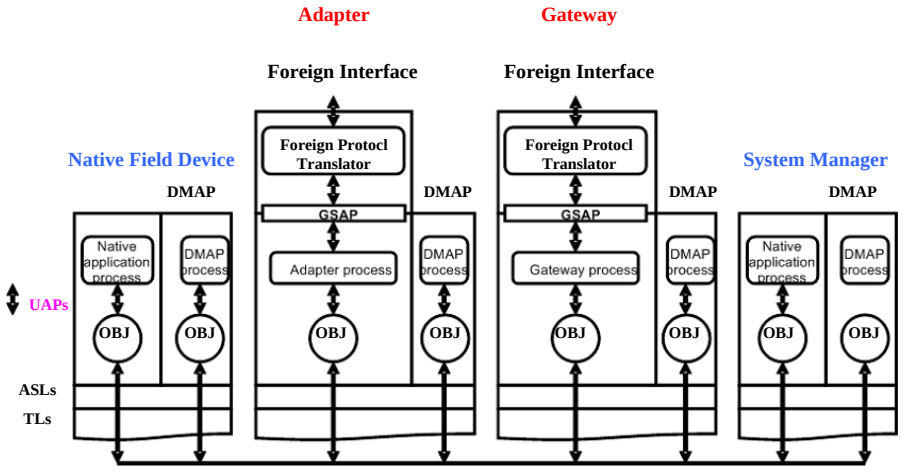

Figure 32, Gateway Service Access Point [1]

4.6.6.2 GSAP Implementation using WirelessHART

Gateway Service Access Point is regarded as the key part of the gateway infrastructure to be a conveyor of wireless data and management services. Being a high side interface to the protocol translator above the lower protocol suite makes it possible for the GSAP to become a common abstraction of any underlying wireless system such as *Wireless*HART. The ANNEX Q of [1] has described an implementation of informative GSAP using existing *Wireless*HART commands and the mapping of relevant parameters in two standards. The

GSAP provides a way of handling the coexistence issues of devices that are geographically located in the same/different standards' wireless field networks via the report e.g. topology, schedule reports from different underlying wireless systems. Hence a standardized infrastructure for the uniform configuration and management of multiple underlying wireless systems (probably with different communication protocols) are supported.

4.7 Join Process, Key Agreement, Key Distribution

Join process is controlled by the administrator of the network to provide new devices with enough information in order to communicate with devices in the same network. After join process, newly joined devices that gain relevant bandwidth and communication resources are able to participate in the normal operations of the network.

4.7.1 Symmetric Key based Join Process

4.7.1.1 Commonalities

ISA100.11a and *Wireless*HART both support symmetric key based join process. In either standard, the general steps of symmetric key based join process follow the same way:

- The device that is ready to join the target network needs to be provisioned with necessary information, e.g. join key, network information, etc.
- The new device listens and captures advertisements from routers (neighbors) that are already in the network. The joining advertisement contains configuration specification for the new device to construct join request.
- The advertising router forwards the join request from the new device to the System Manager (Network Manager). The join request consists of both non-security and security information.
- The System Manager (Network Manager) processes the join request in cooperation with Security Manager that is responsible for checking if the new device possesses enough security credentials.
- Once the join request is approved, the System Manager (Network Manager) replies the new device with join response that is forwarded by advertising router, and admits it into the network.

For hop-by-hop security requirement, global key (well-known key) is utilized for the data integrity of join message at DL level before obtaining DL key (network key) from System Manager (Network Manager). Upon the receipt of new DL key (network key), the joined device must secure subsequent communication with these new keys from System Manager (Network Manager)

4.7.1.2 Differences

4.7.1.2.1 Protection of Join Messages

The join messages in *Wireless*HART are protected by the join key which is temporarily used as a session key to ensure end-to-end security (encryption and authentication) required at NL level. In ISA100.11a, session level security is replaced with UDP checksum (integrity) at TL level. Because the device does not have a session key (no contract existed with System Manager) during the join process, security sub-layer is defined not to process outgoing join request from the device and outgoing join response from advertising router, leaving security header 0 size. Even though the join key in ISA100.11a does not contribute to the session security, it still functions as an important security parameter on the application layer data of join request and key distribution scheme.

According to the time sequence of symmetric key based join process, the device initializes a *Security_Sym_Join.Request()* to send security information to the Security Manager. (Unlike from *Wireless*HART, the join messages separate out the security and non-security information in different services, wherein security information is handled by Security Manager and non-security information is processed by System Manager.) Then the join key is used to compute MIC of the data in *Security_Sym_Join.Request()* for authentication check[4].

[4] *Please refer to chapter 7.5 in ISA100.11a for related data structure and service definition*.

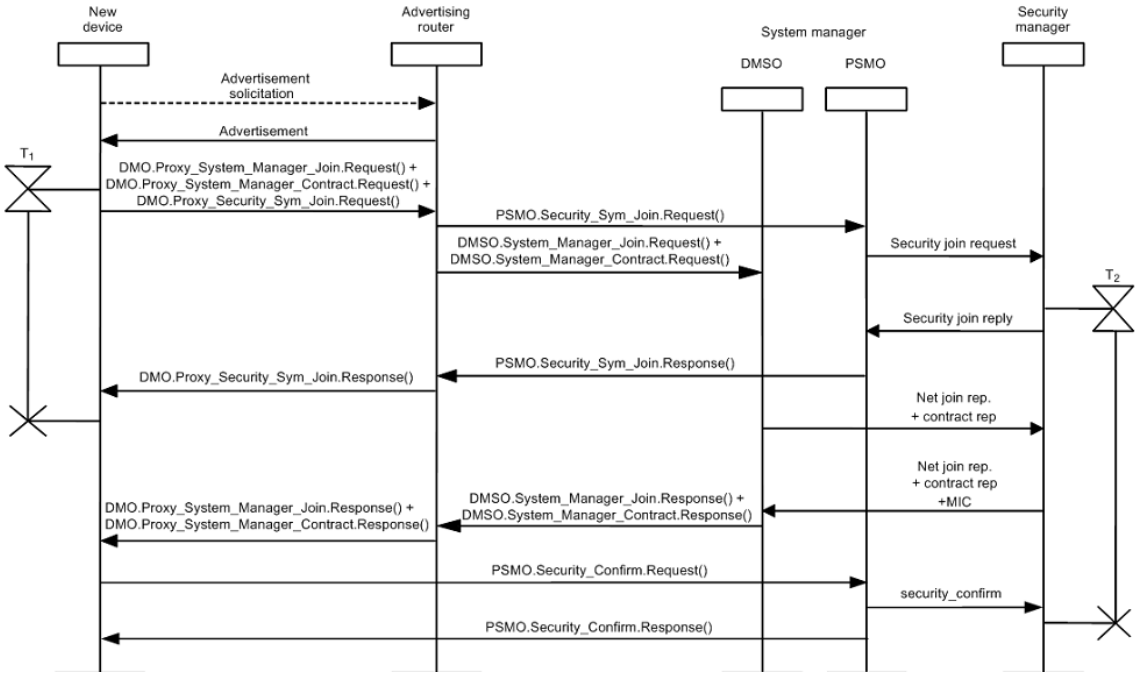

Figure 33, Symmetric Key based Join Process [1]

4.7.1.2.2 Key Distribution

In *Wireless*HART, key distribution is achieved by using "*Write Network Key"* and "*Write Session"* [8] to write network key and session key to the new device. ISA100.11a defines a relatively complicated key distribution scheme by: firstly using Secret Key Generation (SKG) primitive for master key agreement, then using agreed master key to derive the DL key and session key in the encrypted package delivered from System/Security Manager via *Security_Sym_Join.Response()*.

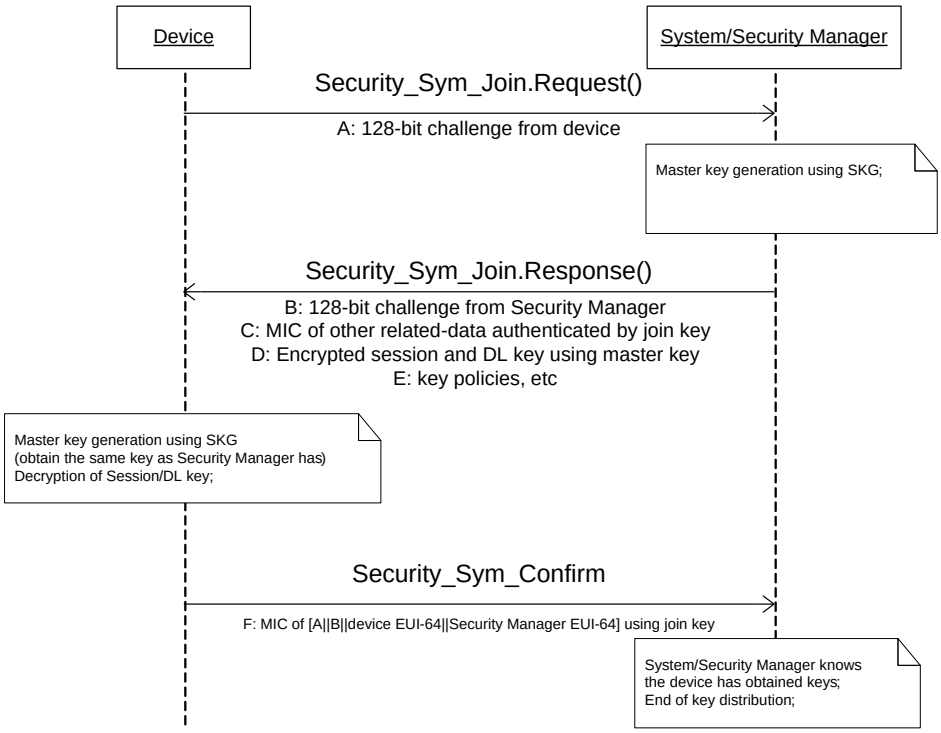

Figure 34, Key Agreement Scheme in Symmetric Join Process

The overall steps of key distribution scheme in ISA100.11a are shown in figure 34, wherein the key agreement is done by using SKG methods featuring join key: Master Key = $SKG_{joinkey}$ [A||B|| device EUI-64||Security Manager EUI-64] (The EUI-64 of Security Manager is to the new device as trust-related information during the provisioning process and the EUI-64 of the new device is sent by *System_Manager_Join.Request*()). Hence without exchanging the master key entity over the air, both the device and Security Manager agree on and obtain the same master key. Then it is straightforward to derive the encrypted package of DL key (communication within the same subnet) and session key (with the System Manager) delivered from System/Security Manager. Meanwhile, the use of data package C and F using $HMAC_{joinkey}$ are for the purpose of mutual data authentication so that the new device and security manager are both proved alive (with the possession of the same join key). Note that the security confirmation sent from the new device to the System/Security manager at the last stage in figure 33 is not forwarded by the advertising router anymore, because the new device has already obtained the contract to have direct communication with System Manager. Thus it also confirms with the Security Manager that it is able to derive the session key from master key and therefore that it has the join key.

4.7.2 Asymmetric key based Join Process

As it is known to all, *Wireless*HART in the current release does not deploy asymmetric cryptography to support its security operation. While ISA100.11a does include the support for the asymmetric key based join process and provisioning process (provisioning is going to be discussed in the following chapter).

After being provisioned with enough credentials including device identity EUI-64 and certificate that is signed by a trustworthy Certificate Authority (CA), the new device is able to start an asymmetric key based join process with the System/Security Manager that supports asymmetric cryptography (which is optional in ISA100.11a). The Asymmetric key based join process also provides an option to the new device to integrate itself into the wireless network under the supervision of System/Security Manager, afterwards take part in the normal operations such as data publishing, network maintenance messaging after obtaining enough information required by the communication within the network.

4.7.2.1 Key Agreement and Distribution

It is defined in the standard that the key distribution scheme and resource allocation (e.g. transmit schedules) steps in asymmetric key-based join process are identical to what they are depicted in symmetric key-based join process. However only the key agreement schemes in two join methods differ from each other:

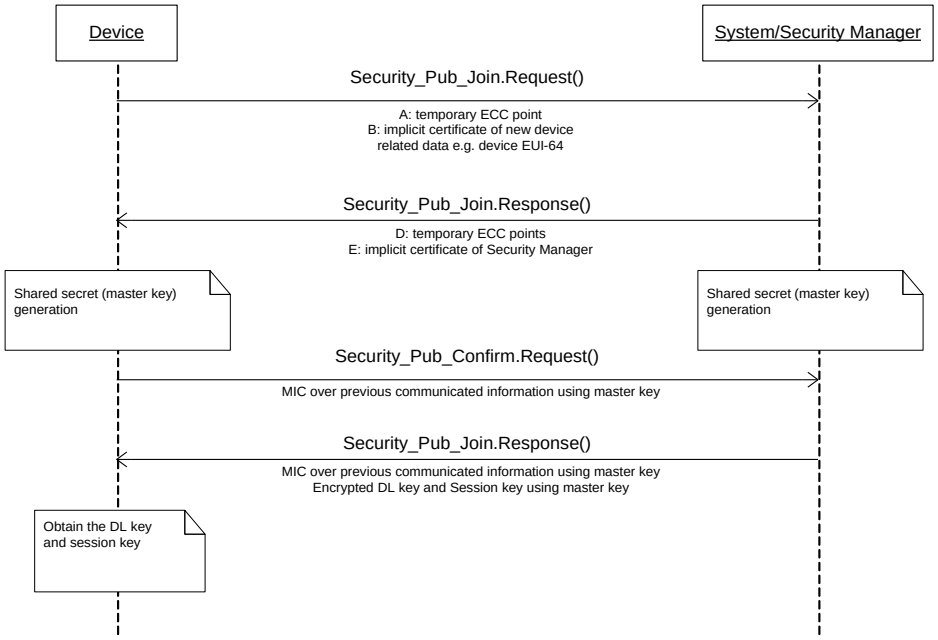

Figure 35, Key Agreement in Asymmetric Join Process

As drawn in the figure 35, the new device and Security Manager communicate to each other with their own ECC points A and B as well as their own implicit certificates. The ECC point herein is actually the public key of the temporary key-pair generated by either device for key agreement. And the implicit certificate contains device's static public key and may include other information such as subject, issuer ID for special purpose. Then all the temporary and implicit public keys as well as their private keys can be used by two parties to agree on the same shared key (master key) because of properties of elliptic curve. Finally a MIC of previous exchanged message is computed by each party and sent to each other to prove the possession of master key. Having the same key distribution scheme as it is in symmetric join process, the new device could derive DL key (within the same subnet) and session key (session with System Manager) sent along by the *Security_Pub_Join.Response()*.

4.7.3 Consideration

The symmetric key based join processes in both standards both describe the procedures of a new device that possesses a secret join key firstly to initialize a join request to the network and finally to obtain the session key and DL (network) key for facilitating the subsequent communication as the end of the join process. However the distribution of relevant keys during the symmetric key based join process is performed in a different way in two standards. The method described in ISA100.11a firstly performs a key agreement stage for a new secret master key using the join key as well as challenge-response mechanism. Then the relevant keys are delivered to the device in an encrypted package that can be decrypted from the newly-generated master key. While the method in *Wireless*HART directly utilizes the join key as its session key to secure join messages and then delivers keys with corresponding commands. It is not easy to determine which way to do the key distribution is much properly securer as it depends on the different required security levels and efficiency (time consumptions from additional cryptographic operations such as HASH and SKG). Nevertheless there is one feature that makes the security consideration of ISA100.11a outweigh the ones of *Wireless*HART, which is the mutual authentication during the join process. The challenge and response exchanged between the new device and System/Security Manager provides the mutual authentication to see if both parties are alive and agree on the same shared key. This method also avoids the man in-the-middle-attack because an eavesdropper cannot derive the master key without knowing secret credentials shared between two parties (EUI-64 of security manager shall be trust-related information that is provided to the new device during the provisioning procedure).

ISA100.11a provides an alternative to perform join process based on asymmetric key, while *Wireless*HART does not include any asymmetric cryptographic scheme. After our discussion above, it is clear that the asymmetric key based join process only differs from the symmetric method with their key agreement schemes wherein properties of ECC is used to derive shared master key instead of SKG. This key agreement scheme highlights enhanced secrecy as even no join key needs to be provisioned before the join process. The security credentials (the private keys) are perfectly protected in their storage, and only ECC curve points (short-term public key) and implicit certificate (including long-term public key) are transmitted. On receipt of the certificates, both parties can be able to verify the authenticity

of devices using implicit certificate signed by a trustworthy Certificate Authority. After computing the shared master key using the asymmetric key materials, the mutual confirmation proves that both of them successfully agree on the same secret to facilitate the subsequent secure key distribution scheme, which is the same as it of the symmetric key join process. However, the asymmetric key algorithms are much computational costly than the symmetric-key algorithm (slower by an order of magnitude) because the much longer length of key needs to be adopted for the same level of security [21].

This chapter is mainly focusing on the different security operations performed in join process of two standards. For elaborate security analysis for two standards, please refer to [11] wherein security attacks against several vulnerabilities and their countermeasures are identified based on threat models in WSN.

5 EVALUATIONS OF PROVISIONING SCHEMES

5.1 Overview

The purpose of this chapter is to elaborate the different scenarios of provisioning examples described in ISA100.11a standard and gives a brief comparison between provisioning schemes in ISA100.11a and different scenarios depicted in [37], This chapter also lists and combs the basic description of roles, terms and scenarios used in ISA100.11a standard to provide reader a general image of policies and interactions involved in the provisioning process. Regarding interesting aspects, such as asymmetric key based OTA provisioning and open symmetric Join key provisioning, workflow sequences are shown to visualize related objects and services required in the process.

5.1.1 Structure

This chapter has the following structure.

Section 2 gives a summarization of cryptographic basics, terms and roles used in provisioning process of ISA100.11a.

Section 3 sums up and draws time sequence for different provisioning examples.

Section 4 makes a brief comparison and evaluation between the previous presented methods in ISA100.11a and key distribution schemes specified in [37]. Interoperability is discussed and conclusion is made.

5.2 Overview of basic elements used in the provisioning process in ISA-100.11a

5.2.1 Roles and Terms

5.2.1.1 Device to be provisioned (DBP)

A device that needs to be provisioned or is in the process of provisioning, the information of which needed to be provisioned by Provisioning Device may be all or part of the settings required to join the target network.

5.2.1.2 Target Network

The wireless sensor network that device to be provisioned is intended to join.

5.2.1.3 Provisioning Device (PD)

A device with the implementation of provisioning role, that is ought to be able to provision a new device arriving from a factory default with enough information required to join the target network. It shall implement the Device Provisioning Service Object (DPSO) in order to provide information intended for Device Provisioning Object (DPO) in DBPs.

The device implementing provisioning role could be:

- The role of System/Security Manager of target network. This role could be on the separate logical side of target network and might be distributed to a series of devices in the target network.
- A device, e.g. handheld device with built-in System/Security Manager and advertising router functionality, that provision the DBP via a separate, temporary mini-network.

After the completion of provisioning the DBP, as a contracted communication has already been set up, the PD may play a part in configuring appropriate Application level objects of the DBP.

5.2.1.4 Provisioning Network over the air

A network formed between the PD and the DBP, using Type A field medium defined by this standard for provisioning device over the air (OTA), could be either:

- A temporary, isolated mini-network between PD (especially handheld device) and the DBP; or
- A separate logical network on the target network itself, if System Manager/Security Manager in the target network plays the role of PD.

There could be different logical networks, which differs widely in priority or security, based on the same physical network that is formed by a series of devices communicating with each other. They are only different instances for the same physical network, such as provisioning network and target network in this case.

With the successful join to provisioning network described above, a contract between the DBP and PD is established for further communication, such as application level primitives and methods to populate attributes in the DPO of the DBP.

5.2.2 At Supplier Site

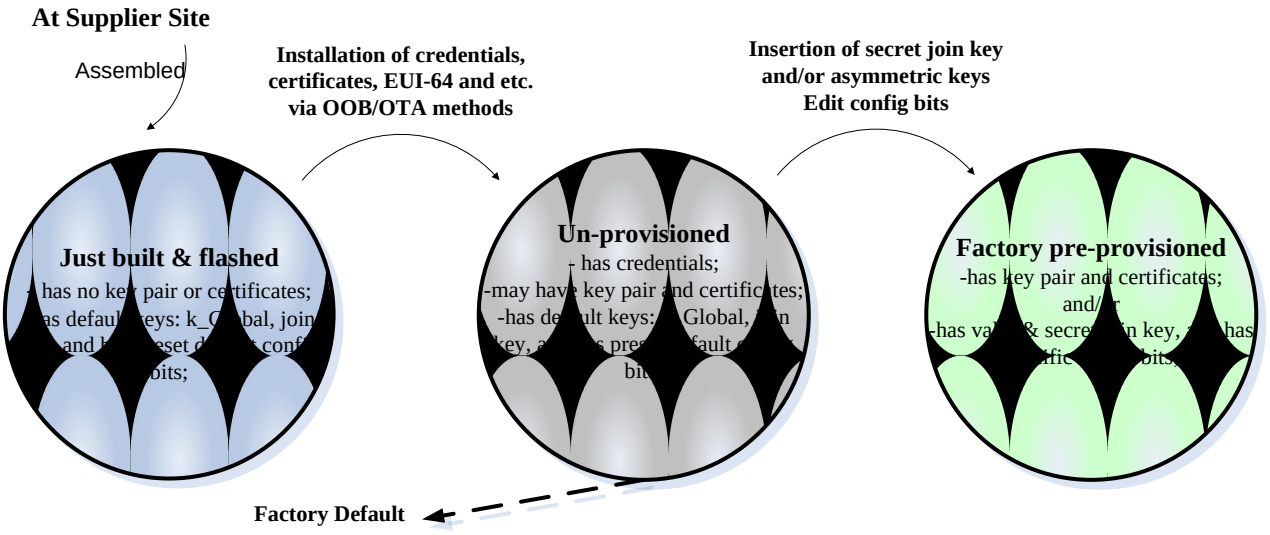

Figure 36, State transition at supplier site [1]

5.2.2.1 Pre-installed Credentials

This pre-installed credentials equipped during the factory pre-provisioned stage may provide conveniences that enable the device to skip the procedure of provisioning. Instead, it can proceed directly to the join process with pre-installed symmetric K_Join/PKI certificate and network-related information. Hence, the setup of a provisioning network is not necessary in this standard if a third party or device manufacturer is delegated to provision pre-calculated keys into the devices. Note that the System Manager/Security Manager of the target network should be synchronized with the same secret keys as well.

5.2.2.2 Factory Defaults

According to Figure 1, the device has possessed EUI-64, K_Global, K_Join (Join Key) and config bits that is preset to default upon entering the factory default stage.

5.2.2.3 Join Key (K_Join)

A secret AES symmetric key for joining the secure target network and providing data confidentiality. Its value that is provisioned by PD or pre-installed at the manufacture site shall only be known between the Security Manager of target network and the device.

5.2.2.4 K_Global

A well-known value is set to the default symmetric key, which is 'ISA100', and it is used to format a provisioning network where network-related and trust-related information is provided. K_Global plays an indispensible part during the asymmetric key based OTA provisioning for authentication of device credentials and reading of device identity and configuration settings. (*It is described in asymmetric key based provisioning 14.6.2 of [1]*)

The scenario when using K_Global which helps improve the data integrity during the provisioning procedure could be summarized as below:

- The DBP has asymmetric/symmetric keys but not the network-related information. K_Global is utilized to obtain relevant information from provisioning network, if the DBP needs these settings and corresponding config bit is set that allows default join. (This is usually an optional step)
- When target network does not support asymmetric cryptographic methods, the DBP has valid PKI certificates and wishes to get a new K_Join to join target network.

5.2.2.5 Open Join Key (K_Join = Open)

K_Join is set to a non-secret value by default, which is used to form an insecure provisioning network providing both network-related and trust-related information over the air. By default, the PD and system manager reject this provisioning method (joining with open symmetric join key).

5.2.2.6 Configuration Bits

Config bits are all preset to '1' by default, which means certain functionality represented by corresponding bit is allowed by default. The default setting could be summarized as below:

A1: Allow OOB provisioning;

A2: Allow asymmetric key based provisioning;

A3: Allow default join (join a default network with default join key);

A4: Allow reset to factory defaults;

In addition, the default settings of device could also be modified during the pre-provisioned stage for special purpose, e.g. unsecure open join key provisioning is not allowed by setting A3, A4 = 0.

5.2.3 The Relationship between the DBP and PD

Figure 37 describes the interaction between DPSO and DPO using the full protocol suite defined by this standard (PHY, DL, NL, TL and AL). During the provisioning procedure, the attributes specifying settings required to join the target network in DPO of the DBP is read/written via application level primitives and methods by the DPSO of the PD, in terms of target network ID, EUI-64 of target Security Manager, DL configuration settings (e.g. superframes, links and hopping patterns), etc.

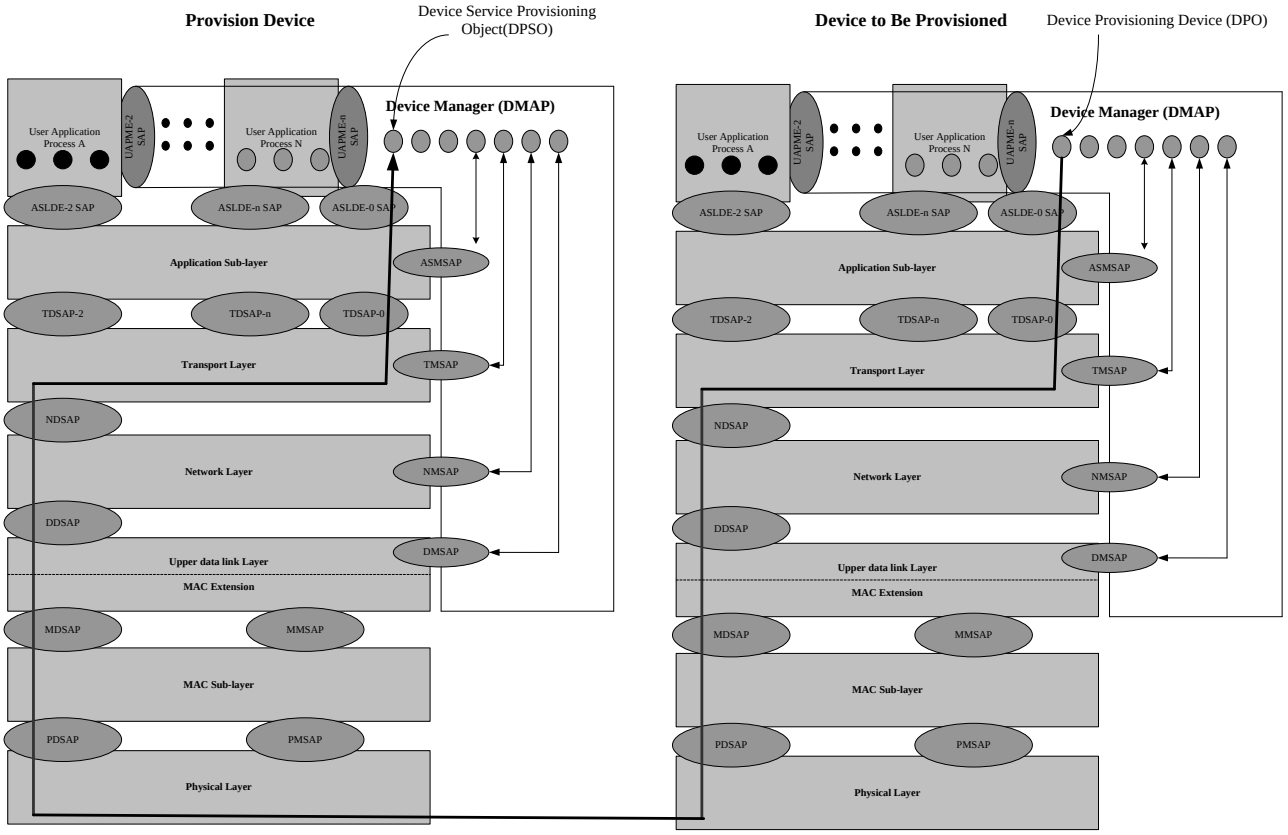

Figure 37, Provisioning data flows in the protocol suite defined in ISA-100.11a [1]

The DPSO implemented in the PD maintains the attributes and methods so as to provision the DBP, including for instance, a list of EUI-64 addresses of devices that are allowed to be provisioned and of symmetric keys that used to provision devices without pre-installed keys[5].

5.2.4 Settings Required for Join Process

To join a specific target network, both network-related and trust-related information are needed to be provisioned into attributes of the DPO in the DBP by the DPSO in the PD using application level read/write primitives and methods. The specific provisioning methods can be either OOB or OTA methods.

Network-related Info (provisioned by PD via OOB or OTA (using K_Global)):

- Subset of frequencies with which device could listen and respond to the correct frequencies, decreasing interferences and join times;
- Network ID;
- 128-bit address of system manager;
- DL configuration settings, such as the superframes, link TsTemplate (timeslot template), channel info, etc;

Trust-related Info:

- Specific Key_Join to join a specific network;
- EUI-64 of Security Manager;
- Network Join Method supported;

5.3 Overview of provisioning process in ISA-100.11a

5.3.1 General

For setting attributes in the DPO of the DBP with network-related and trust-related information, 3 different means of provisioning supported in this standard are provided here:

- Pre-installation at device manufacture site;
- Out of Band (OOB) provisioning;
- Provisioning network methods, where the PD is responsible of provisioning the DBP based on establishment of contract;

[5] *For detailed data type, default value and brief introduction of each attribute in the DPO and DPSO, please refer to table 411, 414 in the ISA-100.11a.*

The information is provisioned for the purpose of enduring sufficient credential and content to support two ways of joining process subsequently, either Symmetric key based or Asymmetric key based method (*refer to 7.5 Join Process in [1]*).

An un-provisioned DL's procedure for searching a provisioning network is defined in this standard, which is passively waiting for any receipt of advertisement from provisioning network without any beforehand solicitations. After being provisioned, all attributes of the DPO used to provision the DL are kept and retained, providing a means to reset the DL back to its provisioned state.

Provisioning procedure may also happen when the device decides to leave for another network. In that case, the System Manager/Security Manager may provision the device with both network and secure settings of the network that the device is intended to join next.

5.3.2 Provisioning Examples

Note that the operations of provisioning network-related information described below are all optional. If the DBP skips this part of provisioning, it will initialize join request with default network settings in DPO to join the networks in its vicinity.

5.3.2.1 Asymmetric Key based OTA Provisioning (with option of OOB provisioning of network-related info)

Prerequisites:

- A device with asymmetric cryptographic capabilities and PKI certificates from factory pre-provisioned procedure.
- Target network does not support asymmetric join process, but asymmetric capability (not mandatory in this standard) of security manager is enabled;
- Config bits A2, A3, A4 are set;
- Security manager of target network already possesses a White List (addresses-EUI64 and asymmetric keys signed by CA). (This installation is out of scope)

Steps:

1. Device arrives from factory pre-provisioned without a valid or pre-installed Symmetric key to join the target network;
2. Optionally, the network-related info could be provisioned using OOB (A1 enabled);
3. Scan (passively listen) for advertisements to join provisioning network, Advertising routers;
4. After capturing advertisement, the device should use K_Global to send join request to join provisioning network, with a contract between DBP and PD established subsequently (with application level read/write primitives and methods involved to

transfer information between DPSO and DPO). If step 2 was not performed, network-related information can be populated;

5. Device forwards credentials to System/Security manager;
6. Security manager checks the credential; Security Manager may check the credential by looking up the White List, obtain the device's asymmetric key signed by CA for following authentication; *Read ANNEX G in ISA-100.11a and Certificate Chain part for detail of authenticity of credentials;* A challenge/response mechanism is utilized to verify the existence of DBP;
7. System Manager/Security Manager provides DBP with a secret symmetric key for joining target network encrypted by device-specific public key, using DPO.Write_Join_Key method; Upon the receipt of join key, the DBP could join the network immediately or later.
8. A dialogue on a HMI connecting to System manager could be utilized to further control the acceptance of device which has the intention to join;
9. The time sequence for asymmetric key based OTA provisioning is provided here. The simplified symmetric join process defined in ISA-100.11a is given informatively[6].

[6] *For detail of symmetric join process and related objects, methods, please refer to 6.3.9.2 and 7.5 in ISA-100.11a.*

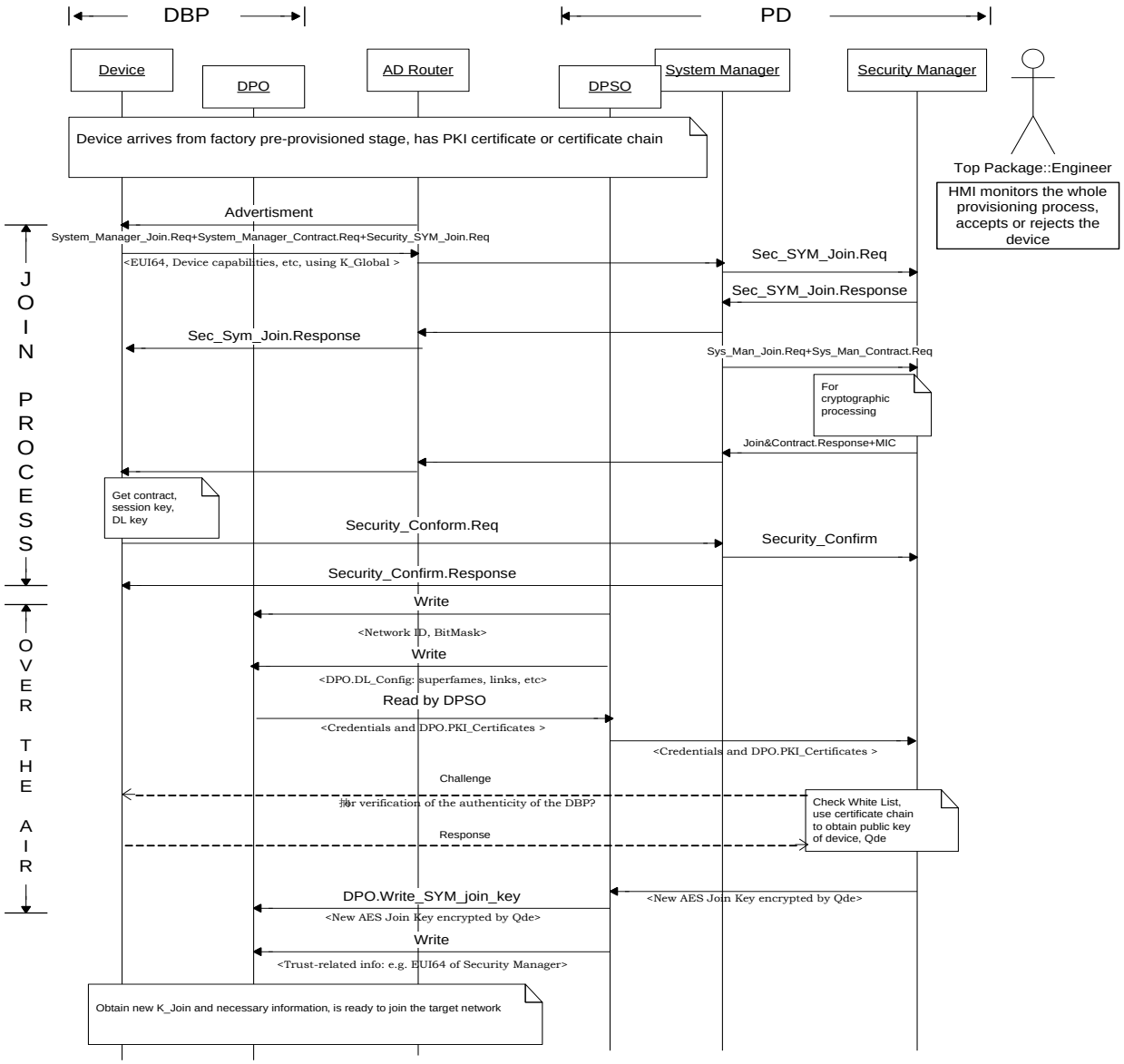

Figure 38, OTA provisioning using asymmetric key[7]

5.3.2.1.1 Certificate Chain Description

The credentials forwarded to Security Manager could be either single device certificate or multiple device certificates. If the option of multiple certificates[8] is used, double check of each certificate is required. It may perform in this way:

---

[7] *Note: DMO.Proxy_System _Manager_Join.Request/Response (), DMSO.System_Manager_Join.Request/Response ()DMO.Proxy_System _Manager_Contract.Request/Response (), DMO.Proxy_Security_Sym_Join.Request/Response () and all the other methods shown in time sequence are all described in ISA-100.11a Standard.*

1. Use asymmetric key of CA that is already possessed in System Manager/Security Manager to read the issuer (Device Manufacturer) certificates and obtain the asymmetric key of issuer;

2. Afterwards, use the issuer key to read subsequent certificate to verify the device identification and related information, and then retrieve the asymmetric key of the specific device;

After the asymmetric key of device is obtained, a challenge/response mechanism is utilized by the PD for the verification for the authenticity of the DBP.

5.3.2.2 OPEN Join Key OTA Provisioning

Prerequisites:

- A device arrives from un-provisioned factory default procedure without valid or pre-installed trust join key, PKI certificate;
- When treating a device with valid PKI certificate, the PD does not have asymmetric cryptographic OTA provisioning capabilities, as it is not mandatory required in this standard.
- This is an unsecure procedure that is vulnerable to eavesdropping. This method of using open symmetric join key is ought to be disabled by default in Security manager and PDs. Additional configuration of Security manager and PDs is needed to enable open join key OTA provisioning;
- At a user site where low level security could be tolerated;

Steps:

1. The DBP passively listens to and captures the advertisement from AD router of provisioning network;
2. The DBP uses K_Join = OPEN to initialize join request to the provisioning network which could be either a dedicated mini-network or a separate logical network of the target network provided by the PD. A contract between the DBP and PD is obtained for the subsequent communication, e.g. data transfer between DPO and DPSO using application level read/write primitives and method;
3. If the PD is allowed to accept DBP with open symmetric join key, it will provision both network-related and trust-related information including new K_Join to the DBP in order to join the target network. (could be sent in clear OTA) The new K_Join is provisioned using DPO.Write_Join_Key method.
4. The Security manager of target network may also be informed by (PD or routers) to add newly provisioned devices in its White List;

---

[8] *see **ANNEX G** of Using certificate chains for OTA provisioning in ISA-100.11a*

5. Once the new join key is written to the DBP, the subsequent communication flows are all under the encryption and authentication of this updated key. The use of open join key is not allowed unless the DBP is set back to factory default.

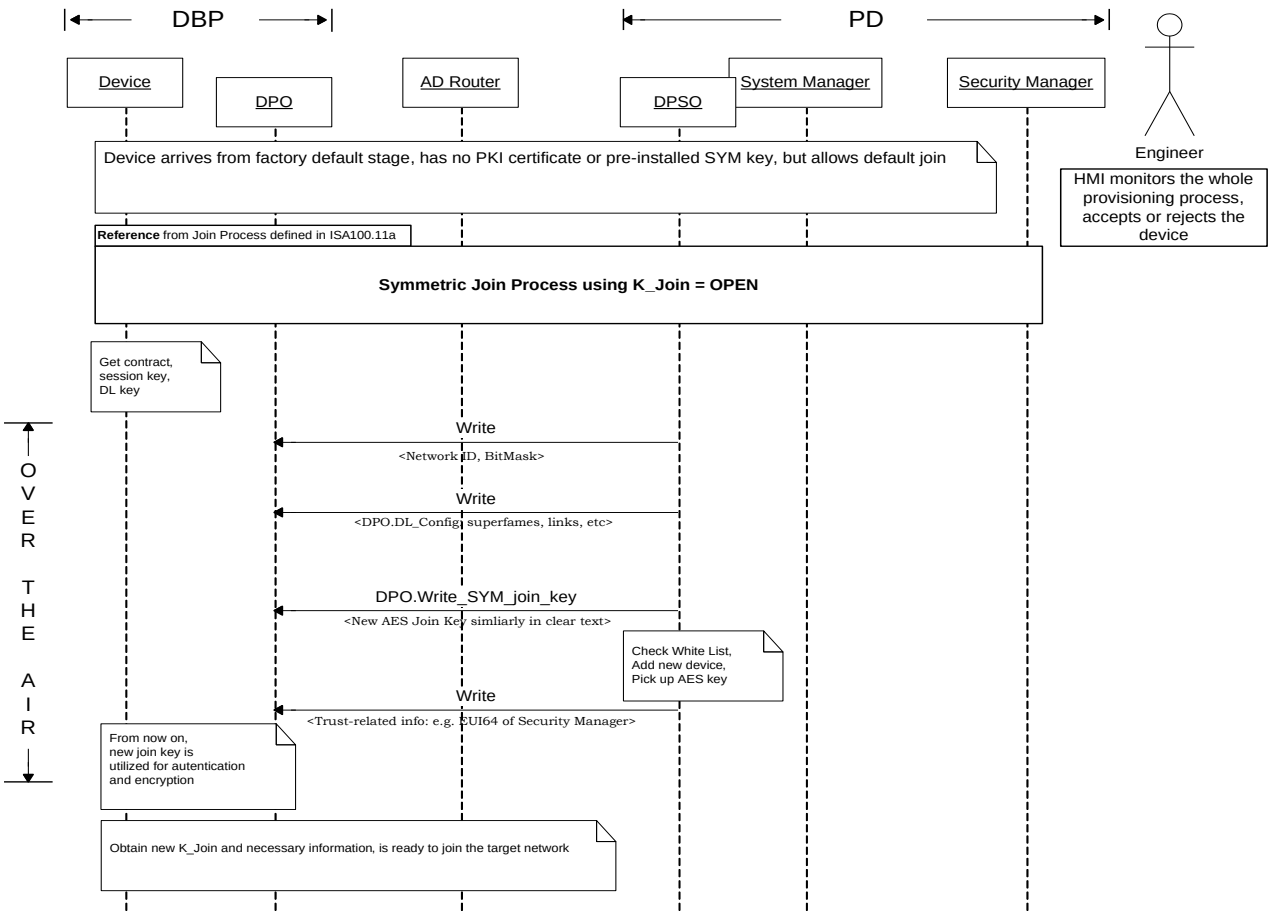

Figure 39, Open symmetric join key provisioning[9]

[9] *Note: no time sequences will be described for the later cases as either only network-related information needs to be provisioned by similarly joining provisioning network or definitions of particular OOB mechanisms are out of scope*.

5.3.2.3 Provisioning with Out-of-Band (OOB) Mechanism

Prerequisites:

- The DBP has factory default (e.g. config bit A1 is set) without pre-installed credentials;
- The PD has a pool or list of valid symmetric keys which are generated and registered in the white list by System manager/Security manager. The keys have the option of being either universal for all devices or specifically chosen for specific EUI64 address, and all of them are time-bounded;

Steps:

1. The PD, especially handheld device with the secure storage of symmetric join keys, is placed close to or connected to the DBP, which is dependent on which kind of communication the OOB adopts. Then the attributes of DPO are written via the OOB communication interface;
2. With the network-related and trust-related information provisioned via OOB mechanism, the DBP gets itself ready to join the target network[10];

5.3.2.4 Provisioning OTA or OOB of Network-related Information on the basis of Pre-installed Symmetric Join Key

Prerequisites:

- Device arrives from factory pre-provisioned procedure at manufacture site with the possession of valid pre-installed symmetric join key to the specific target network;
- The config bit either A1 or A3 is set;
- The Security manager of target network need to have the installation of device addresses and their corresponding symmetric join keys. Note this is only for the validity of join keys in the subsequent join process of joining in the target network;

Steps:

1. If A3 is enabled, the DBP passively listens to and captures the advertisement of provisioning network;
2. Upon the receipt of advertisement, the DBP initialize the join request to provisioning network using K_Global;
3. After successfully join to the provisioning network, a contract between DBP and PD is established in order that the attributes in DPO of the DBP could be provided by the

[10] *Note: The OOB communication means could be any one of infrared, memory cards, wired connectors or near field communication on devices.*

network settings stored in DPSO of the PD via application level read/write primitives and methods;

4. By obtaining the network-related information and already-owned symmetric join key, the DBP get itself ready to join the target network;

   OR

5. If A1 is set, network settings of target network can also be provided by OOB mechanism as defined previously;

5.3.2.5 Provisioning Backbone Devices

Prerequisites:

- A new backbone device compliant to this standard that has default settings without pre-installed keys;
- The PD has a pool or list of valid symmetric keys which are generated and registered in the white list by System manager/Security manager. The keys have the option of being either universal for all devices or specifically chosen for specific EUI64 address, and all of them are time-bounded;

Steps:

1. The PD, especially handheld device with the secure storage of symmetric join keys, is placed close to or connected to the DBP, and it is dependent on which kind of communication the OOB adopts. Then the attributes of DPO are written via the OOB communication interface (probably backbone interface);
2. The 128-bit address of System Manager needs to be provisioned.
3. The backbone device maybe for instance, a gateway residing on the backbone or the first advertisement router connected to the network via backbone. In those cases, the device may not have a DL interface or cannot forward its join request to the target network without the help of an advertising router. So as to join the target network, the device needs to talk directly to the System Manager over the backbone.
4. With the provisioned 128-bit address of System Manager, the device has enough information to construct network header for its join request.

5.3.3 Comparisons

Compared with asymmetric key based OTA provisioning, open join key provisioning is certainly an unsecure procedure that gives birth to potential security risks in data confidentiality (eavesdropping), authentication of device (impostor), etc. For example, a malicious device may eavesdrop in the middle between the PD and DBP, steal join key and other shared credentials because K_Join = OPEN is published by default, and then

pretends to be the supposed DBP join target network, in the meantime denies the service request of innocent DBP. This is why open join key provisioning is default rejected by the PD or System/Security Manager, and might be only enabled under the circumstance where user either requires low-level of security concerns or believes that sufficient counter-measures are against those attacks. Nevertheless, open join key provisioning does offer the convenience for:

- devices without PKI certificates or pre-installed specified symmetric key, or
- devices equipped with PKI certificates but the PD has no asymmetric cryptographic module

to join a provisioning network, where the fact of transferring security information such as join key almost in the clear over the air is tolerable.

Even though a high level of security is brought by asymmetric cryptographic method that guarantees secrecy of trust-related information provided to the DBP, the PD or Security Manager compliant to this standard is not mandatory to have asymmetric cryptographic capabilities. It is recommended that the DM of security manager supports the upgrade of functionalities (e.g. asymmetric cryptographic capabilities) via memory, new firmware, processing power or additional peripherals in order to accommodate the security needs of asymmetric key based provisioning. Nevertheless the huge consumption of energy and time when performing asymmetric cryptographic scheme is also a tricky issue.

Apart from these two distinctive provisioning methods we were talking about, OOB provisioning with handheld and pre-factory provisioning (pre-installation of credentials in the device) may also be two secure alternatives available in special circumstances. When adopting OOB mechanism, no matter which kind of OOB communication means (e.g. infrared, cable connection or near field communication), specialized hardware for corresponding communication interface is needed to be implemented on the handheld. Additionally a stolen, lost or damaged handheld could also pose significant risks to the provisioning procedure. In the case of factory pre-provisioning stage at the supplier site, white list of EUI-64 and symmetric key pairs is required to be securely registered in the System/Security Manager of target network as soon as the DM provisions requisite information to the fresh device. However the means by which the confidential information is delivered to the System/Security Manager are out of scope of this standard e.g. securely emailed or sent on CDs. The feasibility of this provisioning method is yet left to the device manufacturers.

From the both security and energy conservation’s point of view, an external mechanism that acts as a controller of device’s provisioning state, providing legal access of the device’s database, needs to be provisioned by authorized provisioning device only. This controller or more precisely, a switch is required to be well-designed under the goals of minimizing battery consumption by locking provisioning state of the device once the legitimate

provisioning is finished. It is concerned for the risky case that a malicious PD might be commanded to re-provision a device repeatedly.

5.4 Differences of provisioning schemes in ISA100.11a and WirelessHART

For provisioning cases in *Wireless*HART, please refer to [37].

5.4.1 Wired and Wireless

Essentially, one of the biggest differences during the device provisioning procedure between *Wireless*HART and ISA-100.11a lies in the obvious distinction of physical layer communication. *Wireless*HART utilize a wired connection [37] for distributing provisioning information to device with the help of a specialized handheld terminal. However, as it is described in the standard of ISA-100.11a, the provisioning process is implemented mainly in the form of a wireless way, asymmetric key based and symmetric key based provisioning. Moreover, pre-installation at supplier site and out of band (OOB) provisioning is mentioned and supported informatively as well.

In *Wireless*HART case, a handheld terminal either with secure storage of join keys or built-in software of key generator needs to be placed close (physically reachable by wire) to the DBP, and then starts key distribution. *"Imagine the scene where a device, which has already been sent to and fixed in a remote area, is in the status that requires to be provisioned again (exceptions occurs, e.g. current join key needs to be revoked and replaced with a new one)"* But in ISA-100.11a where OTA provisioning is highlighted, a PD having been implemented with the role of System/Security Manager could set up a relatively secure provisioning network e.g. asymmetric key based provisioning, where the DBP is able to be accommodated with network and trust-related settings that are sent in enciphered text over the air. As it is mentioned in the previous chapter, a provisioning network could be conveniently established either in the form of a temporary mini network with a handheld or a separate logic network on the target join network. With the flexibility of OTA communication, specialized engineers only need to sit at the office probably with a HMI monitoring the procedure of provisioning, react when exceptions occur instead of carrying handheld terminal where the DBPs are placed. This OTA process also helps us skip the potential security risk brought by stolen or lost handheld terminal. In addition, after appropriate provisioning of the DBP but before joining process, a provisioning network may be further used to pre-configure appropriate application level objects of the DBP via existed contract between the PD and DBP.

Security Consideration

As we know that ISA100.11a introduces OTA provisioning schemes, wireless security issues need to be taken into consideration to achieve secure operation. Therefore, we are going to list the potential wireless threats against the availability of wireless system that might lead to vulnerabilities in this standard:

OTA provisioning schemes, which consist of the same messaging as basic wireless communication messaging defined in the standard, operate their radios at the 2.4 GHz frequency band that are shared by *Wireless*HART, IEEE 802.11, ZigBee and Bluetooth devices. It is possible that two or more devices that are compliant to those open standards try to access the same channel simultaneously and a series of collisions may occur. If the cause of collision is unintentional (that are caused by random accessing to RF channel of devices), it is not difficult to be minimized with the help of CCA operation at the start of transmitting timeslot (for detecting if the channel is occupied by other wireless standards' devices e.g. IEEE 802.11) and well-scheduled communication (with both time and frequency diversity for minimizing collision of intra-standard's devices). However, what if the source of collision is intentional, such as jamming, then the coexistence mechanism (e.g. CCA) will not work due to the fact that lots of noise and interference signals are inserted into the communication medium so as to make the a certain channel be occupied for a longer time, hence block channel usage and interrupt the scheduled communication. This kind of jamming maybe mitigated by using spectrum management (which is similar to the "blacklisting" method in *Wireless*HART) by blocking or limiting the usage of certain channels that are reported with relatively weak connectivity.

For the worst case, all the channels available to the communication might be flooded by intentionally forged traffic such as "join request flooding" wherein fake join requests with DL MIC calculated using Global key and message content protected by fake join key are flooded towards the System/Security Manager. Even though one single fake join request can never fool System/Security Manager, many of similar malicious requests will consume and exhaust the network resource all the way from and to the System/Security Manager (exhaustion attack). The catastrophic outcome of this attack will not only interrupt the join process operations but also the normal data communication and maintenance of network because the System/Security Manager that keeps performing security check (computationally extensive) might be "all the time" occupied by the fake join requests. Sooner or later, with continuously intense attack, the System Manager will not be able to handle normal network administration and configuration, thus a DOS attack is achieved to paralyze the whole field network.

Other forms of attack may also be utilized as threats to the wireless system, such as spoofing attack, wherein malicious device may pretend to be PD or advertising router that is able to advertise itself to the DBPs. Then the imposter may get the join requests from the DBPs and do traffic analyses probably about crucial network operation parameters in order to launch more effective attacks in the future.

To conclude, being considered as the most crucial step before joining process, OTA provisioning solution brings us the convenience in real-time operation, but it is also vulnerable to some kinds of attacks against the availability of wireless system. The spoofing of PD and advertising router can be detected and terminated by mutual authentication scheme (challenge-response) defined in ISA100.11a. Nevertheless, it can further lead to a DOS attack as many impostors occupying at a close distance of the DBPs keep intercepting the join requests and then discarding join request. There is no definite solution against

Denial-Of-Service attack. Therefore, enhanced network monitoring with strict access control needs to be performed to supervise the malicious actions, suspicious packets and then quench them from the start.

5.4.2 Join Process

The PD in ISA-100.11a standard could be viewed as having somewhat the same role as the handheld terminal in *Wireless*HART during the provisioning process. In the example of *Wireless*HART enabled handheld provisioning [37], feasibility has been offered by online communication between handheld and asset manager via gateway. But the handheld device has to join the target network first as a new device, which should present its credentials to Security Manager and follow all stages required by a join process. Instead, the PD that acts actively in the provisioning operations of ISA-100.11a is actually the other logical side of System/Security Manager. It provides direct interactions with the commander of the target network as the PD is actually System/Security Manager with the implementation of device provisioning service object (DPSO), however, in *Wireless*HART the *Wireless*HART -enabled handheld acts as a proxy between the DBP and Network/Security manager. Nevertheless, the DBP in ISA100.11a still has to first experience a standard join process for the provisioning network that is formed by the PD to obtain a contract, session key and DL key to continue subsequent communication with the PD for provisioning of network or/and trust-related information. It is difficult to say which one of the join processes specified in two standards is more efficient. Another issue about efficiency is that after *Wireless*HART -enabled handheld join the network, it might be able to provision as many as devices possible. But in ISA100.11a, each one of devices that wish to join the target network might need to join provisioning network. From this point of view, the former case might sound more efficient.

5.4.3 Plain and Cipher text

In ISA-100.11a, the default symmetric join key, either K_Global or K_Join = OPEN is used to OTA join provisioning network for prerequisite settings before joining the target network. Even though K_Global = ISA100 is a well-known value, it therefore offers data integrity for devices that do not share a secret join key in the case of provisioning network-related information, authenticating device identity, etc. With the help of K_Global (join provisioning network and establish a contract), the DBP with asymmetric cryptographic modules could receive an updated join key encrypted by its public key from the PD in provisioning network. The fact that new join key is enciphered by device's public key could bring enhanced security for data confidentiality such as avoiding interception of key value for malicious use. In *Wireless*HART, join key is downloaded to the new device in plaintext via wired link, which might pose a potential risk of security that people could eavesdrop on the wired link and the confidential join key that performs as the only protection of the system could almost be read in clear text. However, as the consideration of the extra time and energy consumption brought by cryptographic operations, provisioning with plaintext or cipher text is dependent on the level of security tolerated by the environment of that time.

5.4.4 Management Architecture

The Figure 40 describes the management architecture of ISA-100.11a. Path A and B are defined normatively in the standard, providing two distinct ways in managing and configuring device. The user application process is monitored and configured via gateway by host applications, while the device management application process should be managed by System Manager.

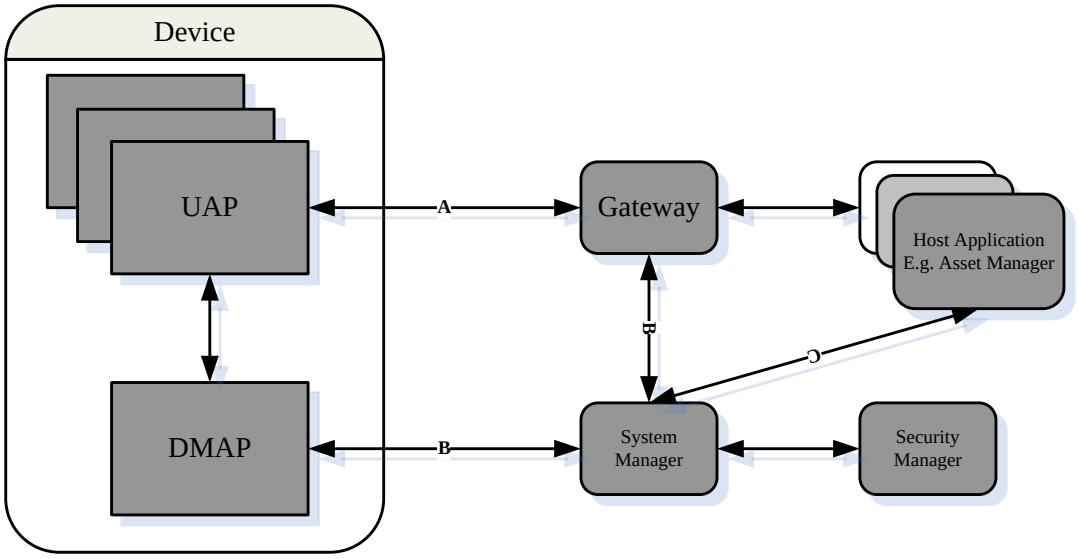

Figure 40, Management Architecture on Application Layer [1]

As we can see from the management architecture, path C that is mentioned (not defined) in informative example of implementations in this standard, does support a connection between host applications and System Manager (e.g. Asset Manager) that enable direct interaction for host applications communicating with system manager in terms of network status and services. With this significantly different management architecture from it in *Wireless*HART *[8],* the gateway is not that actively involved in both provisioning and joining process as it is in *Wireless*HART (no quarantined status is mentioned in ISA-100.11a). This might help ease the workload of gateway as it does not act as a routing hub between host applications and System/Security Manager. Besides, gateway should be implemented to be able to be accessed and configured by system manager via path B.

5.5 Interoperability and Conclusion

5.5.1 The Possibility of Incorporation

As specified [37], provisioning of secret shared keys is achieved by a wired link between handheld terminal and *Wireless*HART field device, it sounds much alike of one of the scenarios mentioned in the out of band mechanism of provisioning in ISA-100.11a, where the PD (e.g. handheld) provisions the DBP via OOB interface that is wired connectors in this special case. The coincidence is that the standard of ISA-100.11a supports this series of specialized OOB provisioning (infrared, wired connectors, memory cards, etc.) but makes their specification out of scope (left to the vendor's implementation). Hence it provides the possibility to incorporate these smart wired solutions specified in the [37] to be active parts of implementation instances in the OOB solutions of provisioning for devices compliant to ISA-100.11a.

However, the tradeoff between convenience and complication introduced by incorporation might be worth of discussing. These tricky issues lie into two distinctive protocol suites above physical layer defined by two standards. At application layer, ISA-100.11a has a series of well-defined objects with attributes in different application processes that communicate with each other via application sub-layer services and primitives. It supports client/server, source/sink, and publish/subscribe application flow type. In *Wireless*HART, application layer is command-oriented that follows a request/response format *[8]*. Therefore, that would be interesting to discuss about how to map application level services and inter-object communication methods with commands, and correspond attributes of objects with parameters (*e.g. mapping "DPO.Write_Join_key" to command "writeJoinKey (joinkey)"*) between two devices compliant to two standards respectively. In addition, the handheld utilized in *Wireless*HART is a portable *Wireless*HART enabled computer with built-in host application for device configuration, calibration and management. So as to fulfill the requirement of being a PD in ISA-100.11a, a necessary functionality of System/Security Manager is needed to be added in the already existed handheld terminal.

5.5.2 Conclusion

To summarize, ISA100.11a defines and supports a wide and general range of provisioning process in terms of over the air schemes and OOB mechanisms. Provisioning with Asymmetric key based scheme provides a highly secure and convenient communication path between the DBP and PD for populating necessary network settings without the requirement of additional tools. But in addition to the extra efforts for performing asymmetric cryptographic operation, this provisioning process may also get affected in these scenarios:

- the installation of valid PKI certificates or certificate chains has not been done at pre-provisioning stage (not factory default stage) or
- the DBP is treated by a PD without asymmetric cryptographic capabilities.

Thus, an optionally adopted open symmetric key provisioning procedure could be used to be the backup measure for the previous two cases mentioned above. Moreover, under the circumstance where transmitting confidential trust-related information almost in clear over the air (as session key might be compromised during the open join key provisioning) is concerned to be potentially risky, ISA-100.11a supports provisioning with OOB mechanisms to be adopted properly. If the incorporation issues of *Wireless*HART provisioning that mentioned previously are proved to be worth adopting, there exists a series of solutions that commission provisioning secret keys to device via cable connected handheld terminal [37] as important implementation instances of OOB mechanisms.

6 CONCLUSIONS AND FUTURE WORK

6.1 Conclusion

In this thesis, we have pointed out and properly analyzed the differences between ISA100.11a and *Wireless*HART step by step from system architecture level to each protocol layer's functionality. In comparison with *Wireless*HART, ISA100.11a offers a vaster coverage and broader view of process automation solutions:

- Role profiles give birth to flexible device configuration according to on site needs;
- Backbone network consideration minimizes the latency of wireless mesh;
- Subnets connecting to the backbone network enable the linear scalability of the network;
- Contract agreed between device and System Manager facilitates control of field device and provides required QOS for device communication;
- Formative specification of security issues guides the security design of the system and enables elastic security deployment to meet different security-strength required;
- IPv6 compatibility extends the use of various internet technologies;
- Object-orientation unifies network management and enhance legacy systems' interoperability;
- Multiple options of length of timeslot, channel hopping, neighbor discovery, join and provisioning schemes;
- and etc.

Nevertheless, *Wireless*HART still dominates the market because *Wireless*HART enabled devices are already available as well as 26 million installed HART devices worldwide. Compared with the huge and new ISA100.11a, the smaller and more focused *Wireless*HART can be adopted and further developed in considerably faster paces.

ISA100.11a can fulfill most of the *Wireless*HART functionalities at Application Level, e.g. commands and parameters can be transformed into inter-object communication methods and attributes. Furthermore, due to the fact that ISA100.11a and *Wireless*HART both share some similar characteristics (such as similar physical condition, length of timeslot) and possess other distinctive features, complementary design according to similarities and difference can be realized to enhance either ISA100 or *Wireless*HART specification. For instance, it seems to be possible to integrate two standards by equipping a device with a double-protocol stack over Media Access Control Layer, and it understands both ISA100.11a and *Wireless*HART so as to separately handle the different messages compliant with different standards. Hence, the newly produced devices can be either installed in a traditional *Wireless*HART network or a versatile ISA100.11a network that is conformed to the unified ISA100 standards. On all accounts, ISA100.11a represents ISA100

committee that aims at a single integrated series of standards, and it is designed by both of end users and suppliers together to have enough open arms for the incorporation of any protocols in process automation field, which is in strong comparison to the HART Communication Foundation which is principally a vendor organization.

6.2 Future Work

As a matter of fact, ISA100.12 subcommittee will provide convergence information of two standards and installation guidance of two systems in a pre-converged environment for developers and end users respectively later in 2010. But this thesis can be served as one of the first-hand comparison documents that outline differences found in two standards before any official comparison documents and convergence guidance contributed from ISA100.12.

Since there are no ISA100.11a-enabled devices available at this moment, detail comparison and evaluation about the real-time performance (such as efficiency of join, provisioning process and security operations) between *Wireless*HART and ISA100.11a is difficult to be performed, which could be left for future efforts.

7 REFERENCES

[1] *Wireless Systems for Industrial Automation: Process Control and Related Applications*, International Society of Automation (ISA) Standard 100.11a, Draft 2a, 2009.

[2] *Wireless medium access control (MAC) and physical layer (PHY) specifications for low rate wireless personal area networks (WPANs)*, IEEE STD 802.15.4: 2006.

[3] *Hart Communication Foundation*, accessed February 2010, http://www.hartcomm.org.

[4] *ISA100, Wireless Systems for Automation*, accessed January 2010,

http:// www.isa.org.

[5] *Zigbee alliance*, accessed May 2010, http:// www.zigbee.org.

[6] *Bluetooth*, accessed May 2010, http://www.bluetooth.com.

[7] T. Lennvall, S. Svensson, and F. Hekland, *A Comparison of WirelessHART and Zigbee for Industrial Applications*, WFCS, 2008.

[8] *HCF WirelessHART Specification.*

[9] Seiichi Shin, *Trend of Process Automation and Factory Automation*, SICE-ICASE, International Joint Conference, October, 2006.

[10] V.C. Gungor and G.P. Hancke, *Industrial WSNs: Challenges, Desgin Principles, and Technical Approaches*, Industrial Electronics, IEEE Transactions, October, 2009.

[11] C. Alcaraz and J. Lopez, *A Security Analysis for Wireless Sensor Mesh Networks in Highly Critical Systems*, Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions, April, 2010.

[12] N. Kushalnagar and G. Montenegro, *6LoWPAN: Overview, Assumptions, Problem Statement and Goals.*

[13] *FIPS 197 AES Standard*, accessed March 2010,

http://csrc.nist.gov/publication/fips/fips197/fips- 197.pdf.

[14] J. Daemen and V. Rijmen, *The Desgin of Rijndael AES – The Advanced Encryption Standard, Springer, 2002.*

[15] *NIST – Special Publication SP80-38a Block cipher modes of operation*, accessed March 2010, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[16] D.L. Evens, P.J. Bond, and A.L. Bement, Jr. *The Keyed-Hash Message Authentication Code (HMAC)*, FIPS PUB 198.

[17] *International Standard*, ISO/IEC 18033-2:2006(E).

[18] X. Zhang, M. Wei, P. Wang, and Y. Kim, *Research and Implementation of Security Mechanism in ISA100.11a Networks*, Electronic Measurement & Instruments, ICEMI, 2009.

[19] G. Montenegro, N. Kushalnagar, J. Hui and D. Culler, *Transmission of IPv6 Packets over IEEE 802.15.4 Networks*, RFC 4944, September 2007.

[20] S. Deering and R. Hinden, Internet Protocol, Version 6 (IPv6) Specification, RFC 2460, December 1998.

[21] A. K. Lenstra and E.R. Verheul, *Selecting cryptographic key sizes*, J.Cryptol., vol. 14, no. 4, pp.255-293, 2001.

[22] Jon Postel, *User Datagram Protocol*, RFC 768, USC/Information Science Institue, August, 1980.

[23] Certicom Research, *Standards for Efficient Cryptography, SEC1: Elliptic Curve Cryptography*, Version 1.0, September, 2000.

[24] K. Ramakrishnan, S. Floyd, and D. Black, *The Addition of Explicit Congestion Notification (ECN) to IP*, RFC 3168, September 2001.

[25] *Chinese Industrial Wireless Alliance*, accessed May 2010, http:// www.industrial wireless.cn/en/06.asp.

[26] *Industrial communication networks – Fieldbus specifications–WIA-PA communication network and communication profile*, accessed March 2010, http://www.iec.ch/.

[27] Carlos Eduardo Pereira, *Applying Object-oriented Concepts to the Development of Real-time Industrial Automation Systems*, Proceedings- Third International Workshop on Object-oriented Real-Time Dependable Systems, 1997.

[28] J. Song, S. Han, A. M. Mok, D. Chen, M. Lucas, M. Nixon, and W. Pratt, *WirelessHART: Applying Wireless Technology in Real-Time Industrial Process Control*, Proc. IEEE Real-Time and Embedded Technology and Applications Symposium, 2008.

[29] *Emerson Process Management*, accessed May 2010,

http://www2.emersonprocess.com/en-US/news/pr/Pages/1009-THUM.aspx

[30] *Emerson Process Management*, accessed May 2010,

http://www2.emersonprocess.com/en-US/news/pr/Pages/809-wirelesshart.aspx

[31] Yosuke Ishii, *Exploiting Backbone Routing Redundancy in Industrial Wireless Systems*, Industrial Electronics, IEEE transactions, October, 2009.

[32] H. Hayashi, T. Hasegawa, and K. Demachi, *Wireless Technology for Process Automation*, ICCAS-SICE, 2009.

[33] S. Raza, A. Slabbert, T. Voigt, and K. Landernäs, *Security Considerations for the WirelessHART Protocol*, Emerging Technologies & Factory Automation, 2009, ETFA 2009, IEEE Conference.

[34] S. Han, J. Song, X. Zhu, A.K. Mok, D. Chen, M. Nixon, W. Pratt, and B. Gondhalekar, *Wi-HTest: Compliance Test Suite for Diagnosing Devices in Real-Time WirelessHART Network*, Real-Time and Embedded Technology and Applications Symposium, 2009, RTAS 2009, 15th IEEE conference.

[35] X. Zhu, W. Dong, A.K. Mok, S. Han, J. Song, D. Chen, and M. Nixon, *A location-determination Application in WirelessHART*, Embedded and Real-Time Computing Systems and Applications, 2009, RTCSA'09, 15th IEEE International Conference.

[36] *Tasks of ISA100.12 Subcommittee*, accessed March 2010,

http://www.isa.org/Template.cfm?Section=Press_Releases5&template=/ContentManagement/ContentDisplay.cfm&ContentID=80911

[37] Thomas Ruschival, *Key Distribution for WirelessHART devices,* ABB internal document.