

**PERFORMANCE EVALUATION OF INDUSTRIAL WIRELESS SENSOR
NETWORK TECHNOLOGIES: ZIGBEE, WIRELESSHART, AND ISA100**

BY

Jebril Ahmad Ali Battsh

A Thesis Presented to the
DEANSHIP OF GRADUATE STUDIES

KING FAHD UNIVERSITY OF PETROLEUM & MINERALS

DHAHRAN, SAUDI ARABIA

In Partial Fulfillment of the
Requirements for the Degree of

MASTER OF SCIENCE

In

COMPUTER NETWORKS

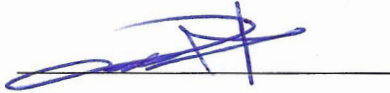
May 2017

KING FAHD UNIVERSITY OF PETROLEUM & MINERALS
DHAHRAN- 31261, SAUDI ARABIA
DEANSHIP OF GRADUATE STUDIES

This thesis, written by **Jebril Ahmad Ali Battsh** under the direction his thesis advisor and approved by his thesis committee, has been presented and accepted by the Dean of Graduate Studies, in partial fulfillment of the requirements for the degree of **MASTER OF SCIENCE IN COMPUTER NETWORKS**.



Dr. Tarek R. Sheltami
(Advisor)



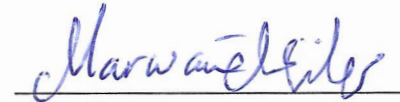
Dr. Ahmad Almulhem
Department Chairman



Dr. Ashraf S. Hasan Mahmoud
(Member)



Dr. Salam A. Zummo
Dean of Graduate Studies



Dr. Marwan H. Abu-Amara
(Member)

25/5/17
Date

© Jebril Ahmad Ali Battsh

2017

To my Family

ACKNOWLEDGMENTS

All Thank be to Allah, Lord of the Worlds

I would like to thank my Advisor (Dr. Tarek Sheltami) and the committee members (Dr. Ashraf Mahmoud and Dr. Marwan Abu Amarah) for their help and guidance, I would also like to thank the University for offering this opportunity to study. Finally, I will never forget to thank my mother for here moral support.

TABLE OF CONTENTS

ACKNOWLEDGMENTS	V
TABLE OF CONTENTS	VI
LIST OF TABLES	X
LIST OF FIGURES	XI
LIST OF ABBREVIATIONS	XIII
ABSTRACT	XVII
ملخص الرسالة.....	XVIII
1 CHAPTER INTRODUCTION	1
1.1 IEEE 802.15.4	1
1.2 IEEE802.15.4 standards	2
1.3 ZigBee.....	2
1.3.1 Basic Features.....	3
1.3.2 Protocol Devices	3
1.4 WirelessHART	4
1.4.1 Basic Features.....	4
1.4.2 Protocol Devices	5
1.5 ISA.100	6
1.5.1 Basic Features.....	6

1.5.2	Protocol Devices	6
1.6	Research Objectives	7
2	CHAPTER 2 PROTOCOL LAYERS	8
2.1	ZigBee Protocol Layers	8
2.1.1	The IEEE 802.15.4 PHY Specifications.....	9
2.1.1.1	Channel Assignments.....	10
2.1.1.2	Energy Detection	11
2.1.1.3	Carrier Sense.....	12
2.1.1.4	Link Quality Indicator.....	12
2.1.1.5	Clear Channel Assessment	13
2.1.1.6	The PHY Constants and Attributes	14
2.1.1.7	PHY Services	15
2.1.1.7.1	PHY Data Service.....	16
2.1.1.7.2	PHY Management Service	17
2.1.1.8	The Service Primitives	18
2.1.1.9	PHY Packet Format	18
2.1.2	IEEE 802.15.4 MAC Layer	22
2.1.2.1	Superframe Structure and Beacon-Enabled Operations	23
2.1.2.2	The Interframe Spacing.....	25
2.1.2.3	CSMA-CA.....	26
2.1.2.4	MAC Services	30
2.1.2.5	MAC Frame Format.....	31
2.1.3	The ZigBee NWK Layer	35
2.1.3.1	ZigBee Topologies	36
2.1.3.2	The NWK Layer Frame Format	38

2.1.4	The APL Layer	41
2.2	WirelessHART Protocol Layers.....	43
2.2.1	WirelessHART PHY layer	43
2.2.2	WirelessHART Data Link Layer	44
2.2.3	WirelessHART NWK layer	46
2.3	ISA100 Protocol Layers.....	49
2.3.1	ISA100 PHY layer	49
2.3.2	ISA Data Link Layer	50
2.3.3	ISA100 NWK layer.....	53
2.3.4	ISA Transport layer	53
2.3.5	ISA100 APL layer.....	54
3	CHAPTER 3 LITERATURE REVIEW.....	55
3.1	Literature Review.....	55
3.2	Summary.....	58
4	CHAPTER 4 WIRELESSHART IMPLEMENTATION DESCRIPTION AND VALIDATION.....	60
4.1	WirelessHART Implementation in NS-2	60
4.1.1	The DL layer.....	60
4.1.2	The NWK layer.....	61
4.1.3	Transport layer	63
4.1.4	The APL layer.....	63
4.1.5	The Network Manager.....	63
4.1.5.1	The Join Procedure	64
4.1.5.2	Graph and Route Definition	65
4.1.5.3	Communication Scheduling and Channel Management.....	70

4.1.5.4	Service Request Procedure	71
5	CHAPTER 5 ISA100 IMPLEMENTATION AND BENCHMARKING	73
5.1	The Implemented ISA100 simulator	73
5.2	ISA100 Benchmarking	78
5.3	Summary.....	82
6	CHAPTER 6 SIMULATION AND RESULTS	83
6.1	Simulation and Results.....	83
6.2	The Conclusion.....	94
6.3	The Recommendations	96
	REFERENCES.....	97
	VITAE.....	101

LIST OF TABLES

Table 2-1 Channel Numbers	10
Table 2-2 PHY Constants	14
Table 2-3 PHY-PIB attributes.....	14
Table 2-4 the lengths and the Durations of the Preamble Field.....	20
Table 2-5 the Field Format of SFD.....	20
Table 2-6 SFD Field Lengths.....	21
Table 2-7 Frame Length Values	21
Table 2-8 Network Commands.....	40
Table 6-1 experiment 1 parameters.....	84
Table 6-2 Experiment 2 parameters.....	89

LIST OF FIGURES

Figure 2-1 Protocol Layers of ZigBee	9
Figure 2-2 PHY and MAC Layers of the IEEE 802.15.4	16
Figure 2-3 Two Devices Data delivery procedure	17
Figure 2-4 the principle of work of the Service Primitive	18
Figure 2-5 PHY Layer Protocol Data Unit Format.....	19
Figure 2-6 The Model of the MAC sublayer	23
Figure 2-7 The Structure of the SuperFrame	24
Figure 2-8 The Timing of the Received and the Transmitted Superframes	25
Figure 2-9 The Interframe Spacing in (a) Acknowledged and (b) Unacknowledged Transmission	26
Figure 2-10 the Algorithm of the CSMA-CA.....	28
Figure 2-11(a) The Hidden and (b) The Exposed Node Problems	29
Figure 2-12 (a) The General frame format of the MAC and (b) the Frame Control Field	31
Figure 2-13 MAC Beacon Frame	33
Figure 2-14 (a) The MAC Data Frame, (b) The MAC Acknowledgment Frame, and (c) The MAC Command Frame Formats	34
Figure 2-15 ZigBee network layer.....	35
Figure 2-16 (a) The Broadcast, (b) The Multicast, and (c) The Unicast Communications	36
Figure 2-17 The hierarchical (Tree) topology	37
Figure 2-18 General Network Frame Format	39
Figure 2-19 The Network Layer (a) data and (b) command frame formats	40
Figure 2-20 The Application Layer	41
Figure 2-21 WirelessHART Protocol Layers	43
Figure 2-22 Data Link Layer Protocol Data Unit	45
Figure 2-23 WirelessHART SuperFrame	46
Figure 2-24 WirelessHART NWK layer Frame format	47
Figure 2-25 WirelessHART Transport Layer Frame Format	48
Figure 2-26 WirelessHART APL Layer Frame Format	48
Figure 2-27 ISA100 Protocol Layers.....	49
Figure 2-28 SuperFrame Structure.....	50
Figure 2-29 (a) slotted Hopping and (b) Slow Hopping.....	51
Figure 2-30 Hybrid Hopping	52
Figure 4-1 WirelessHART Protocol Stack	62
Figure 4-2 the Join Procedure.....	65
Figure 4-3 The Service Request.....	72
Figure 5-1 Slotted Hopping mechanism	76

Figure 5-2 Slow Hopping mechanism	77
Figure 5-3 Simulation Setup	78
Figure 5-4 Network Throughput Comparison	79
Figure 5-5 Average Delay Comparison	80
Figure 5-6 Network Throughput Comparison for Different SD	81
Figure 5-7 Average Delay Comparison for Different SD	81
Figure 6-1 The Average End to End Delay of ZigBee, WirelessHART, and ISA100:(10ms TS ,11ms TS ,12ms TS, CSMA-CA)	86
Figure 6-2 The Throughput of ZigBee, WirelessHART, and ISA100:(10ms TS ,11ms TS ,12ms TS, CSMA-CA).....	87
Figure 6-3 The Energy Consumption of ZigBee, WirelessHART, and ISA100:(10ms TS ,11ms TS ,12ms TS, and CSMA-CA).....	88
Figure 6-4 ZigBee Throughput Beacon-enabled vs non-beacon mode	90
Figure 6-5 WirelessHART End to End Delay vs SuperFrame Interval	91
Figure 6-6 WirelessHART Throughput vs SuperFrame Interval	92
Figure 6-7 ISA100 End to End Delay vs SuperFrame Interval	92
Figure 6-8 ISA100 Throughput vs SuperFrame Interval	93

LIST OF ABBREVIATIONS

WSN	:	Wireless Sensor Network
FFD	:	Full Function device
RFD	:	Reduced Function Device
CSMA-CA	:	Carrier Sense Multiple Access with Collision Avoidance
TDMA	:	Time Division Multiple Access
PHY	:	Physical
DL	:	Data Link
NWK	:	Network
APL	:	Application
CCA	:	Clear Channel Assessment
CAP	:	Contention Access Period
CFP	:	Contention Free Period
PSDU	:	Physical Service Data Unit
WPAN	:	Wireless Personal Area Network
MAC	:	Medium Access Control
AODV	:	Ad-hoc on-Demand Distance Vector

GTS	:	Guaranteed Timeslot
DSSS	:	Direct sequence Spread Spectrum
FHSS	:	Frequency Hopping Spread Spectrum
ISO	:	International Standard Organization
OSI	:	Open System Interconnect
SAP	:	Service Access Point
MLDE	:	MAC Layer Data Entity
ED	:	Energy Detection
CS	:	Carrier Sense
LQI	:	Link Quality Indication
RSS	:	Received Signal Strength
SNR	:	Signal to Noise Ratio
PIB	:	PAN Information Base
SHR	:	Synchronization Header
MLME	:	MAC Layer Management Entity
MPDU	:	MAC Protocol Data Unit
PHR	:	Physical Header

SFD	:	Start of Frame Delimiter
NLME	:	Network Layer Management Entity
BI	:	Beacon Interval
BO	:	Beacon Order
SD	:	Super Frame Duration
IFS	:	Interframe Spacing
LIFS	:	Long Interframe Spacing
SIFS	:	Short Interframe Spacing
MSDU	:	MAC Service Data Unit
MHR	:	MAC Header
DSN	:	Data Sequence Number
BSN	:	Beacon Sequence Number
FHC	:	Frequency Check Sequence
BLE	:	Battery Life Extension
ZDO	:	ZigBee Device Object
APS	:	Application Support
APSME	:	Application Support Management Entity

CRC	:	Cyclic Redundancy Check
O-QPSK	:	Offset Quadrature Phase Shift Keying
IETF	:	Internet Engineering Task Force
PER	:	Packet Error Rate
PGI	:	Packet Generation Interval
RTS	:	Request to Send
CTS	:	Clear to Send

ABSTRACT

Full Name : Jebril Ahmad Ali Battsh
Thesis Title : Performance Evaluation of Industrial Wireless Sensor Network
Technologies: ZIGBEE, WIRELESSHART, AND ISA100
Major Field : Computer Networks
Date of Degree : December 2016

With the continuous developments in communication technology, the use of wireless network devices is increasing rapidly. However, most companies still rely on wired networks and do not trust wireless networks, especially for process control applications. The confidence in wireless technologies can be built by first evaluating the technology before using it for industrial applications. To this end, the performance of three wireless sensor networks (WSNs) standards, namely, ZigBee, WirelessHART and ISA100, is evaluated in this work. The performance metrics are the throughput, the end to end delay, and the energy consumption. The results show that ISA100 and WirelessHART perform better than ZigBee in large networks. In addition, ISA100 is more flexible than WirelessHART, since it allows using the combination of slotted and slow hopping and configurable timeslot sizes.

ملخص الرسالة

الاسم الكامل: جبريل أحمد علي البطش

عنوان الرسالة: مقارنة الاداء لثلاثة انواع من التكنولوجيا المستخدمة في شبكات الاستشعار اللاسلكية (Zigbee, WirelessHART, ISA100)

التخصص: شبكات حاسوب

تاريخ الدرجة العلمية: كانون الاول 2016

مع التطور المستمر في تكنولوجيا الاتصال ، اصبح التوجه الى استخدام الشبكات اللاسلكية اكثر من الشبكات السلكية، لكن الشركات لازات تعتمد وتثق في الشبكات السلكية ، ولا تثق في اداء الشبكات اللاسلكية ، خصوصا في تطبيقات التحكم الصناعي. الثقة في استخدام التكنولوجيا الحديثة تأتي أولا من اختبار هذه الشبكات قبل استخدامها في مجال العمل. لهذا السبب تم في هذا البحث دراسة أداء ثلاثة أنواع من التكنولوجيا اللاسلكية المستخدمة في اجهزة الاستشعار اللاسلكي وهي ZigBee و WirelessHART و ISA100. وتم التقييم بدلالة مقدار استهلاك الطاقة ومقدار التأخير في وصول المعلومات و كمية المعلومات المنقولة. النتائج اظهرت ان WirelessHART و ISA100 افضل من ZigBee في الشبكات الكبيرة نسبيا. و ISA100 يعطي مرونة اكثر من WirelessHART في استخدام التنقل السريع والبطيء بين الترددات وايضا في استخدام عدة أحجام من نطاق ارسال البيانات (timeslot).

CHAPTER 1

INTRODUCTION

1.1 IEEE 802.15.4

Wireless sensor network (WSN) technology is a new area for both research and industry. IEEE 802.15.4 is a standard for low cost, low power, and low data rate transmission that perfectly suits the WSN requirements. Because of these features, it has been always attracting a lot of attention in both industry and research communities [1].

The IEEE 802.15.4 standard works in three channel bands and has three different data rates, namely, 2.4 GHz /250kbps, 915 MHz /40 kbps and 868 MHz /20kbps. The IEEE 802.15.4 physical layer has 27 channels, out of which 16 channels are in the 2.4 GHz band, 10 channels are in the 915 MHz band, and one channel is in the 868 MHz band [3].

The standard defines two type of devices, namely, the reduced function devices (RFDs), and the full function devices (FFDs). The RFD is an end node that works as an I/O device only. On the other hand, the FFD is a router node that works as an I/O device and it has routing capabilities. The RFDs can communicate with FFDs only. If two RFDs want to communicate with each other, they must talk to the FFD to which they are connected.

The 802.15.4 standard specification deals with medium access control sub-layer (MAC) and physical layer (PHY) aspects of many standards such as ZigBee, WirelessHART, and ISA100.11a. Therefore, the performance study for IEEE802.15.4 is very important for the design of wireless sensor networks. The IEEE 802.15.4 standard defines the PHY and MAC layer specifications for low data rate wireless connectivity among relatively simple devices that consume minimal power and operate in the Personal Operating Space [4] [5] [6].

1.2 IEEE802.15.4 standards

IEEE has launched new technologies for low cost and low data rate industrial applications on top of the 802.15.4 standard, and the main three wireless technologies are ZigBee, WirelessHART, and ISA100. The following subsections provide a detailed overview of the three standards.

1.3 ZigBee

The ZigBee standard, developed by the ZigBee alliance based on the IEEE 802.15.4 standard, offers long battery lifetime, transmits at low data rates, and is cost-efficient. ZigBee is intended for short-range wireless communication applications, and it provides long battery lifetime. The technology defined by ZigBee is cheaper and simpler than other Wireless Personal Area Networks (WPANs), such as Bluetooth. Because of these reasons, ZigBee Technology is vastly deployed in wireless control and monitoring applications [7] [8] [9].

1.3.1 Basic Features

ZigBee is a characterization for the upper protocol layer, and it has been built upon the PHY and MAC layers of the 802.15.4 standard.

Zigbee supports ad-hoc on-demand distance vector (AODV) routing algorithm, hence route discovery and peer-to-peer communication are possible. It also supports mesh-networking topologies, but it does not support frequency hopping. The only option to mitigate interference is to scan for a channel with the minimum amount of interference at startup [9] [10].

ZigBee supports two types of devices, namely, FFDs and RFDs. Thus, ZigBee can form mesh and star networks by using a combination of FFDs and RFDs [9].

ZigBee has two operational modes: beacon-enabled and non-beacon mode. In beacon-enabled mode, there are up to seven timeslots that can be used as dedicated timeslots. These time slots, also called guaranteed timeslots (GTS), increase the transmission reliability of the standard [34].

1.3.2 Protocol Devices

Coordinator: This device is responsible for starting and controlling the network. It stores information about the network, so it can act as a Trust Centre that stores security keys [11].

Router: this device enlarges network area coverage, acts as an emergency node because it provides backup routes in case of network congestion or device failure, and dynamically routes around obstacles. It connects to the coordinator and other router nodes, in addition of that it supports child nodes [11].

End Devices: These devices can only send or receive messages. They must be connected to either the coordinator or a router, and do not support child devices [11].

1.4 WirelessHART

WirelessHART is designed to be simple, self-organizing, self-healing, flexible, scalable, reliable, secure, and it supports the existing HART technology. WirelessHART is based on the IEEE 802.5.4 PHY layer, and it specifies a new MAC sublayer. The nodes in this standard are connected in a mesh topology, and they operate in the 2.4GHz band. [9].

WirelessHART devices use Time Division Multiple Access (TDMA) technology for communication. This enables WirelessHART to mitigate the number of the collided messages and minimize the nodes' power consumption [9].

1.4.1 Basic Features

WirelessHART uses both direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS) coexist with other systems in the 2.4 GHz band while mitigating interference. WirelessHART uses the 16 channels that are defined in the IEEE802.15.4 standard by hopping from one channel to another to reduce interference. WirelessHART also uses other mechanisms to reduce interference such as clear channel assessment (CCA), power control, and blacklisting. CCA is an optional feature in WirelessHART and can be performed before transmitting a message, whereas power control can change the transmit power level, and blacklisting disallows the use of certain channels [9][33].

Since WirelessHART aims to be simple, self-organizing, and self-healing, all WirelessHART nodes must have routing capabilities, and must be treated equally in terms of networking capabilities, installation, formation, and expansion [9].

WirelessHART offers two routing schemes that can be used in message delivery: graph and source routing. Graph routing uses predefined paths to route the message from the source node to the destination node. To achieve redundancy and reliability, graph routing has redundant paths between nodes. On the other hand, source routing uses ad-hoc created routes for the messages without providing any path diversity. Therefore, source routing can only be applied for network diagnostics, and cannot be applied for process related messages [9] [12].

1.4.2 Protocol Devices

The following are the key components of Wireless HART.

Gateway: connects the host network to the WirelessHART field devices.

Network Manager: an application that is responsible for managing and maintaining the mesh network.

Security Manager: an application that generates, stores, and manages join network, and session keys [13].

Repeater: responsible for routing WirelessHART messages. Its main use is to extend the range of a WirelessHART network. [14].

Adapter: a wireless device that is connected to the existed wired HART instrument to pass data to the WirelessHART hosts wirelessly. This device could be located anywhere [14].

Terminal: it is a portable device that can be used to diagnose, calibrate, and configure the WirelessHART field devices [14].

1.5 ISA.100

This technology is aimed at offering a reliable and secure wireless operation for noncritical monitoring, supervisory control, open loop control, closed loop control, and alerting applications, where delay in the range of 100ms is acceptable, with optional behavior for lower latency [15] [16].

1.5.1 Basic Features

The ISA100 supports both star and mesh topologies. The star topology supports I/O and portable devices, and the mesh topology supports mesh devices [16].

ISA100 adopts IEEE 802.5.4 PHY layer characteristics that use DSSS and O-QPSK modulation. The standard operates in the 2.4GHz band only, and benefits from the channels (11-25), whereas Channel 26 is marked as an optional channel because of some common regularity standard constraints. The maximum data rate is 250 Kbps [16].

The ISAI00 MAC layer supports TDMA, which allows a device to access the radio frequency medium without having to wait for other devices [16]. The standard mitigates interference by adopting channel hopping mechanism. This standard also uses adaptive channel hopping to determine the occupied channels and/or those with bad performance [17].

1.5.2 Protocol Devices

ISA.100 defines the following components:

Security Manager: an application that is responsible for security services

System Manager: an application that controls how the network devices are communicating.

Gateway: works as an interface between ISA100.11a field network and plant network.

Backbone router: a device that is capable of routing data to/from a backbone network.

Routers: a device that performs routing for field devices.

Field devices: the sensor nodes.

1.6 Research Objectives

The objectives of this Thesis are to:

- Deeply understand IEEE 802.15.4 standards (ZigBee, WirelessHART, and ISA100).
- Perform MAC layer performance evaluation for the three standards under different scenarios using NS2.
- Give recommendations for the suitability for each protocol.

CHAPTER 2

PROTOCOL LAYERS

In Chapter 1 we reviewed the WSN standards: ZigBee, WirelessHART, and ISA100. This chapter provides further insights into the structure and services provided by each layer of these standards. This chapter is divided into three main sections: ZigBee Protocol Layers [28], WirelessHART protocol Layers [29] [30], and ISA100 Protocol layers [29] [30]. Each section lists the components of each layer, and the features of each component.

2.1 ZigBee Protocol Layers

ZigBee protocol layers are shown in Figure 2.1. ZigBee only implements the layers that are mandatory for low-rate, low-power wireless networking. The First two layers, namely the PHY and MAC, are defined by the IEEE 802.15.4 standard. The Network (NWK) and the Application (APL) layers are defined by the ZigBee Alliance. ZigBee's protocol layers are built based on the international standards organization's (ISO) open system interconnect (OSI) basic reference model.

Each layer communicates with the adjacent layer by means of service access points (SAPs). A SAP is a conceptual location at which one protocol layer can request the services of another protocol layer. For instance, in Figure 2.1, the MAC layer data entity service access point (MLDE-SAP) is where the NWK layer requests any data services from the MAC layer.

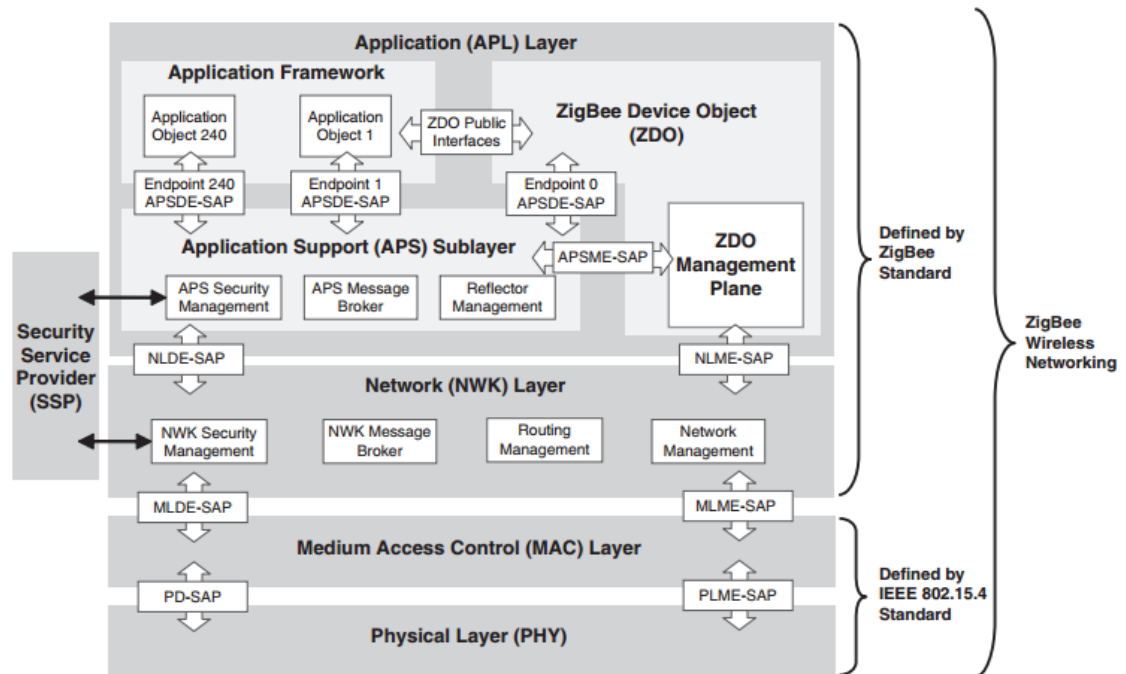


Figure 2-1 Protocol Layers of ZigBee [28]

2.1.1 The IEEE 802.15.4 PHY Specifications

The IEEE 802.15.4 PHY specifies the PHY layer's protocol functions and how it communicates with the MAC layer. Moreover, it defines the PHY hardware requirements, such as the minimum receiver sensitivity level, and the output transmission power of the radio chip.

2.1.1.1 Channel Assignments

The operation channels of the IEEE 802.15.4 standard are described in table 2.1. The table shows the channel pages and numbers, the operating frequency bands, and the type of modulation. The concept of channel page was added to the IEEE 802.15.4 standard in 2006. This implies that the first version of the protocol only supported the channel numbers from 0-26, and there was no support for multiple operating frequency bands.

Table 2-1 Channel Numbers

Channel page	Channel number	Operating frequency band	The modulation type
0	0	868 MHz band	BPSK
	1-10	915 MHz band	BPSK
	11-26	2.4 GHz band	O-QPSK
1	0	868 MHz band	ASK
	1-10	915 MHz band	ASK
	11-26	Reserved	
2	0	868 MHz band	O-QPSK
	1-10	915 MHz band	O-QPSK
	11-26	Reserved	

3-31	reserved	Reserved	
------	----------	----------	--

The Channel pages 3-31 are reserved for future usage. Whereas the channel pages 0-2 are currently used for the 2.4 GHz, 915/868 MHz bands.

The IEEE 802.15.4 2003 release is supported by channel page 0, and the 2006 release is supported by channel pages 2 and 3.

The center frequency for the 868 MHz band is 868.3 MHz; and for the frequency band 915MHz, the center frequency is written as

$$\text{Center Frequency (MHz)} = 906 + 2 * (\text{Channel Number} - 1).$$

The 2.4GHz band's center frequency is given by the following equation:

$$\text{Center Frequency (MHz)} = 2405 + 5 * (\text{Channel Number} - 11).$$

2.1.1.2 Energy Detection

Energy Detection (ED) is one of the methods used to sense the medium. ED detects whether the channel is busy or idle by sensing the energy levels without considering the type of the signal that is occupying the channel.

Before applying ED, the device must change its state to the receiving mode, ED is performed by averaging the signal energy of the desired channel over 8 symbol periods.

The receiver detects signal energy above its minimum sensitivity level, but it only gives an indication that the channel is used when the energy level of the selected channel is 10 dB above the receiver sensitivity level.

2.1.1.3 Carrier Sense

Carrier Sense (CS) is another way to detect the channel. CS differs from ED in that it considers the type of signal that is occupying the channel. If the signal is compliant with the type of signals used by the device itself, the CS indicates that the channel is in use and unavailable for transmission. However, if the signal type is not compliant with the ones used by the device, the CS will indicate that the channel is idle, and the device can use the channel for transmission regardless of the signal's energy level.

2.1.1.4 Link Quality Indicator

The link quality indicator (LQI) measures the quality of the received packets, the received signal strength (RSS), and the signal to noise ratio (SNR). The SNR is used as an indication of the signal quality. LQI may use RSS or SNR as a measurement tool for the quality of the received packets. The SNR is the ratio of the received signal power to the white noise power in the medium, which means that the higher the SNR the better the signal quality.

LQI measurements are passed to the MAC and NWK layers. The NWK layer uses LQI as one of the selection criteria for packet routing, the path that has the highest overall LQI is

selected to route the packets. In addition of the LQI, There are other factors that can affect the path selection, such as routing energy efficiency.

2.1.1.5 Clear Channel Assessment

Clear channel assessment (CCA) is the first step in the carrier sense multiple access with collision avoidance (CSMA/CA) mechanism. The MAC layer orders the PHY layer to perform CCA to know whether the channel is busy or idle. CCA uses the results of ED, CS, or both to tell the MAC layer that the requested channel is used or not.

CCA has three operating modes, and the PHY layer must be able to run any one of these modes:

- Mode 1: uses the ED, and the channel is considered busy if the energy level of the channel is above some ED threshold.
- Mode 2: uses CS, and the channel is considered busy if the sensed signal type is compliant with the PHY layer of the device itself.
- Mode 3: a logical combination of Mode 1 and 2, and the channel is busy when:
 - The energy level is above the threshold and a compliant carrier is sensed.
 - The energy level is above the threshold or a compliant carrier is sensed.

2.1.1.6 The PHY Layer Constants and Attributes

The PHY layer has only two constant values, shown in table 2.2. The constant `aMaxPHYPacketSize` is the maximum value of the PHY layer's service data unit (PSDU), and the `aTurnaroundTime` constant, is the time needed for the receiver to switch from the transmission mode to the reception mode, and vice versa.

Table 2-2 PHY Constants

Constant	Description	Value
<code>aMaxPHYPacketSize</code>	The maximum allowed PSDU size (in octets)	127
<code>aTurnaroundTime</code>	The maximum allowed RX-to-TX or TX-to-RX turnaround time (in symbol periods)	12

The constant value cannot be changed during operation, whereas the value of the attribute can be changed during operation. The PHY layer's PAN information base (PHY-PIB) contains the PHY attributes. Table 2.3 summarizes PHY-PIB. The attributes marked with (^) are read-only, which means that PHY layer can only change the attribute value. On the other hand, the attributes marked with (*) have specific bits that are read only, and the bits that are unmarked as read only can be read and modified by the upper layers.

Table 2-3 PHY-PIB attributes

Attribute	Description
<code>phyCurrentChannel</code>	The frequency channel of operation

phyChannelsSupported^	The array of the available and unavailable channels
phyTransmitPower*	The transmitter output power in dBm
phyCCAMode	The CCA mode of operation (1–3)
phyCurrentPage	The current PHY layer's channel page
phyMaxFrameDuration^	The maximum number of symbols in a frame (55, 212, 266, 1064)
phySHRDuration^	The duration of the synchronization header (SHR) (3, 7, 10, 40)
phySymbolsPerOctet^	The number of symbols per octet for the current PHY (0.4, 1.6, 2, 8)

2.1.1.7 PHY Services

The PHY layer has two types of services, namely, the PHY data services and management services. The PHY data services are accessed through PHY data SAP (PD-SAP), and the PHY management services are accessed through the PHY layer's management entity (PLME) SAP. Figure 2-2 shows the PHY and MAC layers' interfacing. The MAC layer's management entity (MLME) contains the MAC PAN information base (MAC-PIB), whereas the PLME contains PHY-PIB.

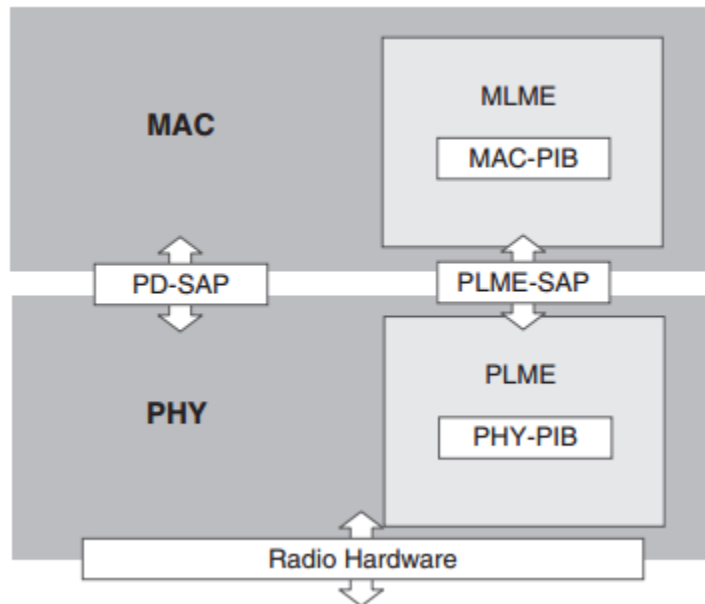


Figure 2-2 PHY and MAC Layers of the IEEE 802.15.4 standard [28]

2.1.1.7.1 PHY Data Service

The MAC layer generates the MAC protocol data unit (MPDU) whenever it needs to transmit data. The PHY layer receives the MPDU, and informs the MAC layer that the data is ready for transmission whenever the data reaches the radio transceiver. The PHY layer also notifies the MAC whether the transmission is successful or not. In the receiving mode, the PHY provides the MAC with the MPDU and LQI information.

Figure 2-3 shows the data transmission steps from one device to another. The data to be transmitted may come from the APL or the other layers.

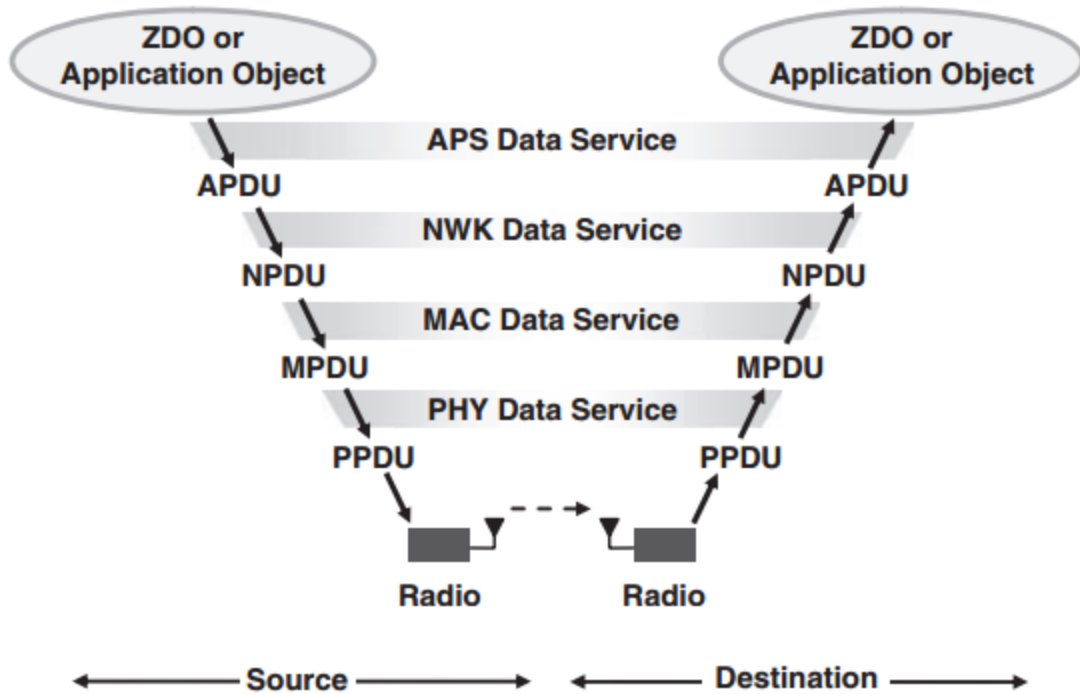


Figure 2-3 Two Devices Data delivery procedure [28]

2.1.1.7.2 PHY Management Service

The PHY management services are exchanged between the PHY and MAC layers by using PLME-SAP. The management services provided are: Clear channel assessment (CCA), setting the value of a PHY-PIB attribute, energy detection (ED), obtaining information from the PHY-PIB, and enabling and disabling the radio transceiver.

2.1.1.8 The Service Primitives

The service primitives are the services the layer provides to the next higher layer. Figure 2-4 shows the concept of the service primitives. The service primitives are described in the following formats:

<The primitive>.request

<The primitive>.confirm

<The primitive>.response

<The primitive>.indication

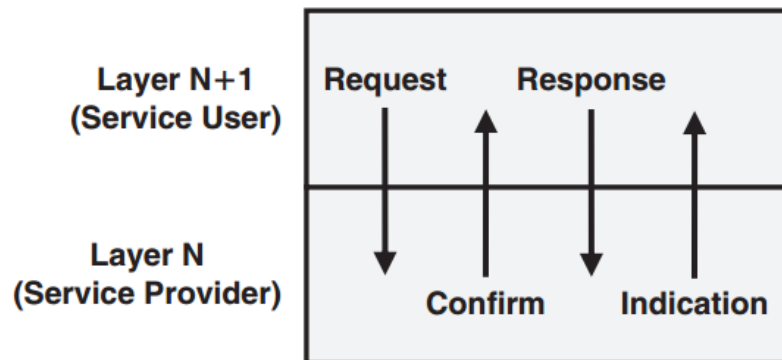


Figure 2-4 the principle of work of the Service Primitive [28]

2.1.1.9 PHY Packet Format

The PHY protocol data unit (PPDU) consists of the PHY payload, the PHY header (PHR), and the Synchronization header (SHR). Figure 2-5 shows the PPDU format.

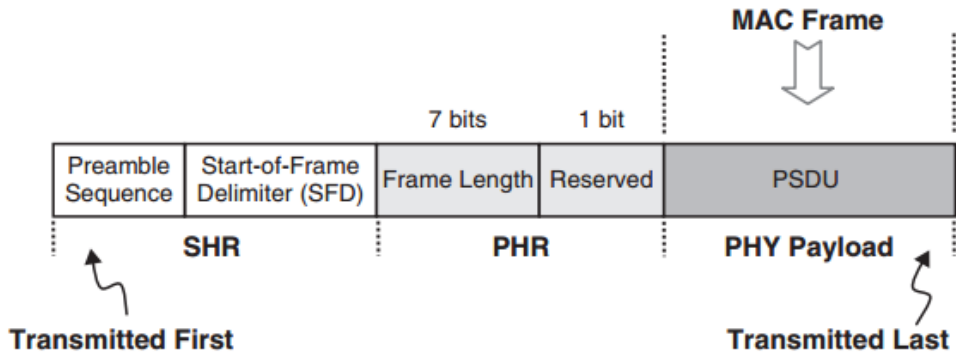


Figure 2-5 PHY Layer Protocol Data Unit Format [28]

The PHY payload contains data from the upper layers, PHR contains information about the frame length, and SHR is required to synchronize the bit stream.

SHR consists of two components, namely, the preamble sequence and start of the frame delimiter (SFD). The preamble field contains the synchronization information, and SFD indicates the end of the SHR and the beginning of the PHR.

Table 2-4 shows the preamble field lengths and durations for different modulation schemes and different channel bands.

Table 2-5 and Table 2-6 show the SFD field format and field length, respectively.

Table 2-4 the lengths and the Durations of the Preamble Field

PHY Option	Length		Duration (μ s)
868 MHz BPSK	4 octets	32 symbol	1600
915 MHz BPSK	4 octets	32 symbol	800
868 MHz ASK	5 octets	2 symbol	160
915 MHz ASK	3.75 octets	6 symbol	120
868 MHz O-QPSK	4 octets	8 symbol	320
915 MHz O-QPSK	4 octets	8 symbol	128
2.4 GHz O-QPSK	4 octets	8 symbol	128

Table 2-5 the Field Format of SFD

Bits	0	1	2	3	4	5	6	7
Values	1	1	1	0	0	1	0	1

Table 2-6 SFD Field Lengths

PHY Option	Length	
868 MHz BPSK	1 octets	8 symbol
915 MHz BPSK	1 octets	8 symbol
868 MHz ASK	2.5 octets	1 symbol
915 MHz ASK	0.625 octets	1 symbol
868 MHz O-QPSK	1 octets	2 symbol
915 MHz O-QPSK	1 octets	2 symbol
2.4 GHz O-QPSK	1 octets	2 symbol

The frame length field contains information about the length of the PHY layer payload (PSDU). The length of the PSDU varies from 0 to 127 octets. Table 2-7 shows the values of the frame length and their meanings.

Table 2-7 Frame Length Values

Frame Length Values	PHY Payload
0 to 4	Reserved

5	Acknowledgment MPDU
6 to 8	Reserved
9 to <i>aMaxPHYPacketSize</i>	Any other MPDU

2.1.2 IEEE 802.15.4 MAC Layer

The MAC layer is the second layer of the IEEE 802.15.4 standard. IEEE 802.15.4 defined the PHY and the MAC layers only, and did not specify the features of the NWK layer. The MAC layer is not defined for a specific technology; therefore, each technology standard specified the required MAC features that must be available to build up the protocol stack.

Figure 2-6 shows the MAC sublayer reference model. The MAC layer has MAC layer management entity (MLME) that communicates with the NWK layer's management entity (NLME) by calling the MLME service access point (MLME-SAP).

The MAC layer has a database of attributes and constants referred to as MAC PAN information base (MAC-PIB). The constants start with (a) prefix, and the attributes start with (MAC) prefix.

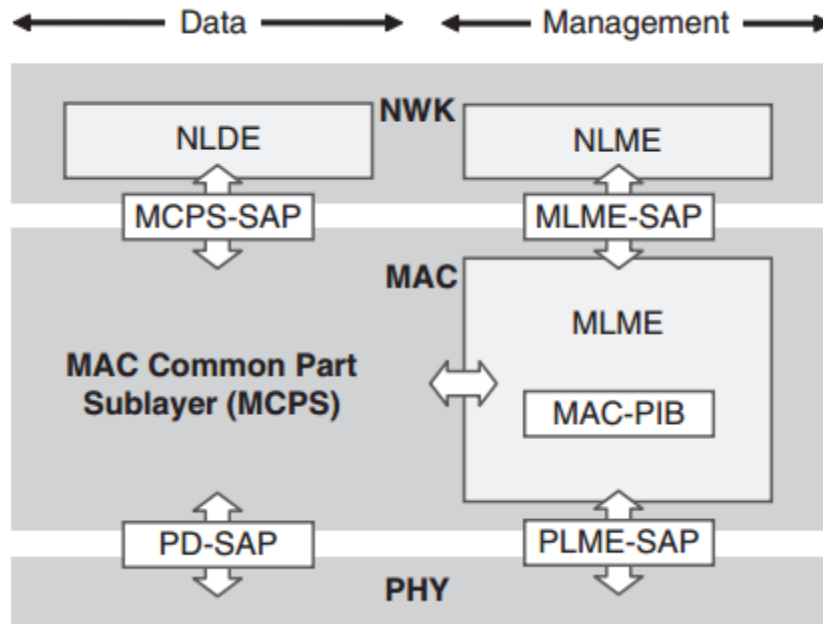


Figure 2-6 The Model of the MAC sublayer [28]

2.1.2.1 Superframe Structure and Beacon-Enabled Operations

The Superframe consists of three parts, namely, the contention access period (CAP), the contention free period (CFP), and the inactive period. Figure 2-7 shows the structure of the superframe.

The Superframe is an optional feature in 802.14.5 standard, and it can be activated by using the beacon mode. The beacon frames are MAC frames that contain information about the time interval between the beacons and the guaranteed time slots (GTS). The contention access period is shared among the nodes, any node can compete for having access to the medium by using the CSMA/CA mechanism.

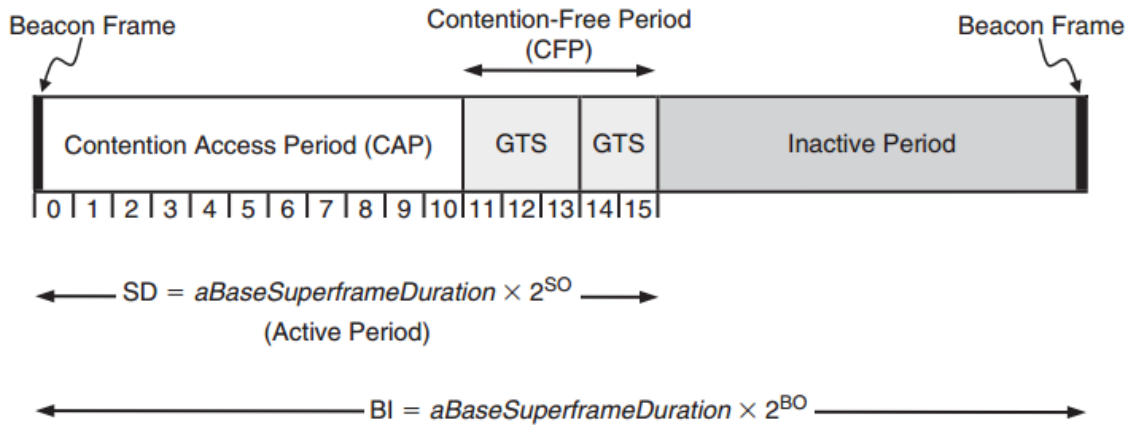


Figure 2-7 The Structure of the SuperFrame [28]

The CFP is the solution for nodes with critical data that needs to be transmitted instantly. CFP offers guaranteed time slots, which is a big advantage of the beacon-enabled operation mode.

The CAP and CFP periods are called the active periods, and the inactive periods allow the coordinator or the PAN to turn off its transceiver to save power during sleep mode. The Superframe has 16 active time slots in total. Five to seven of these time slots are GTSS.

The beacon interval (BI), defined as the time value between two consecutive beacon frames, is calculated as follows:

$$BI = aBaseSuperframeDuration * 2^{BO} \text{ (Symbols).}$$

The BI is determined by the value of *aBaseSuperframeDuration* and the *macBeaconOrder* (BO). The BO can be any value from 0 to 14. To disable the beacon mode, the BO is set to 15.

The superframe duration (SD), also called the active period length, is written as:

$$SD = aBaseSuperframeDuration * 2^{SO}(\text{Symbols})$$

Where SO is the Superframe duration of the MAC. The value of the SO is always less than or equal to the value of the BO.

In the beacon-enabled mode, the PAN and any other coordinator can transmit the beacons and generate a superframe. The beacons transmitted by the PAN are called received beacons, and the beacons transmitted by any other coordinator are called transmitted beacons. The superframe duration for both the PAN and the other coordinators are the same.

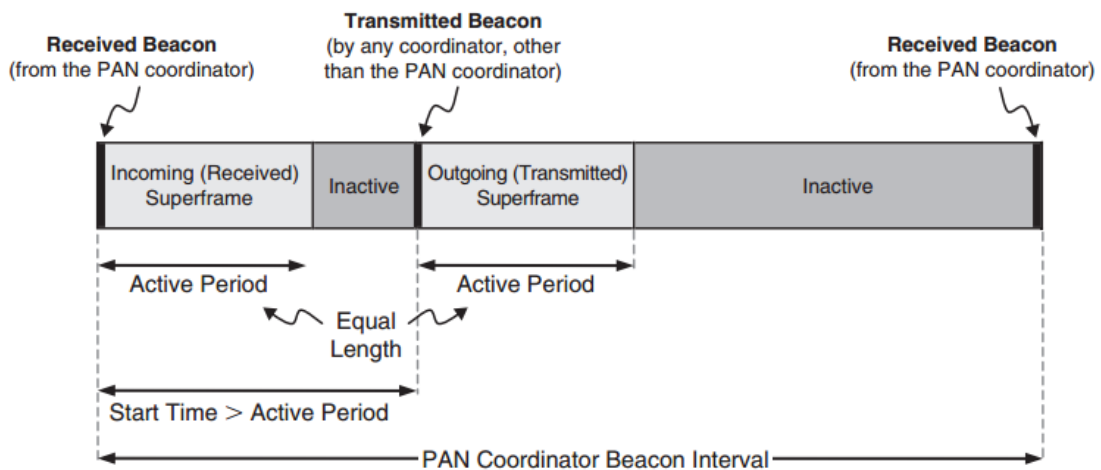


Figure 2-8 The Timing of the Received and the Transmitted Superframes [28]

2.1.2.2 The Interframe Spacing

The inter-frame spacing (IFS) is the time between two successive frames. This time space allows the receiving node or device to process the received frame before a new frame

arrives. There are two types of IFS depending on the frame size, namely, long IFS (LIFS) and short IFS (SIFS).

Figure 2-9 shows the format of the IFS for acknowledged and unacknowledged communications. For acknowledged communication, the long/short IFS's spacing starts after receiving an acknowledgment from the transmitter. In the figure, t_{ACK} is the acknowledgment time.

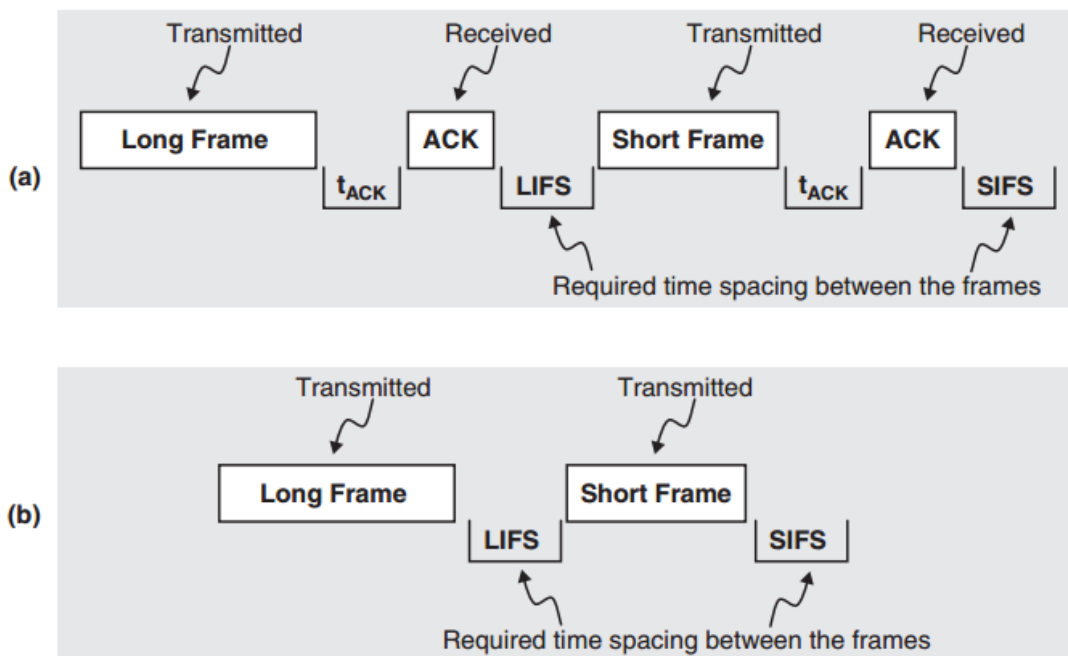


Figure 2-9 The Interframe Spacing in (a) Acknowledged and (b) Unacknowledged Transmission [28]

2.1.2.3 Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA)

CSMA is the channel access mechanism in the IEEE 802.15.4 standard. The first step of the CSMA/CA is the CCA, which helps the device to know whether the channel is busy or not. If it is busy the device backs off for a random time interval.

There are two types of CSMA, namely, slotted and unslotted CSMA. Slotted CSMA is used in beacon-enabled mode and requires back-off slot alignment, and unslotted CSMA is used in nonbeacon-enabled mode and does not require back-off slot alignment.

Figure 2-10 shows the state flow diagram of CSMA-CA. First, a decision is made whether to use slotted or unslotted CSMA-CA. The variables NB, CW, and BE are referred to as the number of backoffs, the contention window length, and the back-off exponent, respectively.

Whenever the channel is busy, the device waits for a back off period determined by the following equation:

$$\text{Back-off} = (\text{A random integer number between } 0 \text{ to } 2^{\text{BE}} - 1) * \text{aUnitBackoffPeriod}$$

In slotted mode, the battery life extension (BLE) affects the BE value. If the BLE is active then the BE is the minimum of two or the macMinBE, and otherwise, BE=macMinBE. The value of the BE is incremented every time the CCA indicates the channel to be busy, but the BE cannot exceed the value of macMaxBE.

The NB counts the number of retries of accessing the channel. If the NB reaches macMaxCSMABackoffs, the CSMA-CA algorithm quits.

The CW is used in slotted CSMA-CA, and it determines the number of backoffs before transmitting the data.

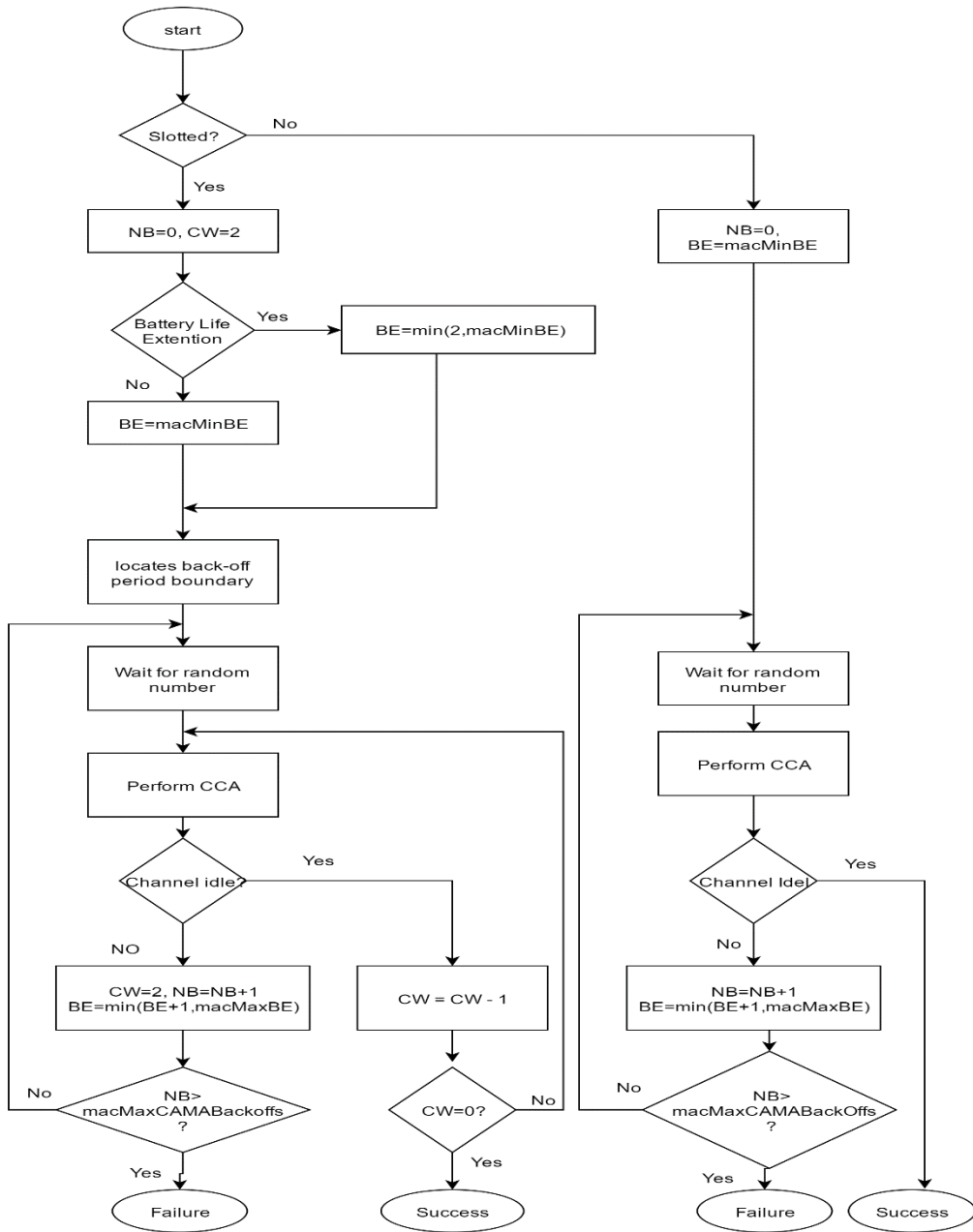


Figure 2-10 The State Flow Diagram of the CSMA-CA

The CSMA-CA mechanism can avoid collision in ZigBee networks, but it has two weaknesses. The First weakness is the hidden node problem, and the second weakness is the exposed node problem.

The hidden node problem happens when two nodes out of the range of each other transmit data at the same time to the same node. As a result, a collision will occur at the receiving node. The exposed node problem occurs when two nodes in the range of each other want to transmit data to two different nodes. The two receiving nodes are out of the range of each other; however, since the two sending nodes are in the range of each other, CSMA-CA will prevent them to transmit at the same time. Figure 2-11 shows the hidden and exposed node problems.

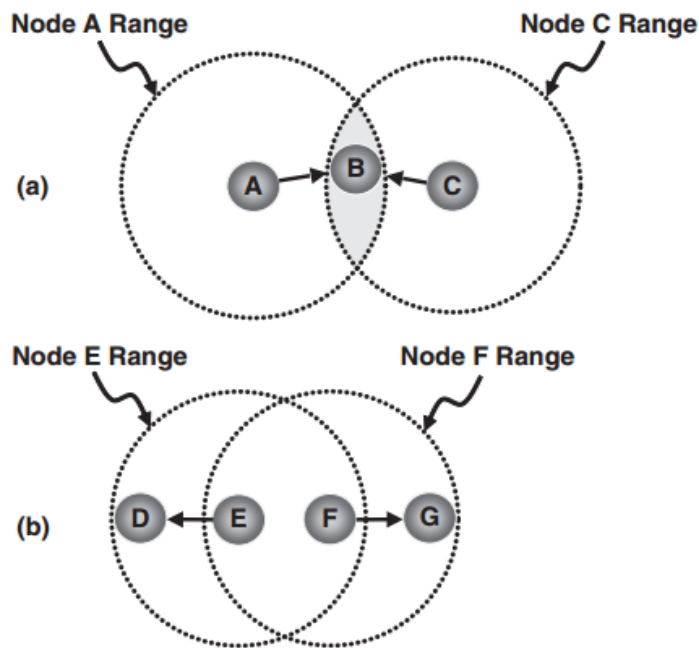


Figure 2-11(a) The Hidden and (b) the Exposed Node Problems

2.1.2.4 MAC Services

The MAC services are divided into two types, namely, management services, and data services. The MAC data services contain the data requested to be sent by the NWK layer. These data are forwarded to the MAC layer from the NWK layer as a network protocol data unit (NPDU). The MAC generates its payload, called the MAC service data unit (MSDU), which contains the NPDU. During the receiving mode, the MAC layer delivers the data to the NWK layer. In addition to the data, the MAC layer provides the NWK layer with the LQI, and the data reception time.

The MAC management services are controlled by the MAC layer management entity (MLME). The MAC management services include the following:

- Managing MAC PIB
- Communication Status
- MAC Reset
- Requesting Data from a Coordinator
- Device Association and Disassociation
- GTS Management
- Orphan Notification
- Channel Scanning
- Enabling and Disabling the Receiver

- Beacon Notification
- Updating Superframe Configuration
- Synchronizing with a Coordinator

2.1.2.5 MAC Frame Format

The general frame of the MAC layer consists of three parts: the MAC header (MHR), the MAC payload, and the MAC footer (MFR). Figure 2-12 shows the general frame format.

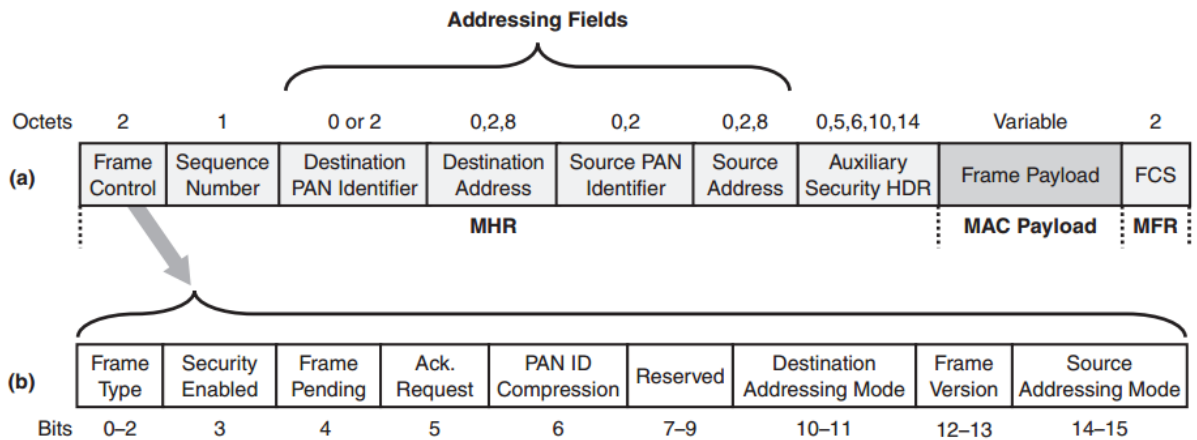


Figure 2-12 (a) The General frame format of the MAC layer and (b) the Frame Control Field [28]

The first section of the MHR is the frame control field. The frame control field includes:

- The frame type: determines the type of the frame, beacon frame, data frame, acknowledgment frame, and MAC command frame.

- The security-enabled: determines whether the frame has security protection or not. The auxiliary header will be part of the MAC frame if the security-enabled subfield is set to one. Otherwise, the size of the auxiliary header is zero.
- The frame pending: if this field is set to one, it means there still some data pending at the transmitter that need to be sent to the receiver.
- The acknowledgment request: the recipient device must send an acknowledgment frame to the sender if this field is set to one.
- The PAN ID compression: if this field sets to one, this means that the source PAN and the destination PAN addresses are the same, and only the destination PAN address is included in the frame.
- The destination and source addressing mode: determine the addressing mode (either 16-bit or 64-bit). The length of the destination and source address fields depends on the addressing mode.
- The frame version: determines what version of the IEEE 802.15.4 is used to build the frame.

The next field of the MHR is the sequence number, which determines the data sequence number (DSN) and the beacon sequence number (BSN). The BSN is used in beacon frames, and DSN is used in any other frames.

The MFR contains the frequency check sequence (FCS). The FCS helps in error detection in the data (i.e., if there is an error the data, and the data need to be transmitted again).

There are four types of MAC frames: beacon, data, acknowledgment, and command frames. The MAC beacon frame format is shown in figure 2-13.

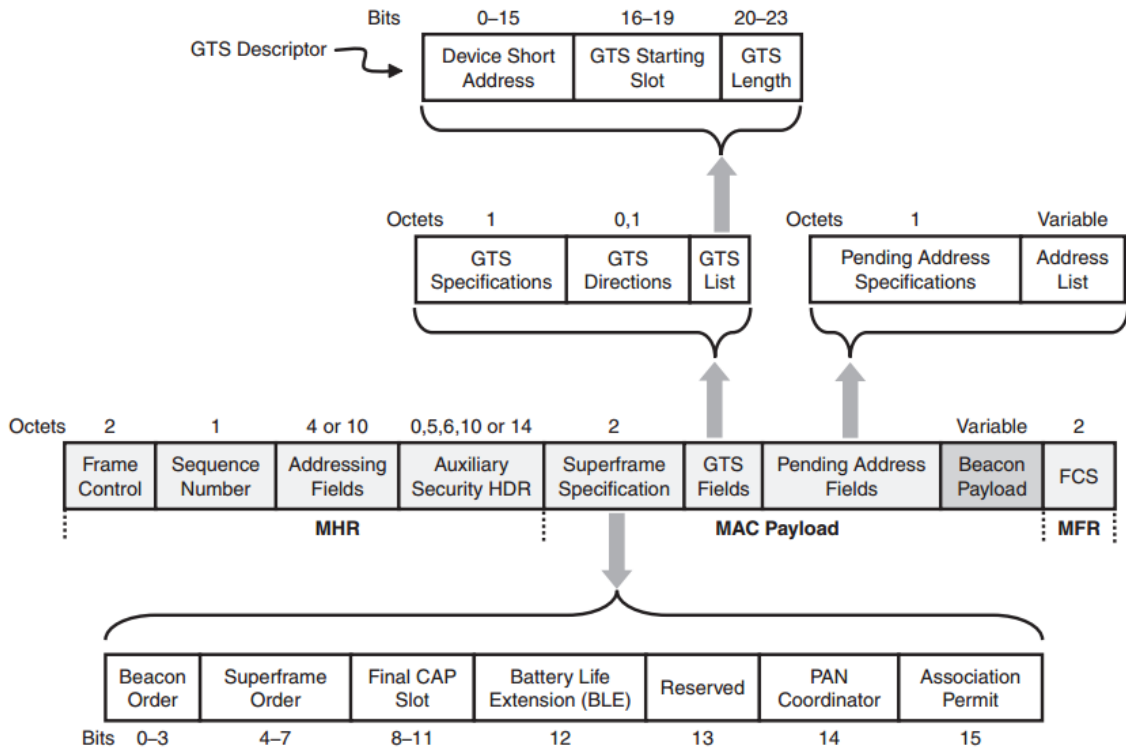


Figure 2-13 MAC Beacon Frame [28]

The superframe specification field consists of the following parts: Beacon order, superframe order, final CAP (which determines the last time slot of the CAP period), battery life extension (BLE), which indicates that the device will turn off its receiver to save energy, PAN coordinator, which indicates that the received frames from the PAN or any other coordinator. The final part is the association permit, which indicates whether the PAN received an association request or not at this time.

The next MAC frame format is the data MAC frame format. Figure 2-14 (a) shows the sections of the MAC data frame format. The MAC data frame payload is provided by the NWK layer.

The MAC acknowledgment frame is sent by the recipient device to the sender device to insure the data reception. Figure 2-14 (b) shows the MAC acknowledgment frame format.

The last MAC frame type is the MAC command frame. Figure 2-14 (c) shows the MAC command frame format. This frame is used to transfer the MAC layer commands to the recipient device.

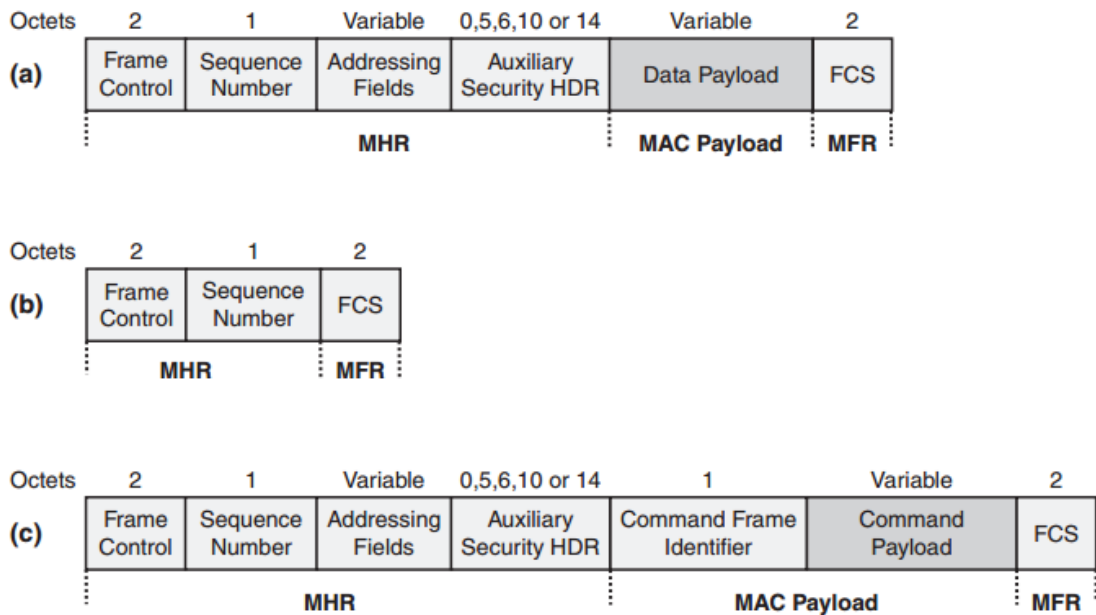


Figure 2-14 (a) The MAC Data Frame, (b) The MAC Acknowledgment Frame, and (c) The MAC Command Frame Formats [28]

2.1.3 The ZigBee NWK Layer

ZigBee NWK layer has two type of services: NWK data services and NWK management services. The NWK layer data entity (NLDE) controls the NWK data services, and the NLDE-SAP is used for data transfer between NWK and APL layers. The NWK layer management entity (NLME) controls the management services, and contains the network information base (NIB) which contains the information of the network layer attributes and constants. The NLME-SAP is a conceptual interface between NWK and APL layers, and is used for exchanging management services between the two layers.

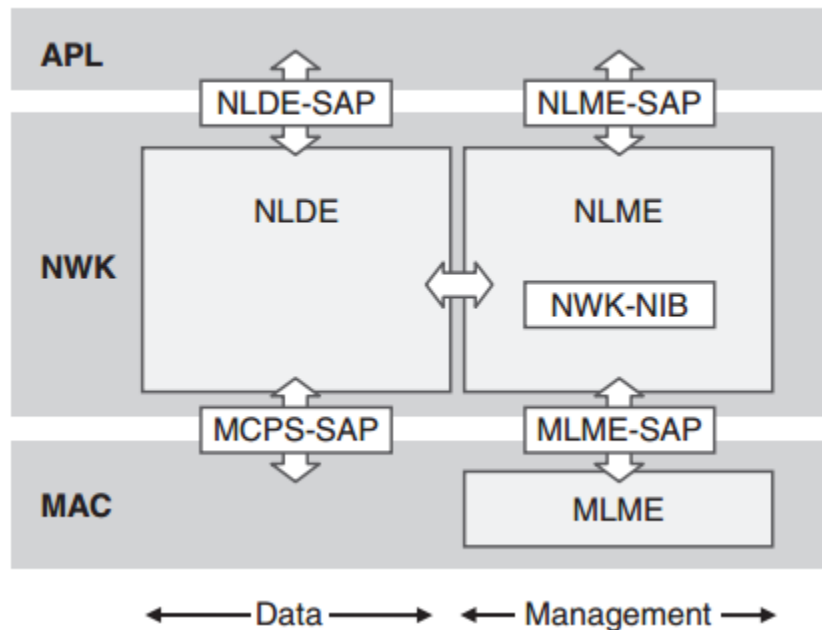


Figure 2-15 ZigBee network layer [28]

The NWK layer management services include route discovery, network formation, establishing the device as a router, joining and leaving the network, resetting the NWK layer, and nodes synchronization.

The ZigBee coordinator assigns the MAC address for each new device joining the network, and the NWK layer of the coordinator device assigns the network address for the new devices. The NWK and the MAC addresses must be the same.

The NWK layer limits the frame time by assigning a constant value called radius-the maximum number of hops the frame can travel. The value of the radius decreases each time the frame crosses a new hop, and the frame is dropped if the radius value reaches zero.

There are three types of communication between nodes in ZigBee networks, namely, broadcast, multicast, and unicast. In broadcast, the message is forwarded to all nodes in the network. In multicast, the message is forwarded to a group of nodes in the network. In unicast, the message is forwarded to specific node in the network. Figure 2-16 shows the different communication types.

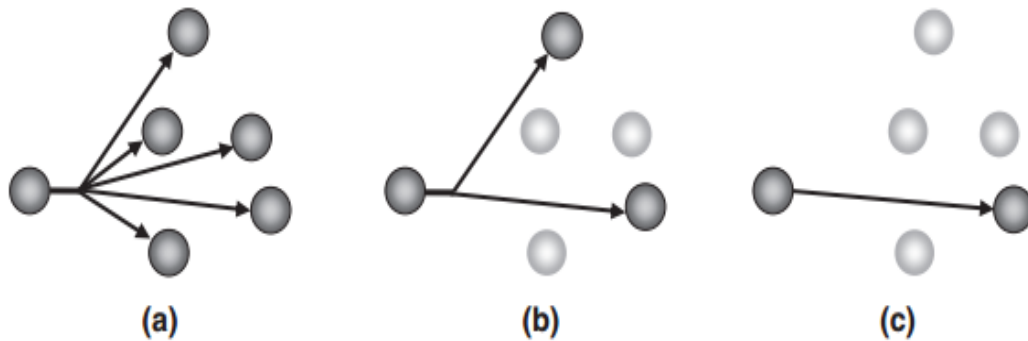


Figure 2-16 (a) Broadcast, (b) Multicast, and (c) Unicast Communications

2.1.3.1 ZigBee Topologies

ZigBee Network can form three different topologies: hierarchical (tree), mesh, and star.

The hierarchical (tree) network, shown in figure 2-17, starts from the ZigBee coordinator as root. The root establishes the network. A node that is directly connected to a ZigBee coordinator or router is called child, and the coordinator or the router is called parent. The ZigBee end device can only act as child. The network depth is the required number of hops to deliver the frame to the root. The ZigBee coordinator's children have a depth of one, because they can deliver the frame to the root by one hop.

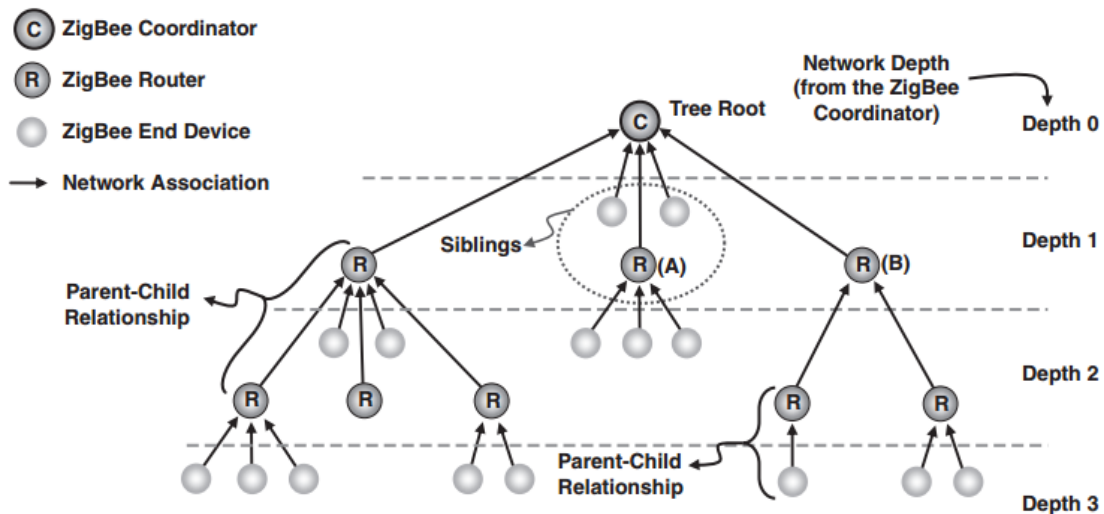


Figure 2-17 The hierarchical (Tree) topology [28]

The star topology is a special case of the hierarchical topology. In star topology, all nodes are connected to the ZigBee coordinator directly with depth of one, and the ZigBee coordinator is considered as the only parent for the network.

The mesh topology, there is no parent-child relationship; the neighboring nodes can communicate directly without a coordinator or a router. The mesh network routing paths

are reliable and multiple, the frame can follow any available path from the source to the destination, and if the previously selected path is down, the routing nodes can find a new path.

2.1.3.2 The NWK Layer Frame Format

The general NWK layer's frame format is shown in Figure 2-18. The NWK layer's frame consists of two main sections, namely, NWK header (NHR), and NWK payload.

The first field of the network frame is the frame control. The frame control field determines the following:

- The frame Type: determines whether the frame is data or command frame.
- Protocol version: determines the ZigBee protocol version
- Discover route: determines the routing option (suppress, enable, or force route discovery).
- Multicast flag: multicast routing is used if the flag is set to one.
- The security: enable or disable the security.
- The source route: this field is set to one if the source route's subframe field is included in the frame.
- Destination IEEE address and Source IEEE address fields: determines the address field length (16-bits or 64-bits).

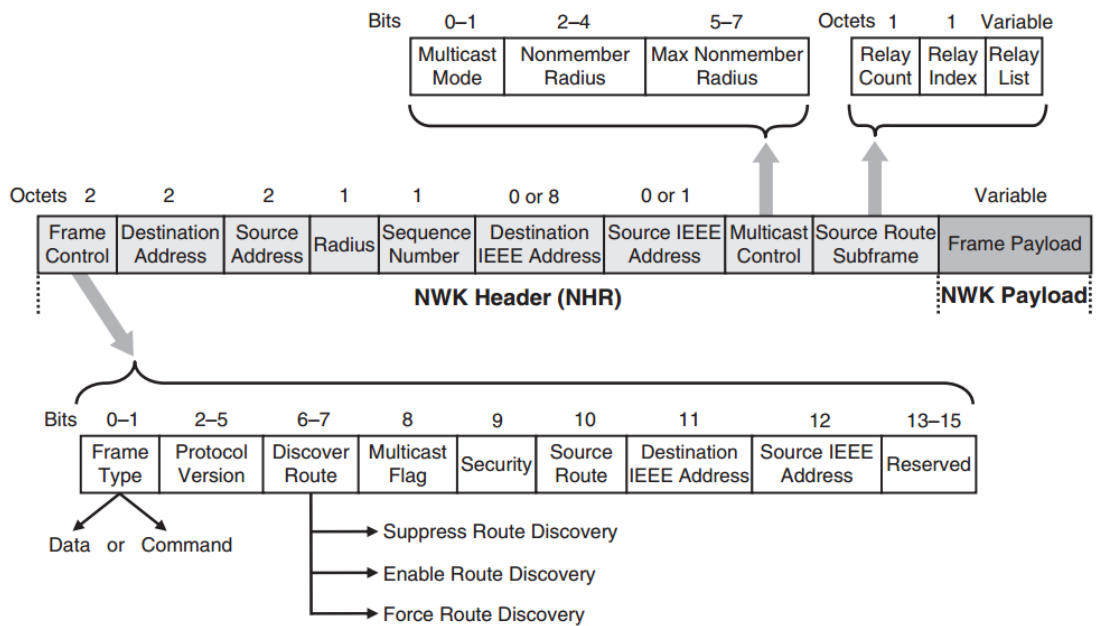


Figure 2-18 General Network Frame Format [28]

The radius field determines the hop count, and the multicast field is added to the frame if the multicast mechanism is used.

The data and command frame formats are shown in Figure 2.19. The routing field is an abstract of the group of fields between the control and the payload fields in figure 2-18. The NWK layer commands are listed in Table 2-8. An 8-bit number called the NWK layer's command identifier identifies each command.

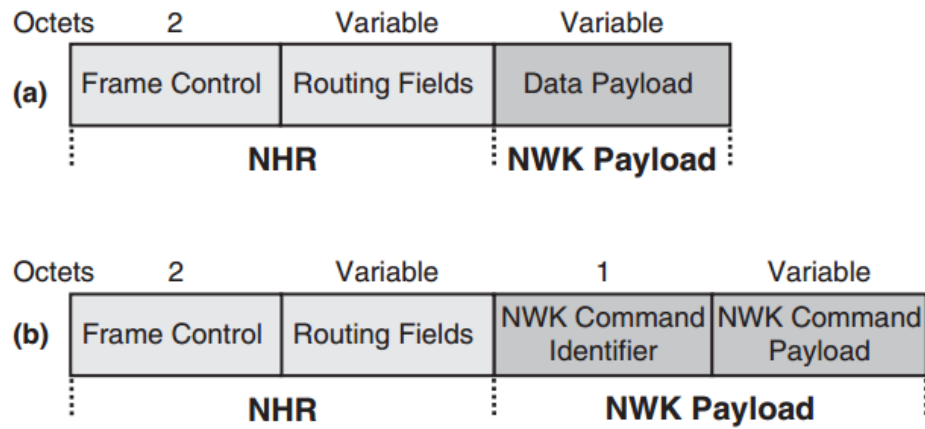


Figure 2-19 The Network Layer (a) data and (b) command frame formats [28]

Table 2-8 Network Commands

Command Frame Identifier	Command
00000001	Route request
00000002	Route reply
00000003	Route error (network status)
00000004	Leave
00000005	Route record
00000006	Rejoin request
00000007	Rejoin response

2.1.4 The APL Layer

The APL layer, shown in Figure 2-20, consists of three main parts: application framework, ZigBee device object (ZDO), and application support sublayer (ABS).

The ABS works as an interface between the APL layer and the NWK layer. The ABS performs management and data services. It contains the APS data entity (APSDE), the APS management entity (APSME), and the APS information base (APS-IB), which includes the information about the attribute values. The APS serves both the ZDO and the application framework in data delivery through APSDE-SAP. The APSDE-SAP is a conceptual interface through which the data services are delivered.

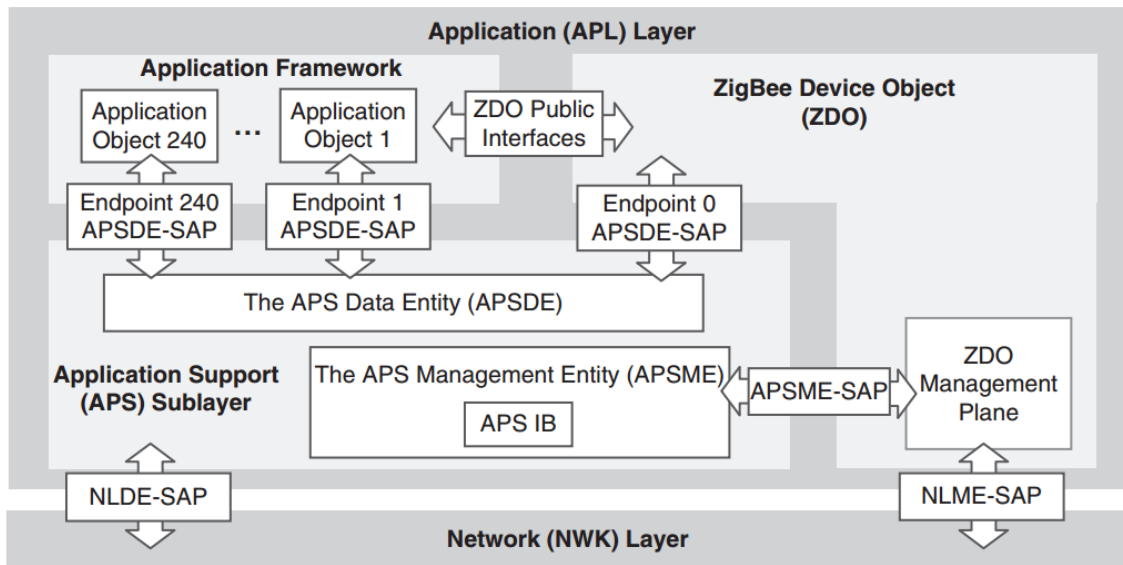


Figure 2-20 The Application Layer [28]

The application framework consists of application objects numbered from 1 to 240. Each application object corresponds to specific endpoint APSDE-SAP. For instance, endpoint zero corresponds to the ZDO.

The ZDOs act as an interface between the APS sublayer and the application framework. Moreover, the ZDOs control the management services of the APL layer, such as defining the node in one of the three types: ZigBee coordinator, router, or end device. The ZDO performs the management services by interacting with APSME by means of APSME-SAP.

2.2 WirelessHART Protocol Layers

WirelessHART defined five layers: PHY layer, data link layer, NWK layer, transport layer, and APL layer. Figure 2-21 shows the protocol layers in WirelessHART.

2.2.1 WirelessHART PHY layer

The WirelessHART's PHY layer is typically the same as the PHY layer in IEEE 802.15.4, and the only difference is that WirelessHART hops over 16 frequency channels. WirelessHART works in the 2.4GHz band with a data rate of 250 Kbps, and a channel's gap of 5 MHz. The nominal transmission power is 10dBm, which is 10 times higher than that of ZigBee.

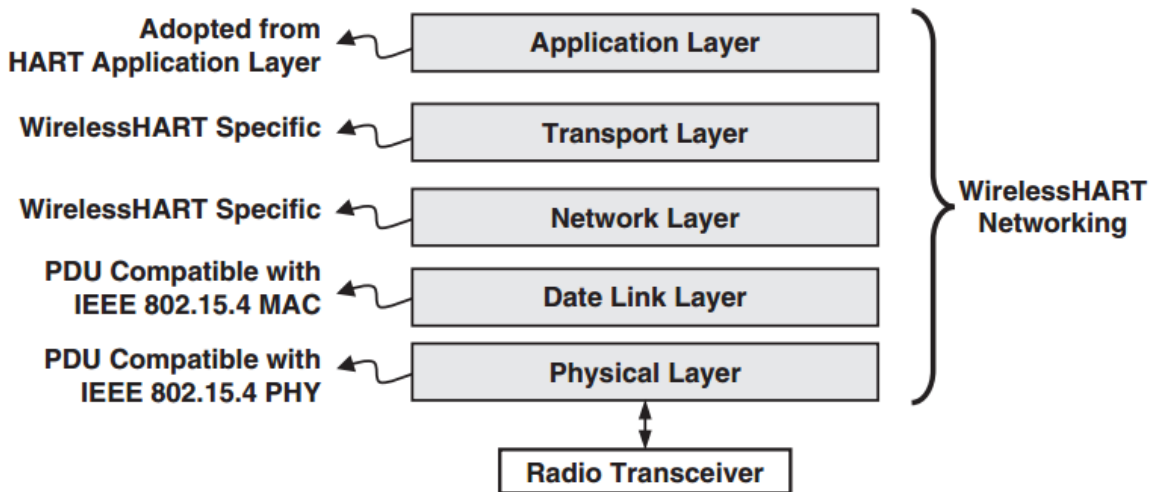


Figure 2-21 WirelessHART Protocol Layers [28]

2.2.2 WirelessHART Data Link Layer

The data link layer is based upon the MAC layer in IEEE 802.15.4 standard with some modifications. The WirelessHART requirement is a reliable error-free communication protocol. To achieve this requirement, WirelessHART adopts the use of channel hopping, together with channel blacklisting and time division multiple access (TDMA) for reliable communication.

Channel hopping uses 16 channels in the 2.4GHz band to overcome the interference issue. WirelessHART blacklists channels that have high interference value, and the channel hopping mechanism avoids using these blacklisted channels. TDMA technology guarantees a reliable communication through assigning timeslots for the nodes. The time slot size is fixed at 10ms.

The data link layer protocol data unit (DLPDU), shown in Figure 2-22, consists of the following fields:

- The address specifier: 1-byte size
- The Sequence number: 1-byte size
- The network ID: 2-byte size
- The destination and source address: 2- or 8-byte size
- The DLPDU: 1-byte size
- The message integrity code (MIC): 1-byte size

- The cyclic redundancy check (CRC): 2-byte size
- The DL payload: variable-length

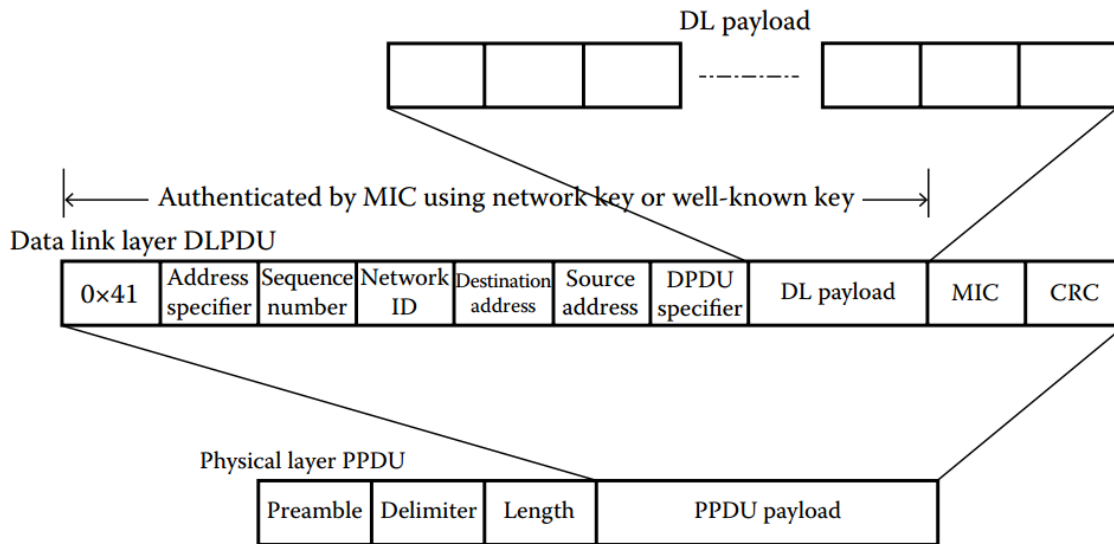


Figure 2-22 Data Link Layer Protocol Data Unit [29]

The superframe, shown in figure 2-23, consists of a group of time slots. Every 100 time slots form one superframe. The WirelessHART network has more than one superframe, but only one superframe is enabled at a time. WirelessHART is a contention-free access network and to ensure that, the time slot is assigned to two nodes, one as a source and the other as a destination.

In the ACK based communication, the transmitter expects to receive an ACK from the receiver after sending the DLPDU. If the transmitter does not receive the ACK from the receiver, the transmitter will retransmit the same DLPDU again. If the routing link fails to deliver the DLPDU to the receiver repetitively, the link will be discarded and an alternate route will be selected.

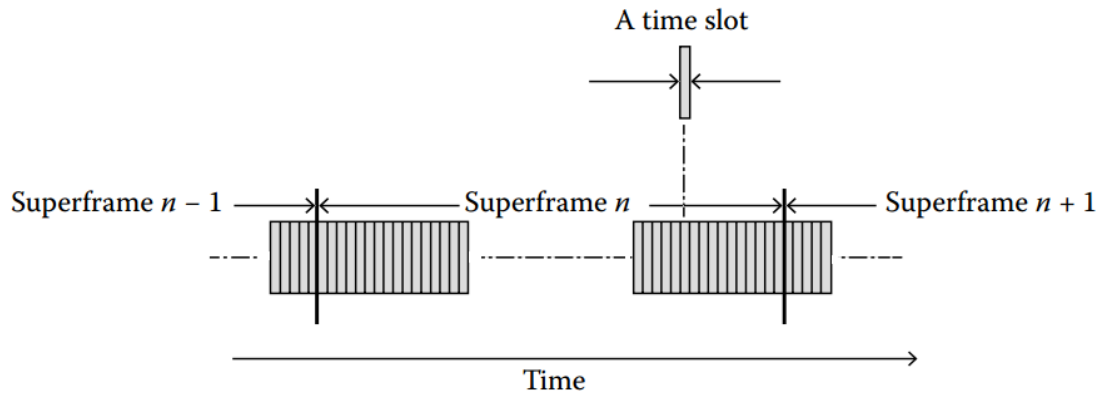


Figure 2-23 WirelessHART SuperFrame [29]

WirelessHART defines five frame types: acknowledgment frame, advertise frame, keep-alive frame, disconnect frame, and data frame. Data frame contains information from the upper layers, and the other four frames are used for data link information only.

2.2.3 WirelessHART NWK layer

The WirelessHART NWK layer frame is shown figure 2-24. The frame consists of the following fields: (1) The control field: determines the addressing mode. (2) The time to live (TTL) field: determines the frame time in by counting the number of hops the frame has crossed. (3) The ASN snippet: gives information about network quality. (4) The Graph ID: stores information about the routing path. (6) The source and destination fields. (7) The expanded routing information: determines whether an extra routing information is needed or not. (8) The security sublayer.

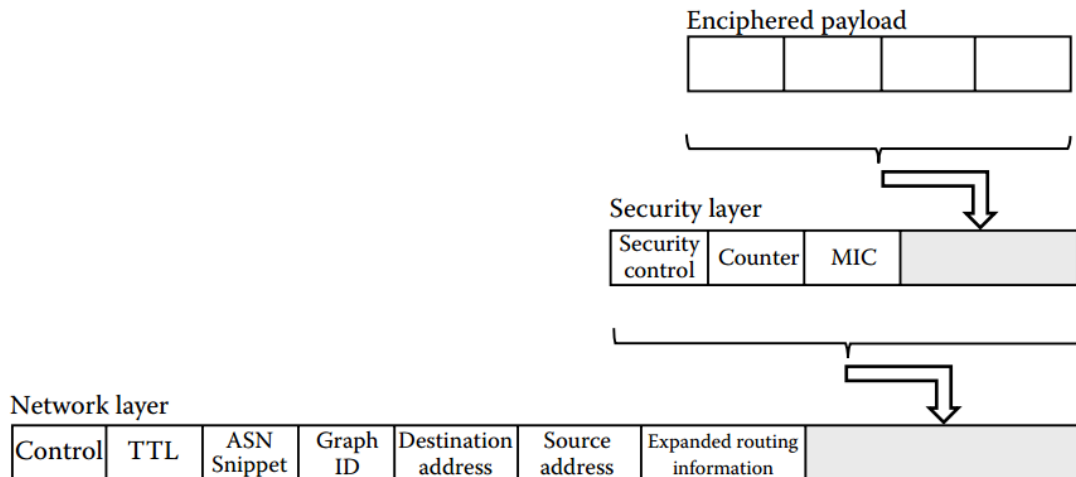


Figure 2-24 WirelessHART NWK layer Frame format [29]

2.2.4 WirelessHART Transport layer

Figure 2-25 shows the WirelessHART transport layer. The transport layer insures end-to-end data delivery and insures reliable communication. The application layer's data is encapsulated in this layer. The Transport layer supports both acknowledged and unacknowledged data delivery.

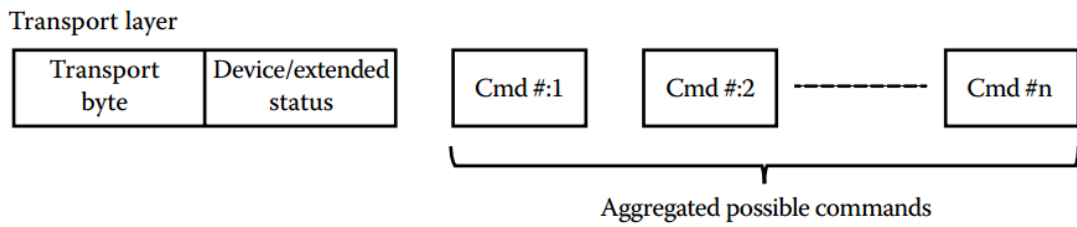


Figure 2-25 WirelessHART Transport Layer Frame Format [29]

2.2.5 WirelessHART APL layer

The APL layer of WirelessHART is adopted from the Hart standard. The APL layer is command based. There are two types of commands, namely, common practice commands, and universal commands. The APL layer is responsible for extracting the command numbers from the messages and perform the required response based on that command. The frame format of the APL layer is shown in figure 2-26.

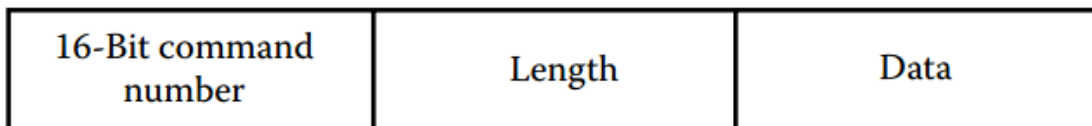


Figure 2-26 WirelessHART APL Layer Frame Format [29]

2.3 ISA100 Protocol Layers

The ISA100 protocol layers are shown in figure 2-27. ISA100 uses a simple version of OSI protocol stack. The ISA100 defines five layers: PHY layer, DDL layer, NWK layer, transport layer, and APL layer.

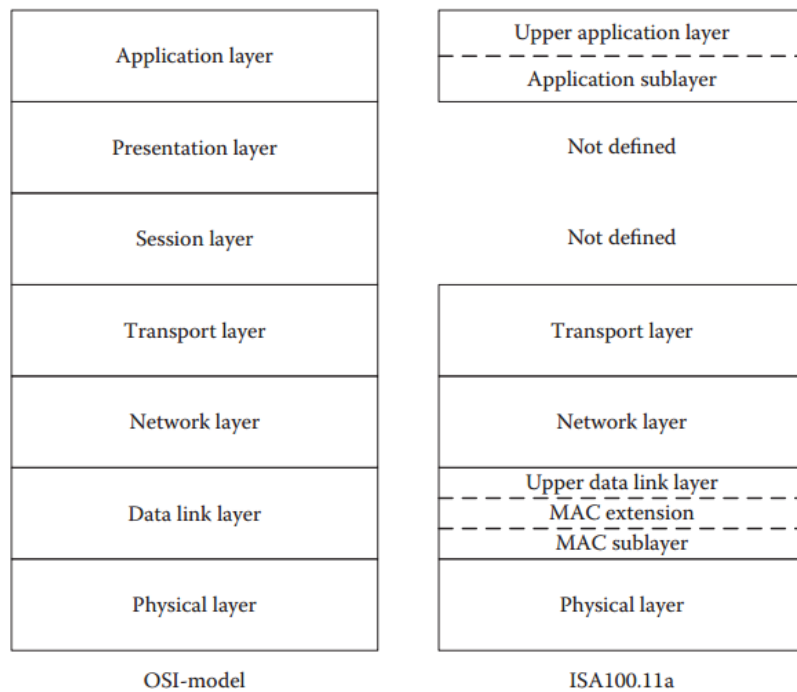


Figure 2-27 ISA100 Protocol Layers [30]

2.3.1 ISA100 PHY layer

The PHY layer of the ISA100 is compliant to the PHY layer of the IEEE802.15.4 standard. ISA100 works in the 2.4GHz band, and uses the channels 11–25 as defined in IEEE802.15.4 standard, with 5MHz gap between adjacent channels. The modulation

technique is direct sequence spread spectrum (DSSS) together with offset quadrature phase-shift keying (O-QPSK). The nominal transmit power is 10mW which gives a transmission range of 100 meters.

2.3.2 ISA Data Link Layer

The ISA100 data link layer consists of three parts: MAC sublayer, MAC extension, and upper data link layer. The MAC sublayer is a subset of the MAC layer in 802.15.14 standard, and the main function of this layer is transmission and reception of data frames. The MAC extension defines extra features not supported in the MAC of 802.15.4 standard, such as frequency hopping and TDMA. The upper data link layer has the functionality of routing across the data link subnet.

The superframe structure is shown in figure 2-28. The superframe is a group of time slots. The time slots in ISA100 have a configurable size (i.e., the size can be 10ms, 11ms, or 12ms). The ISA100 has multiple superframes, but only one superframe can be enabled at a time. The system manager configures the size of the time slot and the superframe.

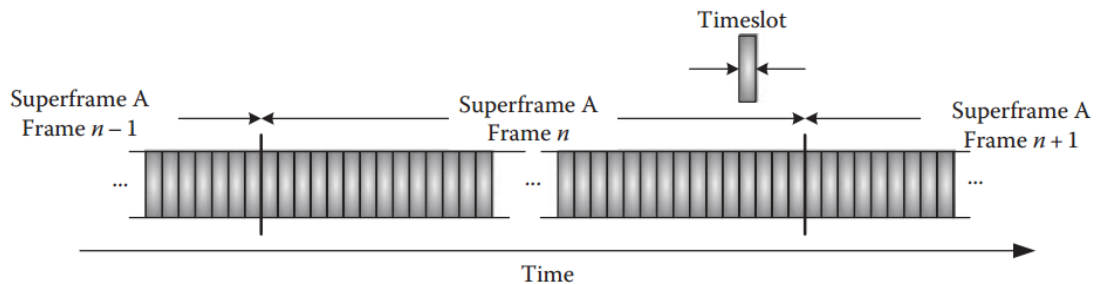


Figure 2-28 SuperFrame Structure [30]

ISA100 uses two types of frequency hopping, namely, slotted hopping, and slow hopping. In slotted hopping, the communication is done in 2D matrix. Thus, each communication link is defined by two parameters: the time slot offset, and the channel offset. Figure 2-29 (a) shows the slotted hopping mechanism.

In slow hopping, a group of adjacent timeslots is combined on a single channel. Consequently, hopping happens to a group of time slots as a single shared medium, and each group is treated as a single slow hopping period. Figure 2.29 (b) shows the slow hopping mechanism.

The slow hopping is helpful for those nodes that have improper synchronization. In addition, slow hopping is required for event-based traffic, which means the occurrence of the event requires immediate transmission. The communication in slow hopping is driven by CSMA-CA, which means the communication is contention based.

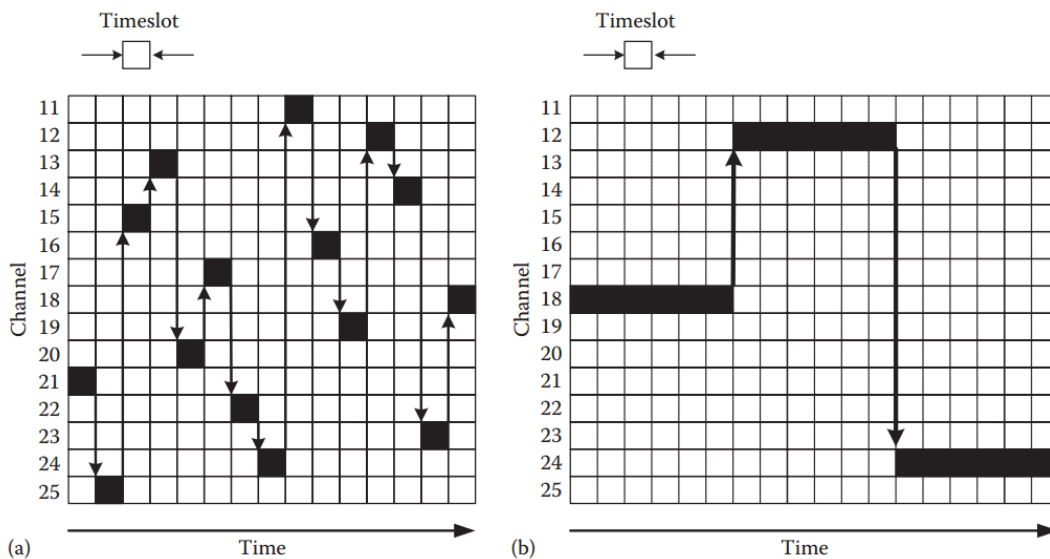


Figure 2-29 (a) slotted Hopping and (b) Slow Hopping [30]

ISA100 can also employ a hybrid hopping combination of slotted and slow hopping; the network has periods of slotted and slow hopping. Figure 2-30 shows the hybrid hopping mechanism.

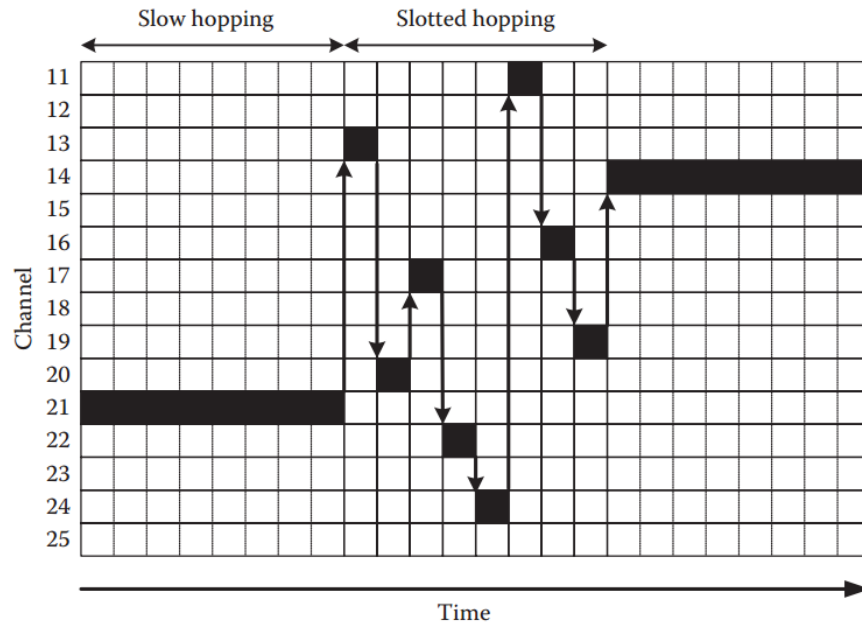


Figure 2-30 Hybrid Hopping [30]

ISA100 defines five programmed hopping patterns supported in all devices:

- Pattern 1: channels numbers 19, 12, 20, 24, 16, 23, 18, 25, 14, 21, 11, 15, 22, 17, 13 (,26)
- Pattern 2: pattern 1 in reverse
- Pattern 3: channels numbers 15, 20, 25

- Pattern 4: pattern 3 in reverse
- Pattern 5: channels numbers 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25 (,26)

Patterns 3 and 4 are used for slow hopping, whereas pattern 5 is used for WirelessHART coexistence.

2.3.3 ISA100 NWK layer

The function of the NWK layer in ISA100 is routing the message beyond the backbone router. It assigns 16-bit short address for DL subnet, and 128-bit long address for backbone networks. The NWK layer is also responsible for fragmentation and reassembly of data packets. The NWK layer also handles address translation between the 16-bit short and the 128-bit long addresses.

2.3.4 ISA Transport layer

The Transport layer handles the end-to-end communications, and provides connectionless services. The transport layer extends the UDP of IETF 6LoWPAN specification. The extension leads for additional authentication and encryption mechanisms and better data integrity checks

2.3.5 ISA100 APL layer

The APL layer is divided into two parts, namely, the upper APL layer, and the APL sublayer. The upper APL layer contains the applications' processes, and the APL sublayer provides the required services for the upper layer, such as object oriented communications.

CHAPTER 3

LITERATURE REVIEW

A lot of research work has been conducted on IEEE's 802.15.4 and the ZigBee standards, in contrast to WirelessHART and the ISA100. This chapter focuses on the research work related to this work.

3.1 Literature Review

In [7], the authors conducted a theoretical comparison between ZigBee, WirelessHART and ISA.100 standards. The authors concluded that WirelessHART and ISA.I00 overcame many of the ZigBee drawbacks. In addition, WirelessHART and ISA.I00 are suitable for industry applications, whereas ZigBee is more suitable for home usage.

The performance of IEEE's 802.15.4 was analyzed in [18] using NS-2. The authors measured the packet reception ratio and the packet routing load over different sending interval times and packet sizes. They concluded that there is a relation between the sending interval time, the packet reception ratio, and the packet routing load. The results showed that the higher is the packet sending interval time (less amount of load), the higher the packet reception ratio and vice versa. Therefore, for each WSN size there is an optimal packet reception ratio based on optimal packet sending interval time.

The possibility of using the WSN standards (ISA100.11a and ZigBee Pro) in aerospace applications was examined in [19]. The authors performed a performance comparison between the two standards, and they concluded that the two standards can be used in aerospace applications. However, the spectrum must be carefully managed to mitigate interference during the operational lifetime of the WSN.

In [16], the performance of the ISA100 was evaluated. The CSMA-CA and TDMA mechanisms were both evaluated. The performance metrics are network throughput, average delay, and energy consumption per superframe. The results showed that ISA100 offers a maximum throughput of 35%, similar to slotted ALOHA. The superframe duration, and the timeslot size has an effect on the network throughput and delay. Long superframe and timeslot sizes produce lower throughput and higher delay. The authors built the ISA100 physical and MAC layers using OPNET modeler. They did not build the full data link layer to support multi-hop routing, which means only star topology network was supported.

In [20], the effect of priority CSMA-CA mechanism of ISA100 was studied. The authors developed ISA100's PHY and MAC layers on the OPNET simulator. They evaluated the performance of the CSMA-CA in terms of packet lifetime and maximum backoff exponent. The authors did not study the effect of multi-hop routing on the CSMA-CA mechanism.

In [21], the performance of ISA100 under interference from IEEE 802.11b was studied. The results showed that ISA100 can tolerate the interference caused by 802.11b and can operate with an acceptable packet error rate (PER) and end-to-end delay. The simulation

was done using OPNET modeler model of ISA100, which supports one hop packet delivery only. Thus the real performance of the ISA100 cannot be tested by this model.

In [22], a special WirelessHART simulator was designed, and the coexistence issue of the WirelessHART with IEEE 802.11b was studied. The designed simulator supports the first two layers the PHY and the MAC of the WirelessHART standard. The results showed that the WirelessHART outperforms the original IEEE 802.15.4 standard. In addition, the WirelessHART can coexist with IEEE 802.11b, which is not the case with IEEE 802.14.5.

In [23], a practical performance evaluation of the WirelessHART was performed. The evaluation of WirelessHART was conducted with and without interference from IEEE 802.11g. The packet loss rate, the packet delivery ratio, and the delay were measured. The results showed that the performance of the WirelessHART is greatly affected by interference from the IEEE 802.11g wireless network. The authors did not apply the WirelessHART blacklisting mechanism, and this might be the reason for the heavily degraded performance.

In [24], the PHY layer of the WirelessHART was implemented in network simulator 3. The PER of different types of packets and the effect of different path loss models was evaluated. The results showed that the maximum transmission range for WirelessHART is 200m, 160m, and 20m for Friis model, Two Ray Ground model, and Log Distance model, respectively. In addition, the maximum packet size (133-byte) experiences a 3.5% PER.

In [25], the full WirelessHART protocol stack was implemented using NS-2. The authors evaluated the performance of the WirelessHART during the establishment phase. The establishment phase is the phase during which the network is first started. The nodes start

scanning the different channels to connect to the gateway then establishing the graph route, and the gateway starts sending the advertisement packets to connect with new nodes to establish the whole network. In this paper, the node joining delay and the connection establishment delay were evaluated. The results showed that the more the hops between the node and the gateway, the more the delay for node joining and for connection establishment.

In [26], the coexistence issue between ZigBee and Wi-Fi standards 802.11b/g was studied. The results showed that the performance of the ZigBee network is affected by the two standards. The possible solution is a proper allocation of ZigBee's nodes to avoid interference from Wi-Fi networks.

In [27], the performance of ZigBee network with mobility was studied, the performance metrics were delay and throughput. The experiments considered different types of topologies, namely, star, tree, and mesh topologies. The results showed that, when the nodes are moving, the performance of ZigBee is better when using tree topology.

3.2 Summary

The previous work covered some of the ISA100 and WirelessHART aspects, and measured the performance of the two standards. Nevertheless, the results were for special cases and did not measure the performance where the mesh or tree topologies and multi-hop networks take place.

The importance of this work comes from the necessity of measuring the IWSN performance over multi-hop networks. To evaluate the performance of such networks there is a need for a simulator that supports multi-hop routing. In this work, an ISA100 simulator is developed to measure the performance of such networks.

CHAPTER 4

WirelessHART Implementation Description

This chapter provides description of the WirelessHART implementation using NS-2 that was performed in [25].

4.1 WirelessHART Implementation in NS-2

Pouria Zand et. Al. [25] implemented WirelessHART using NS-2. They implemented the full WirelessHART protocol stack. NS-2 simulator already has the PHY and MAC layers of the IEEE 802.15.4. WirelessHART adopted both the PHY and the MAC layers of IEEE 802.15.4e 2006 release. The PHY layer is the same as in the previous release, but the MAC layer is different. The MAC has time slot channel hopping (TSCH) property. The authors implemented the DL layer, the NWK layer, the Transport layer, and the APL layer.

4.1.1 The DL layer

The authors in [25] modified the MAC layer's module of NS-2 to support the TSCH, ACKs, concurrent link activation and MLME primitives (mlme_set_slotframe, mlme_set_link, mlme -set-graph, mlme_tsch_mode, mlme_listen, mlme_advertise, mlme_keep_alive, mlme_join, mlme_activate and mlme_disconnect).

The DL layer tables shown in Figure 4-1 were also implemented in NS-2. The tables are:

- The superframes table: contains the superframes. The superframe length is given by 2^n s, where $(-2 \leq n \leq 9)$.
- The link tables: describes all the links in the network. The link is the connection between two nodes, one as source and the other as destination. A link is described by the timeslot number, the channel offset, the superframe ID, the node address, and the link type (data, join, discovery, or broadcast).
- Graph table: each graph lists the potential next hops to which the data can be forwarded.
- Neighbor table: lists the neighbors with which the node can communicate. Unlike the other tables, this table is filled by the node directly without referring to the Network Manager (NM).

4.1.2 The NWK layer

The NWK layer of the WirelessHART provides routing and secure connection over multi-hop. The route table, the source route table, the service table, and the session table, shown in Figure 4-1, are implemented in NS-2.

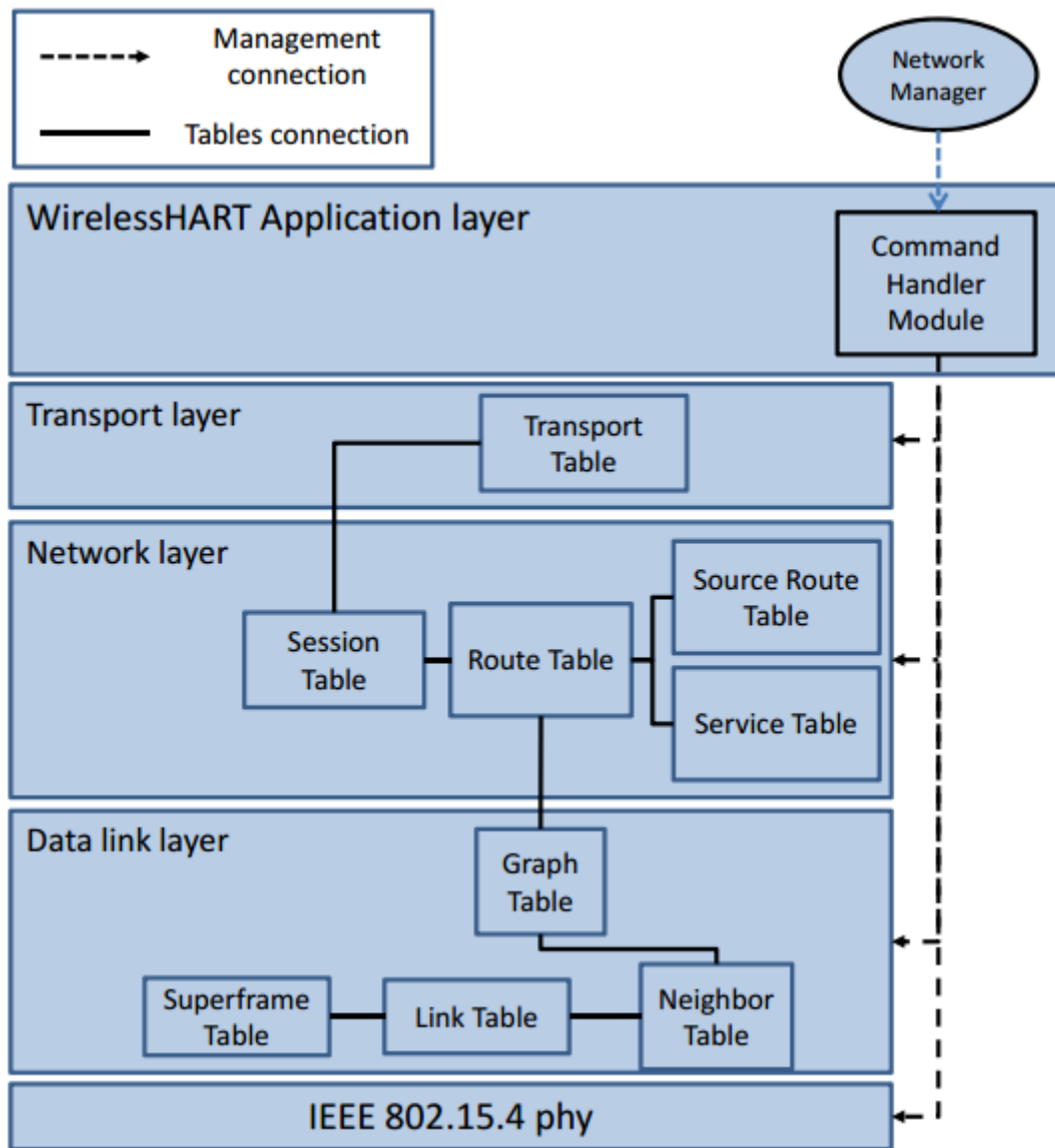


Figure 4-1 WirelessHART Protocol Stack [31]

The session provides end-to-end secure communication between any two devices in the network. There are four types of sessions: a unicast session between the NM and the device, a broadcast session between the NM and all the devices, a unicast session between the gateway and the device, and a broadcast session between the gateway and all the devices.

The services are used to allocate bandwidth for communication between devices. The service table contains the list of services the device can have. There are four types of services: maintenance services, publish services, block transfer services, and event services.

4.1.3 Transport layer

Transport layer supports acknowledged and unacknowledged data delivery. The transport table shown in Figure 4-1 has a new entry after each acknowledged data transfer.

4.1.4 The APL layer

The APL layer contains the list of commands the WirelessHART can support, each of which is identified by a command number. The command number determines the contents of the message. The commands are used by the network manager or the gateway to perform tasks. The implemented commands are graph management and source route commands, managing superframes and link commands, bandwidth management commands, network health reporting and status commands.

4.1.5 The Network Manager

The NM uses centralized network management algorithm to manage the network and schedule communications. The authors implemented the management algorithm in [30]. Each time a new node joins the network, the NM runs the algorithm, and defines the uplink, downlink, broadcast graphs, and the communication schedule for the node. This procedure

is repeated until all nodes join the network. The following sub-sections describe the join procedure, graph and route definition, communication scheduling, and the service request procedure.

4.1.5.1 The Join Procedure

The join procedure is shown in figure 4-2. Any new node willing to join the network listens to the frequency channels in the 2.4GHz band. The advertiser node or the router node always broadcasts the advertisement, which contains information about the superframe structure. The node sends the join request to the selected advertiser. The join request contains information about the neighbors' signal levels. The new node also adds the advertiser's graph ID to the network header of the join request. The advertiser receives the join request then forwards it to the NM/Gateway. The NM receives the join requests and performs the management algorithm to allocate the graphs and the links for the new node. After that, the NM sends the join response or the activation command to the new node. The join response includes the following: write network key (Command 961), write device nickname address (Command 962), and write session (Command 963). At the final stage, the NM sends the links and the graphs to the new device.

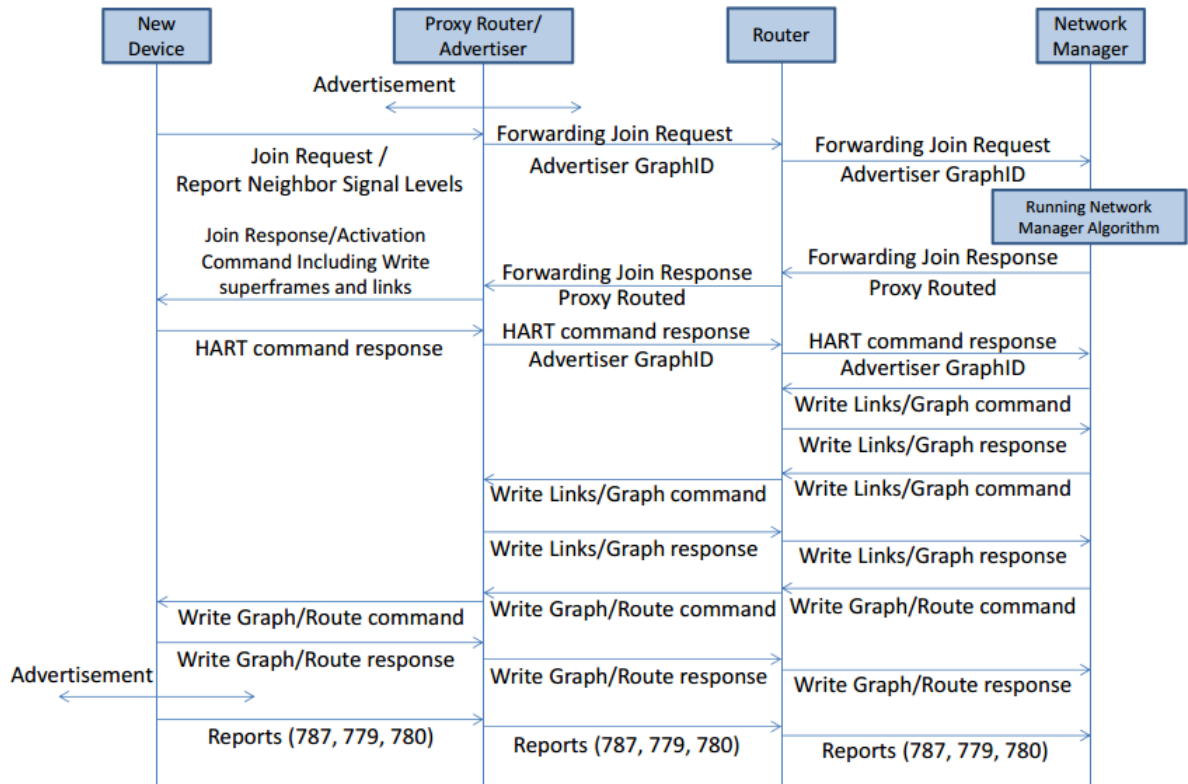


Figure 4-2 the Join Procedure

4.1.5.2 Graph and Route Definition

There are three types of routing graphs in the network:

- The uplink graph: this graph is used to establish connections between the field devices and the gateway. The devices may send management or process data.
- The downlink graph: this graph is used by the NM to establish a unicast connection to every device in the network.
- The broadcast graph: used by the NM to send common data or control data to the whole network.

The following notations are used throughout this chapter:

$G(V, E)$: the original network topology

g : the Gateway

V_{AP} : the set of Access Points

V_D : the set of devices

$\{g\} \cup V_{AP} \cup V_D = V$.

e_v^+ and e_v^- : the outgoing edge set and incoming edge set for each node $v \in V_D \cup V_{AP}$

δ_v^+ and δ_v^- : the v 's outgoing and incoming degree

$G_B(V_B, E_B)$ and $G_U(V_U, E_U)$: the G 's reliable broadcast graph and uplink graph.

$G_v(V_v, E_v)$:the downlink graph for node v

\bar{h}_i : the average number of hops from the gateway for node i

P_i : node i parents in the G_B

C1: v has at least two parents u_1, u_2 , and they form a cycle.

C2: u_1 is u_2 's parent in u_2 's local downlink graph.

C3: $u_2 (u_1)$ has at least one parent from the cycle in $G_{u_1} (G_{u_2})$

Algorithm 1 describes how the network manager can construct the broadcast graph [32].

Algorithm 1 Constructing Reliable Broadcast Graph $G_B(V_B, E_B)$

```

1: //  $G(V, E)$  is the original graph
2: Initially  $V_B = g \cup V_{AP}$  and  $E_B$  contains all links from  $g$  to  $V_{AP}$ .
3:
4: while  $V_B \neq V$  do
5:   Find  $S' \subseteq V - V_B$ :  $\forall v \in S', v$  has at least two edges from  $V_B$ 
6:   if  $S' \neq \emptyset$  then
7:     for all node  $v \in S'$  do
8:       Sort its edges  $e_{u,v}$  from  $V_B$  according to  $h_u$ 
9:       Choose the first two edges  $e_{u_1,v}$  and  $e_{u_2,v}$ 
10:       $h_v = \frac{h_{u_1} + h_{u_2}}{2} + 1$ 
11:     end for
12:   Choose the node  $v$  with min  $h_v$ 
13:   Add  $v$  to  $V_B$  and add  $e_{u_1,v}$  and  $e_{u_2,v}$  to  $E_B$ 

```

```

14: else
15:   Find  $S'' \subseteq V - V_B: \forall v \in S'', v$  has one edge  $e_{u,v}$  from  $V_B$ 
16:   if  $S'' \neq \emptyset$  then
17:     for all node  $v \in S''$  do
18:        $h_v = h_u + 1$ 
19:       Calculate  $n_v$ , the # of its outgoing edges to  $V - V_B$ 
20:     end for
21:     Choose the node  $v$  with maximum  $n_v$ , break tie using  $h_v$ 
22:   else
23:     return FAIL;
24:   end if
25: end if
26: end while
27: return SUCCESS;

```

Algorithm 2 describes the constructions of the uplink graph [32].

Algorithm 2 Constructing Reliable Uplink Graph $G_U(V_U, E_U)$

```

1: //  $G(V, E)$  is the original graph,  $G^R(V, E^R)$  is the reversed graph
2: Construct  $G^R(V, E^R)$ 
3: Construct  $G_B(V_B, E_B)$  from  $G^R(V, E^R)$  by applying Alg. 1
4:
5: if  $V_B = V$  then
6:   // Construct  $G_U$  by reversing all edges in  $G_B$ 
7:    $G_U(V_U, E_U) = G_B^R(V_B, E_B^R)$ 
8: else
9:   // the network topology is disconnected
10:  return FAIL;
11: end if
12: return SUCCESS;

```

Algorithm 3 describes the construction of the downlink routes [32].

Algorithm 3 Constructing Sequential Reliable Downlink Routes

```

1: Let  $S$  be the set of explored nodes with downlink route constructed
2: Initially  $S = g \cup \text{VAP}$ 
3: Initially for each AP  $i$  in  $S$ , set  $G_i = (\{g \cup i\}, \{eg, i\})$  and  $R_i = G_i$ 

```

```

4:
5:   while  $S \neq V$  do
6:   Find  $S' \subseteq V - S : \forall v \in S', v$  has at least two edges from  $S$ 
7:   //  $S_r$  is the reliable node set in  $S'$ , initially  $S_r = \emptyset$ 
8:   if  $S' \neq \emptyset$  then
9:   for all node  $v \in S'$  do
10:  for all edge pair  $(e_{u_1,v}, e_{u_2,v})$  from  $S$  do
11:   $h_{u_1,u_2} = (h_{u_1} + h_{u_2}) / 2$ 
12:  end for
13:  Find  $P_v$ , set of edge pairs of  $v$  satisfying  $C1 \wedge (C2 \cup C3)$ 
14:  if  $P_v \neq \emptyset$  then
15:   $S_r = S_r \cup \{v\}$ 
16:  Choose  $(e_{u_1,v}, e_{u_2,v})$  from  $P_v$  with  $\min h_{u_1,u_2}$ 
17:  else
18:  Choose  $(e_{u_1,v}, e_{u_2,v})$  from  $S$  with  $\min h_{u_1,u_2}$ 
19:  end if
20:   $h_v = h_{u_1,u_2} + 1$ 
21:  end for
22:  if  $S_r \neq \emptyset$  then
23:  Add  $v$  in  $S_r$  with  $\min h_v$  to  $S$ 
24:  else
25:  Add  $v$  in  $S'$  with  $\min h_v$  to  $S$ 
26:  end if
27:  ConstructDG( $G, u_1, u_2, v$ );
28:  else
29:  Find  $S'' \subseteq V - S$  and  $\forall v \in S'', v$  has one edge  $e_{u,v}$  from  $S$ 
30:  if  $S'' \neq \emptyset$  then
31:  for all node  $v \in S''$  do
32:   $h_v = h_u + 1$ 
33:  end for
34:  Add  $v$  to  $S$  with  $\min h_v$ 
35:   $G_v = (\{u \cup v\}, \{e_{u,v}\})$ 
36:   $R_v = R_u \rightarrow G_v$ 
37:  else
38:  return FAIL;
39:  end if
40:  end if
41:  end while
42:  return SUCCESS;

```

Algorithm 4 [32] is called by algorithm 3 in line 27.

Algorithm 4 ConstructDG (G, u_1, u_2, v)

```

1: Let  $E_\delta$  be the set of edges among  $u_1, u_2$  and  $v$ 
2: if  $u_1, u_2$  satisfy  $C1 \wedge C2$  then
3:    $G_v = G(\{u_1, u_2, v\}, E_\delta)$ 
4:   if  $u_1$  is  $u_2$ 's parent in  $G_{u_2}$  then
5:      $R_v = R_{u_2} \rightarrow G_v$ 
6:   else
7:      $R_v = R_{u_1} \rightarrow G_v$ 
8:   end if
9: else if  $u_1, u_2$  satisfy  $C1 \wedge C3$  then
10:  if  $u_1$  has an edge  $e$  from  $u_2$ 's parents in  $G_{u_2}$  then
11:     $G_v = G(\{u_1, u_2, v\}, E_\delta \cup e)$ 
12:     $R_v = R_{u_2} \rightarrow G_v$ 
13:  end if
14:  if  $u_2$  has an edge  $e$  from  $u_1$ 's parents in  $G_{u_1} \wedge (h_{u_2} < h_{u_1})$  then
15:     $G_v = G(\{u_1, u_2, v\}, E_\delta \cup e)$ 
16:     $R_v = R_{u_1} \rightarrow G_v$ 
17:  end if
18:  else
19:    if  $e_{u_1, u_2}$  and  $e_{u_2, u_1}$  both exist then
20:       $G_v = G(\{u_1, u_2, v\}, E_\delta)$ 
21:       $R_v = (h_{u_1} < h_{u_2}) ? R_{u_1} \rightarrow G_v : R_{u_2} \rightarrow G_v$ 
22:    else if there is neither  $e_{u_1, u_2}$  nor  $e_{u_2, u_1}$  then
23:       $G_v = (h_{u_1} < h_{u_2}) ? G(\{u_1, v\}, \{e_{u_1, v}\}) : G(\{u_2, v\}, \{e_{u_2, v}\})$ 
24:       $R_v = (h_{u_1} < h_{u_2}) ? R_{u_1} \rightarrow G_v : R_{u_2} \rightarrow G_v$ 
25:    else if  $e_{u_1, u_2}$  exists then
26:       $G_v = G(\{u_1, u_2, v\}, E_\delta)$ 
27:       $R_v = R_{u_1} \rightarrow G_v$ 
28:    else
29:       $G_v = G(\{u_1, u_2, v\}, E_\delta)$ 
30:       $R_v = R_{u_2} \rightarrow G_v$ 
31:    end if
32:  end if

```

4.1.5.3 Communication Scheduling and Channel Management

Algorithm 5 describes the communication schedule construction between nodes [32].

Algorithm 5 Constructing Data Communication Schedule

```
1:   Sort device sample rates in ascending order:  $r_1 < r_2 < \dots < r_k$ .
2:   Identify the set of nodes with each sample rate:  $N_1, N_2, \dots, N_k$ .
3:   Initialize the schedule for each node as  $\emptyset$ 
4:
5:   for all  $r_i$  from  $r_1$  to  $r_k$  do
6:     Generate the data superframe  $F_i$ 
7:     for all node  $v \in N_i$  do
8:       // Schedule primary and retry links for publishing data
9:       ScheduleLinks( $v, g, G_U, F_i, 0, \text{Exclusive}$ );
10:      ScheduleLinks( $v, g, G_U, F_i, l_i/4, \text{Shared}$ );
11:
12:      // Schedule primary and retry links for control data
13:      ScheduleLinks( $g, v, G_v, F_i, l_i/2, \text{Exclusive}$ );
14:      ScheduleLinks( $g, v, G_v, F_i, 3l_i/4, \text{Shared}$ );
15:
16:      if link assignment is not successful then
17:        // Defer bandwidth request from node  $v$ 
18:        return FAIL;
19:      end if
20:    end for
21:  end for
22:  return SUCCESS;
```

The last algorithm (algorithm 6) describes link scheduling [32].

Algorithm 6 ScheduleLinks(u, v, G, F, t, o)

```
1: //  $u$  and  $v$  are the source and destination of the communication
2: //  $G$  is the routing graph and  $F$  is the superframe
3: //  $t$  is the earliest slot to be allocated and  $o$  is the link option
4:
5: Identify data superframe  $F'$  with  $l_{F'} = 2l_F$ 
6: for all node  $i \in \text{Successor}(u)$  do
7:   Identify the schedule  $S_u$  and  $S_i$  for node  $u$  and  $i$ 
```



```

8: if  $i$  is the only successor of  $u$  then
9:   Identify  $t_i$ , the earliest slot from  $t$  with a channel  $c$  to:
10:  Allocate entries  $M_{k \cdot l_F + t_i, c} (k = 0, 1, \dots)$  on  $M$ 
11:  Allocate the slots  $k \cdot l_F + t_i$  on  $S_u$  and  $S_i$ 
12:  Allocate slot  $t_i$  on  $F$ 
13:
14:  if All allocations are successful then
15:    ScheduleLink( $i, v, G, F, t_i, o$ );
16:  end if
17: else
18:  if  $i$  is the first successor then
19:    Identify  $t_i$ , the earliest slot from  $t$  with a channel  $c$  to:
20:    Allocate entries  $M_{k \cdot l_{F'} + t_i, c}$  on  $M$ 
21:    Allocate slots  $k \cdot l_{F'} + t_i$  on  $S_u$  and  $S_i$ 
22:    Allocate slot  $t_i$  on  $F'$ 
23:  else
24:    Identify  $t_i$ , the earliest slot from  $t$  with a channel  $c$  to:
25:    Allocate entries  $M_{k \cdot l_{F'} + l_F + t_i, c}$  on  $M$ 
26:    Allocate slots  $k \cdot l_{F'} + l_F + t_i$  on  $S_u$  and  $S_i$ 
27:    Allocate slot  $l_F + t_i$  on  $F'$ 
28:  end if
29:
30:  if All allocations are successful then
31:    ScheduleLink( $i, v, G, F', t_i, o$ );
32:  end if
33: end if
34: if No feasible allocations available then
35:  return FAIL;
36: end if
37: end for
38:  return SUCCESS;

```

4.1.5.4 Service Request Procedure

The device that needs to establish connection with other devices in the network requests additional bandwidth from the NM. The service request procedure is shown in figure 4-3.

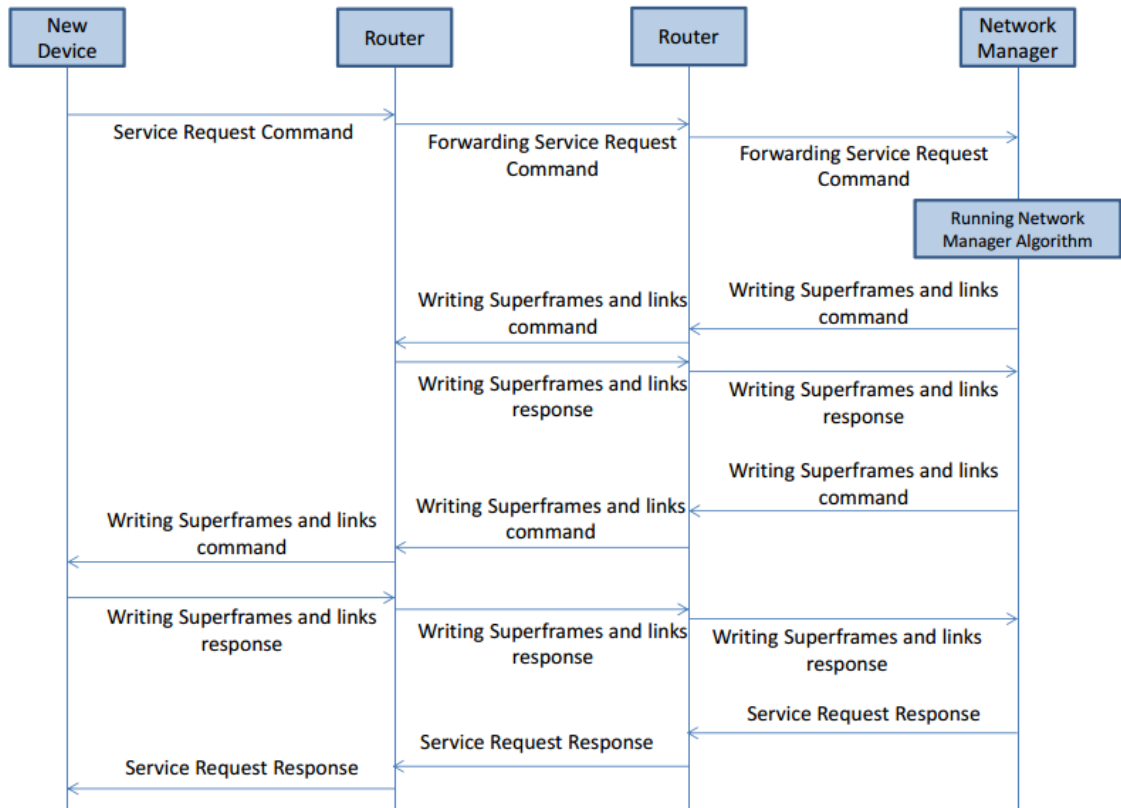


Figure 4-3 The Service Request

CHAPTER 5

ISA100 implementation and Benchmarking

This chapter gives description of our implementation of ISA100 simulator in NS-2, and provides a comparison against another ISA100 simulator.

5.1 The Implemented ISA100 simulator

The ISA100 simulator is built in NS2. It is worth mentioning that the ISA100 simulator is based on the WirelessHART simulator in NS-2 [25]. The WirelessHART simulator was upgraded to support the ISA100 features.

As mentioned in chapter 2, there are differences between the two protocol stacks, and there are similarities. The similarities between the two protocols are:

- They have the same PHY layer. The PHY layer is 802.15.5 IEEE compliant
- The sub-MAC layer is the same in the two protocols, and it is also 802.15.5 IEEE MAC compliant
- The two protocols support graph and source routing.

The differences between the two protocol stacks are:

- The WirelessHART DL layer supports TDMA. TDMA provides guaranteed timeslots for the nodes with fixed timeslot size of 10ms. On the other hand, ISA100 supports configurable time slot size. The timeslot size can be 10ms, 11ms, or 12ms.
- The WirelessHART supports one channel hopping mechanism, which is slotted hopping, and one hopping sequence pattern. ISA100 supports two different channel hopping mechanisms, and 5 different hopping sequences. ISA100's channel hopping mechanisms are slotted hopping and slow hopping, and the 5 hopping patterns are:
 - Pattern 1: channels 19, 12, 20, 24, 16, 23, 18, 25, 14, 21, 11, 15, 22, 17, 13
(,26)
 - Pattern 2: pattern 1 in reverse
 - Pattern 3: channels 15, 20, 25
 - Pattern 4: pattern 3 in reverse
 - Pattern 5: channels 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25
(,26)

Patterns 3 and 4 are used for slow hopping, whereas pattern 5 is exploited to coexists with WirelessHART.

- In slow hopping, the ISA100 devices use CSMA-CA mechanism to access the communication medium, and the active communication period for any node varies from 100ms to 400ms.

The aforementioned differences were considered and the WirelessHART simulator's code was updated.

Figure 5-1 shows the slotted hopping mechanism. First, the system manager configures the slot size (10ms, 11ms, or 12ms). Next, it selects the hopping pattern 1, 2 or 5. Then, it assigns timeslots (TS) and channel numbers to the nodes. If the user wants to change the slot size or the hopping pattern, the communication is stopped and the required changes are made.

Figure 5-2 shows the slow hopping mechanism. At the first stage, the system manager sets the hopping pattern 3 or 4. The communication after that is driven by the CSMA-CA mechanism, where the medium is shared and the nodes compete to have the channel access. After that, the channel number is assigned. If the communication is done, the medium will be available for the competing nodes again. If the user wants to change the hopping pattern the communication is terminated, then the pattern can be changed.

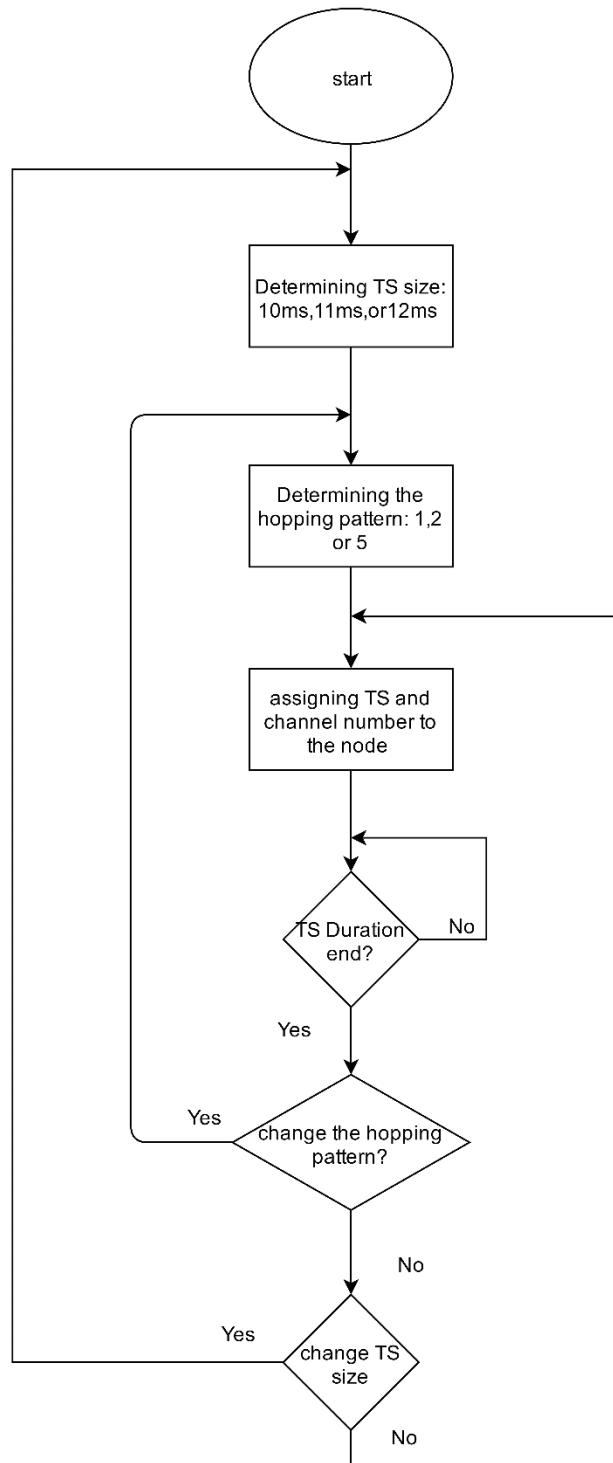


Figure 5-1 Slotted Hopping mechanism

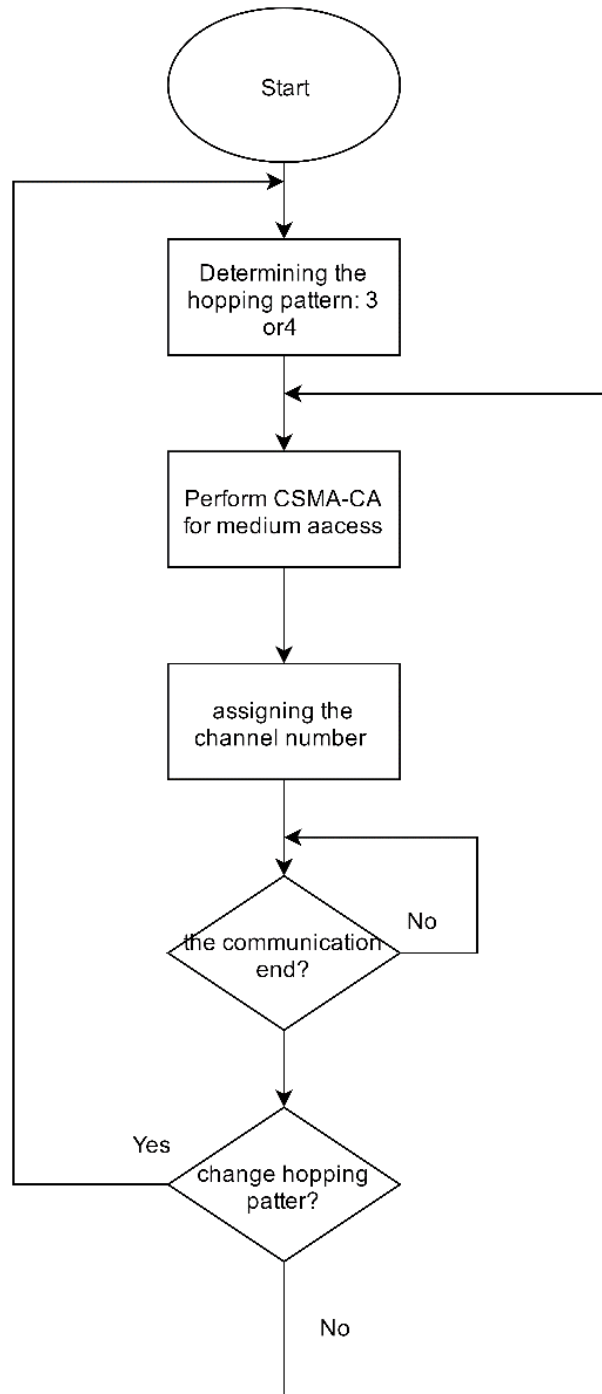


Figure 5-2 Slow Hopping mechanism

5.2 ISA100 Benchmarking

For ISA100 benchmarking, the ISA100 results in [16] are compared to our results. The results in [16] are generated based on ISA100's model in the OPNET. The experiment setup is shown in figure 5-3, where 24 nodes are connected to the gateway in a star topology. The nodes send data to the gateway following the Poisson's traffic model. The TS is 10ms and the SD is 25 slots. The simulation time is 100s and the packets are generated with uniform distribution form 0s to 5s, and the packet size is set to 96-byet. The offered load generated by all nodes is normalized to 250kbps. The network throughput and the average delay are measured throughout this experiment.

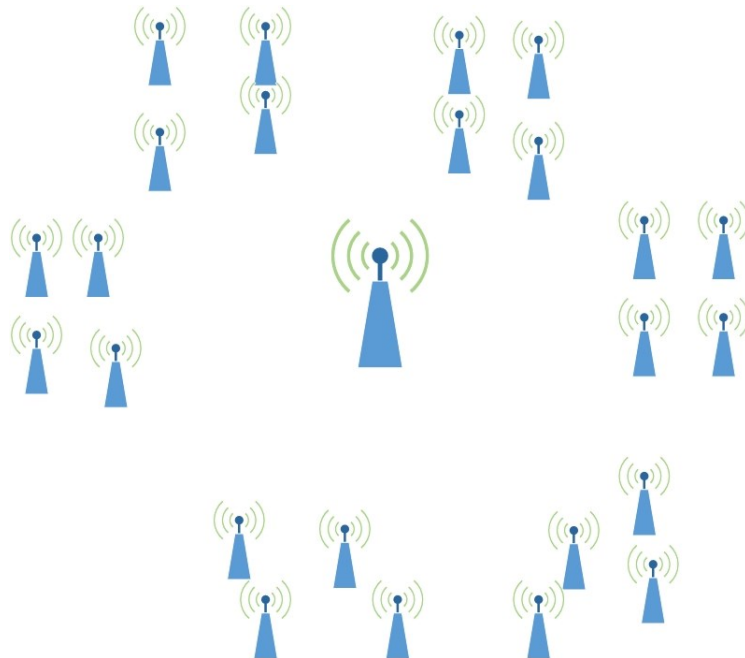


Figure 5-3 Simulation Setup

Figure 5-4 shows the network throughput comparison over different offered loads. The ISA100 network has a maximum capacity of 36%. There is small difference in the throughput measurements between ISA100 OPNET simulator and the ISA100 NS-2 simulator.

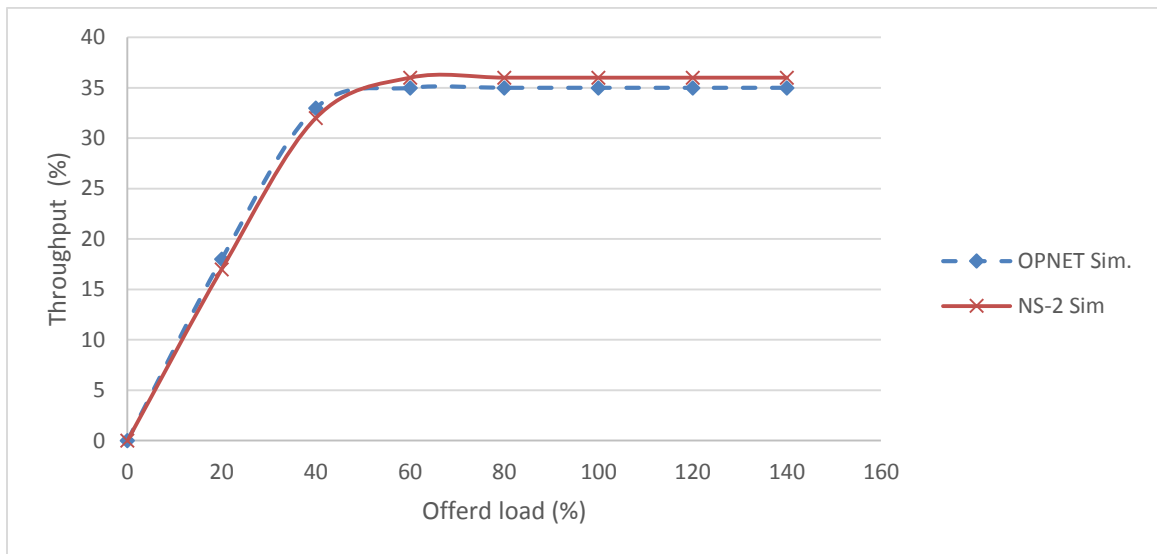


Figure 5-4 Network Throughput Comparison

Figure 5-5 shows the Average delay of the ISA100 network. The network experiences a maximum average delay of 15s. The result comparison shows that the two simulators approximately produce the same amount of delay.

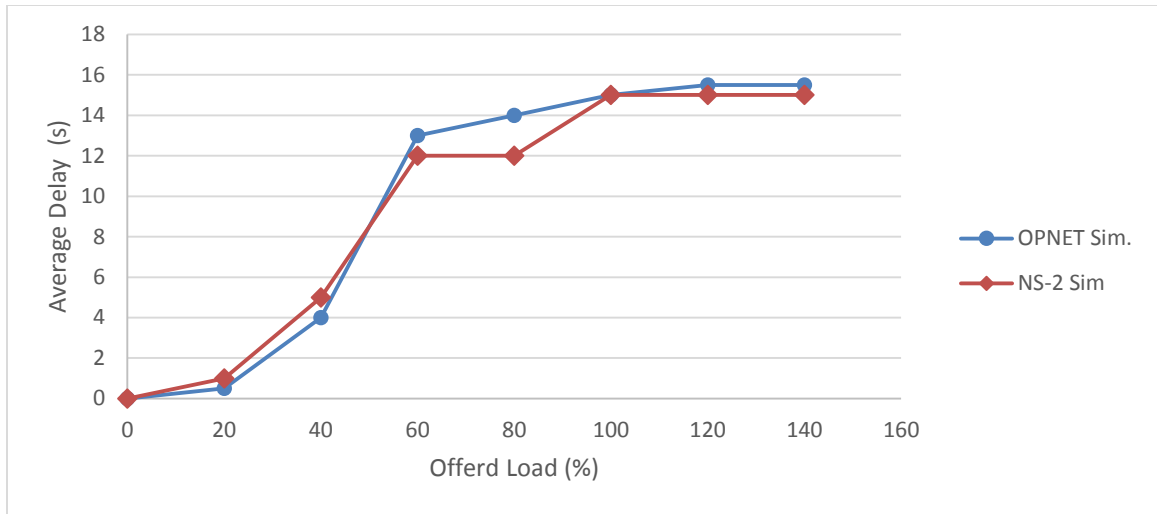


Figure 5-5 Average Delay Comparison

Figures 5-6 and 5-7 show the effect of different superframe durations (SD) on network throughput and average delay, respectively. Figure 5-6 shows that the higher SD, the higher the throughput. Figure 5-6 also shows a little difference in the results for SD 250ms and 400ms, but almost the same for 100ms SD.

Figure 5-7 shows the average delay for different SD. The results indicate that the 100ms SD produces minimum delay. Furthermore, the results for the two simulators are the same. There is considerable difference between the two simulators results for the 250ms SD. On the other hand, there is a little difference between the two for the 400ms SD.

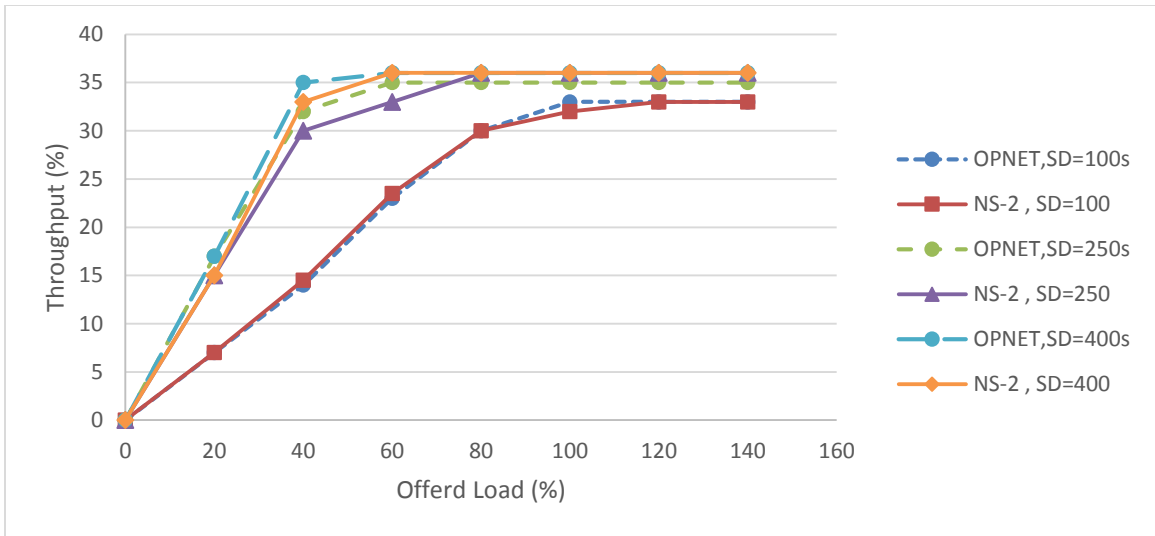


Figure 5-6 Network Throughput Comparison for Different SD

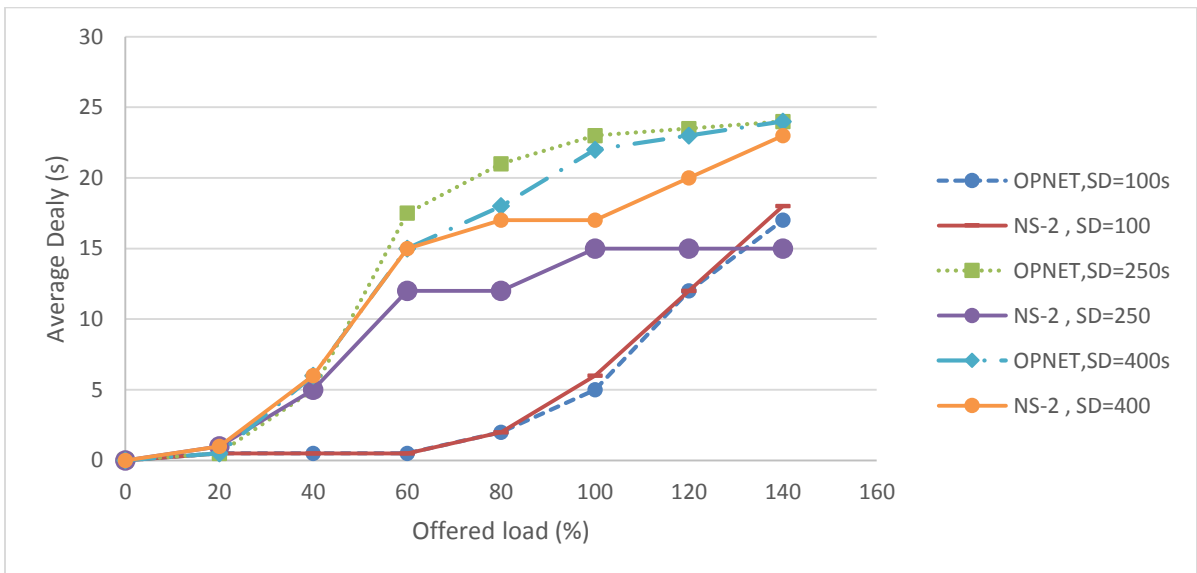


Figure 5-7 Average Delay Comparison for Different SD

5.3 Summary

The simulation results for OPNET and NS-2 simulators imply minor differences in some of the outputs, mainly in the delay part. The reason is that the two simulators are built on two different simulator backgrounds. Moreover, the NM or the system manager's algorithm that is responsible for scheduling communications between nodes is different. The NM algorithm of ISA100 in NS-2 is built by considering its four layers, but the NM algorithm of the ISA100 simulator in OPNET considers only the first two layers, namely, the PHY and MAC layers. This difference produces more processing delay in the NS-2 simulator than in the OPNET simulator.

CHAPTER 6

SIMULATION and RESULTS

This chapter provides an analysis of the simulation results for the three WSN standards (ISA100, WirelessHART, and ZigBee), and gives some recommendations for each standard. This chapter is divided into two parts: simulation & results, and conclusion & recommendations.

6.1 Simulation and Results

This section provides the simulation results of the three WSN standards ZigBee, WirelessHART, and ISA100. The experiments measure the performance of three standards in terms of three performance metrics, namely, the network throughput, the end-to-end delay, and the energy consumption. The throughput is the number of successfully delivered packets per second. The end-to-end delay is the sum of the processing delay, the propagation delay and the queuing delay of the intermediate nodes. The energy consumption is the amount of the consumed energy by the nodes in transmitting and receiving the packets. In addition to the previously mentioned simulation metrics, the effect of beacon-enabled on ZigBee, and the effect of the superframe frame duration on ISA100 and WirelessHART are also measured.

The first experiment is a comparison of ZigBee, WirelessHART, and ISA100. The throughput, the end-to-end delay, and the energy consumption are measured. The simulation area is 100*100 m, the nodes are randomly distributed in the area, and the gateway is always in the center. In ZigBee's experiment, there is one ZigBee coordinator, which acts as a root, and the other nodes are FFDs that act as sensors and routers. In WirelessHART and ISA100 experiments, there is one network gateway, two access points (AP) that act as sensing nodes, bridging devices between the nodes and the gateway, and the other nodes are FFDs. The other simulation parameters are in table 6-1.

Table 6-1 experiment 1 parameters

The Parameter	The value
experiment area	100*100 m
Node numbers	5 to 45 nodes; 5 nodes increment each time.
Traffic type	Constant bit rate (CBR)
Traffic update interval	15 s: 1 message every 15 s
Transmission range	15 m
Routing protocol	AODV for ZigBee, and graph/source routing for ISA100 and WirelessHART.
Experiment run time	100 s
Packet size	100 byte
ACK size	15 byte

Figure 6-1 shows the average end-to-end delay of ZigBee, WirelessHART, and ISA100. The results show that ZigBee has the lowest end-to-end delay of the three standards. This is expected because a node in ZigBee uses slotted CSMA-CA for medium access and does not wait for its turn like the node in WirelessHART or ISA100. ISA100's CSMA-CA has higher average end-to-end delay than ZigBee, because CSMA-CA in ISA100 is pure CASMA-CA, but it has lower average end-to-end delay than ISA100 slotted hopping and WirelessHART. It is noticed that the average end-to-end delay increases by increasing the number of nodes and the hops, which is as expected.

The ISA100 10ms TS size performs exactly as WirelessHART, since both ISA100-10ms TS and WirelessHART have the same TS duration, and they also have the same hopping sequence of 16 channels.

The ISA100 12ms TS size has the highest average end-to-end delay, followed by the ISA100 11ms TS size. The reason is the longer the TS the longer the time the other nodes must wait to have their turns to transmit data.

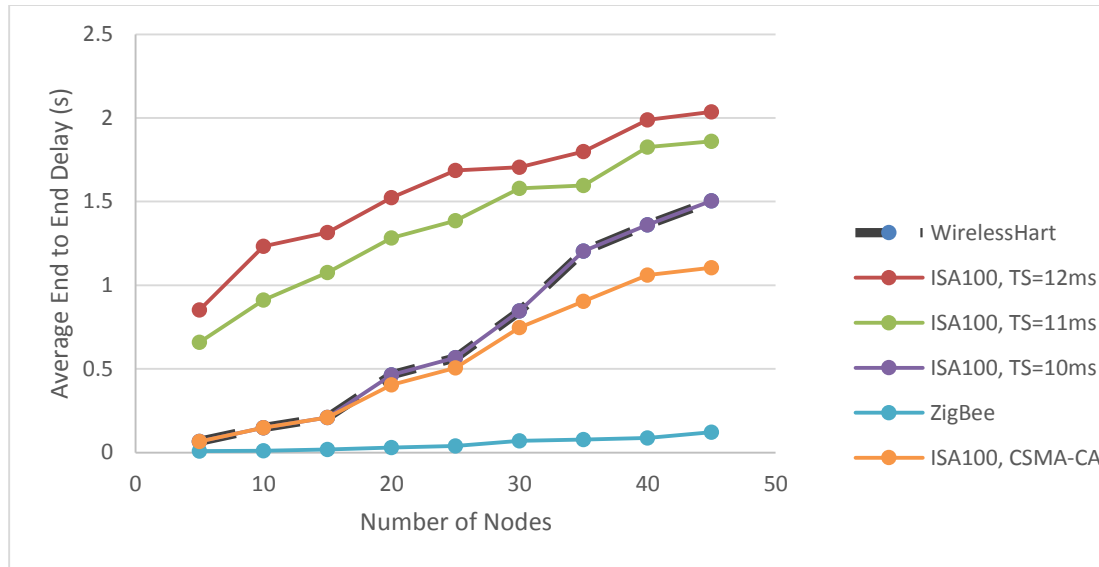


Figure 6-1 the Average End to End Delay of ZigBee, WirelessHART, and ISA100 :(10ms TS ,11ms TS ,12ms TS, CSMA-CA)

Figure 6-2 shows the throughput of ZigBee, WirelessHART, and ISA100. The results show that ISA100 performs similar to WirelessHART, and the two standards are better than ZigBee. ZigBee's network is a contention based access medium, and the number of collided packets becomes large at high traffic values, hence the performance becomes bad. On the other hand, the deterministic medium access of TDMA in ISA100 and WirelessHART grants more reliability than that of ZigBee.

The ISA100 in the slow hopping mode (CSMA-CA) performs similar the WirelessHART and ISA100 slotted hopping in low traffic or small size networks, but the performance becomes worse than both the WirelessHART and ISA100 slotted hopping in high traffic networks or in large networks

The performances of ISA100 (10ms TS, 11ms TS, 12ms TS) and WirelessHART are approximately the same, but there is small difference between them at high traffic. ISA100 12ms TS has slightly less throughput than ISA100 (10msTS and 11ms TS) at high traffic. The performance of ISA100 at 10ms TS size is the same as WirelessHART.

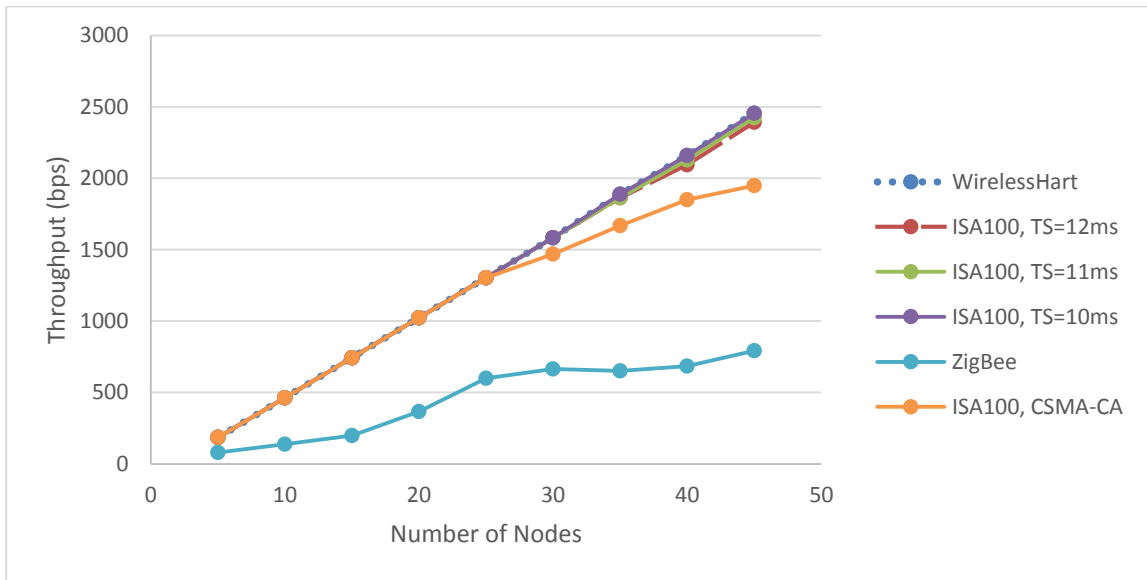


Figure 6-2 The Throughput of ZigBee, WirelessHART, and ISA100 :(10ms TS ,11ms TS ,12ms TS, CSMA-CA)

Figure 6-3 shows the energy consumption of ZigBee, WirelessHART, and ISA100. The results show that ZigBee is an energy-efficient standard, and the reason is that ZigBee has a transmission power of 0dBm, whereas WirelessHART and ISA100 have a transmission power of 10dBm. This means that the power consumption in ZigBee is 10 times less than ISA100 and WirelessHART.

Figure 6-3 shows also that the greater the TS size the more the energy consumption. ISA100 at 10ms TS consumes the same amount of energy as WirelessHART.

ISA100 at slow hopping mode (CSMA-CA) consumes the highest energy. The reason is that during the CSMA-CA mode the nodes at the receiver side keep sensing the medium to receive the incoming traffic for the whole superframe duration.

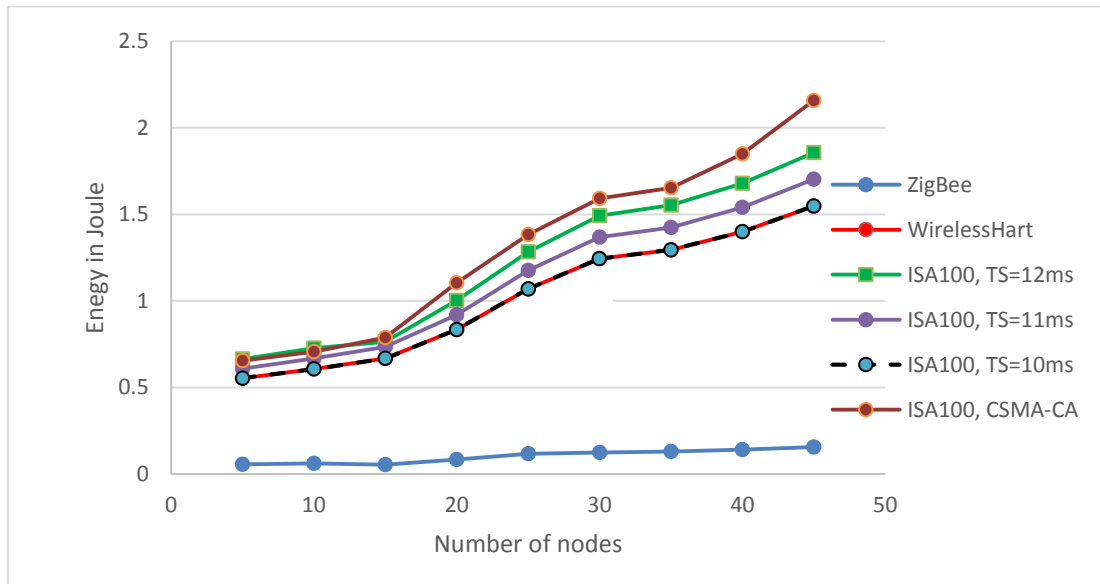


Figure 6-3 The Energy Consumption of ZigBee, WirelessHART, and ISA100 :(10ms TS ,11ms TS ,12ms TS, and CSMA-CA)

The second experiment is a comparison between the two operational modes in ZigBee, namely, the beacon-enabled mode and the non-beacon mode. In this experiment, there are five nodes, and the update interval varies from 5 to 1. The nodes transmit the sensing data to the ZigBee coordinator. The rest of the simulation parameters are shown in table 6-2

Table 6-2 Experiment 2 parameters

The parameter	The value
Number of Nodes	5
Traffic type	CBR
Traffic update interval	5, 4, 3, 2, 1
Transmission range	15 m
Routing protocol	AODV

Figure 6-4 shows the throughput value of ZigBee beacon-enabled mode non-beacon modes. The results show that the beacon-enabled mode enhances the ZigBee performance, especially at high traffic values. The guaranteed timeslots in the beacon-enabled mode partially solve the problem of the collided packets. In beacon-enabled mode there are up to seven contention-free timeslots, which can be assigned to different nodes.

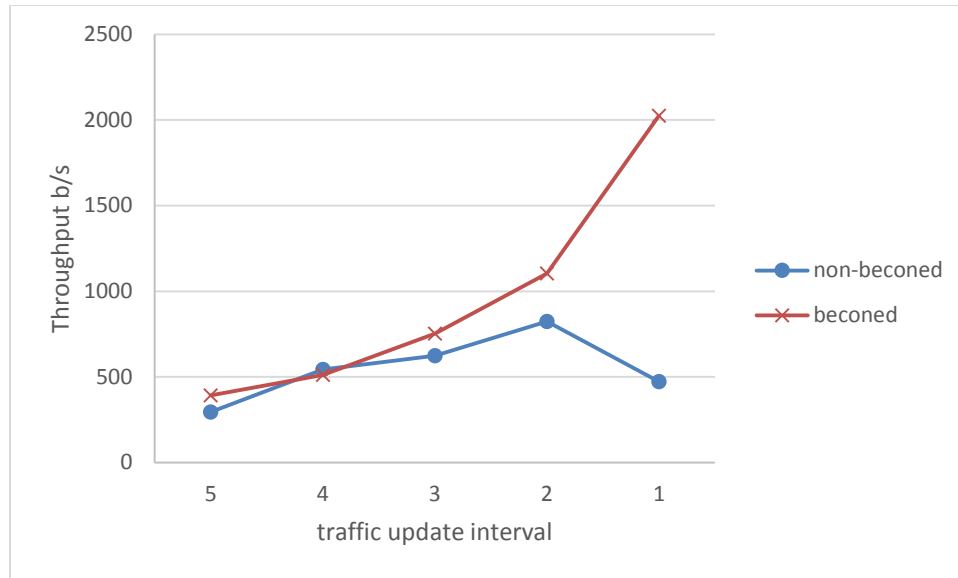


Figure 6-4 ZigBee Throughput Beacon-enabled vs non-beacon mode

The third experiment explores the effect of different time slot sizes on the end-to-end delay and throughput. The two standards WirelessHART and ISA100 are compared in this experiment.

In this experiment, five nodes are randomly distributed in 100*100 m² area. The nodes transmission range is 15 m, and the traffic type is CBR, the packet generation intervals (PGIs) are 1s, 0.5s, and 0.25s. The superframe interval varies from 16s to 0.5s

Figures 6-5 and 6-7 show the effect of the superframe duration on the end-to-end delay for WirelessHART and ISA100, respectively. This effect is clearly noticed at high traffic

values. When the superframe interval is 16s and traffic rate is high, a huge end-to-end delay occurs. This delay is a queuing delay since the nodes generate too much traffic but they have to wait for their turn. This delay decreases by reducing the superframe interval.

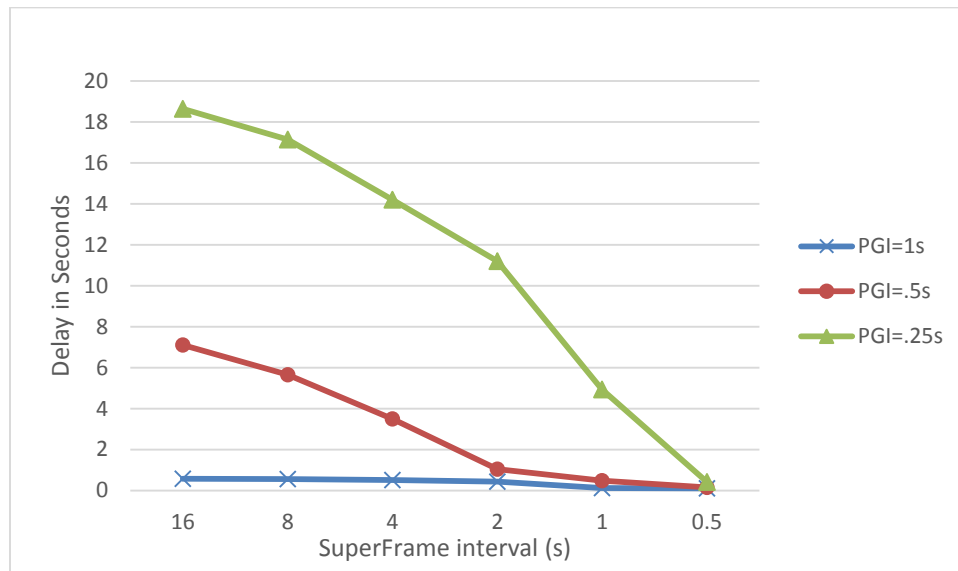


Figure 6-5 WirelessHART End to End Delay vs SuperFrame Interval

Figures 6-6 and 6-8 show the effect of the superframe duration on the throughput for WirelessHART and ISA100, respectively. The effect is clearly noticed at high traffic values. The shorter the superframe the higher the throughput value. This effect must be considered when deploying the nodes. The superframe interval must be carefully assigned by taking into account the node numbers and the traffic intensity.

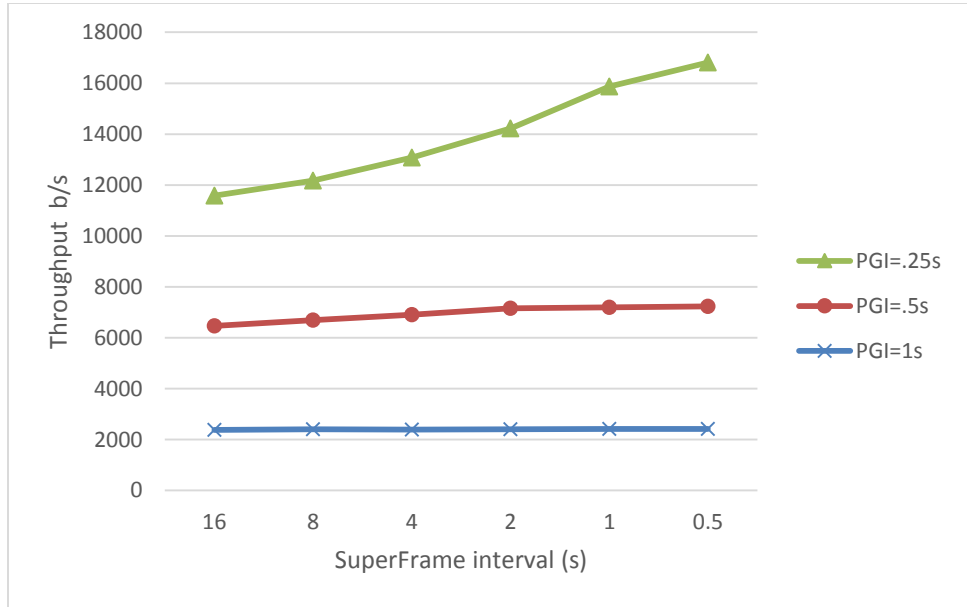


Figure 6-6 WirelessHART Throughput vs SuperFrame Interval

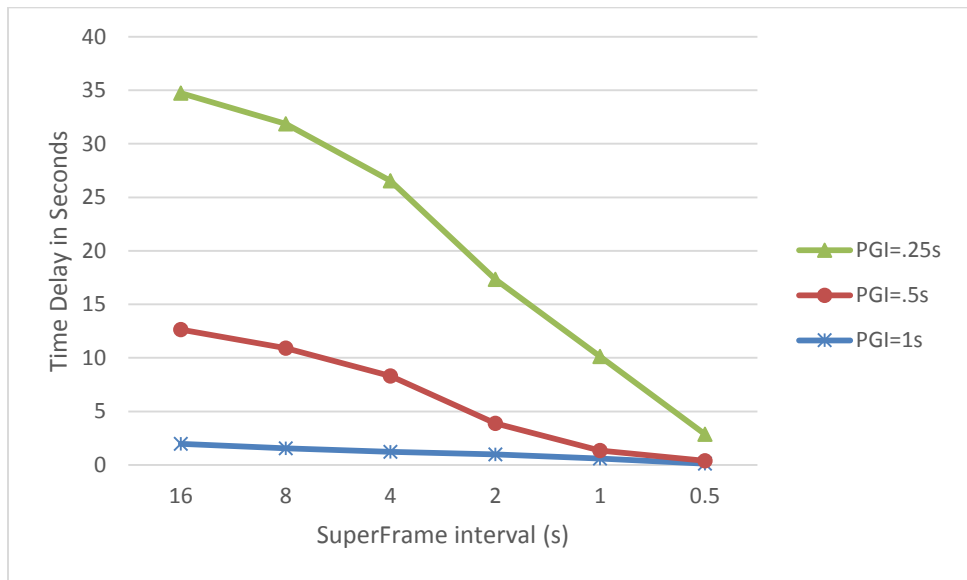


Figure 6-7 ISA100 End to End Delay vs SuperFrame Interval

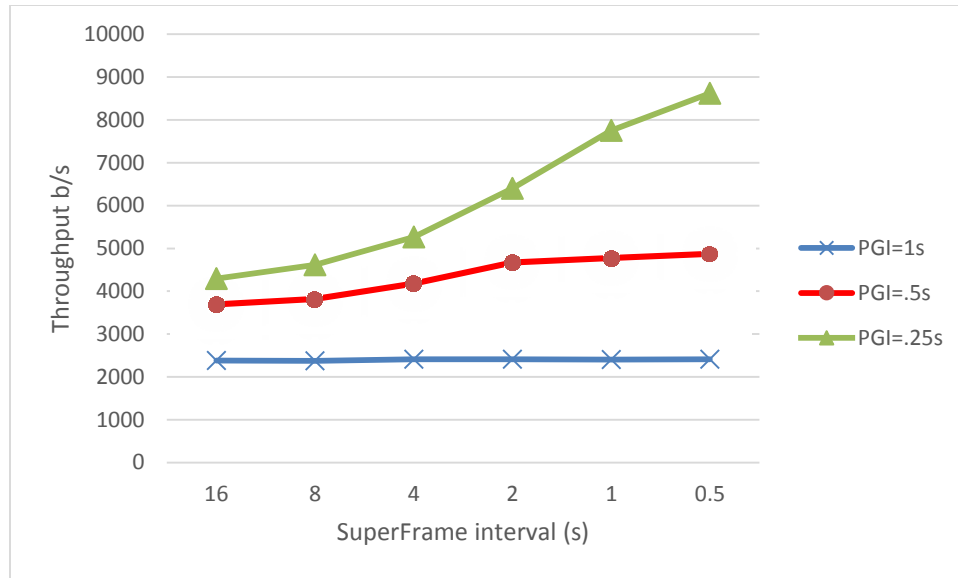


Figure 6-8 ISA100 Throughput vs SuperFrame Interval

6.2 Conclusion

In this work, a full review of the WSN Standards ZigBee, WirelessHART, and ISA100, has been conducted. In addition, a detailed review of the protocol layers for each standard is provided.

An ISA100 simulator in NS-2 has been developed. It is worth mentioning that this simulator is the first ISA100 simulator that supports routing. Hence, this work is the first real testing of ISA100's performance.

We performed a comparative study between ZigBee, WirelessHART and ISA100. The results showed that both ISA100 and WirelessHART outperforms ZigBee in terms of throughput. However, ISA100 consumes more power than WirelessHART and experiences higher end-to-end delay at 11ms TS and 12ms TS. The delay difference is not important in ISA100, since ISA100 is mainly developed for applications where 100ms delay is acceptable.

ISA100 gives more flexibility in choosing the timeslot size, for example, the ISA100 12ms slot size supports the nodes that have inaccurate timing to work.

The results also show that ZigBee is the best performance for time-sensitive and energy-efficient applications. Nevertheless, in terms of scalability and traffic intensity, it is the worst performance.

The selection of the superframe duration of the ISA100 and the WirelessHART influences the performance. For small networks, it is better to choose short superframe intervals. For

instance, the proper superframe size of 10 nodes network is 500ms or less. This choice reduces the average delay and increases the throughput.

ISA100 addressed some of the WirelessHART drawbacks, such as the strict timings of the 10ms timeslot for the nodes and the delay if a retransmission is required. For the strict timing, ISA100 has a configurable timeslot size in the range of 10-12ms, which reduces the need for strict clock timing. This issue is more obvious in multi-hop networks where synchronization over multi-hop is a big problem. For the delay of the retransmission, ISA100 uses a combination of slotted and slow hopping. In slow hopping, CSMA-CA is used and this mode of operation is targeted towards critical network operations such as retransmission of messages if an error happened, which means the node can immediately retransmit the message and does not need to wait its turn like the nodes in TDMA.

6.3 The Recommendations

For ZigBee standard, the hidden node problem and the exposed node problem can be solved by carefully positioning the nodes in the field, but it is recommended to use request to send / clear to send (RTS/CTS) to overcome this issue.

For WirelessHART, it is recommended to use different timeslot sizes instead of the fixed 10ms size. This will solve the problem of synchronization in multi-hop networks. Another recommendation is to use a standardized application layer to be compatible with other vendors.

For ISA100, it is recommended to use CCA mode 2 for carrier sensing in addition to the existing CCA mode 1 of ED.

References

- [1] Pedro Fernandez, Antonio J. Jara and Antonio F. G. Skarmeta, "Evaluation framework for IEEE 802.15.4 and IEEE 802.11 for Smart Cities", *IEEE conferences*, PP 421–426, July 2013.
- [2] Kok Seng Ting, Gee Keng Ee, Chee Kyun Ng, Nor Kamariah Noordin and Borhanuddin Mohd. Ali, "The Performance Evaluation of IEEE 802.11 against IEEE 802.15.4 with Low Transmission Power", *17th Asia-Pacific Conference on Communications (APCC), IEEE*, PP 850–855, October 2011.
- [3] Marina Petrova, Janne Riihijarvi, Petri Määhönen and Saverio Labella, "Performance Study of IEEE 802.15.4 Using Measurements and Simulations", *Wireless Communications and Networking Conference (WCNC), IEEE*, v1, PP 487–492, April 2006.
- [4] Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LRWPANs), IEEE Std. 802.15.4, 2006.
- [5] Sofie Pollin, Mustafa Ergen, Sinem Coleri Ergen, Bruno Bougard, Francky Catthoor, Ahmad Bahai, Pravin Varaiya, "Performance Analysis of Slotted Carrier Sense IEEE 802.15.4 Acknowledged Uplink Transmissions", *Wireless Communications and Networking Conference (WCNC). IEEE*, PP 1559–1564, April 2008.
- [6] Iyappan Ramachandran, Arindam Das, Sumit Roy, "Analysis of the contention access period of IEEE 802.15.4 MAC", *ACM Transactions on Sensor Networks (TOSN)*, V.3, PP 1-29, March 2007.
- [7] Pedram Radmand Alex Talevski, Stig Petersen and Simon Carlsen, "Comparison of Industrial WSN Standards," *4th IEEE International Conference on Digital Ecosystems and Technologies, IEEE*, PP 632-63, April 2010.
- [8] Bo Chen, Mingguang Wu, Shuai Yao, and Ni Binbin, "ZigBee Technology and Its Application on Wireless Meter-reading System", *International Conference on Industrial Informatics, IEEE*, PP 1257–1260, August 2006.
- [9] Tomas Lennvall, Stefan Svensson, and Fredrik Hekland, "A Comparison of WirelessHART and ZigBee for Industrial Applications", *International Workshop on Factory Communication Systems, IEEE*, PP 85 – 88, May 2008.

- [10] S. Tian-Wen and Y. Chu-Sing, "A Connectivity Improving Mechanism for ZigBee Wireless Sensor Networks", *International Conference on Embedded and Ubiquitous Computing, IEEE* , PP 495-500, December 2008
- [11] "Getting Started with ZigBee and IEEE 802.15.4," Daintree Networks, Feb 2008.
- [12] A.K.D.C.L. lianping Song; Song Han; Mok, M.; Nixon, M., "WirelessHART: Applying Wireless Technology in Real-Time Industrial Process Control", *Real-Time and Embedded Technology and Applications Symposium, IEEE*, PP 377-386, April 2008.
- [13] "HART Communication Foundation," <http://www.hartcomm.org/index.html>, 2007.
- [14] "The Components of WirelessHART Technology": HART Communication Foundation, 2009.
- [15] "ISAI00.11 a Release I Status," ISA 2008.
- [16] Fadillah Purnama Rezha and Soo Young Shin, "Performance evaluation of ISA100.11A industrial wireless network", *IET International Conference on Information and Communications Technologies (IETICT), IET*, PP 587-592, April 2013.
- [17] "ISAI00: Wireless Systems for Industrial Automation-Developing a Reliable, Universal Family of Wireless Standards," ISA, Standard 2007.
- [18] Yanjun Zhang, Siye Wang, Zhenyu Liu, Wenbiao Zhou and Dake Liu, "Performance Analysis of Wireless Sensor Network Based on NS-2", *International Conference on Systems and Informatics (ICSAI), IEEE*, PP 1445–1448, May 2012.
- [19] Raymond S. Wagner and Richard J. Barton, "Performance Comparison of Wireless Sensor Network Standard Protocols in an Aerospace Environment: ISA100.11a and ZigBee Pro", *Aerospace Conference, IEEE*, PP 1–14, March 2012.
- [20] Nguyen Quoc Dinh, Sung-Wook Kim, and Dong-Sung Kim, "Performance Evaluation of Priority CSMA-CA Mechanism on ISA100.11a Wireless Network", *International Conference on Computer Sciences and Convergence Information Technology (ICCIT)*, Nov 2010
- [21] Fadillah Purnama Rezha, and Soo Young Shin, "Performance Analysis of ISA100.11a Under Interference from an IEEE 802.11b Wireless Network", *IEEE Transactions on Industrial Informatics, IEEE, Volume: 10, Issue: 2*, May 2014

- [22] C.M. De Dominicis, P. Ferrari, A. Flammini, E. Sisinni, M. Bertocco, G. Giorgi, C. Narduzzi, F. Tramarin, "Investigating WirelessHART coexistence issues through a specifically designed simulator", *Instrumentation and Measurement Technology Conference, IEEE*, May 2009
- [23] Stig Petersen, Simon Carlsen, "Performance evaluation of WirelessHART for factory automation", IEE conference on Emerging Technologies & Factory Automation, IEEE, Sep 2009
- [24] Marcelo Nobre, Ivanovitch Silva, and Luiz Affonso Guedes, "Towards a WirelessHART module for the ns-3 simulator", Conference on Emerging Technologies and Factory Automation (ETFA), IEEE, Sep 2010
- [25] Pouria Zand, Arta Dilo, and Paul Havinga, "Implementation of WirelessHART in NS-2 simulator", *Emerging Technologies & Factory Automation (ETFA) Conference, IEEE*, Sep 2012
- [26] Jakub Neburka, Zdenek Tlamsa, Vlastimil Benes, Ladislav Polak, Ondrej Kaller, Lukas Klozar, Libor Bolecek, Ondrej Zach, Jan Kufa Jiri Sebesta, and Tomas Kratochvi, "Study of the Coexistence between ZigBee and Wi-Fi IEEE 802.11b/g Networks in the ISM Band", *Radioelektronika (RADIOELEKTRONIKA), 25th International Conference*, April 2015
- [27] Amirtipal Kaur, Jaswinder Kaur, and Gurjeevan Singh, "Simulation and investigation of ZigBee network with mobility support" *Advance Computing Conference (IACC), IEEE*, Feb 2014
- [28] Farahani, Shahin. (2008). ZigBee Wireless Networks and Transceivers. Newness: Poston, pp.33-122.
- [29] Zurawski, Richard. (2015). Industrial Communication Technology Handbook. CRC press: Florida, pp.31.1-32.7
- [30] Sen Kumar, Sunit. (2014). Fieldbus and Networking in Process Automation. CRC press: Florida, pp.315-380.
- [31] Pouria Zand, Emi Mathews, Paul Havinga, Spase Stojanovski, Emiliano Sisinni, and Paolo Ferrari, "Implementation of WirelessHART in the NS-2 Simulator and Validation of Its Correctness", *Sensors Journal*, pp.8633–8668, May 2014
- [32] Song Han, Xiuming Zhu, Aloysius K. Mok, Deji Chen, and Mark Nixon, "Reliable and Real-time Communication in Industrial Wireless Mesh Networks" *IEEE Real-Time and Embedded Technology and Applications Symposium, IEEE*, pp.3-12, May 2011.

- [33] J. M. Winter, C. E. Pereira, J. C. Netto, F. A. Souza, I. Muller, S. Y. C. Catunda, "Analysis of a Radio Physical Layer Fault in WirelessHART Networks", *International Instrumentation and Measurement Technology Conference Proceedings, IEEE*, May, 2016.
- [34] J.Jaslin deva gifti, K.Sumathi, "ZigBee Wireless Sensor Network Simulation with Various Topologies", *Online International Conference on Green Engineering and Technologies, IEEE*, NOV, 2016.

Vitae

Name :Jebril Ahmad Ali Battsh

Nationality :Palestinian

Date of Birth :10/15/1987

Email :Jebril.battsh@gmail.com

Address :YATTA-Palestine

Academic Background :MS. of computer Networks