MODIFIED CSMA/CA MAC STRATEGY FOR IOT ENABLE INTRA-VEHICULAR WIRELESS COMMUNICATION SYSTEMS

MD JAHAN ALI

Master of Science

UNIVERSITI MALAYSIA PAHANG

UNIVERSITI MALAYSIA PAHANG

DECLARATION OF THESIS AND COPYRIGHT

Author's Full Name : Md Jahan Ali

Date of Birth : 24 July 1990

Title : MODIFIED CSMA/CA MAC STRATEGY FOR IOT ENABLE INTRA-VEHICULAR WIRELESS COMMUNICATION SYSTEMS

Academic Session : SEMESTER 1, 2018/2019

I declare that this thesis is classified as:

☐ CONFIDENTIAL (Contains confidential information under the Official Secret Act 1997)*

☐ RESTRICTED (Contains restricted information as specified by the organization where research was done)*

☑ OPEN ACCESS I agree that my thesis to be published as online open access (Full Text)

I acknowledge that Universiti Malaysia Pahang reserves the following rights:

1. The Thesis is the Property of Universiti Malaysia Pahang
2. The Library of Universiti Malaysia Pahang has the right to make copies of the thesis for the purpose of research only.
3. The Library has the right to make copies of the thesis for academic exchange.

Certified by:

_____________________	_____________________
(Student's Signature)	(Supervisor's Signature)
_____________________	_____________________
Passport Number	Name of Supervisor
Date:	Date:

NOTE : * If the thesis is CONFIDENTIAL or RESTRICTED, please attach a thesis declaration letter.

SUPERVISOR'S DECLARATION

I hereby declare that I have checked this thesis and in my opinion, this thesis is adequate in terms of scope and quality for the award of the degree of Master of Science.

____

(Supervisor's Signature)

Full Name : DR. MD ARAFATUR RAHMAN

Position : SENIOR LECTURER

Date :

STUDENT'S DECLARATION

I hereby declare that the work in this thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at Universiti Malaysia Pahang or any other institutions.

____

(Student's Signature)

Full Name : MD JAHAN ALI

ID Number : MCC15006

Date : NOVEMBER, 2018

MODIFIED CSMA/CA MAC STRATEGY FOR IOT ENABLE INTRA-VEHICULAR WIRELESS COMMUNICATION SYSTEMS

MD JAHAN ALI

Thesis submitted in fulfillment of the requirements
for the award of the degree of
Master of Science

Faculty of Computer Systems and Software Engineering

UNIVERSITI MALAYSIA PAHANG

NOVEMBER, 2018

ACKNOWLEDGEMENTS

I am grateful and would like to express my sincere gratitude to my supervisor Dr. Md. Arafatur Rahman for his emerging ideas, invaluable guidance, continuous encouragement and constant support in making this research possible. He has always impressed me with his outstanding professional conduct, his strong conviction for science, and his belief that a master program is only a start of a life-long learning experience. I appreciate his consistent support from the first day I applied to graduate program to these concluding moments. I am truly grateful for his progressive vision about my training in science, his tolerance of my naive mistakes, and his commitment to my future career. I would also like to thank Dr. Muhammad Nomani Kabir for his help to develop MATLAB coding for my numerical modeling. I also sincerely thanks for the time spent for proofreading and correcting my many mistakes.

My sincere thanks go to all my lab mates and members of the staff of the Cmputer Systems and Software Engineering faculty, UMP, who helped me in many ways and made my stay at UMP pleasant and unforgettable. Many special thanks go to members of SysNet Lab research group for their excellent co-operation, inspirations and supports during this study.

I acknowledge my sincere indebtedness and gratitude to my parents for their love, dream and sacrifice throughout my life. I also acknowledge the sincerity of my parents, who consistently encouraged me to carry on my higher studies in Malaysia. I cannot find the appropriate words that could properly describe my appreciation for their devotion, support and faith in my ability to attain my goals. Special thanks should be given to my committee members. I would like to acknowledge their comments and suggestions, which was crucial for the successful completion of this study.

ABSTRAK

Konsep *Internet of Things* atau *Internet* untuk segalanya *(IoT)* boleh digunakan di dalam komunikasi kenderaan berikutan peningkatan mendadak di dalam nod peranti pengeran kerana permintaan tinggi terhadap aplikasi perlindungan, keselamatan, keselesaan yang berbeza. Bagi menjalankan komunikasi di antara nod-nod di dalam kenderaan, rangkaian kawalan jaringan beserta seni bina sambungan wayar merupakan solusi yang utama. Walau bagaimanapun, solusi ini tidak berdaya maju dan keanjalan kerana seni bina yang kompleks di dalam sambungan wayar beserta permintaan pengesan yang tinggi di dalam kenderaan; menyebabkan seni bina sambungan wayar digantikan dengan tanpa wayar. Selain itu, boleh skala merupakan isu utama dalam pengenalan konsep *IoT* di dalam *Intra-Vehicular Wireless Sensor Networks* atau Rangkaian peranti pengeran tanpa wayar intra-kenderaan *(IVWSNs). IoT* membolehkan *Intra-Vehicular Wireless Sensor Networks (IoT-IVWSNs)* yang merujuk kepada rangkaian di mana sejumlah besar peranti pengeran berhubung antara satu sama lain untuk berkongsi maklumat status kenderaan dalam membangunkan sistem kenderaan pintar. Bilangan nod peranti pengeran di dalam kenderaan telah meningkat secara mendadak berikutan dari peningkatan penggunaan kenderaan. Fenomena kesesakan lalu lintas menimbulkan masalah di dalam *IVWSNs* di mana bebanan lalu lintas serta bilangan peranti pengeran meningkat. Masalah ini dapat diselesaikan dengan mengurangkan had protokol *Media Access Control* atau Kawalan akses media *(MAC)* yang sedia ada. Dalam kajian ini, pertama sekali, adalah menyelidik prestasi rangkaian di dalam *IoT-IVWSNs* dengan protokol sedia ada dengan mempertimbangkan pelbagai parameter rangkaian yang dioptimumkan serta menentukan batasan-batasannya. Tambahan itu, kajian ini akan membincangkan reka bentuk senario IVWSN, komponen rangkaian, teknologi tanpa wayar yang sesuai dan parameter dalam menilai prestasi dan kebolehpercayaan rangkaian dengan cara yang berskala. Kedua, strategi *History Based CSMA/CA MAC* dicadangkan untuk mempertingkatkan lagi prestasi rangkaian dengan mengurangkan batasan di dalam persekitaran *IoT-IVWSNs*. Akhir sekali, prestasi rangkaian diuji melalui simulasi diskret berangka bagi menunjukkan dapatan berkesan yang diperolehi. Dapatan yang dihasilkan menunjukkan bahawa prestasi rangkaian meningkat 75% dari segi metrik prestasi rangkaian kelewatan hujung-ke-hujung.

ABSTRACT

The concept of the Internet of Things (IoT) can be utilized in vehicular communication since the number of sensor nodes is raising tremendously because of the uplifting demand of different secure, safety and convenience applications. In order to do the communication among these nodes inside the vehicle, controller area network with wired architecture provides a prominent solution. However, this solution will not be viable and flexible because of the architectural complexity of wire connections in the demand of a large number of sensors inside the vehicle; hence the wired architectures are replaced by wireless ones. Moreover, scalability will be an important issue while introducing the IoT concept in Intra-Vehicular Wireless Sensor Networks (IVWSNs). The IoT enabled Intra-Vehicular Wireless Sensor Networks (IoT-IVWSNs) refer to the network where a large number of sensors are connected with each other for sharing the vehicle's status information to develop a smart vehicular system. The number of sensor nodes in the vehicle has increased significantly due to the increasing vehicular applications. The phenomenon of congestion poses a problem in the IVWSNs where the traffic load and the number of sensors are increased. These problems can be resolved by mitigating the limitation of the existing Media Access Control (MAC) protocols. In this study firstly, it is investigated the network performance in IoT-IVWSNs with existing protocol by considering different optimized network parameters and defines the limitations. Moreover, it discusses the design of IVWSN scenario, network components, suitable wireless technology and parameters for evaluating the performance and network reliability in a scalable fashion. Secondly, a History-Based CSMA/CA MAC strategy is proposed to minimize the end to end of the network. The developed new MAC improves the network performance by reducing the limitations in the IoT-IVWSNs environment. Finally, the performance has been tested through discrete numerical simulation to show the result effectively. The results show that the network performance is increased 75% approximately in term of network performance metrics end-to-end delay.

TABLE OF CONTENT

DECLARATION

TITLE PAGE

ACKNOWLEDGEMENTS ii

ABSTRAK iii

ABSTRACT iv

TABLE OF CONTENT v

LIST OF TABLES ix

LIST OF FIGURES x

LIST OF SYMBOLS xi

LIST OF ABBREVIATIONS xii

CHAPTER 1 INTRODUCTION 1

1.1 Background and Motivation 1

1.2 Problem Statement 4

1.3 Research Aims and Objectives 6

1.4 The scope of the Research 6

1.5 Research Methodology 7

1.5.1 Phase 1: Literature Survey and Identify Problem Statements 7

1.5.2 Phase 2: Design and Implementation 7

1.5.3 Phase 3: Proposed Method and Validation 8

1.5.4 Phase 4: Result and Summary 8

1.6 Organization of the Thesis 10

CHAPTER 2 LITERATURE REVIEW **11**

2.1 Introduction 11

2.2 Emergence of WSNs and IoT 11

2.3 Vehicular Wireless Sensor Networks 12

2.3.1 Inter-Vehicular Communication 13

2.3.2 Intra-vehicular Wireless Sensor Networks (IVWSNs) 14

2.4 The Concept of IoT in IVWSNs 17

2.5 Technologies in IoT Paradigm 18

2.5.1 Technology 21

2.6 Challenges for IoT Enabled IVWSNs 26

2.6.1 MAC Layer Issue 26

2.6.2 Energy Consumption Issue 27

2.6.3 Scalability Issue 28

2.6.4 Miscellaneous Challenges 29

2.7 Description of the IEEE 802.15.4 Slotted MAC Protocol 29

2.7.1 Approaches to Improve IEEE 802.15.4 MAC 34

2.8 Comparative Study to others with IEEE 802.15.4 MAC 41

2.9 Critical Discussion on IVWSNs 43

2.10 Summary 50

CHAPTER 3 RESEARCH DESIGN AND METHODOLOGY **51**

3.1 Introduction 51

3.2 System Design and Implementation for Development of the First Research Gap 54

3.2.1 Developing IoT Enabled IWVSNs 54

3.2.2 Network Components 55

3.2.3 Network Architecture 56

3.2.4 System Design and Implementation 57

3.2.5 Implemented Technology for IoT-IVWSNs 59

3.3 System Design and Implementation for Development of the Second Research Gap 60

3.3.1 Proposed MAC Solution: History-Based MAC 60

3.3.2 Communication Parameters Selection 62

3.3.3 Validation 63

3.3.4 Result Analysis and Documentation 64

3.4 Network Simulator OPNET 64

3.5 Summary 67

CHAPTER 4 RESULTS AND DISCUSSION 68

4.1 Introduction 68

4.2 Performance Investigation of IoT-IVWSNs 68

4.2.1 Performance Analysis of IoT-IVWSNs 69

4.2.2 Link analysis between End-Device and Central Entity 70

4.2.3 Performance Evaluation 73

4.3 Performance Evaluation of Proposed Solution: History-based MAC for IoT-IVWSNs 76

4.3.1 Proposed Solution: History-Based CSMA/CA MAC for IVWSNs 77

4.4 Validate the Proposed Solution: History-Based MAC 80

4.4.1 Experimental Setup 80

4.4.2 Simulation Results 83

4.5 Summary 90

CHAPTER 5 CONCLUSION AND RECOMMENDATIONS 91

5.1 Concluding Remarks 91

5.2 Contributions 91

5.3 Limitations 93

5.4 Future Work 93

REFERENCES 95

APPENDIX A SAMPLE APPENDIX 1 108

APPENDIX B SAMPLE APPENDIX 2 109

LIST OF TABLES

Table 2.1	Description of IEEE 802.15.4 Attributes and Parameters	31
Table 2.2	Comparison of different improving approaches of IEEE 802.15.4	39
Table 2.3	Comparison table among existing major technologies	42
Table 2.4	Summary of literature review	47
Table 4.1	Communication Parameters	74
Table 4.2	Communication Parameters for History-based MAC for IVWSNs.	81
Table 4.3	Different combinations of traffic load.	82

LIST OF FIGURES

Figure 1.1	Research process in this thesis	9
Figure 2.1	ECUs and CAN networks interface	15
Figure 2.2	Estimated number of devices connected to the internet from 2012 to 2020.	19
Figure 2.3	Google search trends since 2004 for terms Internet of Things, Wireless Sensor Networks, Ubiquitous Computing.	20
Figure 2.4	Internet of Things enabling environments	21
Figure 2.5	ZigBee stack architecture	23
Figure 2.6	ZigBee network topology	24
Figure 2.7	Superframe structure of IEEE 802.15.4	30
Figure 2.8	Flowchart of slotted CSMA/CA algorithm	33
Figure 2.9	IEEE 802.15.4 classifications to improve the performance	35
Figure 3.1	Flowchart of the methodology.	53
Figure 3.2	IoT enabled IVWSNs scenario	55
Figure 3.3	Network architecture and its data flow	56
Figure 3.4	Flowchart of History-based CSMA/CA algorithm	61
Figure 3.5	Simulation scenario for 70 EDs	66
Figure 3.6	Parameter setup for the coordinator	66
Figure 4.1	Effects of Log-normal Shadowing on the received power.	72
Figure 4.2	CDF versus End to End Delays: varying Traffic-Load and Network Size.	75
Figure 4.3	History based Slotted CSMA/CA MAC algorithm	78
Figure 4.4	Performance comparisons between traditional and proposed solution: History-based MAC in the scenario I	85
Figure 4.5	Performance comparisons between traditional and proposed solution: History-based MAC in scenario II	86
Figure 4.6	Performance comparisons between traditional and proposed solution: History-based MAC in scenario III	87
Figure 4.7	Performance comparisons between traditional and proposed solution: History-based MAC in scenario IV	88
Figure 4.8	Performance analysis between the proposed solution: History-based MAC with single BS and traditional MAC with multiple BSs.	89

LIST OF SYMBOLS

dBm	Decibel-milliwatts
d	Distance
P_L	Path loss
P_t	Transmit power
P_r	Receiver power
C_f	Carrier frequency
Rs	Receiver sensitivity
Xσ	Gaussian random variable
σ	Shadowing deviation
γ	Path loss exponent

LIST OF ABBREVIATIONS

BE	Backoff Exponent
BEB	Binary Exponent Backoff
CAN	Controller Area Network
CAP	Contention Access Period
CCA	Clear Channel Assessments
CEF	Contention-Free Period
CSMA/CA	Carrier Sense Multiple Access-Collision Avoidance
CU	Control Unit
ECU	Electronic Control Unit
ED	End Device
FFD	Full Function Device
GST	Guaranteed Time Slot
IoT	Internet of Things
ITS	Intelligent Transportation System
IVWSNs	Intra-Vehicle Wireless Sensor Networks
IoT-IVWSN	IoT enabled Intra-Vehicle Wireless Sensor Networks
IVS	Intelligent Vehicular System
NB	Number of Backoff Stages
MAC	Medium Access Protocol
PAN	Personal Area Network
PHY	Physical
PU	Processing Unit
RFD	Reduced Function Device
RFID	Radio Frequency Identifier
SBE	Saved BE
SNB	Saved NB
UWB	Ultra-wideband
VANETs	Vehicular Ad-hoc Networks
V2V	Vehicle-to-Vehicle
V2I	Vehicle-to-Infrastructure
WSNs	Wireless Sensor Networks

CHAPTER 1

INTRODUCTION

1.1 Background and Motivation

Internet of Things (IoT) is an environment where objects are tagged with smart devices (e.g., sensor, actuator, etc.) having unique identifiers and able to transfer information throughout the network without involving human interaction(Conti, Dehghantanha, Franke, & Watson, 2018; X. Li et al., 2018). The IoT is an emerging concept that introduces several new paradigms in communication such as, Device-to-Device (D2D), Machine-to-Machine (M2M) communication. It can also work with existing networks (e.g., Monitoring and Rescuing Network, Intra-vehicular Network, Inter-vehicular network, etc.) in order to design fully automated smart system (Gubbi, Buyya, Marusic, & Palaniswami, 2013). With the advance of Wireless Sensor Network (WSN) technology, the IoT environment is essential to interface with the sensor node for collecting the sensor data. Recently a variety of adaptation emerging IoT enabling wireless technologies is available such as Radio-frequency Identification (RFID), Bluetooth, Ultra-Wide Brand (UWB) and ZigBee for embedded sensor and actuator nodes. Now a day, the modern vehicles are equipped with various kind of sensor for safety purpose. The researchers expect that vehicles will be equipped with a large number of sensors by 2020 (Lu, Cheng, Zhang, Shen, & Mark, 2014; Pinelis, 2013).

However, there are several wired technologies such as Controller Area Network (CAN) FlexRay, TTEthernet, that need wire connection between ECUs and sensors for designing intra-vehicle communication. Among them, CAN is one of the widely used communication architecture for wired intra-vehicular communications. The serial communication paradigm of the CAN makes it highly secure and robust for real-time vehicular systems. However, the CAN may not be efficient and flexible because of the growing architectural complexity of the modern vehicles. Hence wired architecture is replaced by wireless one (Jin, Kwak, & Kwak, 2012). Additionally, there is harsh and complex architecture inside vehicle occurs because of limited spaces and wires and its others accessories increase the weight (up to 50 kilograms) of the vehicle significantly (Ahmed et al., 2007a). Furthermore, the wired solution is not scalable and viable because of the internal structure and complexity of vehicular structures (Takayama & Kajiwara, 2016). With the increasing number of sensors inside modern vehicles due to the reliability and safety requirement, it requires integrating more wire connections for implementation. As a result, the weigh, complexity and manufacturing cost will increase. Due to these reasons, the Intra-Vehicle Wireless Sensor Networks (IVWSNs) have recently been focused to minimize the above complexity in the automotive industry (Tuohy et al., 2015). High growth of the sophisticated electronic systems inside the modern vehicles raises the necessity of deploying more number of sensors to monitor them. To fulfill this aim, the concept of IoT can be introduced in intra-vehicular communication, referred as IoT enabled Intra-Vehicle Wireless Sensor Networks (IoT-IVWSNs). It is a network where a large number of sensors are connected to each other for sharing the vehicular status to develop a smart vehicle system.

The IVWSN has tremendous benefits over wired technology inside the vehicle. Especially, the short-range wireless sensor technology offers many opportunities as mentioned below:

- Wireless sensor communications eliminate the wiring harness or the complex connections which are responsible for exposing sensor related faults. Moreover, wireless sensor connections minimize the maintenance cost and increase the reliability of the communication.

- Fewer sensor variants are leading to reduced overhead since variations in sensor pigtails, and connector encoding require additional administration and inventory.

- Easier installation of sensors on the assembly line due to the elimination of harness routing a predominantly manual operation because a wireless sensor offers a single point of installation.

- New possibilities for sensing, since there are areas of the vehicle where physical and logistical difficulties in deploying a wire harness would usually preclude the installation of a wired sensor.

Vehicle wireless sensor technologies and various communication protocols have the potential to strengthen several new and revolutionary applications. These innovative developments can greatly develop the safety, privacy, and convenience value of new vehicles, as well as infotainment and telematics functions. Positive progressions in the next generation vehicle inter-communications will enable communication all-around the world, the embedded appliances and with each other, making each vehicle a communications hub.

In addition, the scalability will be an important issue while introducing IoT on IVWSNs. Since the different types of sensor nodes increase day by day inside the vehicles for improving driver assistance and vehicle safety. The existing network becomes congested and the traffic load significantly increases (Singh & Lobiyal, 2013). To overcome these problems, ZigBee wireless sensor technology is a good candidate for implementing IoT concept in IVWSNs. The ZigBee supports more end devices comparing with others wireless technologies such as Bluetooth, Wi-Fi, or RFID (Xia & Song, 2017; Zulkifli & Noor, 2017). It provides a robust, reliable, low cost, low power, a self-configuring mesh network with strong security tools and total interoperability (Lu et al., 2014; Rahman, 2014a). In short, ZigBee is a low cost, low power wireless technology developed by Open Global Standard. It is built upon PHY layer and MAC layer for IEEE 802.15.4 standard which operates in unlicensed bands at 2.4GHz, 900MHz and 868MHz for low rate WPANs (Hashemi, Si, Laifenfeld, Starobinski, & Trachtenberg, 2013).

This work investigates the performance in IoT enabled IVWSNs with the promising protocol IEEE 802.15.4. Furthermore, it proposes a History-based MAC strategy on IEEE 802.15.4 to improve performance in term of end to end delay by mitigating the congestion and collision problem in the network.

1.2 Problem Statement

Ubiquitous sensing enabled by Wireless Sensor Network (WSN) technologies involves many areas in the modern day. The expansion of these devices in a communicating actuating network system creates the Internet of Things (IoT), wherein sensors and actuators combine seamlessly with the environment around us, and the information is shared across platforms to develop a smart environment system (Al-Fuqaha, Guizani, Mohammadi, Aledhari, & Ayyash, 2015; Conti et al., 2018). Moreover, the modern vehicles are also furnished with various types of sensors such as water level temperature, detecting road condition, monitoring the aside obstacles, overseeing fuel tank, checking speed sensor, etc. Recently, researchers estimated that the number of sensor nodes inside the vehicle will significantly increase to 200 by 2020 (Lu et al., 2014; Pinelis, 2013). As the number of sensor node keeps increasing inside the modern vehicle, the cost, more sensor installing complexity, and weight associated with others integrated parts are also growing tremendously (Bas & Ergen, 2013). With these scenarios in mind, this thesis defines the term IoT-IVWSN as "an IoT enabled Intra-Vehicle Wireless Sensor Networks (IoT-IVWSNs) where a large number of sensors are connected to each other for sharing the vehicular status in order to develop a smart vehicle system." Hence, such a network of a large number of sensor nodes in intra-vehicle wireless sensor communication should be carefully designed such as efficient communication protocol, network architecture, and associated others parameters.

The IEEE 802.15.4 MAC is a good protocol for designing IVWSNs since it supports a large number of end devices (Singh & Lobiyal, 2013). For efficient communication, the IEEE 802.15.4 protocol includes the collision resolution mechanism called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), which allows sensor devices to avoid packet collision caused by multiple simultaneous transmissions. However, in the Contention Access period (CAP), it tolerates collision-free communication in a certain number of nodes, and after exceeding these numbers it began to increase retransmission process which further maximizes the packet loss and degrades the network performance. The traditional CSMA/CA mechanism of this protocol has two main problems. First, aggressive binary exponential backoff may hamper the efficient communication of sensors. Whenever a

Clear Channel Assessment (CCA) reports that the channel medium is not clear, sensors simply increment the Binary Exponent (BE) at a time up to the maximum value (maxBE). This mechanism can waste idle slits and eventually result in throughput degradation since it may impetuously increase the BE even under a transient channel busy condition. Moreover, BE is simply reset to the initial value (minBE) upon a successful transmission or a packet drop. As a result, sensors may frequently suffer from meaningless backoffs and additional CCAs due to the initialized BE that is insufficient to resolve the current network contention level. Second, the sporadic CCA operation decreases not only energy efficiency but also network throughput. The sensors do not know whether or not there is an ongoing transmission while they are counting down from $2^{BE} - 1$. This may also result in a waste of energy and bandwidth since they should perform a meaningless CCA and succeeding backoff if the backoff timer expires under busy channel conditions.

The slotted CSMA/CA mechanism in a CAP, the sensor node maintains two parameters namely, the number of backoffs (NB) and backoff exponent (BE) for every structure of the data frame. When a sensor wants to transmit, it initiates the BE from the minimum backoff value (minBE) and the NB chosen from randomly from the range 0 to $2^{BE} - 1$. After selecting the BE and NB randomly, the sensor carries out for CCA to check the channel medium at the backoff boundary. The sensor can transmit the data frame only when two consecutive CCA reports channel is idle. On the other hand, if either of those two CCAs reports that the channel is busy, NB is incremented, and an additional random backoff process is initiated, as long as NB does not exceed the maximum value for backoff retries (maxNB). In addition, BE is incremented up to maxBE, and thus the range of backoff period will be randomly chosen from 0 to $2^{\min(BE, maxBE)} - 1$. The above procedure will continue until successful transmission. However, the above procedures are designed without proper consideration of practical environments such as various traffic loads, a large number of sensor nodes in a certain domain, and designing scalable network phenomena (Jung, Lee, Lim, & Suh, 2014). Therefore, it is likely to suffer from severe performance degradation, especially under heavy traffic load and increased a large number of sensor nodes.

Furthermore, to implement the CSMA/CA of IEEE 802.15.4 mechanism in IoT enabled IVWSNs, it is very important to investigate whether the IEEE 802.15.4 MAC protocol can provide a suitable solution for such an IoT-IVWSNs. It can be assumed easily that the existing mechanism will not perform better due to the collision and congestion of the network because of the high traffic of the large network. In order to mitigate those issues, a CSMA/CA MAC mechanism is needed to design for such kind of environment. Additionally, large numbers of sensor nodes are needed to place inside the vehicle. So the network scenario should be well designed and network performance will be evaluated. The problem is considered while designing the network scenario and provides the optimum solution to design an intelligent vehicle.

1.3 Research Aims and Objectives

The aim of this thesis is to conduct a study thorough of the IEEE 802.15.4 MAC protocol and develop a mechanism with efficient enhancements its algorithm which is suitable for IoT enabled IVWSN. In more details, this study considers the following objectives:

- To investigate the performance of existing protocols on IoT enabled IVWSNs and identify the limitations.
- To modify the MAC strategy for IoT enabled IVWSNs to overcome the identified limitations.
- To implement and validate the performance through the numerical simulations.

1.4 The scope of the Research

The research scope of this thesis mainly comprises the area of wireless sensor communication inside the vehicle. To implement the IoT concept with wireless communication inside the vehicle, this work has considered the suitable wireless communication technology. To validate the proposed solution, a numerical network simulator “OPNET” is used with its ZigBee wireless sensor technology module.

The following key points incorporate in the research scope:

- The ZigBee wireless sensor technology which includes
- Protocol IEEE 802.15.4

- CSMA/CA MAC strategy for WSNs application
- Topology used for the network
- Star topology
- Nodes use for the simulation
- Maximum 110 sensor nodes which are deployed randomly within one to six meters
- Simulation tools
- OPNET network simulator 14.5 which support the star topology.

1.5 Research Methodology

The key research procedure in this thesis involves four phases which are discussed in the following: (1) the first phase is focused on describing the problem statements by conducting a literature survey in this thesis. (2) The second phase concentrates design issue of MAC and investigates the problem while IoT is introducing with IVWSN. (3) The third phase describes the proposed MAC strategy and validates the expected requirements. (4) Finally, the fourth phase describes the result and discussion with ascertaining explanation and subsequently the summary is presented with future recommendations. Figure 1.1 summarizes the phases that involved the research methodology.

1.5.1 Phase 1: Literature Survey and Identify Problem Statements

The extensive critical literature survey guides on existing different MAC protocols in IVWSN towards some directions to design a suitable strategy of MAC. This phase defines different challenging issues on designing IoT-IVWSN. The designing issues include reliability, scalability, energy consumption, and enabling IoT with IVWSN. Finally, related work is presented with a tabular diagram.

1.5.2 Phase 2: Design and Implementation

To establish reliable and robust communication, the design and implementation phase has been designed by considering the issue that has been identified. The system design issue includes High Reliability, Short End to End Delay, Low Power Consumption, Low Data Throughput, Low Duty Cycle, Low-Cost Privacy, and Security. The network components and network architecture are also presented.

1.5.3 Phase 3: Proposed Method and Validation

A History-Based CSMA/CA MAC strategy has been proposed for IoT-IVWSN has been tested with numerical discrete simulation and details about the results of the testing.

1.5.4 Phase 4: Result and Summary

At this phase, the experimental results are analyzed, and a detailed discussion has been made. In the consequent phases, the success of the proposed solution is evaluated. Finally, a summary is presented with future recommendations.

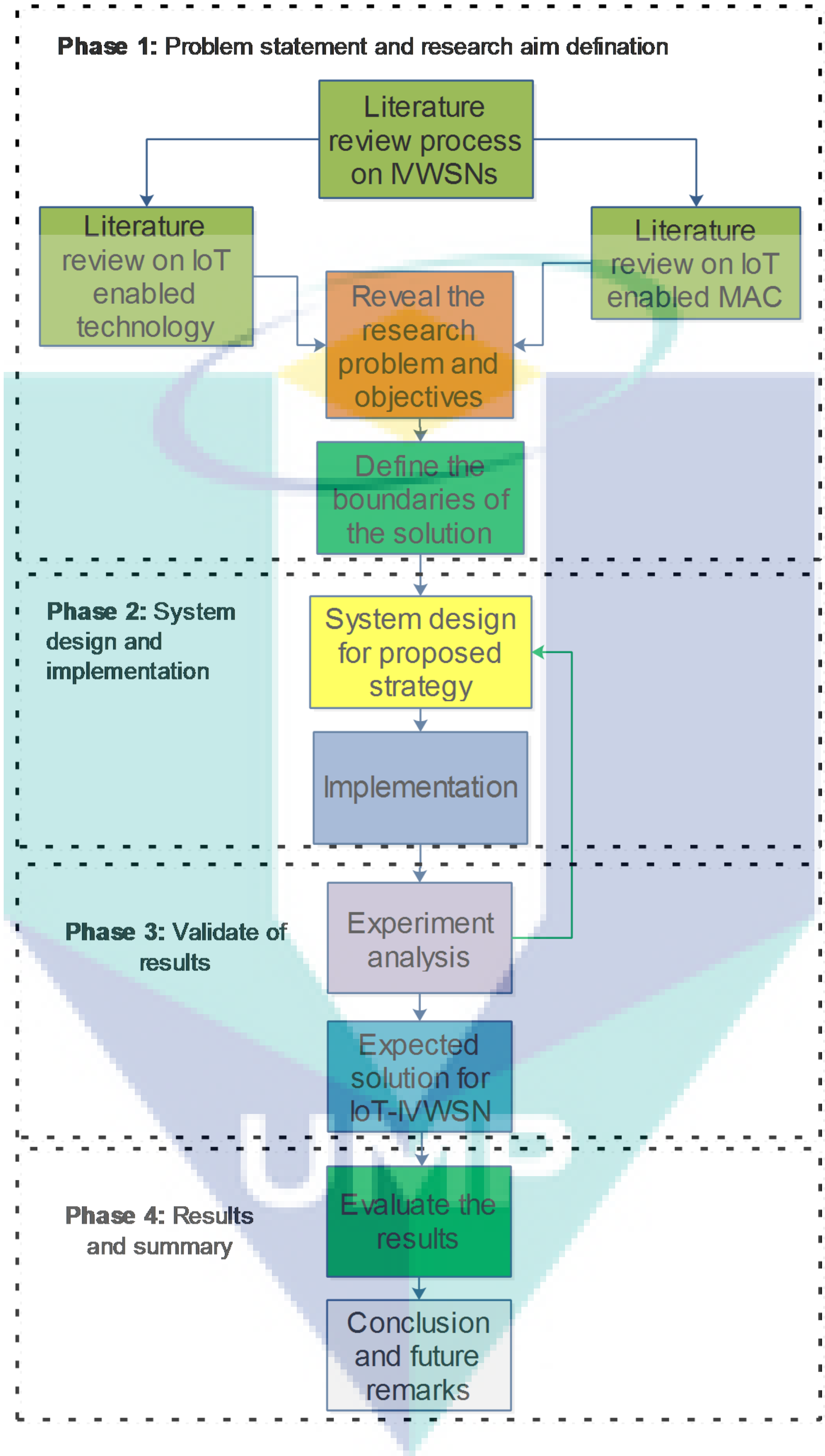


Figure 1.1 Research process in this thesis

1.6 Organization of the Thesis

This thesis contains five chapters namely, Introduction, Literature Review, Design and Methodology, Result Analysis and Discussion, and Conclusion and Recommendation. The rest of the thesis is organized as follows:

Chapter 1 introduce the work incorporating the problem statement, objectives, research scope, methodology of the research, and the scope of the research.

Chapter 2 presents the related works and the finding of their limitations and the current research direction.

In Chapter 3, research design and methodology will be provided.

Computational result and discussion on evaluating the concept by choosing the different criteria are given in Chapter 4.

Finally, in Chapter 5, the conclusion and recommendation are provided including the main finding of the work and the outline of the future directions with potential research areas.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter presents an extensive literature review on different Wireless Sensor Network (WSN) in the vehicular communication systems. It also includes the IoT concept to integrate with such type of environment. It discusses the vehicular wireless sensor network that is divided two main research areas named inter vehicular communication and intra-vehicular communication. This chapter focuses mainly on the intra-vehicular communication with wireless sensor technology. The Zigbee/IEEE 802.15.4 is considered for this communication. Moreover, it investigates the different approaches of IEEE 802.15.4 MAC protocol to find suitable method. Finally, it finds the research gaps by doing extensive literature on intra-vehicular wireless sensor communication.

2.2 Emergence of WSNs and IoT

WSN is an emerging solution to enable the physical devices into a smart object. It has several important applications that are being used for real-time tracking and monitoring the remote environment. Rapidly expanding the automotive microelectronics system for increasing safety, security, observing critical electronics system, acquiring information from surrounding environments, the low-cost, energy consumption, highly secured, and reliable communication wireless sensor technology has become an active research area in the field of automotive wireless communication (P. Huang, Xiao, Soltani, Mutka, & Xi, 2013; Parthasarathy, Whiton, Hagerskans, & Gustafsson, 2016; Yang, 2014). Recently, with increasing automotive intelligence, modern vehicles are furnished by different types of sensor such as water level temperature, detecting road condition, monitoring the aside obstacles, fuel tank, speed sensor, and blind zone alert sensor. As a result, the numbers of sensors inside the vehicle are increasing every year significantly.

Moreover, it is estimated to extend to 200 sensors in a vehicle (Lu et al., 2014). Such a large number of sensors are not easy to implement inside a vehicle traditionally. As a result, the network will be large, and the collision, as well as the congestion, will happen among the sending data of the network. To solve this problem, an intra-vehicle wireless sensor communication network should be properly designed. The concept of IoT, where the large numbers of nodes are interconnected with others can be carried out an important role in eliminating those difficulties.

The IEEE 802.15.4 standard is a group of specifications suggested to use WSNs and in IoT paradigm (S. Li, Da Xu, & Zhao, 2015; Sheng et al., 2013). The wide range of applications influenced by the advent of WSNs, combined with the various performance demands of those applications, have enticed the study community to concentrate on improving IEEE 802.15.4 MAC to mitigate its shortcomings. IEEE 802.15.4 MAC happens to be underneath the range of research interest for over ten years, with various goals encouraging different research teams. These goals consist of primarily reducing energy usage, enhancing channel utilization/throughput, enhancing packet distribution ratio/reliability, reducing the likelihood of a collision, and reducing end-to-end delays. Into the remainder of this chapter, an extensive literature review has been made on vehicular sensor networks that will include Inter-vehicle, Intra-vehicle, associated emerging technologies and the IoT enabling concept in-vehicle network by exploring the targeted enhancing IEEE 802.15.4 MAC protocol.

2.3 Vehicular Wireless Sensor Networks

The vehicular wireless sensor network is a promising paradigm as Intelligent Transportation System (ITS) to make the safety roads and reduced congestion (An, Lee, & Shin, 2011; Zhou, Cao, Zeng, & Wu, 2010). The usage of sensor nodes and its systems are used to identify road end automobile phenomena and deliver sensor data to appropriate entities that provide towards the concept of Vehicular Sensor Networks (VSNs). VSNs are a subset of Vehicular Ad-hoc Networks (VANETs) placed either in automobiles or alongside roadways producing a reliable end-to-end network for disseminating sensor information collected from a vehicular environment. With regards to the communication path, VSNs encompass Vehicle-to-Infrastructure or Infrastructure–to-Vehicle (V21 and I2V, correspondingly) architectures and Vehicle-to-Vehicle (V2V) architecture (Lu et al., 2014). The previous traditional way addresses communication between sensors from a vehicular environment and particular path Side devices or outside gateways, whereas the latter one describes the communication among sensors in a vehicular environment in a random. The VSNs are commonly examined and turned out to be invaluable for supporting vehicle and road security, traffic pattern analysis, road area diagnosis, metropolitan ecological monitoring, road degree polluting of the environment monitoring, and several other transport application systems. There increasing appeal emphasizes the necessity to the analysis of the appropriate features so that it can pave the way how toward VSNs' complete practical implementation.

2.3.1 Inter-Vehicular Communication

Inter-vehicular communication (IVC) is an interesting emerging area of research that provides the improvement of the current advances in microprocessing control and electronic equipment. It sets inside the vehicles to improve wireless communication features with different sensor devices in the environment (Jawhar, Mohamed, & Zhang, 2010).

It is commonly considered that the advances of inter-vehicle communications will reshape the ongoing future of road transport systems in where inter-connected vehicles are no more information-isolated. In the form of inter-vehicle communications or V2V communications, information produced by the vehicle-borne computer, control system, onboard sensors, or people are efficiently disseminated among automobiles in proximity, or even to automobiles numerous hops away in a vehicular ad hoc network (VANET). Without the support of any built infrastructure, a number of active road security applications (e.g., collision detection, lane changing alert, and cooperative merging) and infotainment applications (e.g., interactive video gaming, and file along with other valuable information sharing) are enabled by inter-vehicle wireless links (Hartenstein & Laberteaux, 2010). VANETs have attracted extensive research attentions for many years, and how to establish efficient and reliable wireless links between vehicles is a major research focus. The long-range communication technology is used for in the inter-vehicular communication like WiMax, LTE and other long-range technology.

Security, integrity, availability, reliability, and safety are one of the primary needs for the IVC systems. However, designing wireless communication in IVC is challenging due to the result of packet collisions, channel fading, shadowing while the Doppler changes because of the high level of speed of vehicles. It is then a huge challenge to manage sensor nodes that travel at high speed. The latency requirement is critical, due to the high rate for the cars. Safety requirements are crucial (Lu et al., 2014).

IVC systems involve two categories of communication; which are

(i) Vehicle-to-Vehicle (V2V) communication: In V2V communication, vehicles keep in touch with one another to be able to help various applications and solutions such as cooperative motorist help and decentralized moving vehicle information (e.g., traffic state monitoring information).

(ii) Vehicle-to-Infrastructure (V2I) communication: In this sort of communication, automobiles have the ability to communicate with fixed infrastructure alongside associated with the road so that it can offer individual communication and information services.

2.3.2 Intra-vehicular Wireless Sensor Networks (IVWSNs)

Due to the exponential growth of intelligent electronic devices in vehicles, the intra-vehicle wireless sensor networks (IVWSNs) are becoming an active research area in the field of intelligent transportation (Blumenstein, Mikulasek, Prokes, Zemen, & Mecklenbrauker, 2015; Hashemi et al., 2013; T.-Y. Huang, Chang, Lin, Roy, & Ho, 2015b; Mamdouhi, Khatun, & Ahmadi, 2009; Parthasarathy et al., 2016; Takayama & Kajiwara, 2016; Tuohy et al., 2015). It can reduce the cost of assembly, fuel efficiency, maintenance saving through eliminate the wire harness and introducing the new sensor technology inside the vehicle. The existing vehicular sensor network inside the vehicle, each sensor node is connected with ECU by wire, and each ECU shares common bus named CAN. Each sensor node is connected with ECU which samples and processes the data of sensor nodes and delivers them to CAN for further process. ECUs are connected with a single CAN which increases the bandwidth consumed significantly. The power supply of ECU comes from a battery of the vehicle. In the present vehicles, the wiring harness for all parts (up to 4000) may have about 40 kilograms, which is 4 kilometers long (Lin, Talty, & Tonguz, 2015a; Takayama & Kajiwara, 2016). Due to these reasons, the Intra-Vehicle Wireless Sensor Networks (IVWSNs) have recently been introduced to minimize the above complexity in the automotive industries. With the help of wireless technologies inside a vehicle, the weight, cost and the fuel consumption of the vehicle can be reduced, and better performance can be achieved (Bas & Ergen, 2012; S.-K. Chen et al., 2012; Jin, Kim, & Kwak, 2011).

There are harsh and complex environments inside the vehicle, so the design of wireless sensor network inside the vehicle is challenging phenomena. When the viable and robustness of wireless sensor technology will be proven better compare to wired sensor network like ECU and CAN depict in Figure 2.1, then it will be feasible to remove the existing systems. The ECU connects the each sensor node and CAN network. The ECU collects the information from the sensor node and transmits to the CAN network the processing. However, the sensor node increases such type of wire technology that creates complex and the wire harness.

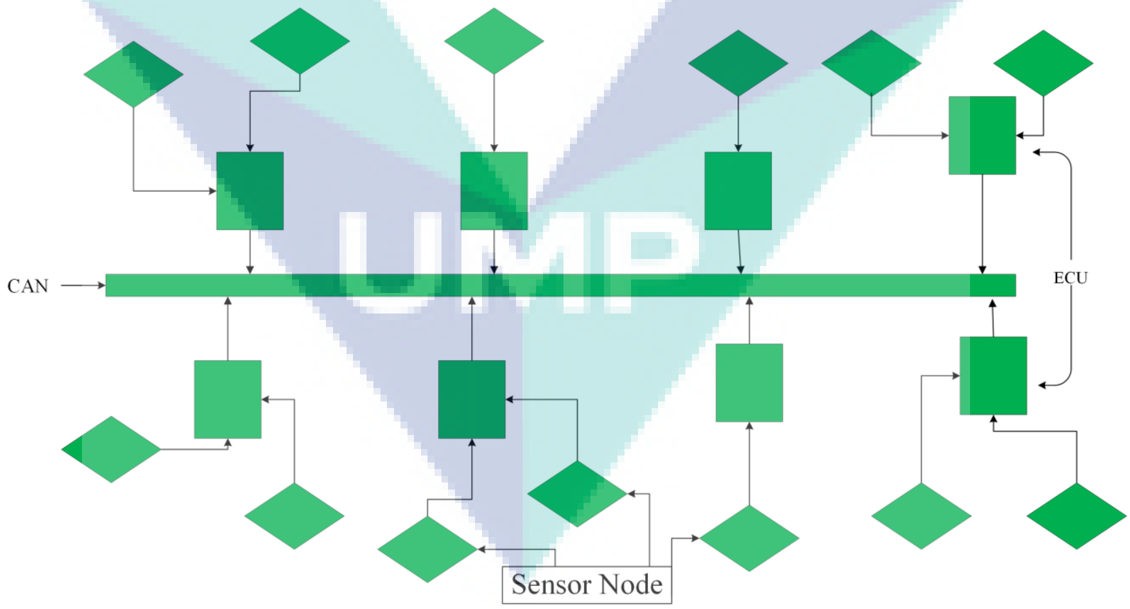


Figure 2.1 ECUs and CAN networks interface

Present improvements in computers and processing energy have resulted in numerous innovations within the automotive environment. In-vehicle electronic systems are quickly advancing in complexity and variety. A variety of sensors and processors are utilized in various areas of the automobile for different functions. Antilock Braking System (ABS) and electronic security control are types of systems that monitor a vehicles' interior performance and characteristics; whereas digital camera, radar, and ultrasonic sensors are increasingly being utilized to sense the environmental surroundings across the automobile and offer motorists with additional information regarding their environments. The wireless interconnection of sensors as well as other products inside the car, such as for example radio regularity in the event of tire pressure monitoring systems (Faezipour, Nourani, Saeed, & Addepalli, 2012), ultra-wideband (Blumenstein et al., 2015), or IEEE 802.x based solutions (Mourad, Heigl, & Hoeher, 2016), is being examined. While wireless solutions provide benefits over wired systems for the reason that they relieve cabling demands, in-vehicle wireless products nevertheless need a link with the electrical energy supply into the car, which mitigates this benefit. The authors in (McClellan et al., 2014) raised concerns about protection in wireless systems, demonstrating that eavesdropping on this network and also reverse engineering and inserting false information, is achievable in a moving automobile. As a result of the absolute significance of dependability and safety in safety-critical systems, wired solutions are anticipated to take over for the near future. Historically, each new electronic sensor or application in an automobile was implemented with the addition of a new stand-alone electronic control unit (ECU) unit and subsystem (Tuohy et al., 2015). It has resulted in in-vehicle companies growing both in size and complexity in a natural fashion. This frequently causes numerous complex sandboxed heterogeneous systems in one car. This might be unwelcome as there might be several different network protocols being used, which inhibits the interaction between systems.

Additionally increases expense to make regarding equipment expenses, development expenses, and help expenses. To conquer these issues, interaction links had been founded between relevant ECUs, enabling ECUs to share with you information with each other and enabling more complex functionality. As an example, the ABS subsystem may keep in touch with a seat gear pretension system to stimulate it in the eventuality of a collision. This method is quite ineffective as, with point-to-point links, how many connections needed exponentially increases utilizing the quantity of

ECUs installed within the car. To conquer this issue, numerous ECUs are attached to each other utilizing bus-based companies such as for example controller area network (CAN) (Tuohy, Glavin, Jones, Trivedi, & Kilmartin, 2013) or FlexRay (Khanapurkar, Bajaj, & Gharode, 2008). Making use of bus-based companies is a marked improvement in the point-to-point link system; but, it creates its own problems since, due to the fact amount of ECUs attached to increases with time, the bandwidth ingested somewhat increases. The issue of bandwidth does not generally speak manifest as an important problem in charge applications inside the car as a result of the restricted bandwidth needs associated with sensors included. Nevertheless, the bandwidth problem was brought into razor-sharp focus through the development of infotainment and camera-based Advanced Driver Assistance Systems (ADAS) (Tuohy et al., 2015).

2.4 The Concept of IoT in IVWSNs

The IoT enables with the advanced of developments in wireless technologies, for example, RFID, smart sensors, communication technologies, and Internet protocols. Basically, In the IoT ecosystem, intelligent devices communicate with each other autonomously to assemble, communicate, and forward heterogeneous information in multi-hop manner without any human centralized control and collaboration (Conti et al., 2018). The recent change in Internet-centric phenomena, mobile communication, and overall machine-to-machine (M2M) or device-to-device (D2D) communication technologies can be seen as the basic concept of the IoT (Bello & Zeadally, 2016). In the emerging coming years, the growing of IoT is predicted to integrate enormous wireless communication technologies to enable unique applications by connecting with physical objects together in support of intelligent decision making. Likewise, today's automobiles have a rising range effective Electronic Control Devices (ECU) and associated distributed sensor and actuator elements. For instance, significantly more than fifty sensors are implemented nowadays in a mid-range vehicle while the industry estimates for any automotive sensor market volumes surpass 665 million devices and 2237 million devices, in the united states and globally, respectively (Ahmed et al., 2007b). This represents a multi-billion dollar market in electronic sensors alone in 2007 and analyst estimate significantly more than 80 percent of the latest functions in cars become electronic devices based (Ahmed et al., 2007a). As a result, the designing concept, production and installing of the wiring harness for the transmission of energy and information for several of these sensor elements require considerable engineering work. At present, wiring harness inside a vehicle within 4,000 parts may have weighed about to forty kilograms and up to 4 kilometers long (Lin et al., 2015a). By eliminating or reducing the number of wire may potentially provide mass savings, cost savings, warranty savings, and overall cost saving. Moreover, those opportunities pave the way to enable wireless technology inside the vehicle and monitoring the critical parts of the vehicle that is the concept of Intelligent Transportation System (ITS).

2.5 Technologies in IoT Paradigm

The IoT is enabled by the newest innovations in ZigBee, RFID, smart sensors, wireless communication technologies, and Internet protocols. The fundamental principle is to have smart sensors work together directly without human interaction to deliver a new class of applications. The present movement in the Internet, mobile, device-to-device (D2D) and machine-to-machine (M2M) innovations can be observed as a key element of the IoT. In the upcoming consequence years, the emerging of IoT is predicted to build a bridge in different technologies to enable new applications by connecting them with physical objects to smart environment together in support of intelligent decision making (K.-C. Chen & Lien, 2014).

It is assumed that in the near upcoming years, comparably more electronic devices and equipment will be connected to the Internet to make life easier. The principle of the Internet of Things (IoT) is promising, and there might be a significant number of wireless technologies being integrated with the potential IoT protocol stack (Al-Fuqaha et al., 2015). By considering this issue, the IVWSNs in the near future might be no longer a separated wireless networks phenomena inside a vehicle. For instance, in an ongoing smart home, smart city or smart agriculture management system, there might be IoT devices that support the same wireless sensor technology of IVWSNs or run in a similar frequency band.

The idea of the Internet of Things (IoT) has captured the interest of individuals and research community around the world with the eyesight of expanding internet connectivity to a great number of “things” into the physical environment (Al-Fuqaha et al., 2015; S. Li et al., 2015). This may, in turn, transform our ability to communicate with real-world items, procedure information, and work out decisions along with saving us money and time. In general, the IoT represents the next thing associated with using the internet by which practically everything will undoubtedly be on the internet. Daily, how many things attached to the net is increasing multi-fold. Therefore, the penetration of connected things as a whole thing in the world is anticipated to achieve 2.7% in 2020 from 0.6 percent in 2012 showing in Figure 2.2 (Whitmore, Agarwal, & Da Xu, 2015).

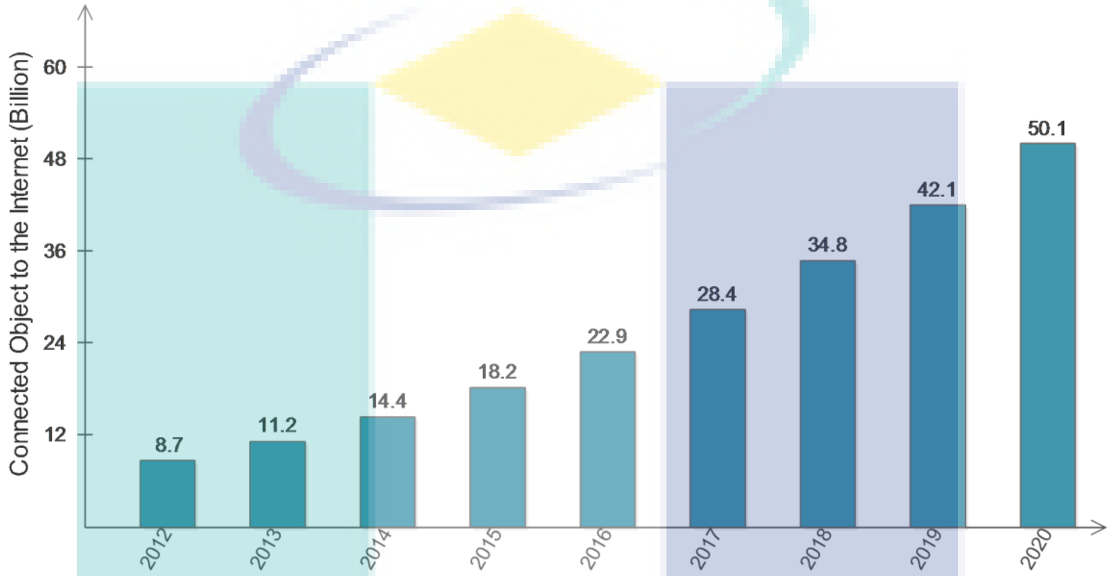


Figure 2.2 Estimated number of devices connected to the internet from 2012 to 2020.

Source: Rawat, Singh, & Bonnin (2016)

The google search trend for ongoing research in term of IoT, WSNs and ubiquitous computing in the recent last few years are shown in Figure 2.3. The popularity of different paradigms varies with time. The web search popularity, as measured by the Google search trends during the last ten years for the terms Internet of Things, Wireless Sensor Networks and Ubiquitous Computing are shown in Figure 2.3. As it can be seen, since IoT has come into existence, search volume is consistently increasing with the falling trend for Wireless Sensor Networks. As per Google's search forecast (dotted line in Figure 2.3), this trend is likely to continue as other enabling technologies converge to form a genuine Internet of Things.

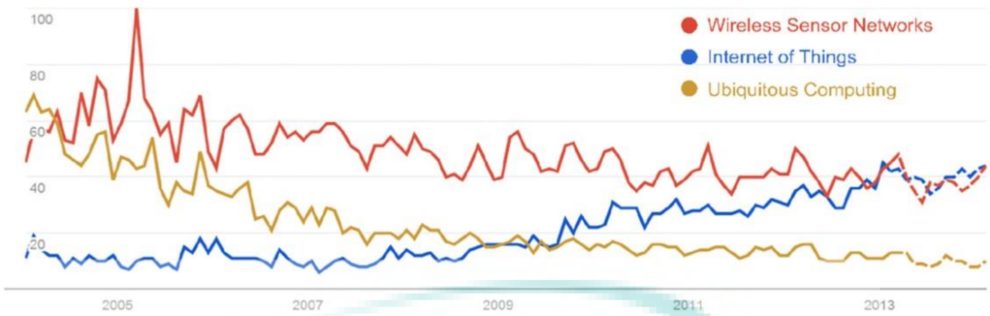


Figure 2.3 Google search trends since 2004 for terms Internet of Things, Wireless Sensor Networks, Ubiquitous Computing.

Source: Gubbi et al. (2013)

The use of IoT products will pervade every sector and industry from the smart house and smart town, training, healthcare, manufacturing, mining, gas and oil, power, resources, business, transport, surveillance, infrastructure administration, to produce string and logistics. A schematic of that interconnection of objects is depicted in Figure 2.2, where the application domains are chosen based on the scale of the impact of the data generated. The users span from individual to national level organizations addressing wide-ranging issues. The possibilities application areas in the IoT ecosystem are endless, and its own complete potential will soon be realized in the near future with a large number of devices getting connected to the Internet (Al-Fuqaha et al., 2015).

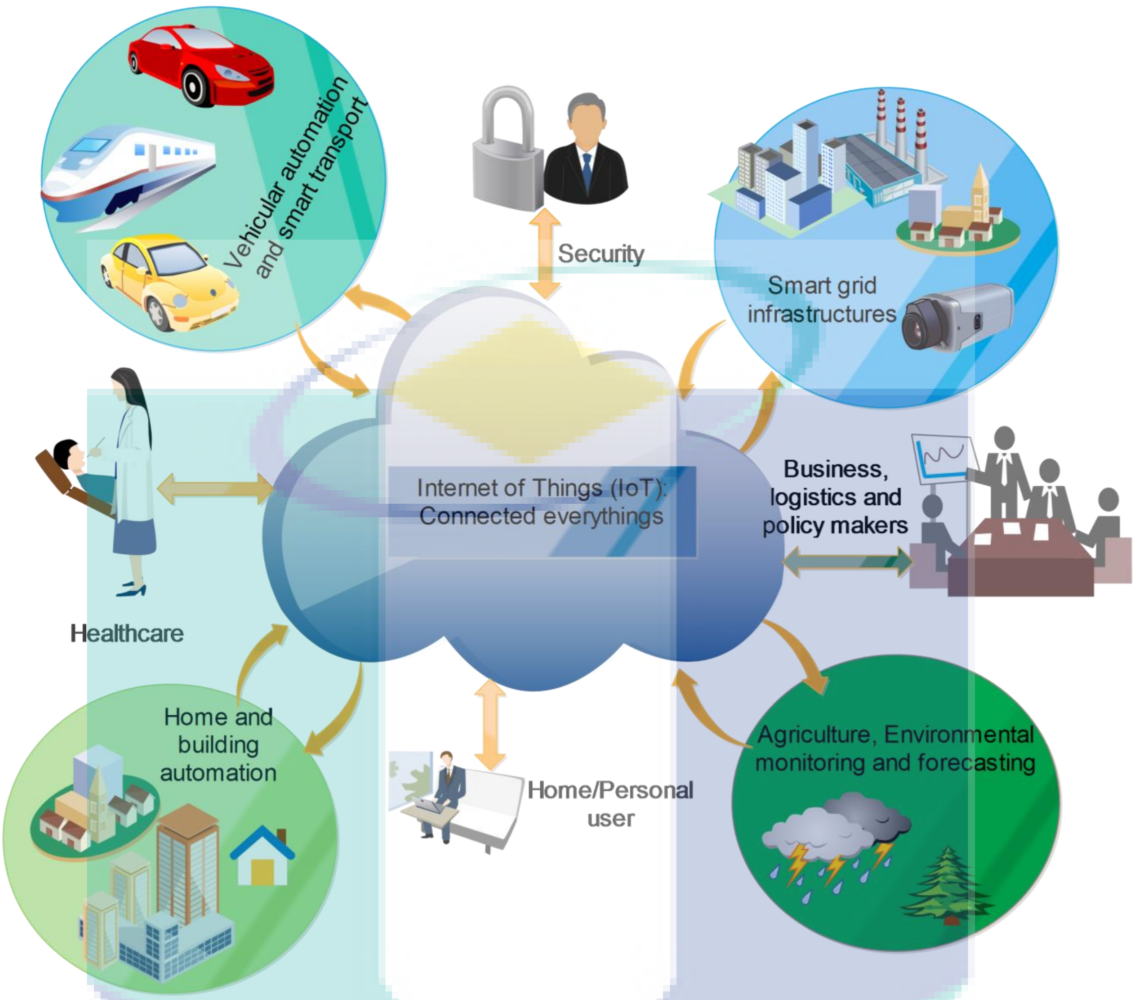


Figure 2.4 Internet of Things enabling environments

Source: Gubbi et al. (2013)

2.5.1 Technology

Wireless communication techniques can also be used to perform automotive functions inside a vehicle. Several wireless standards can be utilized for an intra-vehicle wireless sensor network, for example, ZigBee, Bluetooth, RFID, and Ultra- Wideband (UWB).

ZigBee: ZigBee defines the higher layer communication protocols built on the IEEE 802.15.4 standards for LR-PANs (Rault, Bouabdallah, & Challal, 2014; Wadhwa, Deshpande, & Priye, 2016). ZigBee is a simple, low cost, and low power wireless communication technology used in embedded applications. ZigBee devices can form mesh networks connecting hundreds to thousands of devices together. ZigBee devices use very little power and can operate on a cell battery for many years. There are three types of ZigBee devices: ZigBee coordinator, ZigBee router, and ZigBee end device. ZigBee coordinator initiates network formation, stores information, and can bridge networks together. ZigBee routers link groups of devices together and provide multi-hop communication across devices. ZigBee end device consists of the sensors, actuators, and controllers that collects data and communicates only with the router or the coordinator (Peng, Qian, & Wang, 2015). The applications areas of this wireless communication are data collection, supervising, military surveillance and in medical diagnosis. (Cuomo, Abbagnale, & Cipollone, 2013). The main advantages of ZigBee technology lies in the following aspects (Cuomo et al., 2013): (a) Reliable and self-configuration, (b) Supports large number of nodes, (c) Easy in deployment, (d) Very long battery life, (e) Secure, (f) Low cost, and (g) Can be used globally.

IEEE 802.15.4 is the proposed standard for low rate wireless personal area networks (LR-WPAN's). IEEE 802.15.4 focuses on the low cost of deployment, low complexity, and low power consumption (Al-Jemeli & Hussin, 2015; W. Li, Hu, & Jiang, 2018). IEEE 802.15.4 is designed for wireless sensor applications that require short-range communication to maximize battery life. The standard allows the formation of the star and peer-to-peer topology for communication between network devices. Devices in the star topology communicate with a central controller while in the peer-to-peer topology ad hoc and self-configuring networks can be formed. IEEE 802.15.4 devices are designed to support the physical and data-link layer protocols. The physical layer supports 868/915 MHz low bands and 2.4 GHz high bands (Khanafer, Guennoun, & Mouftah, 2014). The MAC layer controls access to the radio channel using the CSMA-CA mechanism. The MAC layer is also responsible for validating frames, frame delivery, network interface, network synchronization, device association, and secure services. Wireless sensor applications using IEEE 802.15.4 include residential, industrial, and environment monitoring, control and automation (P. Huang et al., 2013; Rault et al., 2014). The ZigBee stack architecture is shown in Figure 2.5. The stack architecture contains different communication layer such as application layer, network layer, security layer, and the MAC layer. The security layer takes supports from various layer for security mechanisms like application support sub-layer (APS) and network layer (NWK). The network layer takes care of all network related operations such as network setup, end device connection and disconnection to network, routing, and device configurations. The MAC layer is responsible for reliable transmission of data by accessing different networks with the carrier sense multiple access collision avoidance (CSMA). This also transmits the beacon frames for synchronizing communication.

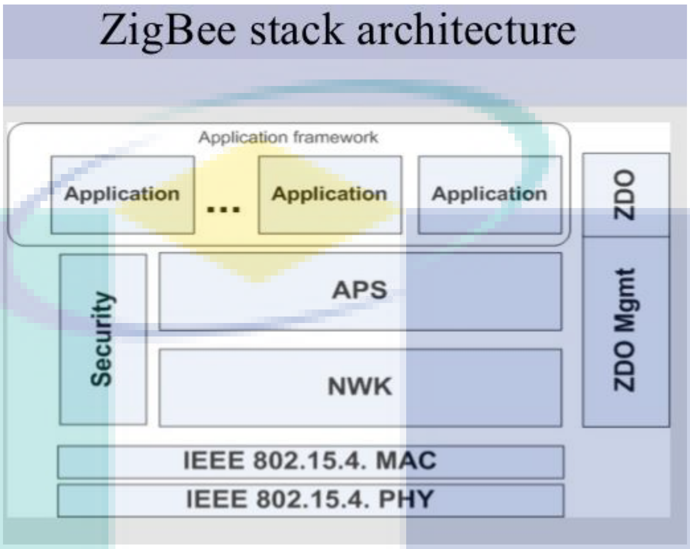


Figure 2.5 ZigBee stack architecture

Source: Cuomo et al. (2013)

IEEE 802.15.4-2003 standard and ZigBee the IEEE 802.15.4 PHY runs in three various commercials, scientific, and medical (ISM) bands; 2450, 915, and 868 MHz respectively (Wadhwa et al., 2016). The 2450 MHz global range organization provides 16 channels; the 915 MHz (United States) and 868 MHz (European countries) bands are assigned ten channels and an individual channel, respectively. For the 3 ISM bands, two PHY options, 2450 MHz and 915/868 MHz PHY, are specified that help information prices of 250 kb/s and 40/20 kb/s, respectively (Rawat, Singh, Chaouchi, & Bonnin, 2014). The fundamental channel access system of IEEE 802.15.4 is a carrier sensing multiple access with collision avoidance (CSMA/CA), and it is ideal for the extremely low-duty period procedure. For applications needing certain information bandwidth, certainly, one of two optional super framework structures provides a guaranteed time slot (GTS) for low latency. A tool applying the IEEE 802.15.4 protocol could be categorized as the full function device (FFD) or reduced function device (RFD) as shown in Figure 2.6 (P. Huang et al., 2013). Any topology consists of one or more coordinator. In a star topology, the network consists of one coordinator called FFD which is responsible for initiating and managing the devices over the network. All other devices are called RFD that directly communicates with coordinator. This is used in industries where all the end point devices are needed to communicate with the central controller, and this topology is simple and easy to deploy.

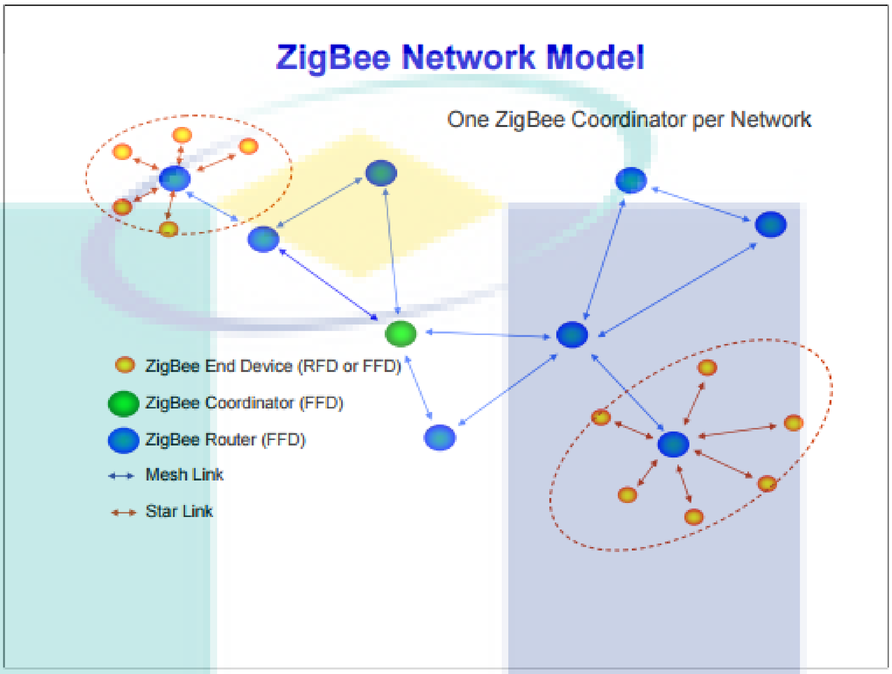


Figure 2.6 ZigBee network topology

Source: Rault et al. (2014)

The ZigBee specification defined by a link of organizations called the ZigBee Alliance provides top layer stacks and application section is being developed by the IEEE 802.15 TG4 PHY and MAC sub levels. Much like RFD and FFD, the specification additionally defines nodes as network coordinators, routers, and end devices. Network coordinators handle the network and router direct communications between nodes. ZigBee specifies three types of network traffic such as regular, periodic, and repeated low-latency traffic. Based on these traffic kinds, optimized network setup may be selected. Generally speaking, ZigBee systems are appropriate low responsibility cycle (<1%) communications for very long battery life. Aside from the technical requirements, the ZigBee Alliance additionally manages item branding of ZigBee-compliant platforms. Recently complimentary scale and lots of other businesses announced platforms including chipsets, development environment, and protocol stacks (Rault et al., 2014).

Bluetooth: Bluetooth is a very short-range wireless technology which is based on the IEEE 802.15.1 standard and can operate in the industrial, scientific, and medical (ISM) frequency band (2.4 GHz). It allows the communication between portable devices at a data rate up to 3 Megabit/second and is highly commercialized for consumer electronics (Yu, Xu, & Li, 2012). The Bluetooth devices are common in current automobiles, such as the Bluetooth headset and rear-view mirror. Bluetooth has a few benefits which will make it the absolute most widely used standard today. It is an established technology, and it is reasonably inexpensive. It may send voice and information, and it has a more information framework payload. Also has low energy needs and will penetrate hurdles such as walls. This has a sizable installed base and a guaranteed latency, along with a reliable specification.

It enables the interaction between portable products at a data rate up to 3 Megabyte/second, and it is highly commercialized for electronic gadgets (Khaleel, Al-Rizzo, & Rucker, 2012). The Bluetooth products are typical in present cars, like the Bluetooth headset and rear-view mirror. However, the Bluetooth transmission requires relatively more energy consumption such that it may not be viable for battery-driven sensors in vehicles (Qu, Wang, & Yang, 2010b). Furthermore, as a result of the less scalability, a Bluetooth network can only configure eight active end devices (seven slave end devices and one master device) (Ye, Heidemann, & Estrin, 2004).

RFID: The feasibility of utilizing the radio-frequency recognition (RFID) technology for building intra-vehicle sensor systems is examined in (O. K. Tonguz, Tsai, Talty, Macdonald, & Saraydar, 2006) and (O. Tonguz, Tsai, Saraydar, Talty, & Macdonald, 2007). The explanation associated with considered passive RFID solution is each sensor has an RFID tag and a reader linked to the ECU, which occasionally retrieves the sensed information by delivering an energizing pulse every single label. Considerable experiments have already been carried out in both of these studies for comprehending the abilities and limits of RFID technology, such as the wireless channel faculties between reader and RFID tags at various places, packet reception rate, and a maximum packet waiting time. The passive RFID solution has apparent benefits: cheap with no energy supply to RFID tags. Moreover, the experiments show promising results with regards to the coherence bandwidth together with the transmission reliability of the network (Coronato, De Pietro, Park, & Chao, 2010).

UWB: Ultra-wideband (UWB) refers to radio technology that operates in the 3.1–10.6 GHz ISM frequency band and can allow short-range communications at a moderate and high data rate up to 480 Mb/s and at a very energy efficient. UWB techniques have a lot of unique benefits, such as, prevention to severe wireless channel fading effect and shadowing, high time domain resolution suitable for localization and tracking applications, low cost, and low controlling complexity (Lu et al., 2014).

2.6 Challenges for IoT Enabled IVWSNs

The communication protocols at the sensing end of IoT will play a critical role in complete realization. They make the platform for the data tunnel between sensors and the physical world. For the system to move effectively, a low energy efficient MAC protocol and proper routing protocols are important. Several issues need to address that can arise while the IoT environment will introduce within the vehicle. For example, MAC layer, energy efficient, scalability, and others miscellaneous challenges could be discussed.

2.6.1 MAC Layer Issue

IEEE 802.15.4 is a typical created for low data rate wireless personal area networks (LR-WPANs), and it is also considered a promising solution for low energy and short-range communication while achieving high networking freedom. The scope of its applicability and functionality goes beyond what traditional applications, such as habitat and healthcare monitoring, target tracking, military surveillance, smart grid, and house automation (Aziz & Pham, 2013; Jung et al., 2014). One of the more issues which are challenging IEEE 802.15.4 sites is the concern of how exactly to reduce power usage to be able to expand community lifetime. Therefore, unlike much interaction that is wireless which primarily concentrates on achieving high throughput performance, the IEEE 802.15.4 standard aims at assisting short range and low power wireless communication. For efficient interaction, it includes the collision resolution mechanism called carrier sense multiple access with collision avoidance (CSMA/CA), which allows sensor devices to prevent power-consuming packet collisions caused by numerous simultaneous transmissions. However, the IEEE that is conventional CSMA/CA has two primary issues. First, aggressive binary backoff that is exponential hampers the efficient communication of sensors. Whenever a channel that is clear

(CCA) reports that the channel medium is busy, sensors increment the binary exponent (BE) at a time as much as the maximum value (maxBE). This process can waste idle slots and finally end up in throughput degradation as it may impetuously rise the BE also under a transient channel condition that is busy (Tavakoli, Mišić, Mišić, & Naderi, 2015).

Moreover, BE is merely reset towards the value that is initialminBE) upon a successful transmission or a packet fall. Because of this, sensors may frequently have problems with meaningless backoffs and additional CCAs due to the initialized BE that is inadequate to resolve the community contention degree that is current. Second, the sporadic CCA procedure decreases not only energy consumption but the throughput. The CCA of IEEE 802.15.4 is not constantly carried out unlike the IEEE 802.11 distributed coordination function (DCF) instead; sensors perform CCA only if they have finished the procedure in the backoff period. In other words, sensors do not know whether it performs the previous on-going transmission or not and it starts to count down backoff periods (BP) which are arbitrarily chosen within 2BE -1. This may also waste of energy and bandwidth, simply because they should perform a meaningless CCA and succeeding backoff if the backoff timer expires under the busy channel (Park, Fischione, & Johansson, 2013).

2.6.2 Energy Consumption Issue

The newly disclose IoT is envisioned to enable understanding of WSNs. However, the key criterion to enable successfully of WSNs of IoT depends on the energy efficiency and reliability. The reliability requirements can vary with regards to the application or the content for the data itself. A certain portion of data loss could be tolerated for delivering heat data within normal range; while a high-temperature dimension should be delivered at very high dependability, as it could be the indication of a fire for example, for temperature monitoring in a smart home. In a health monitoring application, delivery of all of the sensory information may need dependability that is high. For WSNs, just as much as reliability, power usage can also be critical, since all of the sensor and nodes that are wireless battery powered. Energy efficiency is basically dependent on the trade-off between dependability and energy costs, both of that are dependent on employed wireless communication technology and medium access schemes (Anchora, Capone, Mighali, Patrono, & Simone, 2014).

The protocols during the sensing end of IoT will play a role that is complete key understanding. They create the backbone for the data tunnel between sensors and the real world. For the device to work efficiently, an energy efficient MAC protocol and appropriate routing protocol are critical. Several modified MAC protocols have been proposed for IEEE 802.15.4 in the perspective of various domains such as TDMA, CSMA/CA, and FDMA (Anusha, Vemuru, & Gunasekhar, 2015; Rasheed et al., 2014). Energy saving for expanding the total lifetime of IEEE802.15.4 based ZigBee protocol is a prime issue of current research efforts

IoT has diverse items including low energy sensors, smartphones, etc., with diverse energy consumption information. Energy-efficient designs and communications must be addressed for a much longer lifetime of IoT things. Energy maintenance should be adaptable to various means of opportunistic power harvesting and scavenging. Energy conserving interaction is required because, typically, within the interaction products, interaction component may be the primary way to obtain energy usage (Anchora et al., 2014; Pantazis, Nikolidakis, & Vergados, 2013).

Moreover, the interacting object needs to have enough processing energy for efficient power management and optimization. Therefore, power optimization and management algorithm are built to additionally think about the low processing abilities of a few of the IoT products.

2.6.3 Scalability Issue

Sensor nodes are implemented densely to make a WSN. This significant amount of nodes has a primary effect on the style of schemes and protocols at various levels. For instance, a MAC protocol (data-link layer) should certainly give, in a good fashion, each node usage of the medium while minimizing or preventing collisions, that is very hard provided the massive wide range of available nodes. Additionally, a routing protocol (network layer) that depends upon exchanging routing tables among nodes might not be efficient since there will see extortionate control traffic that underutilizes the bandwidth associated with medium (Iova, Picco, Istomin, & Kiraly, 2016; Yaala & Bouallegue, 2016). Furthermore, it would be a big challenge to design scalable network in which the network behaves in the same way whether it is a small or large network.

2.6.4 Miscellaneous Challenges

It should be considered following other important challenges for designing IoT enabled IVWSNs:

Large numbers of sensors need to be considered compared to the traditional IVWSNs. The network is unable to give better performance when it becomes large. Therefore, to design a scalable network for IVWSNs will be a big challenge.

Due to the small-scale fading, three different propagation mechanisms (such as reflection, diffraction, and scattering) can change the behavior of the transmitted signal from the transmitter to the receiver inside the vehicle. Hence, these mechanisms have to be considered while designing the IoT-IVWSNs.

The wireless channel can be characterized by two fading distribution functions, such as Rice (it occurs in the presence of Line of Sight (LOS) propagation path) and Rayleigh (it occurs in the presence of Non-Line of Sight (NLOS) propagation path distributions. However, these traditional concepts may not work properly, because of the architectural complexity inside the vehicle. Therefore, the actual distribution needs to be estimated through the experimental analysis that introduces additional design challenge for IoT-IVWSNs.

In order to design the link between the transmitter (Tx) and receiver (Rx), the communication parameters such as transmit power, received signal threshold, the distance between Tx and Rx, and value for path-loss exponential are needed to be set properly.

Selecting the suitable technology for designing an IoT-IVWSN from existing technologies, need to be analyzed comprehensively. Also, new technology could be thought for such a network.

2.7 Description of the IEEE 802.15.4 Slotted MAC Protocol

The IoT communication protocol connects heterogeneous physical objects to provide particular smart services (Sun, Liu, Li, FAN, & SUN, 2010). Generally, the IoT end nodes should run using very low power in the existing communication links. There are various kinds of communication protocols used for the IoT are IEEE 802.15.4, WiFi, Bluetooth, Z-wave, and LTE-Advanced. In this thesis focuses on the IEEE 802.15.4 standard emerging protocol in the IoT paradigm (Gubbi et al., 2013). IEEE 802.15.4 standard specifies for both physical and MAC layer for low energy efficient wireless protocol focusing on getting reliable and scalable communications. The subsequence subsections will discuss the comprehensive study of performance evaluation and different type of methods those have been conducted with this protocol.

In a standard protocol, nodes communicate with each other according to a slotted CSMA/CA protocol based on a superframe structure. Each superframe consists of an active period and an inactive period. The active period consists of a beacon period, a contention access period (CAP), and a contention-free period (CFP). During the inactive period, the coordinator and the nodes shall not interact with each other and may enter a low-power mode. The active period of the superframe is divided into equal 16-time slots. To clarify this phenomenon, Figure 2.7 is presented.

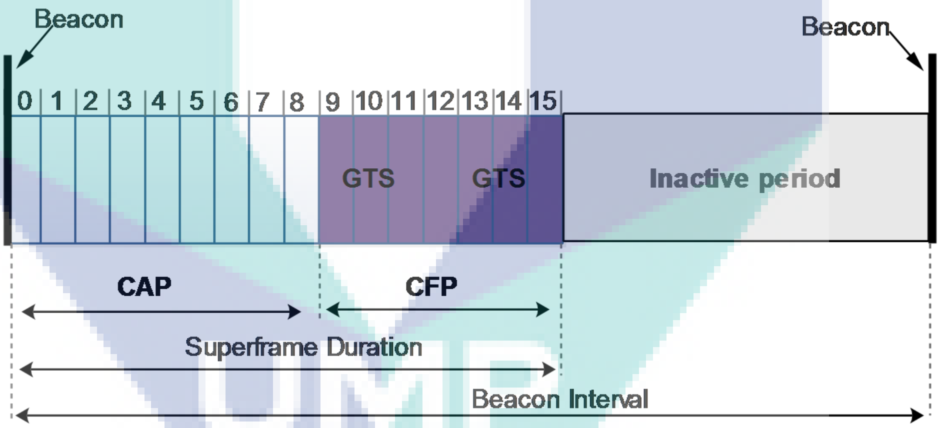


Figure 2.7   Superframe structure of IEEE 802.15.4

Source: Park, Fischione, et al. (2013)

At the initiate of each superframe, the Personal Area Network (PAN) coordinator transmits a beacon frame that carries relevant system parameters, such as a beacon order (BO) that determines the length of a beacon interval (BI = 16 * 60 * 2BO symbols) and a superframe order (SO) that determines the length of a superframe duration (SD =16 * 60 * 2BO symbols). All the default attributes and parameters of IEEE 802.15.4 MAC are listed in Table 2.1. During the CAP period, each node communicates with the PAN coordinator and other nodes using the slotted CSMA/CA. The slotted algorithm is depicted in Figure 2.8. The timeframe of one slot is a Unit Backoff Period (standard value =20 symbols). When a node has a new data frame to transmit, it initializes relevant parameters such as a backoff exponent (BE) and the number of backoffs or backoff stages (NB), which are set to macMinBE (standard value =3) and 0, respectively. In addition, it uniformly selects a backoff counter value from a window (0, 2BE− 1). The backoff counter value is decremented by one for each time slot, regardless of the channel state, and BE whenever the backoff counter value is zero; the node performs carrier sensing that requires two clear channel assessments (CCAs) at the physical (PHY) layer before a transmission. If the channel is assessed to be idle at the two consecutive CCAs, then it transmits the data frame (Park, Fischione, et al., 2013).

Table 2.1 Description of IEEE 802.15.4 Attributes and Parameters

Attributes and Parameters Names	**Descriptions**
aUnitBackoffPeriod	Basic time period used by the CSMA-CA algorithm
BE	Backoff Exponent
BI	Beacon Interval
BO	Beacon Order
CAP	Contention Access Period
CCA	Clear Channel Assessment
CFP	Contention Free Period
CW	Contention Window
GTS	Guaranteed Time Slots
macMaxCSMABackoffs	Maximum number of backoffs allowed

Table 2.1 Continued

Attributes and Parameters Names	Descriptions
	before declaring channel access failure
macMaxFrameRetries	Maximum number of transmission retries allowed after a collision
macMaxBE	Maximum value of BE
maxMinBE	BE Minimum value of BE
NB	Number of times a node has
SD	Superframe Duration
SO	Superframe Order

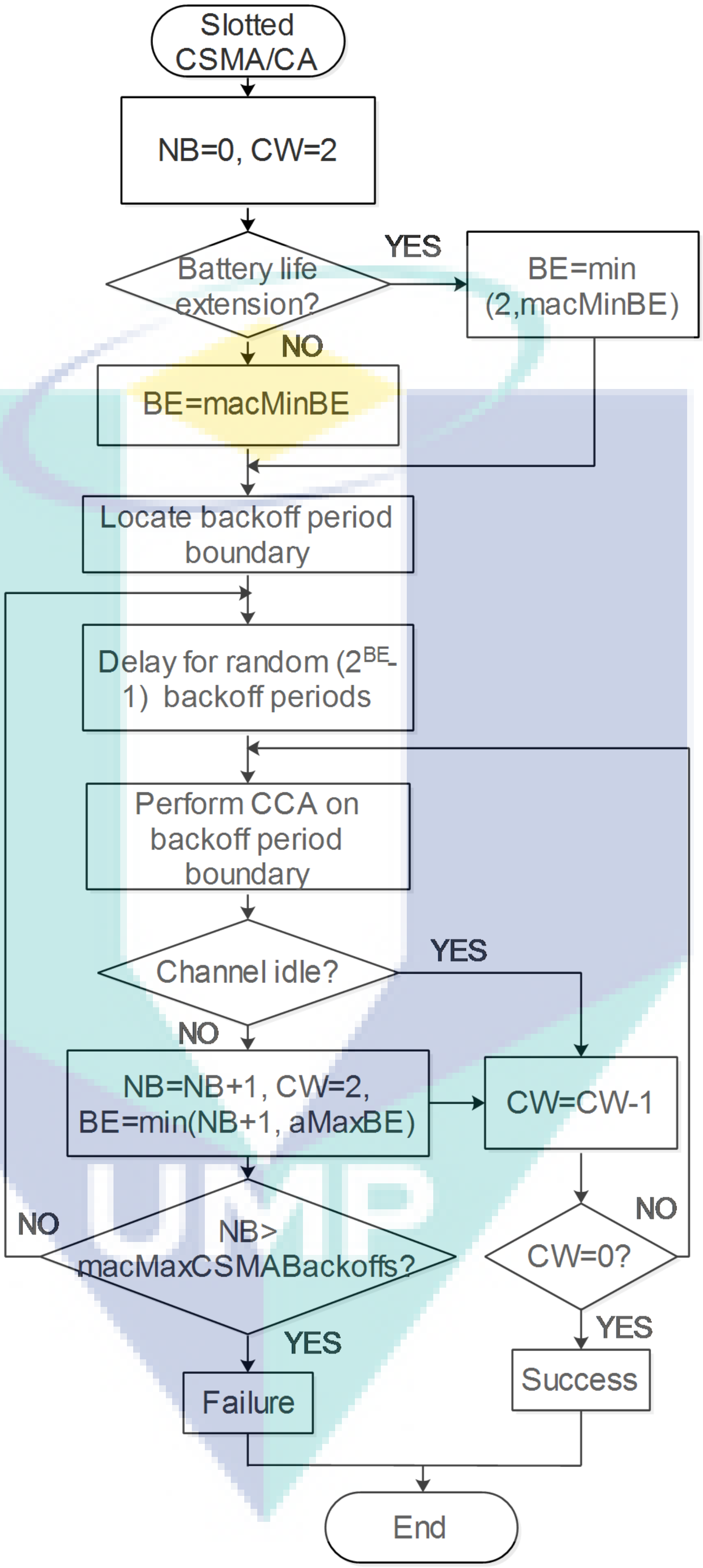


Figure 2.8 Flowchart of slotted CSMA/CA algorithm

Source: Akyildiz & Vuran (2010)

If the channel is assessed to be busy, it increases the values of BE and NB by one and delays the transmission for a random number of time slots that are uniformly chosen from (0, 2BE – 1), where BE is no more than a MaxBE (standard value =5). The above procedure is continued until the successful transmission; however, if the NB value is greater than macMaxCSMABackoffs (standard value =4), then the CSMA/CA algorithm shall be terminated with a channel access failure. If either a channel access failure occurs or a frame transmission failure occurs due to a collision, the node retries the aforementioned procedure for retransmissions up to aMaxFrameRetries (standard value = 3) times. Since the transmission of an Ack frame shall commence at a slot boundary, the duration Ack time BE from the reception of the last symbol of the data frame to the transmission of the first symbol of its Ack frame is between aTurnaroundTime (standard value = 12 symbols) and aTurnaroundTime + aUnitBackoffPeriod (32 symbols), that is, one time slot can be included in the duration t at most. After transmitting a data frame, the node waits for its Ack frame during the duration that is specified by the parameter macAckWaitDuration (standard value = 54 symbols) (Rasheed et al., 2014).

2.7.1 Approaches to Improve IEEE 802.15.4 MAC

Nowadays, The IEEE 802.15.4 standard is considered group of requirements suitable for implementation in WSNs. IEEE 802.15.4 defines the specs for the PHY layer and also the MAC sub-layer in wireless products that use low data cost, low-power, and short-range radio regularity transmissions in a wireless individual area network (WPAN) (D.-M. Han & Lim, 2010; Shih, Chen, Shih, & Tseng, 2010). This standard is very appropriate implementation in WSNs since it conforms for their requirements and constraints. The reason being it orchestrates the sensor nodes' usage of the communication medium, and so, it plays an important part in consuming nodes' energy resources. Because of the diverse domain of WSN-based applications, IEEE 802.15.4 MAC has enticed considerable research tasks to reveal its abilities and enhance its performance. As a whole, these tasks have centered on two measurements: (i) Analytical Mathematical modeling of IEEE 802.15.4 MAC and (ii) Enhancing IEEE 802.15.4 MAC. Figure 2.9 depicts the different improvement approaches of IEEE 802.15.4. The improvement has been implemented based on the following issues; cross layer, parameter tuning, hidden term resolution, IEEE 802.11, priority, duty cycle, backoff, and Quality of Service (QoS) based approaches.

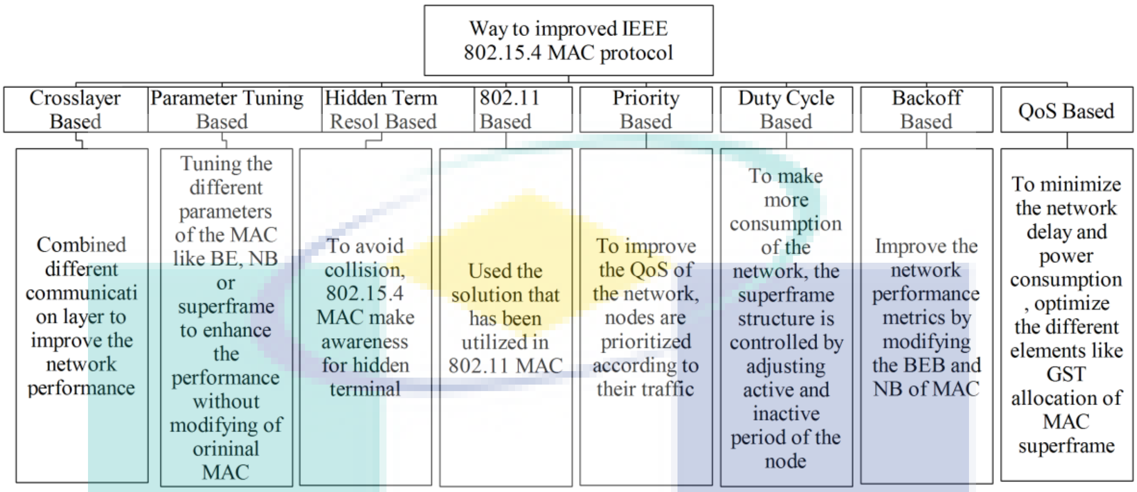


Figure 2.9 IEEE 802.15.4 classifications to improve the performance

Comprehensive reports have been employed by on developing accurate analytical models that will anticipate the theoretical behavior of IEEE 802.15.4 MAC. A significant part of these reports utilized Markov-based analysis to produce their models. The aim of these models is always to recognize possibilities to boost the performance of IEEE 802.15.4 MAC and mitigate any way to obtain deterioration inside it (Palattella et al., 2014; Striccoli, Boggia, & Grieco, 2015).

Parameter Tuning-Based approaches: These strategies are applied to get better performance without changing the original algorithm of MAC. These approaches are beneficial because they retain the different supporting characteristics of WSNs. Therefore, to achieve the optimal performance, the different parameters are tuned properly. The most significant advantages of these techniques are to avoid additional sensor node overhead to minimize power consumption. However, the main weakness of these approaches is needed to incorporate the sensor nodes optimization in a specific application to find appropriate tuneable parameters (Alvi et al., 2012; Buratti, 2010; Pollin et al., 2008; Shih, Chen, et al., 2010). To improve the power efficiency substantially while guaranteeing reliability and delay constraints of the networks, an adaptive tuning of MAC parameters that uses the physical layer measurement of channel sensing is proposed in (Park, Fischione, & Johansson, 2011). The proposed adaptive tuning based algorithm is equipped with two different properties, the main and most important feature is to run the functional characteristics of algorithm without modifying the original one, and second property makes it does not require any modification of the existing standard, and it makes an optimization of all the MAC parameters of IEEE 802.15.4. However, this algorithm does not provide any acknowledge guarantee of the network.

To guarantee the application reliability requirements by minimizing the energy consumption of the networks, a Just-in-Time LEarning-based Adaptive Parameter tuning (JIT-LEAP) algorithm is proposed in (Brienza, Roveri, Guglielmo, & Anastasi, 2016). It adjusts the CSMA/CA parameter by setting to the time-varying operating conditions by exploiting the history to find the most appropriate setting for the current conditions. It is appropriate for real-life operations and does not require more energy to find out the appropriate history setting.

Some limitations have been found in term of network reliability and timeliness in parameter setting in IEEE 802.15.4 (Anastasi, Conti, & Di Francesco, 2011; Pollin et al., 2008). Particularly, (Anastasi et al., 2011) have presented the unreliability of IEEE 802.15.4 WSNs which is decreased the performance by the pure CSMA/CA parameter setting even though the number of sensor nodes is low. The authors have suggested that employing additional appropriate parameter values increases reliability, at the cost of improved latency and energy consumption.

Some solutions based on parameter tuning studies investigate the performance of IEEE 802.15.4 by tuning different parameters with applying appropriate tuning methodology. A few solution focus on a single parameter tuning of CSMA/CA parameter (Rao & Marandin, 2006; Zhao, Zhang, Niu, Zhang, & Zhao, 2010). However, modifying a single parameter may not adequate to satisfy the reliability requirements of the application (Anastasi et al., 2011). As a result, a number of authors (Brienza, De Guglielmo, Anastasi, Conti, & Neri, 2013; Di Francesco, Anastasi, Conti, Das, & Neri, 2011; Park et al., 2011; Park, Fischione, et al., 2013) have considered the whole set of parameters of CSMA/CA. Different parameters tuning methodology are classified according to their taxonomy in (Brienza et al., 2013; Park, Di Marco, Fischione, & Johansson, 2013), model-based adaption (Park, Di Marco, et al., 2013), and measurements-based adaptation (Brienza et al., 2013; Di Francesco et al., 2011). Parameter tuning based schemes provide better performance regarding throughput, energy consumption, power consumption, and end-to-end delay by tuning the multiple parameters like SO, BO, SD, BI, packet size and a number of nodes. These schemes can dynamically adapt heavy traffic. These schemes are application specific, and hence they provide a good quality of service by enhancing network lifetime (Bhosale & Ladhe, 2018)

In a study conducted by B. Han, Cao, Shi, and Wang (2018), it has provided a comprehensive Markov-based analytical evaluation of slotted CSMA/CA algorithm for both saturated and unsaturated network conditions in the presence of acknowledged and unacknowledged up-link data transmissions. The results of the developed model are significant in at least two major respects; firstly, it increases the network throughput and secondly, minimizes the power consumption of the node.

IEEE 802.11-Based approaches: The IEEE 802.11 based approaches utilize the solution that has been successfully implemented in IEEE 802.11 MAC strategy. In (S.-Y. Lee, Shin, Lee, & Ahn, 2014), they developed IEEE 802.11-based approach to improving the performance of 802.11 Wireless LANs to 802.15.4 WSNs. The proposed strategy minimizes the collision rate of the network by increasing the backoff window size. However, the main disadvantage of this strategy does not support energy efficiency solution which is the principal concern of IoT environments. However, (Minooei & Nojumi, 2007) performed a similar series of experiments to show that maximum throughput can be achieved by reducing the level of contention over the medium. The contention window (W) is randomly selected from the range (W_{i-1}, W_i) rather than (0, W_i), where W is the contention window of the i^{th} backoff stage.

Cross Layer-Based approaches: These strategies advocate the cooperation and share of information among the various communication layers of the protocol stack such that a better tuning of the MAC layer parameters is achieved. While these approaches may not necessarily change the standard itself, they base its parameters' configuration on the information provided by other layers, and thus excessive latency may be incurred. This is beside the overhead of changing the architecture of the protocol stack such that a new control channel or layer is used to convey the configuration data from a layer to another. However, the benefit of these approaches is that they work on having a comprehensive solution that optimizes the performance of the sensor node. Examples of these approaches include (Di Francesco et al., 2011; Hamid & Hussain, 2014; Tseng & Chuang, 2013).

Duty Cycle-Based approaches: These techniques work on controlling access of the nodes to the medium throughout the active and inactive periods within the superframe to make the protocol more power-efficient. The advantage of these approaches is that they expose the additional opportunities to save more power in the WSN without reducing other important performance metrics. Examples of these strategies include (D. Lee & Chung, 2010; Rasouli, Kavian, & Rashvand, 2014; Zhuo, Wang, Song, Wang, & Almeida, 2013).

Protection-Based approaches: These approaches are applied to the security issues in which the BEB algorithm is modifying to prevent the vulnerabilities of a node. The principal obstacle towards these techniques is how to establish strong security algorithms that are power-efficient. Generally, the strong security algorithms are commonly complex and power-hungry, and any simplification to their design may result in weak protection to the sensor nodes. Examples of these approaches include (Anastasi et al., 2011; Shih, Chen, et al., 2010).

Backoff-Based approaches: These methods concentrate on enhancing the overall performance of IEEE 802.15.4 MAC through formulating new backoff algorithms which control the medium access in a more efficient manner. A number of these approaches can make the backoff process more adaptive and dynamic. Varieties of these approaches include (Park, Fischione, et al., 2013; Ranjit & Shin, 2013).

Priority-Based approaches: These techniques implement on enhancing the IEEE 802.15.4 MAC by identifying the need of prioritization of the individual node to access to the medium. These methods identify the limitations that the default protocol does not have special measures to classify the nodes in case of emergency traffics, each node is treated as the same priority either urgent or general execution. Examples of these approaches include (Collotta, Scatà, & Pau, 2013; Shen, Zhang, Barac, & Gidlund, 2014).The main key features comparison among the improvement approaches are mentioned in Table 2.2.The comparison is analyzed on the different characteristics of the network such as scalability, data traffic, network delay, and the collision rate.

Table 2.2 Comparison of different improving approaches of IEEE 802.15.4

Modified MAC Approaches	Key design principles	Data traffic	Scalable	Delay	Collision	Strengths	Weakness	Experiment: Analytical	Experiment: Simulation
Parameters tuning based	Avoid additional sensor node overhead to minimize the power consumption to achieve the optimal performance; the different parameters are tuned properly without changing the default MAC mechanism.	Medium	Less	Yes	Yes	Provide better performance without changing the original algorithm of MAC.	Needed to incorporate the sensor nodes optimization in a specific application to find appropriate tunable parameters.	Yes	Yes
IEEE 802.11 based	Minimizes the collision rate of the network by increasing the backoff window size.	Low	Less	Moderate	Yes		Does not support energy efficiency solution which is the principal concern of IoT environments.	Yes	No
Cross-layer based	Advocate the cooperation and share of information among the various communication layers of the protocol stack for better tuning of the MAC layer parameters	High	More	Medium	Medium	Provides a comprehensive solution that optimizes the performance of the sensor node.	Excessive latency is incurred.	Yes	Yes

Table 2.2 Continued.

Modified MAC Approaches	Key design principles	Data traffic	Scalable	Delay	Collision	Strengths	Weakness	Experiment	
								Analytical	Simulation
Duty Cycle-based	Control the access of the nodes to the medium throughout the active and inactive periods within the superframe to make the protocol more efficient.	Low	Low	Medium	Medium	Save more power in the WSN without reducing other important performance metrics	Applicable for low data rate applications	Yes	Yes
Protection-based	These approaches are famous for security driven issues to establish strong security algorithms that are power-efficient	Low	Less	High	High	Ensure the security of sensor node and less power consumption	Provide less network performance in term of throughput, an end to end delay	No	Yes
Backoff-based	Enhancing the overall performance of IEEE 802.15.4 MAC through formulating new backoff algorithms which control the medium access in a more efficient manner, Ability to outperform the IEEE 802.15.4 MAC protocol regarding the reduction in the transmission delay under heavy traffic load.	High	Medium	Medium	Less	Improving in the throughput by reducing packet collisions	Energy consumption and duration of the backoff time slot increased in the CAP	Yes	Yes
Priority-based	Identify the need of prioritization of the individual node to access to the medium at the case of emergency and critical surveillance	Low	Less	More	No	Minimizes the data collision and congestion	Increase the network end to end delay	Yes	Yes

2.8 Comparative Study to others with IEEE 802.15.4 MAC

An intra-vehicular wireless network varies from a regular wireless network, including the popular 802.11-type systems, in many key aspects. For instance, for network topology, vehicular sensors and actuators are arranged in really a star-configuration with an associated ECU serving while the main computer. This topology is significantly different from a normal ad-hoc network setup, where nodes can develop tracks to virtually any other node (Qu, Wang, & Yang, 2010a). Data rate requirements may also be varied for WASNs-typically bits to kilobits for demand, control, and sensor/situation information. Finally, the protocol demands and information dependability needs can be various for WASNs when compared with generic random networks. For instance, many two-way wireless information applications nowadays utilize the TCP/IP suite of network protocols (Toscano & Bello, 2012). The notable exclusion the following is mobile telephony.

Nevertheless, an IP based network is most likely inappropriate for an intra-vehicular sensor network. The key rationale is the fact that offered the application form behavior, reliability and data rate requirements for intra-vehicle networks, the overhead related to TCP/IP systems is simply too high priced for much in-vehicle control or sensing applications. Also, the wireless information reliability for WSNs needs to equal or go beyond the wired comparable performance if wireless is ever become implemented for in-vehicle applications. Typically, an ad hoc wireless network operation, applications attempt to mask network heterogeneity by protocol wrappers that will be good of solution (e.g., via TCP/IP or OSI stack models). Such general schemes are improper for protocol-light automotive applications. Frequently the information being shuttled from supply to location in automotive applications is merely a couple of bytes, representing an example of a sensor reading, but which needs to be delivered with excessively high reliability (Hasbollah, Ariffin, & Hamini, 2009).

Also, 802.11x solutions are not suitable for WSNs due to some reasons including chipset price and size, low power demands, protocol overhead, and a shortage of real-time latency guarantees. Table 2.3 provides the main specifications of these technologies with regards to a few parameters (Ahmed et al., 2007a; Tuohy et al., 2015). Table 2.3 compares the principle different among the technology which can be used in IVWSN such Bluetooth, Wi-Fi, UWB, and ZigBee. The table shows that all wireless technologies support low power consumption as well as the desired transmission nominal range. However, the other supporting attributes like topology, scalability, network size, and the maximum number of sensor node are varied among the technologies. Furthermore, to implement the wireless technology in a high-density environment like IoT-IVWSNs, the ZigBee is the best choice because of supporting maximum number sensor node and high scalability.

Table 2.3 Comparison table among existing major technologies

Standard	**Bluetooth**	**Wi-Fi**	**UWB**	**ZigBee**
IEEE specification	802.15.1	802.11a/b/g	802.15.3a	802.15.4
Frequency band	2.4 GHz	2.4 GHz; 5 GHz	3.1-10.6 GHz	868/915 GHz; 2.4 GHz
Max signal rate	1 to 3 Mb/s	54 Mb/s	110 Mb/s	250 Kb/s
Nominal range	10 m	100 m	10 m	10-100 m
Max number of cell nodes	8	2007	8	> 65000
Chip price	$5	$20-25	$1	$2
Data Protection	16-bit CRC	32-bit CRC	32-bit CRC	16-bit CRC
Topology	Star, mesh, and point-to-point	ESS,BSS	Peer-to-peer	Tree, star, mesh, and hybrid.
Scalability	Very low	Low	High	Very high
Interoperability	Low	Low	Moderate	Very High
Power Consumption	Low	Moderate	Moderate	Low
Network Size Handle	Very small	Large	Small	Very large

Source: Ahmed et al., (2007a); Tuohy et al. (2015)

The key issue is that many wireless requirements have not been developed using the intra-vehicle application space in mind and therefore the technical specs usually do not match certain requirements. The short-range wireless technologies are within their infancy, and now we can get a few more iterations of those technologies in the future to ascertain which standard or strategy emerges due to the fact low-cost and high-performance in available on the market.

The simplified MAC protocol design and high-cost sensor node of RFID technology make it unsuitable for IVWSNs whereas the latency and reliability requirements for Bluetooth, the system complexity, cost, and power consumption requirements are too high. On the other hand, ZigBee promises wireless technology which is based on the IEEE 802.15.4 standard. It is low cost, low data rate, and low latency required short-range wireless technology. As well as some suitable improvements, that IEEE 802.15.4 represents the absolute most promising solution for IVWSNs (Gao, Wang, Wang, & Yao, 2018).

ZigBee products may well be more environmental than its predecessors saving megawatts at it complete implementation. Low priced (device, installation, maintenance) towards the users means low unit expense, low installation, and maintenance cost. ZigBee products enable batteries to endure up to years making use of main cells without the chargers. ZigBee permits inherent setup and redundancy of network products provides low-to-zero maintenance. The maximum density of nodes per network ZigBee's utilization of the IEEE 802.15.4 PHY and MAC enables the network to manage a variety of end devices. These characteristics are important for a large number of sensor arrays and control the networks. It is estimated that ZigBee allows the more easy and simple protocol compare to Bluetooth or IEEE 802.11 (Ramya, Shanmugaraj, & Prabakaran, 2011; Somani & Patel, 2012).

2.9 Critical Discussion on IVWSNs

Much work has been conducted on vehicular communications specifically for inter-vehicular, intra-vehicular and vehicle to infrastructures wireless-sensor-networks (WSNs). Due to uplifting demand for driver safety and assistant in a modern vehicle, the intra-vehicle WSNs become more interesting research area nowadays.

Consequently, different networking devices, e.g., UWB, RFID, Wi-Fi, Bluetooth, and ZigBee have been deployed inside a vehicle to facilitate communication.

In Jin et al. (2011), the authors investigated the performance of intra-vehicle communication in term of a different number of time bandwidth and transmitted pulses per symbol condition exploiting UWB technology. In Qu, Li, Yang, and Talty (2011), the authors evaluated the channel capacity of UWB with a multi-antenna approach for the high speed intra-vehicle wireless communication system. They also compared different UWB pulse modulation schemes for finding suited modulation scheme for in-vehicle communication systems in Khuandaga, Iqbal, and Kwak (2011). Again in (Bas & Ergen, 2012, 2013), the authors discussed the small and large scale path loss statistics using UWB band deployed sensors in different locations inside a car. In Sadi and Ergen (2013), the authors used a UWB channel in IVWSNs for investigating the optimal l power control, rate adaption and scheduling in one Electronic Control Unit (ECU) and multiple ECU cases.

Several works have been done exploiting RFID technology for Intra-vehicular communication. In Song, Li, Tang, and Zhang (2016), the authors proposed an in-vehicle sensors fusion strategy for positioning vehicle that is completely under GPS defined environment using RFID technology protocol. In Ferdous, Reza, and Siddiqui (2016), the authors investigated the most energy harvesting protocol for a wireless sensor network, and they proposed the RFID passive tag for renewable and sustainable energy harvesting for wireless sensor networks. In Yue, Zhang, Pan, Fang, and Chen (2012), they investigated how to design an efficient protocol for collecting data from deployed sensors in numerous locations in large-scale RFID systems. In Mandal et al. (2011), the author proposed an algorithm for a traffic monitoring system using combined active RFID and GSM technology.

Moreover, Bluetooth technology has also been introduced for such communication systems. In Kandhalu, Xhafa, and Hosur (2013), the authors proposed a solution to reduce power consumption of sensor nodes using Bluetooth technology for in-vehicle wireless communication. In (Bronzi, Frank, Castignani, & Engel, 2014; Lin, Talty, & Tonguz, 2015b), the authors reported that Bluetooth consumes low energy for an intra-vehicle wireless communication system. However, due to the poor efficient and less reliability of MAC protocol, requiring a high power level, supporting a number of insufficient end nodes, and propagation and security problem, the above technologies are not suitable for intra-vehicle wireless sensor networks especially for comparatively large network (Lu et al., 2014; Qu et al., 2010b; Zhang, Antunes, & Aggarwal, 2014).

On the other hand, ZigBee communication protocol is a viable and prominent technology for intra-vehicular communication that provides a real-time monitoring system to design low cost, low data rate, and low power wireless communication systems. In Iturri, Aguirre, Azpilicueta, Garate, and Falcone (2014), the authors investigated the radio channel of ZigBee in the complex vehicular environment. In Lin et al. (2015a), the authors examined the versatile platform for IVWSNs which enables side blind zone alert system for other vehicles. Other authors proposed a remote monitoring and controlling system for a home network based on ZigBee technology with the help of web service in Hwang and Yu (2012). In S.-K. Chen et al. (2012), the authors showed that the ZigBee communication protocol is the reliable transmission protocol for a patient monitoring system. In Rahman (2014b), the author analyzed the link and network reliability for ZigBee based intra-vehicle wireless sensor network. In Rahman, Kabir, Azad, and Ali (2015), they use ZigBee for tracking the vehicular positional coordinate with the aid of Vehicular Ad-hoc Network (VANETs). ZigBee is the viable and robust technology to design intra-vehicle wireless sensor network as analyzed by Bhargav and Singhal (2013). A designed and implementation for Hybrid-Backpressure Collection Protocol (HybridBCP) to joint load balancing and routing solution for data collection in an intra-car hybrid wired/wireless networks in Si, Starobinski, and Laifenfeld (2018). Hybrid-BCP is backward-compatible with existing intra-car wired technologies since no modification of the CAN protocol is needed. They demonstrate that the load balancing and routing functionalities of Hybrid-BCP in testbed experiments as proof of concept and Hybrid-BCP can be used to alleviate the impact of DoS attacks on the CAN bus. They have also shown that Hybrid-BCP is robust to jamming attacks on the wireless links.

All the aforementioned works are applicable for small networks where the numbers of end nodes are limited. It is noticed that all the existing solutions are suitable for small scaled network. Therefore, a scalable solution is needed to introducing the IoT concept with intra-vehicular communication since various types of sensor nodes are increasing day by day inside the vehicle for the demand of driver assistance, fatigue detection, road safety, and so on. Recently, researchers estimate that the numbers of sensor nodes inside the vehicle will be significantly increased by 2020 (Lu et al., 2014). In order to do reliable communication for such a scalable network will be challenging due to the internal complexity inside the vehicle. As a consequence, it is an important issue to investigate the performance of such a network by exploiting the ZigBee technology.

The summary of the literature in this section is briefly mentioned in Table 2.4 by indicating the main key points.

The table briefly describes the summery of the literature review by considering the applied technology, introducing the IoT concept, deemed network size, validation methods, and the implemented the mechanism of the network in the IVWSN environment.

Table 2.4 Summary of literature review

Author	Brief Description	Technology Used	IoT Concept	Network Size	Simulation	Test-Bed	Mechanism used
(Lin et al., 2015a)	IVWSN-based blind zone alert system	BLE standard protocol stack.	NO	Allows limited devices	NO	YES	
(Bas & Ergen, 2013)	Analyze the small-scale and large-scale statistics of the UWB channel beneath the chassis of a	UWB	NO	Moderately large	NO	YES	Vector network analyzer (VNA) (Agilent VNA 8719ES).
(Lin et al., 2015b)	Bluetooth Low Energy (BLE) and outline a new architecture for IVWSN	BLE	NO	Allows limited devices	NO	YES	CC2540 BLE chip
(Rahman , 2014b)	reliability analysis of intra-vehicle wireless sensor networks	ZigBee	YES	Large	YES	NO	CSMA/CA
(T.-Y. Huang, Chang, Lin, Roy, & Ho, 2015a)	propose an intra-vehicle network routing algorithm to simultaneously minimize the wiring weight and the wireless transmit power	ECU sensor network	NO	Small	YES	NO	Minimum cost maximum flow formulation(MCMF)

Table 2.5 Continued.

Author	Brief Description	Technology Used	IoT Concept	Network Size	Simulation	Test-Bed	Mechanism used
(Takayama & Kajiwara, 2016)	Measurements propagation degradation within the vehicle using UWB-IR in various locations using an antenna	UWB	NO	Moderately large	NO	YES	UWB-IR propagation
(Wampler, Fu, & Zhu, 2009)	Implementing security services on top of a higher level Controller Area Network (CAN) protocol	CAN	NO	Small	YES	NO	CAN network
(Nguyen, Singh, Le, & Soh, 2009)	Proposed a Hybrid TDMA MAC protocol which provides a Static Segment for periodic transmission as well as a	UWB	NO	Moderately large	YES	NO	TDMA MAC protocol
(Lu et al., 2014)	Discuss the potential wireless solutions for vehicle-to-sensor, vehicle-to-vehicle,	ZigBee	YES	Large	NO	NO	CSMA/CA
(Tuohy, Glavin, Jones,	Proposed an automotive network simulation which allows for the injection and extraction	CAN	NO	Small	NO	YES	CAN network

Table 2.5 Continued.

Author	Brief Description	Technology Used	IoT Concept	Network Size	Simulation	Test-Bed	Mechanism used
(Liu, Herbert, Table 2.5 Wassell,	Measurement effect of fading effect and interference by Continued. for Line-of-Sight (LOS) and	ZigBee	NO	Large	NO	YES	
(Jin et al., 2012)	Investigates the effect of MUI (multi-user interface e) on the performance of intra-vehicle UWB NCS (Networked control	UWB	NO	Moderately large	YES	NO	MUI and NCS
(Si et al., 2018)	Proposed a new model named Hybrid-Backpressure Collection Protocol (Hybrid-BCP), to efficiently collect data from sensors in intra-car networks.	ZigBee	No	Moderate	Yes	Yes	CAN and ZigBee

IoT-IVWSN is considered a network with a large number of various sensor nodes related to observing of the vehicle components and the status. ZigBee wireless technology supports a large number of sensor nodes in the network, and it is suitable for implementing in this environment. The others technologies like Bluetooth low power, USB, RFID that support an only limited number of sensor nodes in their network architecture.

2.10 Summary

The research contributions have reviewed in this chapter highlights the criticality of the IEEE 802.15.4 standard and the importance of improving it to support a diverse field of applications. Based on the flexible and autonomous concept of wireless sensor networks, opportunities have been created for exciting application areas requiring remote sensing and actuation for optimized results. However, the existing technology poses many issues that need to be handled for the long-term viability of developed systems. Issues like energy consumption for autonomous operation of sensor nodes dictate design and development issues including communication, protocols, and deployment. However, in the context of this review which describes the issues that are critical for application of WSN in IVWSN domain. It considers the various wireless technologies and their application in IVWSN and found out the individual problem of their communication protocols. This chapter also scrutinizes the problem-related IEEE 802.15.4 MAC protocol in regards to design IoT enable IVWSN.

CHAPTER 3

RESEARCH DESIGN AND METHODOLOGY

3.1 Introduction

In the literature review chapter has already mentioned the problem when the CSMA/CA mechanism of MAC of IEEE 802.15.4 protocol is introducing with IoT and high traffic load. This phenomenon happens because of the limitations of the existing MAC protocol. This section discusses the proposed method to overcome those limitations and also mention the hypothesis regarding those issues. Moreover, the MAC of IEEE 802.15.4 CSMA/CA mechanism includes several issues; the thesis will focus only the Backoff Exponent (BE) portion of MAC. Because this study assumes that, when the network with existing protocol want to transmit high traffic then the collision and congestion will happen. As a result, the network will be congested, and an end to end delay will be increased. To understand clearly the above-mentioned issues, firstly, the study needs to know the standard IEEE 802.15.4 MAC mechanism and its limitations. The subsequence paragraph will try to highlight the key point of MAC and also discuss hypothesis based on the proposed method. After an extensive literature review, this study has found the gaps and made the hypothesis to eliminate the gaps. This chapter discusses the developed method for validating the hypothesis by describing the following methodology flowchart in Figure 3.1.

1st Gap: Need to investigate the performance of the existing protocols which will work with IoT-IVWSNs.

1st Hypothesis: The Existing MAC protocols are not expecting to perform well in IoT-IVWSNs because of collision and congestion due to the high traffic of the network.

2^{nd} Gap: There has been no such MAC protocol proposed that adopt with IoT-IVWSNs.

2^{nd} Hypothesis: This study proposes a history based CSMA/CA MAC strategy that can be implemented in IoT-IVWSNs in order to mitigate congestion and collision in the network.

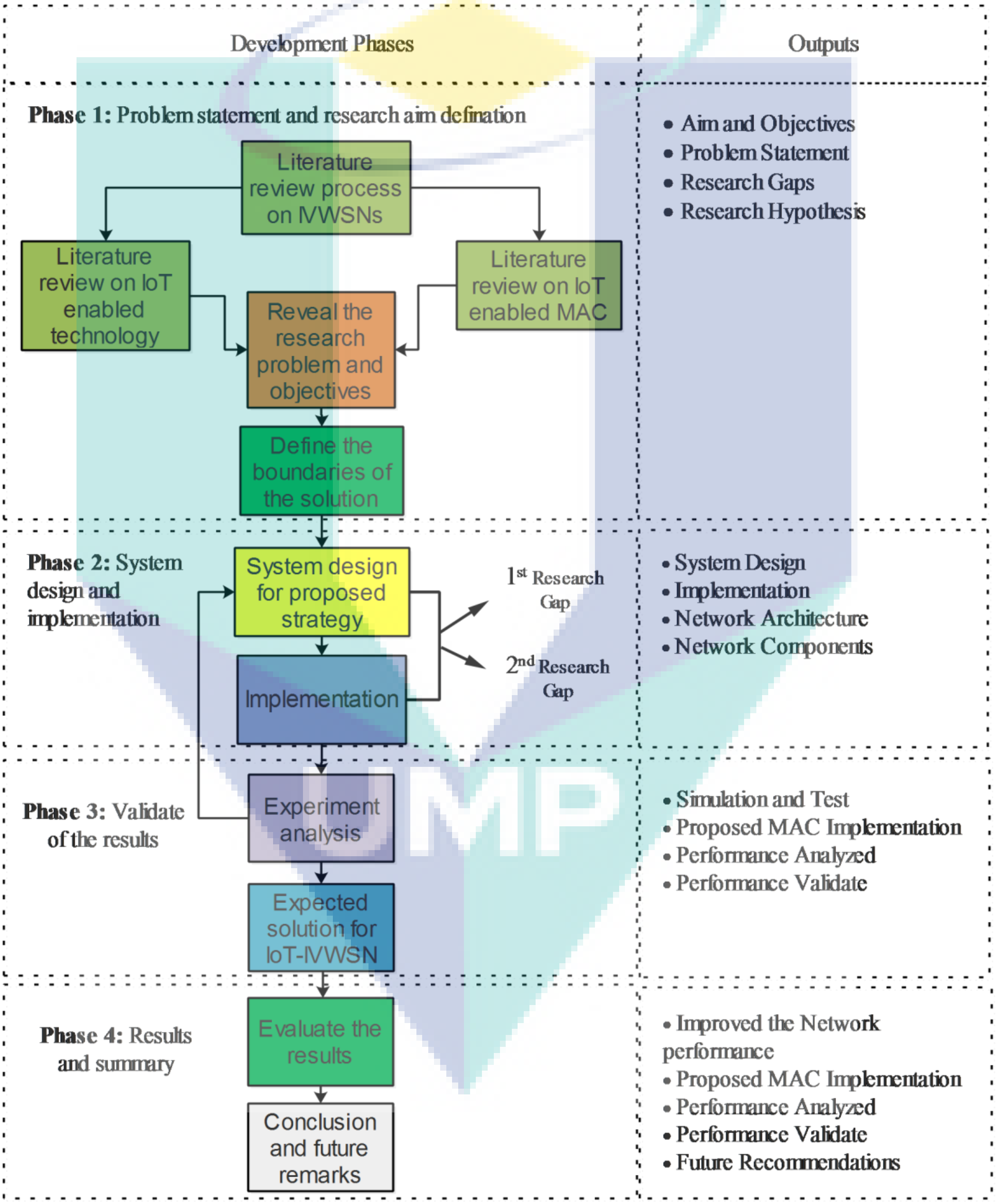


Figure 3.1 Flowchart of the methodology.

3.2 System Design and Implementation for Development of the First Research Gap

It is an important thing to implement a suitable communication protocol to get better performance and reliability of the network. Additionally, the network components, network architecture, and the system design issue play also an important phenomenon to get the overall output of the network. The consequent subsections discuss the system design and implementation for development of the first research gap.

3.2.1 Developing IoT Enabled IWVSNs

IoT can accommodate various nodes to be sensed and controlled remotely within the existing communication infrastructure. It makes integration of a computer-based system directly with the physical world. As a result, the efficiency, accuracy, the complexity of maintenance, and economic benefit of the system improve significantly. Moreover, nowadays modern vehicles are equipped with various types of sensors for improving driver safety, convenient transportation and traffic monitoring system.

Consequently, the numbers of sensor nodes inside the vehicle are increasing day by day. The existing wired Electronic Control Unit (ECU) device and subsystem integrated with Controller Area Network (CAN) has some problems due to limiting the range of sensor installation, and the network complexity. With the increase of sensors inside a vehicle, more wire connections are required for implementation. As a result, the weight, complexity, and manufacturing cost significantly increase (Bas & Ergen, 2013; Lin, Talty, & Tonguz, 2013; Lin et al., 2015a). Due to these reasons, the Intra-Vehicle Wireless Sensor Networks (IVWSNs) have recently been introduced to minimize the above complexity in the automotive industries. With the help of wireless technologies inside a vehicle, the weight, cost and the fuel consumption of the vehicle can be reduced, and better performance can be achieved. Therefore, a large number of nodes need to be integrated with each other for reliable and efficient communications. To realize this aim, in this thesis, the IoT concept is taken into account for designing IVWSNs referred as IoT enabled IVWSNs (IoT-IVWSNs), as shown in Figure 3.2. The IoT-IVWSNs can be defined in definition 3.1.

Definition 3.1 (IoT-IVWSNs): It refers the network where large numbers of sensors retrieve the status of the critical components of the vehicle and transmit them to the central entity in order to monitor the functionality of the system.

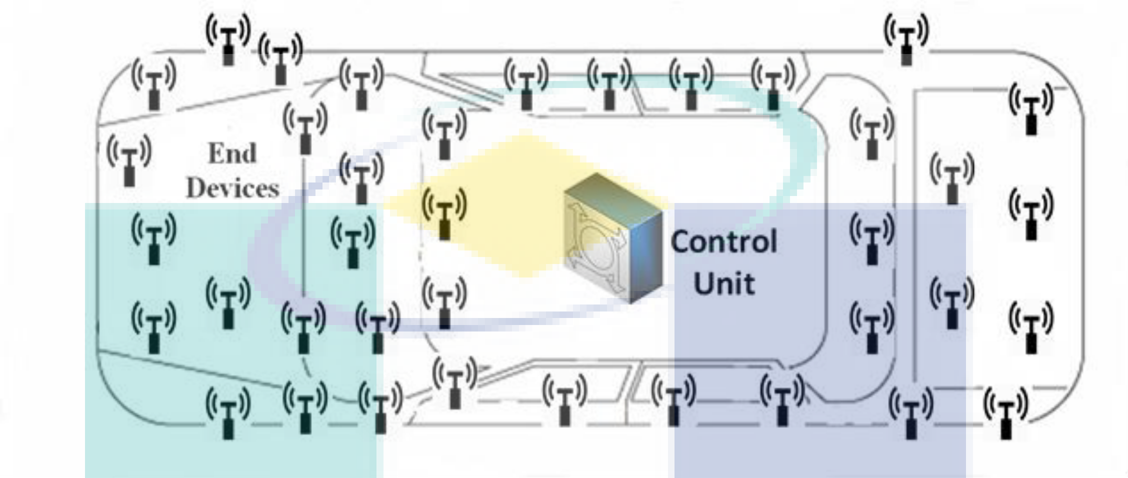


Figure 3.2 IoT enabled IVWSNs scenario

In the following sections briefly discuss the network components, network architecture and data flow of the network.

3.2.2 Network Components

This subsection will discuss the main and subcomponents of the network. The network mainly comprises three types of component namely, End Device (ED), Control Unit (CU) and Display. Each ED is embedded with a Transmitter and specific Sensor. Different type of sensors are installed (e.g., temperature sensor, speed sensor, defect sensor, water sensor, heat sensor, tire-pressure monitoring sensor, parking sensor, knock sensor, etc.) inside a vehicle to collect the current status of critical components of a vehicle. The sensors sense the information of a component and the transmitter, which is integrated with the sensor transmits the information to the CU. The CU also contains two types of subcomponents such as Transceiver and Processing Unit (PU). The Transceiver can receive and send data. The PU can decide whether the data will send to the display or not. If the new information is different from the old one, then it will send the result to display through Transceiver of CU. The display will show all the current status of the different components of the vehicle.

3.2.3 Network Architecture

The performance and reliability of a network depend on the proper design and the architecture of the network. Since the complexity of the network is increasing, future intra-vehicular communication needs to be properly designed. There is a critical and harsh environment inside the vehicle. So the network architecture should be adjusted. In this network architecture diagram as depicted Figure 3.3 (a), it can be seen that there are two tiers of the network, one is information acquisition, and another one is information processing (Rahman, Ali, Kabir, & Azad, 2017). The information acquisition section is collecting data from various components of deployed the different type sensor inside the vehicle. Then, the acquired data is received by the CU and processed by the PU in order to know the status of the vehicle. Here, it can be considered single hop star topology for the network. As a result, every ED can communicate with the same signal strength. The main advantage of this topology is to reconfigure the network to skip broken nodes, and it is possible to choose the shortest path to a certain destination. Moreover, the data flow of the network is shown in Figure 3.3 (b).

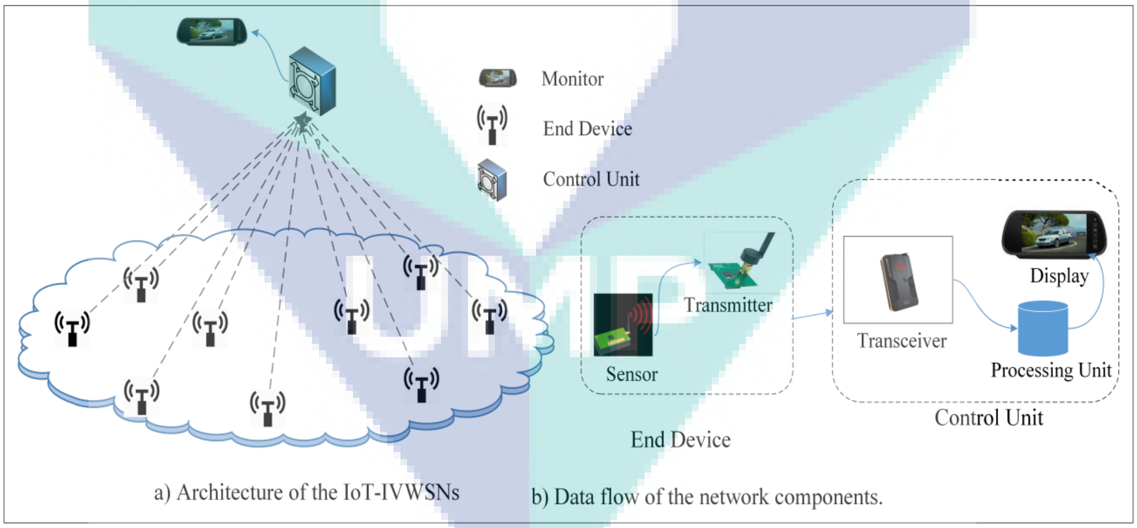


Figure 3.3 Network architecture and its data flow

3.2.4 System Design and Implementation

In order to design a IVWSNs system having robust connectivity, it is important to know the radio propagation characteristics in intra-vehicular environments. Also, the feasibility of different technologies, (i.e., the uniqueness of ZigBee, Bluetooth, UWB or RFID), to minimize the impact of interference and fading need to be explored since they have the potential to improve wireless channel quality while lowering transmit power and hence reducing power consumption. During the MAC layer, in order to quantify the latency guarantees supported by short-range wireless technologies, it models a wireless intra-vehicle subsystem as a star network topology. Even though some nodes are probably not in a position to achieve the CU over a single-hop focuses on single-hop star designs in this initial research while focusing on Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) because of its collision-free nature that is needed for providing latency guarantees.

Consequently, it concentrates on slotted scheduled MAC schemes, through the fully guaranteed time slots (GTS) into the contention-free duration (CFP) of IEEE802.15.4, where each sensor/switch reading fits precisely in one single time slot. It concentrates on the MAC and interference challenges within an individual intra-vehicle subsystem in the place of interference between various subsystems. Mitigating inter-subsystem interference and outside sourced elements of interference during the unlicensed 2.4 GHz organization calls for the growth of interference-resilient PHY layer waveforms that is out of scope in this thesis and it is a topic of future research (Ahmed et al., 2007a; Tuohy et al., 2015).

Vehicle manufacturers might progressively introduce wireless sensors into automobiles in the future to have the possible benefits of IVWSNs. Such a gradual scheme could begin from a few feasible forms of sensors; those are not safety-critical, those in hard-to-reach areas, or the ones that are easy and simple to change with wireless sensors. Additionally, for automobile manufacturers, the extra cost of the wireless equipment may be the major barrier for the implementation of IVWSNs (Lin et al., 2015a, 2015b). In order to massively deploy wireless sensors in automobiles, the system cost of a sensor with a wireless transceiver should not be higher than a typical sensor. The expense of a wireless sensor is dependent upon the selection for wireless technology as well as the complexity associated with the system. Consequently, an initiating point is always to determine and assess a viable wireless technology to aid the forms above of sensors. This type of sensors will often have subsequent requirements and properties (Blumenstein et al., 2015; Rahman, 2014a, 2014b).

To design reliable and viable wireless technology inside the vehicle, the following highlighted key points must be considered:

High Reliability: Reliability is amongst the key problems in IVWSNs. The technique has to deliver ascertained data transmissions to a destination point.

Short End to End Delay: For a few of the wireless sensor technology, having a short delay for example, for ZigBee a few milliseconds, is desirable since the system can be highly dynamic or require a prompt response.

Low Power Consumption: For some for the wireless sensors, their energy is supplied by a battery pack. Consequently, the energy usage for wireless communications needs to be low sufficient to guide an acceptable battery lifetime.

Low Data Throughput: The sensor data are really small, i.e., just a few bytes. For ZigBee, the packet size is 220 bits only.

Low Duty Cycle: A lot of the applications have a low duty cycle, e.g., significantly less than 5%. For ZigBee wireless sensor technology, the duly cycle is extremely low (<0.1%).

Low Cost: Lower complexity seems to indicate lower cost. Also, if the method can be implemented by an established existing wireless technology with minimum changes, then, it will be possible to reduce the cost.

Privacy and Security: The security and privacy of the system should be considered. ZigBee Specification includes lots of protection conditions and choices. In specific, ZigBee provides facilities to carry down protected communications, protecting the establishment and transportation of cryptographic secrets, cyphering frames, and managing devices. ZigBee improves the essential safety framework defined in IEEE 802.15.4.

3.2.5 Implemented Technology for IoT-IVWSNs

Many wireless sensor technologies have been introduced in recent years, such as Bluetooth, Wi-Fi, UWB, ZigBee and RFID. Every technology has specific criteria to operate in a suitable area (Lu et al., 2014). Such as, Bluetooth is a short-range wireless technology complying with IEEE 802.15.1 standard (Lin et al., 2015b). It can communicate up to 3Mb/s in portable devices. The transmission needs a high power level so that it is not appropriate for battery enabled sensors in the vehicle. Again, Ultra-Wideband (UWB) is a radio technology, which operates with 3.1-10.6 frequency band and supports short-range communication data rate up to 480 Mb/s. RFID physical layer waveform and simple MAC protocol design (coupled with high cost of RFID readers) make it unsuitable for WSN reliability and latency requirements (Ahmed et al., 2007a).

Additionally, ZigBee is a short-range communication technology maintaining IEEE 802.15.4 standard. It operates on the industrial, scientific, and medical radio band (ISM) radio spectrum (868 MHz, 915 MHz, and 2.4 GHz). It is characterized by low cost, high data rate, low power consumption, and supports star, mesh and hybrid topology. It has a long life battery and provides more security by its encryption technique. ZigBee transmission power is –25 dBm, which is significantly lower than others (Rahman, 2014a).

Moreover, it needs only 15 milliseconds to wake up. This emerging feature allows the transmission device to remain most of the time in sleeping mode, which preserves the device’s battery power. In (Rahman, 2014a, 2014b), the author has evaluated the performance for the intra-car wireless sensor network. This study showed that ZigBee is a viable and promising technology for the intra-car wireless sensor network. ZigBee is designed to last for six months to two years on just two AA batteries (Parthasarathy et al., 2016). Hence, IEEE 802.15.4 protocol is a good candidate to design IoT application with low power consumption. As a result, the ZigBee is expected to play an important role to design IoT-IVWSNs for future generation. Moreover, the ZigBee supports different types of network topology, and its MAC protocol is designed with CSMA/CA features that provide extra facilities to ensure data transfer robustly. The main advantage of this protocol is to allow large sensor nodes in a single network. The number of sensor nodes inside a vehicle continues to increase every year. So, this huge number of sensor nodes can be maintained through this protocol.

3.3 System Design and Implementation for Development of the Second Research Gap

According to the second hypothesis, it is assumed that it is necessary to develop a suitable MAC solution for IoT enabled IVWSNs to minimize the collision and congestion in the networks. The consequent subsections discuss the system design and implementation for development of the proposed MAC solution to fulfill those aims.

3.3.1 Proposed MAC Solution: History-Based MAC

In this subsection, the proposed MAC solution will be discussed, which is the enhancement of the IEEE 802.15.4 MAC protocol. In this protocol, nodes communicate with each other according to a slotted CSMA/CA protocol based on a superframe structure. Each superframe consists of an active period and an inactive period. The active period consists of a beacon period, a contention access period (CAP), and a contention-free period (CFP). During the inactive period, the coordinator and the nodes shall not interact with each other and may enter a low-power mode. Since the proposed protocol is the enhancement of the IEEE 802.15.4 MAC protocol, therefore, there are some similarities in both versions. Here, it only highlights the difference that mainly lies in the slotted CSMA/CA protocol. For detail information about the IEEE 802.15.4 MAC protocol refers to the paper (Shih, Chang, Chen, & Chen, 2010) to the reader. In the History-based MAC protocol, the CSMA/CA strategy consists of several steps with the enhancement of some highlighted parts, as shown in Figure 3.4.

The History-based algorithm of CSMA/CA strategy sets the relevant parameters such as a backoff exponent (BE) and the number of backoff stages (NB), while a node has a new data frame to transmit. This BE and NB are set according to the previous history of the sensor referred to as Saved BE (SBE) and Saved NB (SNB), respectively. During the first data transmission, the value of the BE and NB are set to macMinBE (default value =3) and 0, respectively, as similar to the traditional IEEE 802.15.4 MAC protocol. Since IoT enabled IVN is congested due to high traffic load, the traditional set up for BE and NB will be wasting CAP. Therefore, it prefers to set BE and NB according to the previous history of the sensor for utilizing the CAP. Before a station attempts to send a frame, it uniformly selects a backoff counter value from a window (0, 2^{BE-1}). The backoff counter value is decremented by one for each time slot, regardless of the channel state, i.e., the channel is busy or idle. This is the main difference with IEEE 802.11 MAC protocol, where backoff counter value is only decremented while the channel is idle otherwise it is frozen.

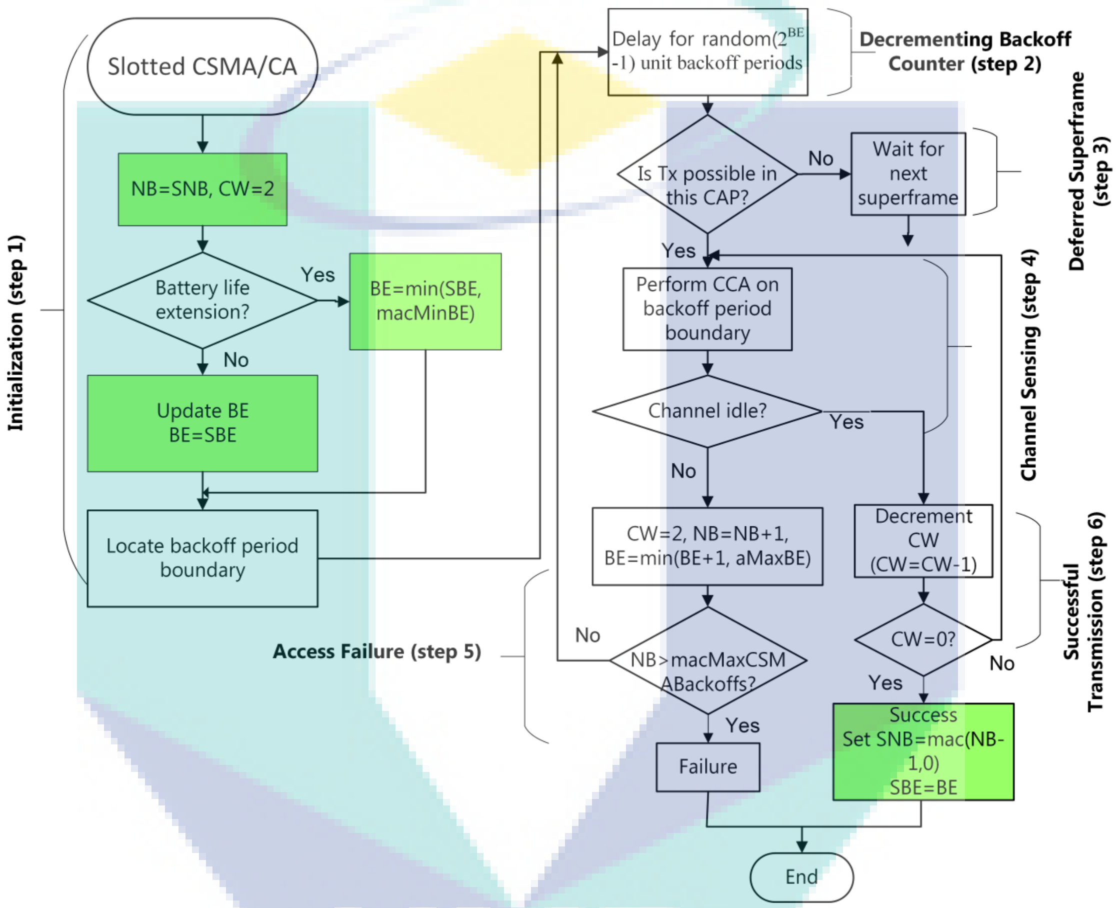


Figure 3.4 Flowchart of History-based CSMA/CA algorithm

Whenever the backoff counter value is zero, the node performs carrier sensing that requires two Clear Channel Assessments (CCAs) at the physical (PHY) layer before a transmission. If the current CAP does not have enough slots to do sensing then wait for the next superframe, otherwise, performs channel sensing. If the channel is not assessed to be idle at the two consecutive CCAs, then it increases the values of BE and NB by one and delays the transmission for a random number of time slots that are uniformly chosen from (0, 2^{BE-1}), where BE $\leq$ aMaxBE (default value 5). The above procedure is continued until the successful transmission; however, if the NB value is greater than macMaxCSMABackoffs, then the CSMA/CA algorithm shall be terminated with a channel access failure. If either a channel access failure occurs or a frame transmission failure occurs due to a collision, the node retries the procedure above for retransmissions up to aMaxFrameRetries times. If the channel is assessed to be idle at the two consecutive CCAs, then it transmits the data frame and set the SNB = max (NB-1,0) and SBE = BE. These values will be used for further communication.

The highlighted steps are indicating the major modifications of History-based CSMA/CA strategy over standard method. For the first time transmission of a node, the History-based behaves like standard one. However, it saves the parameters of current successful transmission of a node. For subsequence transmission, it utilizes the saved parameters to prevent the redundant initializing every time for each node's parameter.

3.3.2 Communication Parameters Selection

The 802.15.4 supports two types of MAC schemes, namely contention-based CSMA/CA MAC during the contention access period (CAP) and contention-free MAC during the contention-free period (CFP) using the concept of guaranteed time slots (GTS). The CAP and CFP periods alternate and they both constitute what is referred to as the MAC super-frame. The superframe is divided into 16 equally sized slots, where the beacon is transmitted in the first slot in the superframe. Even though it focuses on 802.15.4 in this analysis, the obtained results would apply on IoT enabled IVWSNs. It is assumed that the following communication parameters will be suitable for IoT-IVWSNs (Rahman, 2014a, 2014b). The appropriate network parameters are:

Transmit Power set: {-10, -15, -20, -25} dBm, which is suitable for ZigBee, such as the Crossbow MICAz MPR2400.

Carrier frequency: 2.4 GHz (ISM band), which is used on ZigBee sensor node.

Receiver sensitivity: The reception threshold of the CU is set equal to -95dBm, typical for ZigBee.

The distance between ED and CU: 1 to 6 meters (with intervals of 1 meter), which is usually cover the entire length (or more) of a passenger car.

Transmission Period: 10 ms (millisecond).

Packet size: 220 bits (ZigBee packet header 120 bits + data 100 bits);

Parameters MAC: Retransmissions have been disabled in order to focus on the quality of the connection.

3.3.3 Validation

The result is validated through the numerical discrete event simulator OPNET in term of different optimized communication parameters. The major performance metrics of a network are Collision Rate, Data Drop, Throughput, and End to End delay.

Collision Rate: Collision rate is the number of collisions happening in a network during a specified period. It shows the rate at which data collide or are missing in collisions. Collision rate is calculated as a percentage of the Frames correctly delivered. Collisions occur when two or more network nodes try to send data at the same time, causing in collisions and possible damage of transmitted data. This will result in the nodes having to resend the data, which may have a negative effect on system efficiency.

Data Drop: The numbers of data packets are dropped during the communication.

Throughput: Throughput refers to the efficiency of work by a calculating service during a specific period. It measures the amount of completed work versus time taken. Throughput is conceptualized to evaluate the productivity of the computer network. This is calculated regarding tasks per second.

End to End Delay: The time needed to cross the network is typically calculated as the period between the sender indicating that the transmission is to start, and the delivery of the last bit of the packet to the destination. This time is the total of times required to cross each sector of the network and includes a number of different contributions.

3.3.4 Result Analysis and Documentation

In order to validate the proposed model, an extensive experiment is conducted. The performance of the proposed solution: the History-based algorithm is analyzed based on the experimental results. Chapter 4 discusses the performance investigation of IoT-IVWSNs and the details of the experimental results are analyzed with History-based MAC solution. Finally, the thesis is ended up with the conclusion and future recommendations.

3.4 Network Simulator OPNET

The OPNET Modeler is used for developing, namely due to its accuracy and to its sophisticated graphical user interface (Biswas, 2017). The OPNET Modeler is an industry-leading discrete-event network modeling and simulation environment. The wireless module extends the functionality of the OPNET Modeler with accurate modeling, simulation, and analysis of wireless networks. This module is one of the several add-on modules available from OPNET (Koubaa, Alves, & Tovar, 2006). The actual version of the simulation model only supports the star topology where the communication is established between devices, called inside the model End Devices (EDs), and a single central controller, called PAN Coordinator. Each device operates in the network must have a unique address. The sensor node model is comprised of four functional blocks: (1) The physical layer consists of a wireless transceiver (rx for reception and tx for transmission) compliant to the IEEE 802.15.4 specification operating at the 2.4 GHz frequency range, where each channel has a bandwidth of 2 MHz. The modulation scheme is Quadrature Phase Shift Keying (QPSK). (2) The MAC sublayer implements the slotted CSMA/CA It is also responsible for generating beacon frames and synchronizing the network when used in a PAN coordinator node. (3) The battery module computes the consumed and remaining energy levels. (4) The application layer consists of two generators (Jurčík & Koubâa, 2007). The sensory data module generates unacknowledged frames, and the MAC command module generates acknowledged frames.

This work has developed a CSMA/CA MAC strategy over the IEEE 802.15.4 slotted CSMA/CA technique using OPNET network simulator. This thesis uses the default wireless models of OPNET library for emulating the acknowledgement wait duration, a number of retransmission, maximum backoff exponent, the maximum number of backoff, and average bit error rate. Therefore, to measurement the time for end-to-end delay in the network, some communication parameters have been selected as shown in Table 4.2. The network layer has been implemented according to the ZigBee specifications, whereas the MAC and PHY layers are compliant to the IEEE 802.15.4 specifications. The following physical channel attributes are set as follows. The transmit power is set to -15 dBm, the path loss model is set Rayleigh fading with NLOS is $\gamma = 4$, and the reception threshold for the coordinator is -95 dBm. The sensing sensitivity is set to 0.1 seconds, thus enabling each node to detect the channel as busy if any frame is being transmitted. The acknowledgement wait duration is set 0.05 second. The number of retransmissions is set five times. The number of minimum and maximum backoff exponent is set three and four times, respectively. The transmission period for each sensor node is 120 milliseconds (ms) for low traffic load and 60 milliseconds for high traffic load. Four types of traffic load are considered in this thesis, namely Low-Traffic-Load (all are 120ms EDs), Medium-Traffic-Load (70% 120ms and 30% 60ms EDs), Relatively-High-Traffic-Load (50% 120ms and 50% 60ms EDs) and High-Traffic-Load (30% 120ms and 70% 60ms EDs). Furthermore, to vary the network size, it considers four types of scenarios i.e., Scenario-I, Scenario-II, Scenario-III and Scenario-IV which consist of 50, 70, 90 and 110 EDs, respectively. The simulation is conducted hundred times for each scenario and it measures the delay of end to end communication of the network.

The simulation scenario for 70 EDs is shown in Figure 3.5 in which the each ED is connected with the single coordinator. The coordinator collects the data from the ED and process for the further actions. The maximum distance of EDs from the coordinator is 6. The transmit power is set for each sensor node is -15 dBm. The star network topology is considered. Figure 3.6 shows the parameter setup for the history-based CSMA/CA MAC algorithm.

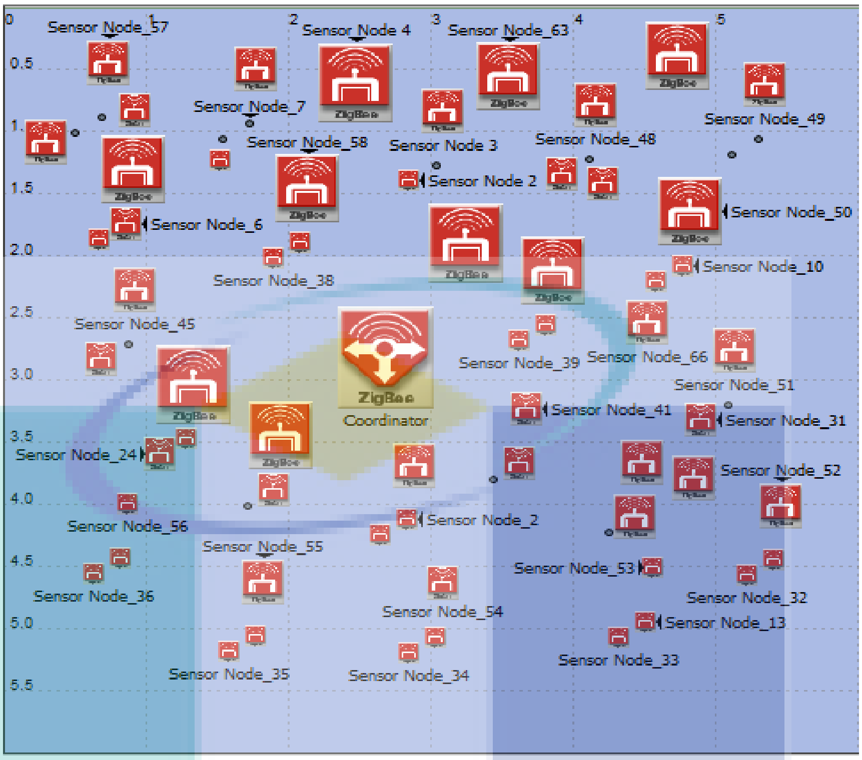


Figure 3.5 Simulation scenario for 70 EDs

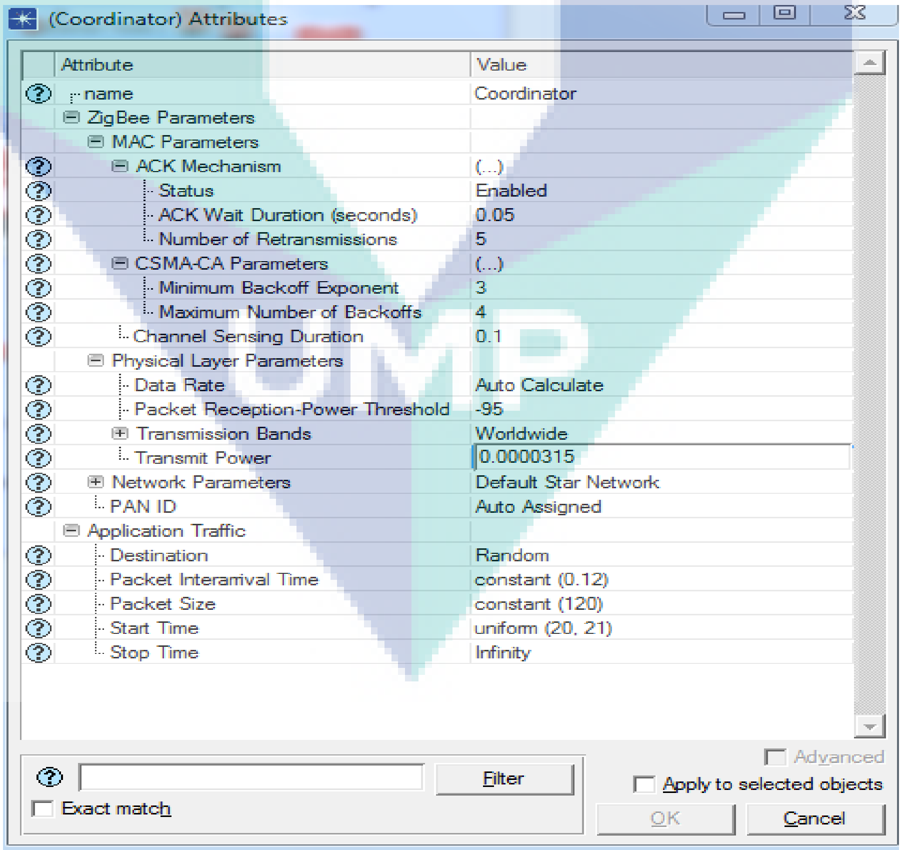


Figure 3.6 Parameter setup for the coordinator

3.5 Summary

This chapter has developed two model in the IoT-IVWSN based on two hypothesizes. The 1st developed model has designed the IoT-IVWSN environment to investigate the network performance. In this case, it considers the various network components like sensor node, transmitter, receiver, and monitor. After that, it creates network architecture by considering the optimal network topology suited with IoT-IVWSN. It also includes the system design issues like high reliability, short end to end delay, high throughput, low power consumption, and low duty cycle in the network. The suitable wireless technology has been selected to implement in the IoT enabled environment for deploying a large number of the sensor node. The second developed method has designed a history-based CSMA/CA MAC strategy for IoT-IVWSN environment. It considers the optimal tuning based communication parameters to design such an environment.

CHAPTER 4

RESULTS AND DISCUSSION

4.1 Introduction

In this chapter, the outcome of the work is presented by considering two discussion phases. The first phase explores the limitations of existing CSMA/CA MAC strategy by investigating the network performance under different network sizes (small to large). It also considers the link design between the end devices and the coordinator by examining the type of channel. The second phase develops a MAC strategy named History-based over default IEEE 802.15.4 CSMA/CA beaconed enabled technique by considering different optimal communication parameters for the IoT-IVWSNs environment.

4.2 Performance Investigation of IoT-IVWSNs

This study defines the IoT-IVWSNs as the network where large numbers of sensors are connected with each other for monitoring the different critical component information of the vehicle in order to develop a smart vehicle system. The network congestion and collision problem can play a vital role to degrade the overall performance of the network due to increasing the number of nodes. In this case, it is necessary to find out the main reason for decreasing the network performance and provide a suitable solution by considering compatible network architecture and different optimal network parameters, especially for this environment. This section investigates the performance of IoT-IVWSNs by considering the criteria mentioned above.

The concept of the Internet of Things (IoT) can be utilized in vehicular communication since the number of sensor nodes in vehicles is raising tremendously because of the uplifting demand of applications for security, safety, and convenience. In order to do the communication among these nodes inside a vehicle, controller area network with wired architecture provides a prominent solution. However, this solution is not flexible because of the architectural complexity and the demand for a large number of sensors inside the vehicle; hence wired architectures are replaced by wireless ones. Moreover, scalability will be an important issue while introducing the IoT concept in Intra-Vehicular Wireless Sensor Networks (IVWSNs). In this chapter, a comprehensive performance investigation on IoT enabled IVWSNs (IoT-IVWSNs) has been carried out in order to address this issue. i) The complete overview of the IoT-IVWSNs with a comparative study of the existing technologies and the design challenges for such network are provided, ii) the link design between an end-device and the control unit is analyzed, and iii) the performance of the network has been investigated, and some open research issues are addressed. The results reveal that delay in packet transmission increases due to higher traffic loads and number of end-devices (Rahman et al., 2017). This result demonstrates that existing MAC protocol works well for a small network (i.e., a network with maximum 50 nodes) but is not suitable for a large network (i.e., a network with more than 50 nodes). The outcome of this research helps to design a smart car system (Rahman et al., 2017).

4.2.1 Performance Analysis of IoT-IVWSNs

This section presents a detailed evaluation of performance investigation of IoT-IVWSNs. The aim of this section arises two questions: (i) Is the IEEE 802.15.4 MAC compatible to run with IoT-IVWSNs? (ii) What are the criteria should improve to get better performance of IoT-IVWSNs environment to compare to existing methods by considering key performance metrics in the networks?

To answer these questions, an extensive performance investigation experiment has been conducted by considering various optimized communication parameters in IoT-IVWSNs environment.

- This study has implemented the IoT-IVWSNs scenarios by considering network architecture, system design and suitable communication parameters of the network such as backoff exponent, number of backoffs, transmission power, nature of the channel, and reception threshold.

- This study has also implemented the network in a large size(comprises 10 to 110 sensor nodes) by considering for both high and low traffic to verify the performance and find the key trigger of performance metrics degradation.

4.2.2 Link analysis between End-Device and Central Entity

In this sub-section, it is analyzed the link between ED (end Device) and CU (Control Unit) of IoT-IVWSNs in terms of throughput and received power. In order to do that, it has been carried out a simulation through discrete event simulation software called OPNET, with the relative packages for the ZigBee module. It considers the analysis of single link reliability between CU and ED since the design of an IVWSNs cannot be separated from the study on the link between the different sensor nodes distributed in the vehicle. A pair of the transmitter (i.e., ED) and receiver (i.e., CU) communicates each other within a vehicle. The CU collects the packets that are transmitting periodically by the ED. The CU and the ED are placed at a distance d. The path loss model is defined at " d " distance between transmitter and receiver in a wireless sensor network by the following equations:

At distance d, path loss P_L is defined as

$$P_L = P_t / P_r > 1 \quad 4.1$$

Where P_t = Transmitted power and P_r = Received power. Path Loss (P_L) represents signal attenuation and is defined as the difference between the effective transmitted power and received power.

The above equation can be expressed in dB units as:

$$P_L\ (dB) = 10\ \log_{10}(P_t/P_r) \quad 4.2$$

Moreover, the logarithm distance path loss model can be expressed as:

$$P_L\ (dB) = P_L(d_0) + 10\,\gamma\,\log_{10}(d/d_0) + X\sigma \quad 4.3$$

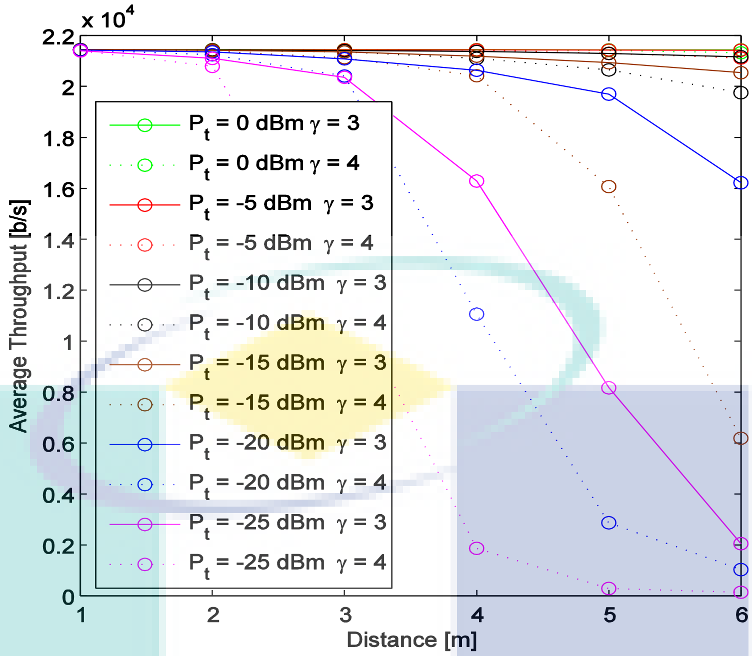
Where $X\sigma$ is a Gaussian random variable, γ is the path loss exponent and σ is the standard deviation, $P_L(d_0)$ is the path loss in dB at the reference distance d_0. The smaller value of σ indicates better accuracy of path loss model.

The performance of this model not only depends on the distance between transmitter and receiver, but also the path loss exponent and the variance of the lognormal shadowing.

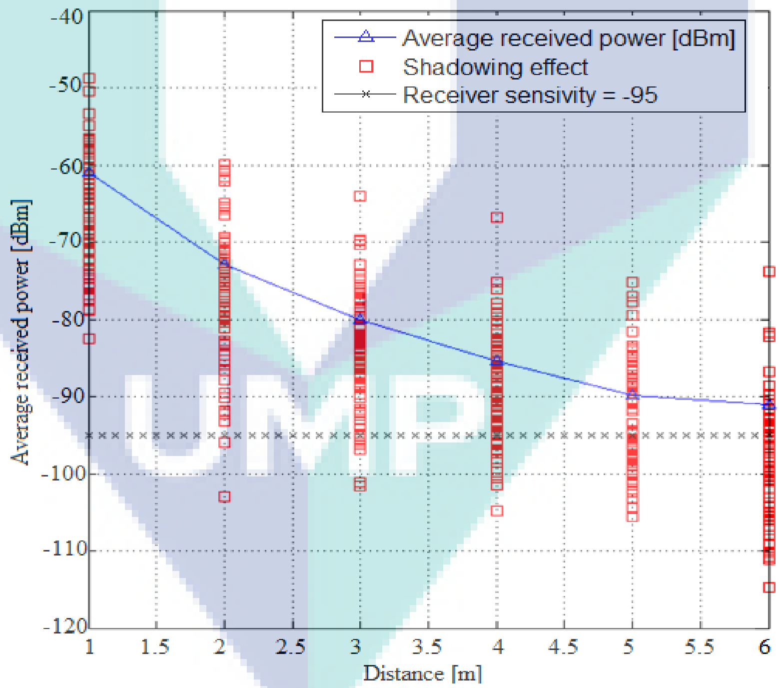
Throughput is defined as the total number of data traffic successfully delivered to 802.15.4 MAC layer of the receiver and sent to the higher levels in per unit time.

The ED and CU are placed at a distance d, where Distance Set: {1, 2, 3, 4, 5, 6}. It is also considered a set of Transmit Power (denoted by Pt) (i.e., {0, -5, -10, -15, -20, -25} dBm), as it is suited for ZigBee (Qu et al., 2010b). Considered Carrier Frequency (Cf) is 2.4 GHz. It is also considered both Rice and Rayleigh fading distribution functions in order to analyze Line of Sight (LOS) and Non-Line of Sight (NLOS) propagation paths where the value of K is 20.16 dB and 16.08 dB, respectively. The path-loss exponent γ set is {3,4}. The shadowing deviation σ is considered as 8 dB.

Figure 4.1 investigates the performance of the IoT-IVWSNs in terms of average throughput. It is observed that the average throughput of the network declines with the increase of the distance and decrease of the transmission power (Pt), as exhibited in Figure 4.1 (a). This is understandable according to the path-loss model where the path loss increases with distance, and the effect of the log-normal shadowing involves a fluctuation of the time of the received power, which can further degrade the performance of the communication (Ross & Schuhmacher, 2017; Uddin, 2016). Due to this fluctuation, the received power may go below the Receiver Sensitivity (Rs) (-95 dBm). Thus CU considers the received signal as noise that leads to lower throughput. Again, the result shows that the performance of the network is better in the case of Rician fading compared to Rayleigh fading because of the presence of dominating signal component, as depicted in Figure 4.1 (b).



(a) Path-loss exponent γ= 3



(b) Path-loss exponent γ= 4.

Figure 4.1 Effects of Log-normal Shadowing on the received power.

To clarify the above issue, it is shown in Figure 4.1 (a) the effect of log-normal shadowing, with σ = 8 dB, on the received power when the ED transmits with power Pt = 25 dBm and γ = 3. The results clearly show the distance increases; it increases the probability that the received power level falls below RS, even when the average received power is greater than the threshold (X. Chen, Ng, & Chen, 2016). Moreover, a packet may be discarded, even if it has received power level is greater than the threshold, but the Signal-to-Noise Ratio (SNR) is not sufficient for the correcting the packet(Ganesh & Amutha, 2013). If the SNR is not sufficiently high, it can happen that a number of bits within the packet are incorrect. Unlike Figure 4.1 (b), when γ = 4 the effects of shadowing can bring the received power below the RS even when the distance between CU and ED is 2 meters. Based on the above discussion, the considered communication parameters are summarized in Table 4.1. There are ten parameters have been used for the experiment.

4.2.3 Performance Evaluation

This section investigates the performance of IoT-IVWSNs by varying the traffic load, and network nodes since these features play an important role after introducing IoT concept on IVWSNs in order to address the scalability issue (Abdmeziem, Tandjaoui, & Romdhani, 2016; Snigdh & Gosain, 2016). Suitability of the communication parameters is justified in the previous section, as listed in Table 4.1. In order to investigate the network performance, the study uses discrete event simulator, OPNET, with ZigBee module. Four types of traffic load are considered in this experiment, namely Low-Traffic-Load (all are 120ms EDs), Medium-Traffic-Load (70% 120ms and 30% 60ms EDs), Relatively-High-Traffic-Load (50% 120ms and 50% 60ms EDs) and High-Traffic-Load (30% 120ms and 70% 60ms EDs). Furthermore, to vary the network size, here consider four types of scenarios. The scenarios are Scenario-I, Scenario-II, Scenario-III and Scenario-IV which consist of 50, 70, 90 and 110 EDs, respectively.

Table 4.1 Communication Parameters

Name	Value
P_t	-15 dBm, it has mentioned in the previous section
C_f	2.4 GHz (ISM band) that is used for sensor node (Rahman, 2014a)
R_s	The reception threshold of Coordinator of ZigBee is set equal to -95 dBm, it is usually for ZigBee Module (Rahman, 2014a)
Transmission Period	120 ms and 60 ms for low and high traffic, respectively
Packet size	210 bits
Channel	The path loss exponent for Rayleigh fading with NLOS is $\gamma = 4$ The shadowing deviation is 8 *dB*. This value is appropriate for intra-vehicle communication (Rahman, 2014a).
Acknowledgment Wait Duration	0.05 second
Number of retransmissions	5
Minimum Backoff Exponent	3
Maximum Number of Backoffs	4
Channel Sensing Duration	0.1 second

From Figure 4.2, the result shows the number of EDs and traffic load increase in IoT-IVWSNs, CDF extends to the right implying rising delay times. Performance worsens when the number of EDs as well as the traffic load increases which bring about the collision among the packets (Jabeen, Khan, Khan, & Jan, 2016). When the collision occurs among the packets of ED, the ED needs to wait until the allocated next time slot begins and the channel is free. It again tries to retransmit the failed packet that already made collision previously. The new re-transmissions may again cause another collision. This recursive procedure is clarified in the CSMA-CA protocol. From the above discussion, it can be noted that the end-to-end delay of the network increases when the number of collision rises among the packets (Rahman et al., 2015).

In addition, with the increasing number of EDs with high traffic load, congestion continues to grow for IoT-IVWSNs. This network can handle the traffic up to a certain point, when the traffic increases beyond that point, the network begins to enter into congestion. As a result, a number of packets of ED will be delayed to reach to the destinations. The more congestion in the network implies that the more packets will be delayed to reach to the destination. Additionally, it is noticed the distorted result.

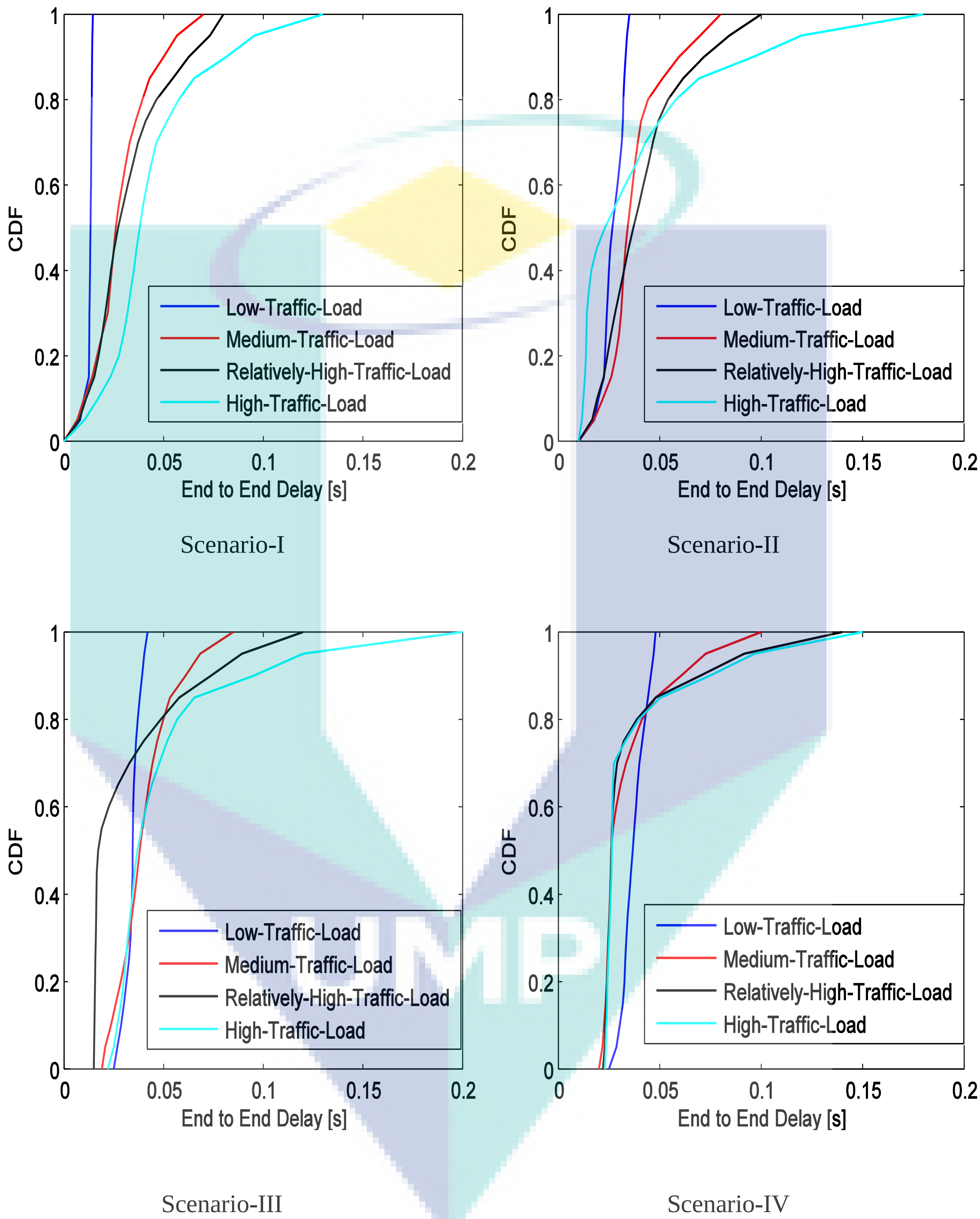


Figure 4.2 CDF versus End to End Delays: varying Traffic-Load and Network Size.

While with the increasing of traffic load, CDF becomes lower than the low traffic load scenario. In this situation of congestion decreases the end-to-end delay that causes the different trajectories of the CDF curves, since in OPNET the end-to-end estimated delay depends on the of packets that already reached to their destination.

This subchapter investigates the performance of IoT enabled Intra-Vehicular Wireless Sensor Networks. The overview of IoT-IVWSN is presented considering its architecture, components, suitable existing technologies, and the design challenges. The communication link between the ED and the CU is analyzed by selecting the suitable communication parameters. The selected parameters were obtained as: transmit power Pt = -15 dBm, channel frequency Cf = 2.4 GHz, transmission period = 60-120 milliseconds, packet size = 210 bits, and channel path loss exponent $\gamma = 4$. Using these parameters, the studies designs the network scenario and investigate its performance by varying the traffic load with average inter-arrival time 60 to 120 milliseconds and network size with 50 to 110 nodes. The test results demonstrate that delay in packet transmission increases due to higher traffic loads and a larger number of end nodes. The result shows that existing MAC protocol is not scalable, i.e., it works well for a small but is not suitable for a large network. The behavior of the scalability of IVWSNs significantly changes due to collision, congestion, and collaboration in the network. A suitable MAC protocol design could provide the best solution for such a network, which will be discussed in the subsequence sections of this thesis.

4.3 Performance Evaluation of Proposed Solution: History-based MAC for IoT-IVWSNs

In this section, the performance of the History-based MAC is evaluated via discrete event network simulator OPNET and compared with the IEEE standard 802.15.4 MAC. The performance metric the End-to-End delay of the network is evaluated.

The emerging concept of IoT is a rapidly expanding area in automotive electronic fields to make them as a smart scenario. The IoT enabled Intra-Vehicular Wireless Sensor Networks (IoT-IVWSNs) is a network integrated by a large number of sensor nodes inside the vehicle in order to provide real-time information of different parts of the vehicle. However, the network congestion and collision among packets play an important role in IVWSNs because of high traffic load and the huge number of sensor nodes are installing nowadays. Currently, various types of sensor nodes are integrated inside the vehicle to provide driver assistance, road safety, fuel efficiency, easy assembly, and reduce the cost. However, to design faster and reliable wireless communication protocol is quite difficult because of the internal architecture of the vehicle. In the real-time scenario, the crucial phenomenon is to allocate the time slot efficiently for each node to perform traffic flow transmission smoothly in IEEE 802.15.4 communication protocol. Furthermore, it is important that Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) algorithm IEEE 802.15.4 protocol is able to ensure the performance of each sensor node through its medium especially for the time-critical environment. Therefore, this subchapter proposes a reliable and IoT-IVWSNs suit MAC solution called History-based MAC which ensures the network performance by minimizing the congestion and collision for time-critical phenomena like IoT-IVWSNs.

4.3.1 Proposed Solution: History-Based CSMA/CA MAC for IVWSNs

To mitigate the data collision and congestion of the network, this study proposed a History-based MAC strategy especially for IVWSNs using emerging IEEE 802.15.4 MAC protocol.

The History-based CSMA/CA algorithm is developed over standard IEEE 802.15.4 MAC protocol with some modifications as shown in Figure 4.3. The node communicates through a superframe time slot in the beacon-enabled mode of CSMA/CA mechanism. The superframe consists of two time slots, namely active period and an inactive period. The active period is made with a beacon period, a contention access period (CAP), and a contention-free period (CFP). The coordinator does not communicate with sensor nodes during the inactive period.

The slotted CSMA-CA mechanism uses the Binary Exponential Backoff (BEB) algorithm to minimize the probability of congestions and collisions among the packets in the wireless channel. The BEB initializes the relevant parameters like the Number of Backoff stages (NB), the Contention Window (CW), and the Backoff Exponent (BE) before attempting any transmission. While a node attempts to transmit a data frame, it uniformly chooses a backoff counter value in the range $(0, 2^{BE-1})$. This value is decremented by one for each time slot. When this value becomes zero and has enough time slots in the CAP, the node completes two times Clear Channel Assessment (CCAs) before attempting any transmission. If the channel is not accessed in two consecutive

CCA, the value of BE and NB will be increased with the range (0, 2^{BE-1}) random time up to BE ≤ aMaxBE. The above procedure will continue until the successful transmission. The CSMA/CA algorithm will be terminated while NB> macMaxCSMABackoff (Khanafer et al., 2014; Rahman et al., 2015).

1: Initialization
2: Initialize *CW = 2*
3: *If* first time data transmission for a node **then**
    $NB = NB_{min}$
    $BE = BE_{min}$
4: *Else*
    Initialize *NB = SNB*
    Initialize *NB = SNB*
    Lable: 1
    The//Decrementing backoff counter
5: *While BE! = 0*
    BE = BE - 1
    //deferred superframe
6: *If* Tx is possible in this CAP **then** //channel sensing
    Perform CCA on backoff period boundary
7: *If* the channel is idle for two consecutive CCA **then**
    // transmission successful
    SNB = max(NB – 1, 0)
    SBE = BE
8: *Else*
    CW = 2
    NB = NB + 1
    BE = min(*BE* + 1, aMaxBE)
9: *If NB* > macMaxCSMAbackoff **then**
    Transmission failure
10: *Else*
    Go L1
11: Wait for next superframe

Figure 4.3 History based Slotted CSMA/CA MAC algorithm

The slotted CSMA-CA mechanism uses the Binary Exponential Backoff (BEB) algorithm to minimize the probability of congestions and collisions among the packets in the wireless channel. The procedures of the History-based algorithm are described step by step in the following points:

1. ***Parameter Initialization*** When a node needs to transmit a data frame, it initializes the relevant basic parameters such as contention windows (CW), backoff exponent (BE) and the default number of backoff stages (NB). The successful transmission parameters of a node which contains BE and NB is saved as Saved BE (SBE) and Save NB (SNB), respectively. While a node is at a first data transmission mode, it sets the macMinBE (default value=3) and 0 for BE and NB respectively. Hence, the IoT-IVWSNs is supposed be congested because of high traffic load and a large number of the sensor node, the parameters like BE and NB of traditional one is set every time for each node that leads to waste of CAP. It that case, it chooses the value of BE and NB from previous successful transmission history of the node for preventing the wasting of CAP.

2. ***Decrementation of Backoff counter*** While a node attempts to transmit a data frame, it uniformly chooses a backoff counter value in the range (0, 2^{BE-1}). This value is decremented by one for each time slot whether the channel is busy or idle.

3. ***Deferred Superframe*** When the backoff counter value becomes zero and has enough time slots in the CAP, the node completes two times Clear Channel Assessment (CCAs) before attempting any transmission at the physical (PHY) layer. If the current CAP unable to sense because of insufficient time slot then it needs to wait for next superframe, otherwise proceeds for channel sensing.

4 ***Channel Sensing*** If the channel is not accessed in two consecutive CCA, the value of BE and NB will be increased with the range (0, 2^{BE-1}) for random time up to BE ≤ aMaxBE (aMaxBE is a default value which is 5).

5 ***Access Failure*** The above procedure will continue until the successful transmission. The CSMA/CA algorithm will be terminated while NB > macMaxCSMABackoff with a channel access failure. If this failure is caused for collision, then the node retries the aforementioned procedure for retransmissions up to aMaxFrameRetries times.

6. Successful Transmission If the channel is assessed to be idle at the two consecutive CCAs, then it transmits the data frame and set the SNB = max (NB-1,0) and SBE = BE. These values will be used for further communication.

4.4 Validate the Proposed Solution: History-Based MAC

The details experiment setup, simulation environment, and the analyzing results are evaluated of Proposed Solution: History-Based MAC in the subsequence subsections.

4.4.1 Experimental Setup

The simulation model configured in OPNET discrete event network simulator is presented. The main objective of the simulations is to show how the IoT-IVWSNs designed to give the performance and pave the way to design a new MAC strategy to improve the performances of such networks.

Therefore, to validate the performance, end-to-end delay is selected as metrics for performance evaluation by adjusting different communication parameters as shown in Table 4.2. The network layer has been implemented according to the ZigBee specifications, whereas the MAC and PHY layers are compliant to the IEEE 802.15.4 specifications. The proposed strategy has been introduced into the MAC layer as a manager for the IEEE 802.15.4 MAC protocol.

One of the key mechanisms of the History-based MAC strategy is to save the previous successful parameters of packets which did not commit any collision within the network. This saved value of parameters is subjected to use further communication parameters of subsequence packets with some mandatory changes.

Table 4.2 Communication Parameters for History-based MAC for IVWSNs.

Name	Value
Pt	-15 dBm, it has mentioned in the previous section
Cf	2.4 GHz (ISM band) that is used for sensor node (Rahman, 2014a)
Rs	The reception threshold of Coordinator of ZigBee is set equal to -95 dBm, it is usually for ZigBee Module (Rahman, 2014a)
Transmission Period	120 ms and 60 ms for low and high traffic, respectively
Packet size	210 bits
Channel	The path loss exponent for Rayleigh fading with NLOS is $\gamma = 4$ The shadowing deviation is 8 dB. This value is appropriate for intra-vehicle communication (Rahman, 2014b).
Acknowledgment Wait Duration	0.05 second
Number of retransmissions	5
Minimum Backoff Exponent	3
Maximum Number of Backoffs	4
Channel Sensing Duration	0.1 second

The network topology is a single hop star configuration, and the area in which nodes are distributed is set at ten meters as considered inside the vehicle environment. Each node is provided with an onboard sensor that generates data packets with a fixed size of 210 bits at the application layer. Variable transmission periods are chosen for low to high traffic load since the WSNs are often used in applications aimed at simultaneously or periodic environmental monitoring. Moreover, it considers particularly high packet rates, which are usually used, for instance, in frequent surveillance the critical condition of various components of the vehicle (e.g., tire pressure, temperature, water level, etc.). The channel sensing time has been set 0.1 second which is the duration for which each channel will be scanned for beacons after the beacon request is sent out. The Pt indicates the transmission power with -15 dBm which is suitable for a sensor node of the ZigBee module in OPNET. The transmission frequency band used is worldwide that is 2.4 GHz. It is also considered both Rice and

Rayleigh fading distribution functions in order to analyze LOS and NOLOS propagation paths where the value of K is 20.16 dB and 16.08 dB, respectively. The path-loss exponent γ set is {3,4}. The shadowing deviation σ is considered as 8 dB.

Furthermore, for designing several network scenarios for analyzing the result for traditional MAC strategy for IoT-IVWSNs, four types of network scenarios are considered with varying traffic load as shown in Table 4.3. In order to investigate the network performance in a scalable fashion, different sizes of networks are considered. The subsequent studies evaluate the performance considering the measurement metrics end-to-end delay of Cumulative Density Function (CDF) and packet delivery ratio in the network.

There is only one BS that is placed in the center of the vehicle, and several numbers of SNs are placed around it. There are two different SNs: one is Green (G), and other is Yellow (Y), whose transmission period is 120 milliseconds and 60 milliseconds, respectively. The scenario considers four different cases according to the traffic load in the networks as shown in Table 4.3. In the first case, 100% Green, in the second case, 70% Green and 30% Yellow, in the third case 50% Green and 50% Yellow, and in the fourth case, 30% Green and 70% Yellow SNs are considered from the total sensor nodes. The more number of Yellow SNs means the more traffic in the network because of its less transmission period.

Table 4.3 Different combinations of traffic load.

Number of Sensor Node (SN)	**Scenario I**		**Scenario II**		**Scenario III**		**Scenario IV**	
	Green (%)	**Yellow (%)**	**Green (%)**	**Yellow (%)**	**Green (%)**	**Yellow %**	**Green (%)**	**Yellow (%)**
10	10	0	7	3	5	5	3	7
30	30	0	21	9	15	15	9	21
50	50	0	35	15	25	25	15	35
70	70	0	49	21	35	35	21	49
90	90	0	63	27	45	45	27	63
110	110	0	77	33	55	55	33	77

4.4.2 Simulation Results

This section analyses the performance of the network in terms of end-to-end delay by varying of traffic load. Due to the increasing of traffic load, the intra-vehicle network becomes more congested. The effect of congestion on the network is investigated and mitigated through the History-based MAC strategy. To assess the network performance, this study has carried out a series of simulations through discrete event simulation software, OPNET, with the relative packages for the ZigBee module.

At the scenario, I (a) in Figure 4.4 show the CDF of the end-to-end delay versus the number of nodes for analyzing the performance in the first case. From the figure, the result shows the number of SN increases in IVWSNs, the CDF shift to the right. The cause of this performance is due to the collisions among the packets, which increases with the increasing number of SN in the network. After the collision SN waits for a certain period (Back-off + sensing period) and then if the channel is free, it retransmits the packet that already caused collision previously. The new re-transmissions can be subjected to other collision. The repetition of the procedures is explained under the CSMA/CA protocol. It is easy to understand at this point that the increasing number of collisions results in the increasing end-to-end delay experienced by the packets. However, in the proposed strategy, the probability of the collisions among the packets are low, since the node is used its previous value of the parameters, where the transmission was successfully done. As a result, the History-based MAC outperforms the traditional one.

Furthermore, with the increasing number of sensor nodes in the network with high traffic load, congestion and collision continue to increase in IoT enabling environments. The IEEE 802.15.4 network can handle the traffic up to a certain point when the traffic increases beyond that point, the network begins to enter into congestion. As a result, some packets of the node will be delayed to reach to the destination. The more congestion in the network implies that the more packets will be delayed to reach to the destination. From the discussion above, it is clear that the collision rate and packet losses are increasing dramatically while the number of the nodes increased. Similarly, the network throughput deteriorates with the increasing number of nodes. Under those circumstances, the existing different types of MAC protocols are not suitable for the large network. In this case, the scalability issue of the existing MAC is needed to enhance for designing such a communication system in the IoT environment in the near future.

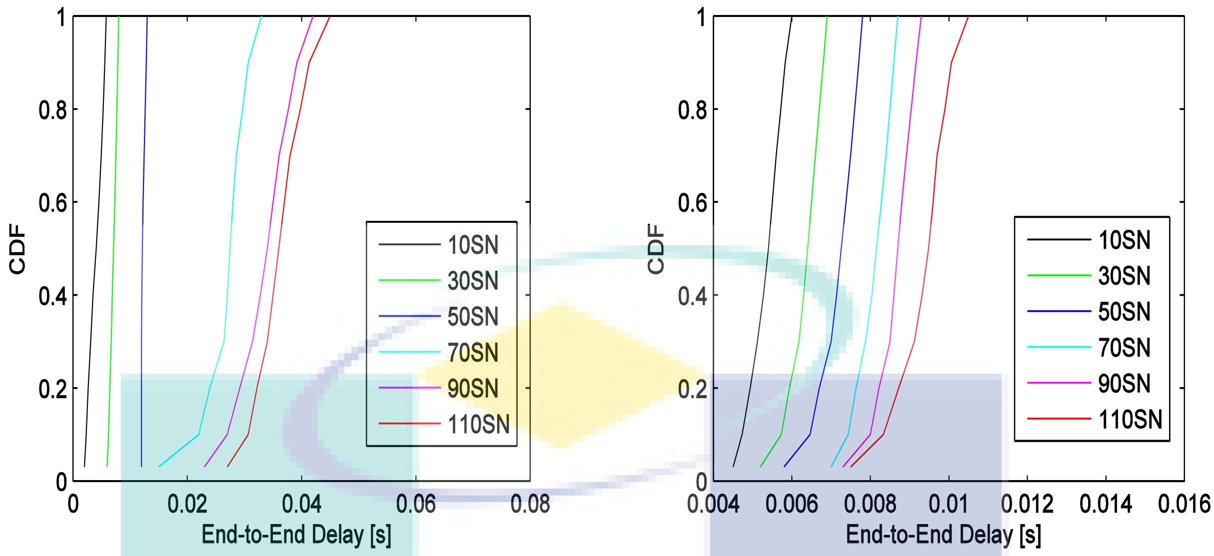
After the collisions occurred among the packets of the sensor node, every time the sensor node needs to wait (backoff + sensing period) until the new time slot begins and the channel is free. It tries again to retransmit the failed packet that already caused collision previously. The new re-transmissions may again cause another collision. This recursive procedure is clarified by the CSMA/CA MAC protocol. From the above discussion, it is easy to recognize that the End-to-End delay of the network increases when the number of collision rises among the packets. However, in the proposed strategy, the probability of the collisions among the packets are low, since the node is used its previous value of the parameters, where the transmission was successfully done. As a result, the History-based MAC outperforms the traditional one. In consequence the scenarios I, II, III, and IV for figures 4.4, 4.5, 4.6, and 4.7, respectively, mitigate the collision rate significantly in the network compared to traditional MAC protocol.

The improved performance in the History-based MAC can be obtained from the calculation in equation 4.4.

$$P_{improved} = \frac{f_1 - f_2}{f_1}\ (\%) \qquad 4.4$$

Where $P_{improved}$ is the increased the performance, f_1 is the final value of the original scenario, and f_2 is the final value of the modified scenario.

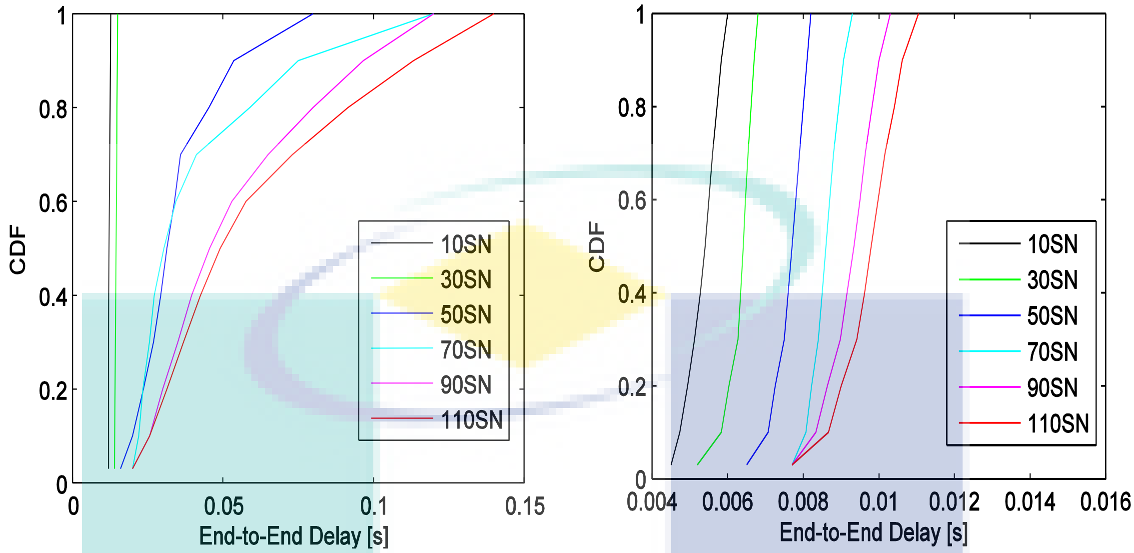
As shown in Figure 4.4, the network end to end delay varies greatly depending on the number of sensor node increased. However, the network performance is increased 75% approximately in term of network performance metrics end to end delay in the History-based MAC strategy compare to the traditional one. In the first scenario, the traffic load is remaining same for both MAC as mentioned in Table 4.3.



(a) Traditional MAC (b) History-based MAC

Figure 4.4 Performance comparisons between traditional and proposed solution: History-based MAC in the scenario I

Figure 4.5 shows the great impact on performance with the variations of the traffic load. It should be mentioned that when the number of the sensor node is less in the network with a low traffic load, there is no significant difference of end to end delay. However, as the traffic load increases, the IEEE 802.15.4 in Figure 4.5 (a) performance is saturated after certain sensor node exceeds 50 because of congestion problem among the nodes' traffic. On the other hand, the History-based MAC in Figure 4.5 (b) treats as same instead of the number of sensor node increased in the network. In this scenario, the performance is improved by 90% approximately in the proposed MAC compare with the traditional one.

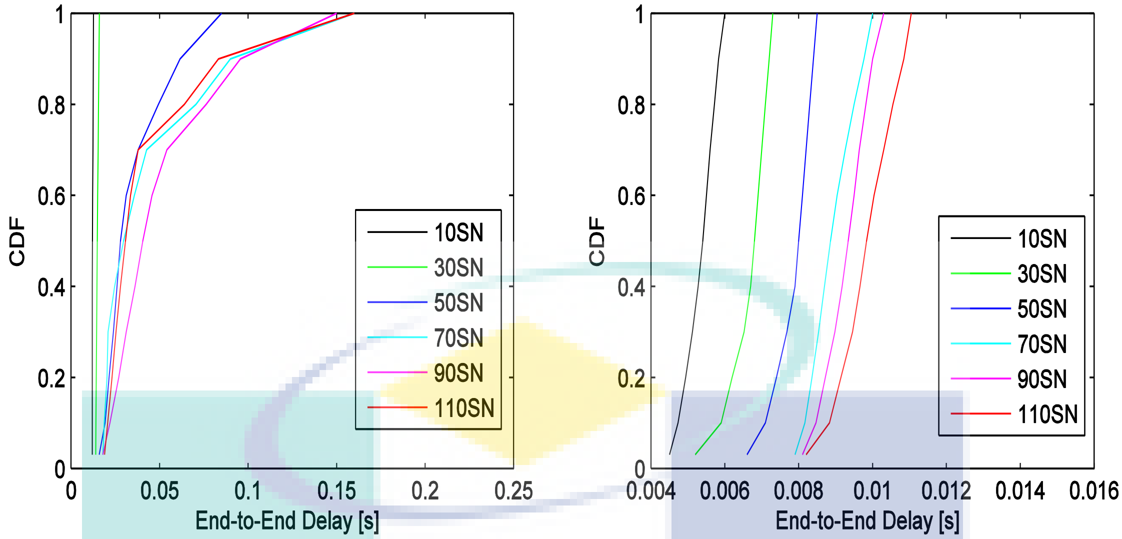


(a) Traditional MAC

(b) History-based MAC

Figure 4.5 Performance comparisons between traditional and proposed solution: History-based MAC in scenario II

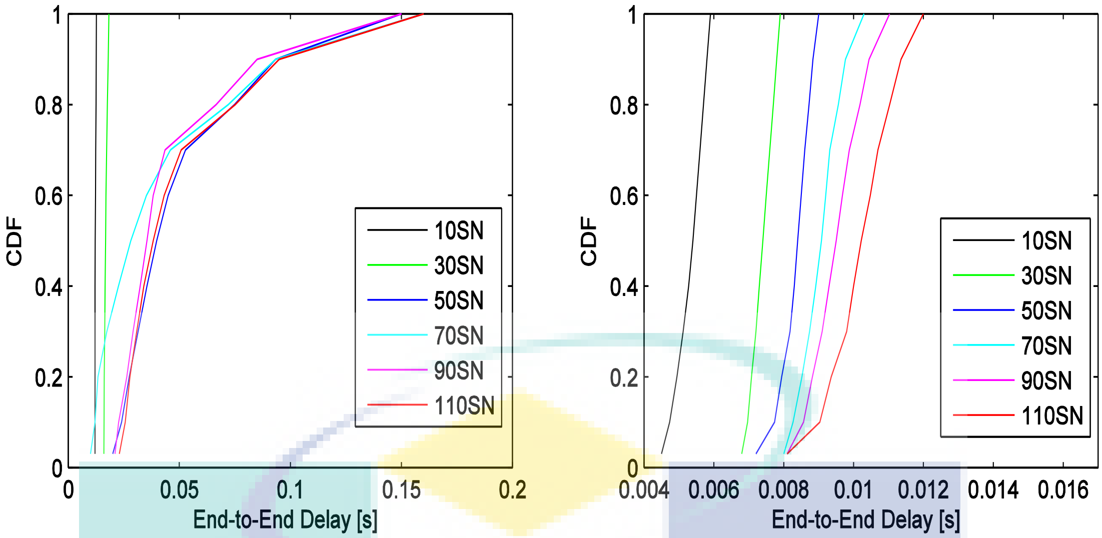
Figure 4.6 compares the results by varying the number of sensor nodes with traffic load. As the traffic load increases more, in the IEEE 802.15.4 in Figure 4.6 (a) sensor node attempt to transmit data frames more often, that leads to redundant CCAs and a number of collisions due to multiple simultaneous transmissions. As a result, the sensor nodes carry out redundant CCAs and a number of retransmissions that increase the congestion among the data frames. However, in the History-based MAC in Figure 4.6 (b) ensure to defend the retransmission process by utilizing the successful transmission nodes' parameters which minimizes the network end to end delay and node energy consumption. In this scenario, the performance is improved by 92% approximately in the History-based MAC compare with the traditional one.



(a) Traditional MAC (b) History-based MAC

Figure 4.6 Performance comparisons between traditional and proposed solution: History-based MAC in scenario III

Figure 4.7 presents the result of scenario IV with more traffic load as shown in Table 4.3. In the traditional MAC in Figure 4.7 (a), the network becomes saturated due to heavy traffic load and end to end delay is significantly increased. Some packets cannot be immediately transmitted after generation due to high contention. Thus, many of them have to be buffered until all the packets generated earlier are transmitted. This result in a longer delay, and thus the delay gradually increases as the traffic load increases. However, the History-based MAC decreases the probability of the collisions among the packets, since the node is used its previous value of the parameters, where the transmission was successfully done. In the last scenario with heavy traffic load, the performance is improved by 91% approximately in the History-based MAC compare with the traditional one as shown in Figure 4.7 (b).



(a) Traditional MAC (b) History-based MAC

Figure 4.7 Performance comparisons between traditional and proposed solution: History-based MAC in scenario IV

To make more effectiveness of the History-based MAC strategy, it also introduces two BSs for traditional MAC with a single BS to compare the performance in the network as shown in Figure 4.8. The network performance is getting better when more base stations are added within the network. Also, we can see that the History-based MAC algorithm is working like traditional MAC with two base stations. However, adding more base stations in a network causes more complexity of network routing and imposes high installation cost.

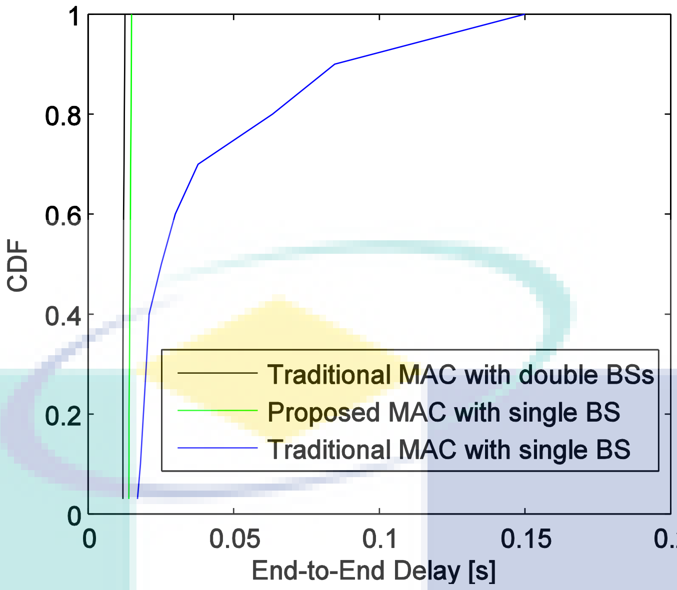


Figure 4.8 Performance analysis between the proposed solution: History-based MAC with single BS and traditional MAC with multiple BSs.

From the above discussion, it is clear that the two major impacts which are responsible for affecting the performance of the network greatly. They are the following:

- Impact of the number of sensor nodes and
- Impact of the traffic load

This section studies the impact of a number of sensors on performance with varying it from 10 to 110. The above figures 4.4-4.8 show the performance variation in term of performance metric end to end delay of the network. The end to end delay of the four scenarios decreases as the number of sensors increases in the network. This is obvious because many sensor nodes deployed in the same area contend with each other to access the shared channel. The unavoidable collisions are caused when a number of sensors contending with each other to transmit their data frame. Therefore, it is natural that contention level increases as the number of contending sensor increases, and thereby it adversely affects performance metrics such as the throughput, network delay, and end to end delay. However, the history-based MAC strategy outperforms over traditional one, since it can avoid unnecessary delay during nodes initializing of their default parameters every time.

Likewise, the above results show the combination of various traffic loads. It is varied the traffic load combination of 120 and 60 milliseconds in four scenarios. For all scenarios, the network end to end delay increases as the traffic load increases. This is noticeable because a slight increase in the traffic load causes large congestion among the data frame of the node. The heavy traffic load brings the significant contention between the sensors. Moreover, as the traffic load increases, the sensor nodes can attempt to transmit more packets. This increases the probability of the two or more sensor nodes perform the transmission simultaneously.

4.5 Summary

The IEEE 802.15.4 CSMA/CA MAC protocol expects the future wireless intra-vehicular networks. The IoT-IVWSNs concept reveals as the number of the sensor node is increasing for improving various safety levels in the modern vehicle. In the first phase of this chapter investigates the performances by introducing the IoT-IVWSNs environment by considering relevant network communication parameters, architecture, components, and system design issues. It identifies two major issues for affecting the performance metrics in IEEE 802.15.4 MAC protocol and need to develop an algorithm for MAC strategy to overcome the limitations which are responsible for increasing the network collision. The second phase develops a History-based algorithm which is suit for IoT-IVWSNs. The evaluation of the results of the developed algorithm on CSMA/CA MAC strategy validates the effectiveness of desired IoT-IVWSNs.

From the above discussion, it can point out the following remarks:

Remark 1: The behavior of the IVWSNs changes significantly by introducing the concept of IoT. Hence the existing IVWSNs is not completely scalable.

Remark 2: It is clear that the collision and congestion among the packets decrease the network performance significantly due to a large number of sensor nodes.

Remark 3: The proposed MAC strategy mitigates the congestion and collision problem in the network significantly.

CHAPTER 5

CONCLUSION AND RECOMMENDATIONS

5.1 Concluding Remarks

This thesis provides an in-depth analysis of the beacon-enabled IEEE 802.15.4 CSMA/CA MAC strategy in the perspective of Wireless Sensor Networks (WSNs). It explains in details the properties of WSNs and the significant specifications for designing intra-vehicular wireless sensor network. The implementation of IEEE 802.15.4 in WSNs is motivated by the fact that the specifications it defines for the PHY layer and the MAC sub-layer are in harmony with the unique characteristics of WSNs. It considers the various designing challenges and substantial pros and cons of IEEE 802.15.4 MAC protocol during implemented in IoT-IVWSNs environment. This thesis finds the various key issues to design IoT-IVWSNs by delving into an extensive review of the research contributions which reveal the scope and expose the ideas that are missing in the protocol to improve the efficiency. Based on that, it describes a clear roadmap for designing efficient MAC protocols for IoT-IVWSNs. This roadmap determines what required to design adaptive and power-efficient, and collision-free backoff algorithms to minimize various problems associated with IEEE 802.15.4 MAC.

5.2 Contributions

There are three following contributions for enhancing the IEEE 802.15.4 MAC protocol in IoT-IVWSNs environment:

1 An extensive investigation has been done on IoT-IVWSNs by considering different tuneable optimal communication parameters which are suitable for IoT-IVWSNs environment. Within this thesis, firstly, an extensive investigation to evaluate the performance of IoT-IVWSN has been done by considering

different optimized tuning parameters in the IEEE 802.15.4 MAC standard. The essential requirement of IoT-IVWSN is introduced by considering its architecture, components, suitable existing technologies, and the design challenges. The communication link between the ED and the CU is studied by choosing the appropriate communication parameters. The test results indicate that delay in packet transmission increases due to higher traffic loads and a larger number of end nodes. The result indicates that existing MAC protocol is not scalable, i.e., it works well for a small but is not suitable for a large network. The behavior of the scalability of IVWSNs significantly changes due to collision, congestion, and collaboration in the network. This experiment also reveals that the IoT-IVWSN is a network with a large number of sensor nodes and relatively high traffic loads, it finds that the traditional MAC is not properly working after exceeding a certain number of nodes with high traffic because of packet collision and retransmission phenomena.

2 This work has developed an History-based CSMA/CA MAC solution for IoT-IVWSNs suit which minimizes the congestion and collision problem among the data frame of sensor nodes and reduces the delay of the network.

3 It has validated the proposed solution "History-based CSMA/CA MAC" through the numerical simulations. It analyses the History-based MAC strategy for IoT-IVWSN with numerical simulation. Numerical tests are carried out to find the desirable communication parameters and to study the IoT-IVWSN with a large number of nodes and high traffic load. The results show that with the History-based MAC strategy, the traffic congestion and collision reduce quite significantly. It decreases the network end to end delay significantly by minimizing the packet retransmission and collision. The network performance is increased 75% approximately in term of network performance metrics end to end delay in the History-based MAC strategy compare to the traditional one. The results indicate that the new MAC strategy improves the network performance by reducing the network delay in the IoT-IVWSNs environment.

5.3 Limitations

The IoT-IVWSNs is related to a large number of sensor nodes and high traffic loads which increases the probability of collision and congestion among the packets in the network. The performance of the CAP of IEEE 802.15.4 MAC protocol is significantly responsible for the collision probability and the network throughput. Because, if a large number of nodes are densely deployed in a small territory, the contention complexities increase significantly which lead to a high probability of collision and energy consumption of the network. The priority-based MAC ensures the QoS of every packet and overall reduces the power consumption of the network by minimizing the complexity of the CAP. The energy consumption is increasing because of packet retransmission caused by congestion and collision among the packets. In the default algorithm, the energy consumption increases sharply with the number of sensor nodes increased. The complex structure of contention windows causes a high probability of packet collision rate and results in a large number of retransmissions. Sensor node priority mechanism significantly reduces the packet collision rate and packet retransmission. The sensor node wakes up every time to send information to the base station whenever sensor data available in the transmitter. However, the priority based MAC strategy will allow the sensor node transmitting data in a specific time interval and minimize the frequently wake up time of the sensor node. However, this work is unable to utilize the priority concept.

5.4 Future Work

The IoT-IVWSNs is related to a large number of sensor nodes and high traffic loads which increases the probability of collision and congestion among the packets in the network. The performance of the CAP of IEEE 802.15.4 MAC protocol is significantly responsible for the collision probability and the network throughput. Because, if a large number of nodes are densely deployed in a small territory, the contention complexities increase significantly which lead to a high probability of collision and energy consumption of the network. The priority-based MAC ensures the QoS of every packet and overall reduces the power consumption of the network by minimizing the complexity of the CAP. The energy consumption is increasing because of packet retransmission caused by congestion and collision among the packets. In the default algorithm, the energy consumption increases sharply with the number of sensor nodes increased. The complex structure of contention windows causes a high probability of packet collision rate and results in a large number of retransmissions. Sensor node priority mechanism significantly reduces the packet collision rate and packet retransmission. The sensor node wakes up every time to send information to the base station whenever sensor data available in the transmitter. However, the priority based MAC strategy will allow the sensor node transmitting data in a specific time interval and minimize the frequently wake up time of the sensor node. However, this work is unable to utilize the priority concept.

Functional extension of priority based MAC for IoT-IVWSNs with a true cross-layer design may be undertaken in the future. To do this, it may develop a hybrid MAC strategy which is a combination of the two proposed techniques. Prioritizing the various types of nodes is still an open area in the context of IEEE 802.15.4. It focuses on this thesis on prioritizing the nodes based the urgency. One can take this opportunity to exploit the collision-aware concept in developing a node-priority aware IEEE 802.15.4 MAC protocol.

REFERENCES

Abdmeziem, M. R., Tandjaoui, D., & Romdhani, I. (2016). Architecting the internet of things: state of the art *Robots and Sensor Clouds* (pp. 55-75).

Ahmed, M., Saraydar, C. U., ElBatt, T., Yin, J., Talty, T., & Ames, M. (2007a). Intra-vehicular wireless networks. Paper presented on IEEE Globecom Workshops.

Ahmed, M., Saraydar, C. U., ElBatt, T., Yin, J., Talty, T., & Ames, M. (2007b). Intra-vehicular wireless networks. Paper presented on IEEE Globecom Workshops.

Akyildiz, I. F., & Vuran, M. C. (2010). Wireless Sensor Networks (Vol. 4): John Wiley & Sons.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: a survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials, 17*(4), 2347-2376.

Al-Jemeli, M., & Hussin, F. A. (2015). An energy efficient cross-layer network operation model for IEEE 802.15. 4-based mobile wireless sensor networks. *IEEE Sensors Journal, 15*(2), 684-692.

Alvi, A. N., Naqvi, S. S., Bouk, S. H., Javaid, N., Qasim, U., & Khan, Z. A. (2012). Evaluation of slotted CSMA/CA of IEEE 802.15. 4. Paper presented at the 7th International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA).

An, S.-h., Lee, B.-H., & Shin, D.-R. (2011). A survey of intelligent transportation systems. Paper presented at the 3rd International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN).

Anastasi, G., Conti, M., & Di Francesco, M. (2011). A comprehensive analysis of the MAC unreliability problem in IEEE 802.15. 4 wireless sensor networks. *IEEE Transactions on Industrial Informatics, 7*(1), 52-65.

Anchora, L., Capone, A., Mighali, V., Patrono, L., & Simone, F. (2014). A novel MAC scheduler to minimize the energy consumption in a wireless sensor network. *Ad Hoc Networks, 16*, 88-104.

Anusha, M., Vemuru, S., & Gunasekhar, T. (2015). TDMA-based MAC protocols for scheduling channel allocation in multi-channel wireless mesh networks using cognitive radio. Paper presented at the International Conference on Circuit, Power and Computing Technologies (ICCPCT).

Aziz, S. M., & Pham, D. M. (2013). Energy efficient image transmission in wireless multimedia sensor networks. *IEEE Communications Letters, 17*(6), 1084-1087.

Bas, C. U., & Ergen, S. C. (2012). Ultra-wideband channel model for intra-vehicular wireless sensor networks. Paper presented at the IEEE Wireless Communications and Networking Conference (WCNC).

Bas, C. U., & Ergen, S. C. (2013). Ultra-wideband channel model for intra-vehicular wireless sensor networks beneath the chassis: from statistical model to simulations. *IEEE Transactions on Vehicular Technology, 62*(1), 14-25.

Bello, O., & Zeadally, S. (2016). Intelligent device-to-device communication in the internet of things. *IEEE Systems Journal, 10*(3), 1172-1182.

Bhargav, K. K., & Singhal, R. (2013). Zigbee based VANETs for accident rescue missions in 3G WCDMA networks. Paper presented at the Global Humanitarian Technology Conference (GHTC).

Bhosale, V., & Ladhe, S. (2018). Survey on beacon-enabled IEEE 802.15.4 MAC mechanisms. *International Journal of Applied Engineering Research, 13*(6), 3725-3737.

Biswas, S. (2017). Simulation model of beacon enabled 802.15.4 networks with OPNET modeler. Paper presented at the IEEE Electrical Engineering Congress (EECON).

Blumenstein, J., Mikulasek, T., Prokes, A., Zemen, T., & Mecklenbrauker, C. (2015). Intra-vehicular path loss comparison of uwb channel for 3-11 GHz and 55-65 GHz. Paper presented at the IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB).

Brienza, S., De Guglielmo, D., Anastasi, G., Conti, M., & Neri, V. (2013). *S*trategies for optimal MAC parameter setting in IEEE 802.15. 4 wireless sensor networks: A performance comparison. Paper presented at the IEEE Symposium on Computers and Communications (ISCC).

Brienza, S., Roveri, M., Guglielmo, D. D., & Anastasi, G. (2016). Just-in-time adaptive algorithm for optimal parameter setting in 802.15.4 WSNs. *ACM Transactions on Autonomous and Adaptive Systems (TAAS), 10*(4), 27.

Bronzi, W., Frank, R., Castignani, G., & Engel, T. (2014). Bluetooth low energy for inter-vehicular communications. Paper presented at the IEEE Vehicular Networking Conference (VNC).

Buratti, C. (2010). Performance analysis of IEEE 802.15. 4 beacon-enabled mode. *IEEE Transactions on Vehicular Technology, 59*(4), 2031-2045.

Chen, K.-C., & Lien, S.-Y. (2014). Machine-to-machine communications: technologies and challenges. *Ad Hoc Networks, 18*, 3-23.

Chen, S.-K., Kao, T., Chan, C.-T., Huang, C.-N., Chiang, C.-Y., Lai, C.-Y., Wang, P.-C. (2012). A reliable transmission protocol for zigbee-based wireless patient monitoring. *IEEE Transactions on Information Technology in Biomedicine, 16*(1), 6-16.

Chen, X., Ng, D. W. K., & Chen, H.-H. (2016). Secrecy wireless information and power transfer: challenges and opportunities. *IEEE Wireless Communications, 23*(2), 54-61.

Collotta, M., Scatà, G., & Pau, G. (2013). A priority-based CSMA/CA mechanism to support deadline-aware scheduling in home automation applications using IEEE 802.15.4. *International Journal of Distributed Sensor Networks, 9*(5), 139804.

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of things security and forensics: challenges and opportunities. *Future Generation Computer Systems, 78*, 544-546.

Coronato, A., De Pietro, G., Park, J.-H., & Chao, H.-C. (2010). A framework for engineering pervasive applications applied to intra-vehicular sensor network applications. *Mobile Networks and Applications, 15*(1), 137-147.

Cuomo, F., Abbagnale, A., & Cipollone, E. (2013). Cross-layer network formation for energy-efficient IEEE 802.15.4/zigbee wireless sensor networks. *Ad Hoc Networks, 11*(2), 672-686.

Di Francesco, M., Anastasi, G., Conti, M., Das, S. K., & Neri, V. (2011). Reliability and energy-efficiency in IEEE 802.15. 4/zigbee sensor networks: an adaptive and cross-layer approach. *IEEE Journal on Selected Areas in Communications, 29*(8), 1508-1524.

Faezipour, M., Nourani, M., Saeed, A., & Addepalli, S. (2012). Progress and challenges in intelligent vehicle area networks. *Communications of the ACM, 55*(2), 90-100.

Ferdous, R. M., Reza, A. W., & Siddiqui, M. F. (2016). Renewable energy harvesting for wireless sensors using passive RFID tag technology: a review. *Renewable and Sustainable Energy Reviews, 58*, 1114-1128.

Ganesh, S., & Amutha, R. (2013). Efficient and secure routing protocol for wireless sensor networks through SNR based dynamic clustering mechanisms. *Journal of Communications and Networks, 15*(4), 422-429.

Gao, M., Wang, P., Wang, Y., & Yao, L. (2018). Self-powered zigbee wireless sensor nodes for railway condition monitoring. *IEEE Transactions on Intelligent Transportation Systems, 19*(3), 900-909.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of things (IoT): a vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645-1660.

Hamid, Z., & Hussain, F. B. (2014). QoS in wireless multimedia sensor networks: a layered and cross-layered approach. *Wireless Personal Communications, 75*(1), 729-757.

Han, B., Cao, X., Shi, H., & Wang, L. (2018). An analytical model for IEEE 802.15. 4 wireless networks with periodic traffic under interference. Paper presented at the 33rd Youth Academic Annual Conference of Chinese Association of Automation (YAC).

Han, D.-M., & Lim, J.-H. (2010). Smart home energy management system using IEEE 802.15. 4 and zigbee. *IEEE Transactions on Consumer Electronics, 56*(3), 1403-1410.

Hartenstein, H., & Laberteaux, K. (2010). VANET: vehicular applications and inter-networking technologies (Vol. 1): Wiley Online Library.

Hasbollah, A. A., Ariffin, S. H., & Hamini, M. I. A. (2009). Performance analysis for 6loWPAN IEEE 802.15.4 with IPv6 network. Paper presented at the IEEE Region 10 Conference (TENCON).

Hashemi, M., Si, W., Laifenfeld, M., Starobinski, D., & Trachtenberg, A. (2013). Intra-car wireless sensors data collection: a multi-hop approach. Paper presented at the Vehicular Technology Conference (VTC).

Huang, P., Xiao, L., Soltani, S., Mutka, M. W., & Xi, N. (2013). The evolution of MAC protocols in wireless sensor networks: a survey. *IEEE Communications Surveys & Tutorials, 15*(1), 101-120.

Huang, T.-Y., Chang, C.-J., Lin, C.-W., Roy, S., & Ho, T.-Y. (2015a). Intra-vehicle network routing algorithm for wiring weight and wireless transmit power minimization. Paper presented at the IEEE 20th Asia and South Pacific Design Automation Conference (ASPDAC).

Hwang, S., & Yu, D. (2012). Remote monitoring and controlling system based on zigbee networks. *International Journal of Software Engineering and Its Applications, 6*(3), 35-42.

Iova, O., Picco, G. P., Istomin, T., & Kiraly, C. (2016). RPL, the routing standard for the internet of things... Or Is It? *IEEE Communications Magazine*, *54(12),* 16-22.

Iturri, P. L., Aguirre, E., Azpilicueta, L., Garate, U., & Falcone, F. (2014). Zigbee radio channel analysis in a complex vehicular environment. *IEEE Antennas and Propagation Magazine, 56*(4), 232-245.

Jabeen, Q., Khan, F., Khan, S., & Jan, M. A. (2016). Performance improvement in multihop wireless mobile adhoc networks. *the Journal Applied, Environmental, and Biological Sciences (JAEBS), 6*, 82-92.

Jawhar, I., Mohamed, N., & Zhang, L. (2010). Inter-vehicular communication systems, protocols and middleware. Paper presented at the IEEE 5th International Conference on Networking, Architecture, and Storage (NAS).

Jin, Y., Kim, K. J., & Kwak, K. S. (2011). Performance analysis of UWB intra-vehicle transmitted-reference communication systems. Paper presented at the IEEE Consumer Communications and Networking Conference (CCNC).

Jin, Y., Kwak, D., & Kwak, K. S. (2012). Performance analysis of intra-vehicle ultra-wide band propagation in multi-user environments. Paper presented at the IEEE 1st International Workshop on Vehicular Communications, Sensing, and Computing (VCSC).

Jung, K.-H., Lee, H.-R., Lim, W.-S., & Suh, Y.-J. (2014). An adaptive collision resolution scheme for energy efficient communication in IEEE 802.15. 4 networks. *Computer Networks, 58*, 39-57.

Jurčík, P., & Koubâa, A. (2007). The IEEE 802.15. 4 OPNET simulation model: reference guide v2. 0. *IPP-HURRAY Technical Report, HURRAY-TR-070509*.

Kandhalu, A., Xhafa, A., & Hosur, S. (2013). Towards bounded-latency bluetooth low energy for in-vehicle network cable replacement. Paper presented at the International Conference on Connected Vehicles and Expo (ICCVE).

Khaleel, H. R., Al-Rizzo, H. M., & Rucker, D. G. (2012). Compact polyimide-based antennas for flexible displays. *Journal of Display Technology, 8*(2), 91-97.

Khanafer, M., Guennoun, M., & Mouftah, H. T. (2014). A survey of beacon-enabled IEEE 802.15.4 MAC protocols in wireless sensor networks. *IEEE Communications Surveys & Tutorials, 16*(2), 856-876.

Khanapurkar, M., Bajaj, P., & Gharode, D. (2008). A design approach for intelligent vehicle black box system with intra-vehicular communication using lin/flex-ray protocols. Paper presented at the IEEE International Conference on Industrial Technology (ICIT).

Khuandaga, G., Iqbal, A., & Kwak, K. S. (2011). Performance analysis of modulation schemes in intra vehicle communications (IVC) channel. Paper presented at the 13th International Conference on Advanced Communication Technology (ICACT).

Koubaa, A., Alves, M., & Tovar, E. (2006). A comprehensive simulation study of slotted CSMA/CA for IEEE 802.15.4 wireless sensor networks. Paper presented at the IEEE International Workshop on Factory Communication Systems.

Lee, D., & Chung, K. (2010). Adaptive duty-cycle based congestion control for home automation networks. *IEEE Transactions on Consumer Electronics, 56*(1), 42-47.

Lee, S.-Y., Shin, Y.-S., Lee, K.-W., & Ahn, J.-S. (2014). Performance analysis of extended non-overlapping binary exponential backoff algorithm over IEEE 802.15.4. *Telecommunication Systems*, *55*(1), 39-46.

Li, S., Da Xu, L., & Zhao, S. (2015). The internet of things: a survey. *Information Systems Frontiers, 17*(2), 243-259.

Li, W., Hu, X. Y., & Jiang, T. (2018). Path loss models for IEEE 802.15.4 vehicle-to-infrastructure communications in rural areas. *IEEE Internet of Things Journal, 5(5)*,3865-3875.

Li, X., Niu, J., Kumari, S., Wu, F., Sangaiah, A. K., & Choo, K.-K. R. (2018). A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments. *Journal of Network and Computer Applications, 103*, 194-204.

Lin, J.-R., Talty, T., & Tonguz, O. K. (2013). An empirical performance study of intra-vehicular wireless sensor networks under wifi and bluetooth interference. Paper presented at the IEEE Global Communications Conference (GLOBECOM).

Lin, J.-R., Talty, T., & Tonguz, O. K. (2015a). A blind zone alert system based on intra-vehicular wireless sensor networks. *IEEE Transactions on Industrial Informatics*, *11*(2), 476-484.

Lin, J.-R., Talty, T., & Tonguz, O. K. (2015b). On the potential of bluetooth low energy technology for vehicular applications. *IEEE Communications Magazine*, *53*(1), 267-275.

Liu, R., Herbert, S., Loh, T. H., & Wassell, I. J. (2011). A study on frequency diversity for intra-vehicular wireless sensor networks (wsns). Paper presented at the Vehicular Technology Conference (VTC).

Lu, N., Cheng, N., Zhang, N., Shen, X., & Mark, J. W. (2014). Connected vehicles: solutions and challenges. *IEEE Internet of Things Journal, 1*(4), 289-299.

Mamdouhi, H., Khatun, S., & Ahmadi, K. (2009). An intra wireless communication and remote control mechanism in vehicular ad-hoc network. Paper presented at the 3rd Uksim European Symposium on Computer Modeling and Simulation (EMS).

Mandal, K., Sen, A., Chakraborty, A., Roy, S., Batabyal, S., & Bandyopadhyay, S. (2011). Road traffic congestion monitoring and measurement using active RFID and GSM technology. Paper presented at the 14th International IEEE Conference on Intelligent Transportation Systems (ITSC).

McClellan, S., Follmer, T., Maynard, E., Capps, E., Larson, G., Ord, D., Vo, V. (2014). System and method for monitoring vehicle parameters and driver behavior: Google Patents.

Minooei, H., & Nojumi, H. (2007). Performance evaluation of a new backoff method for IEEE 802.11. *Computer Communications, 30*(18), 3698-3704.

Mourad, A., Heigl, F., & Hoeher, P. A. (2016). Performance evaluation of concurrent IEEE 802.11 systems in the automotive domain. Paper presented at the IEEE 41st Conference on Local Computer Networks (LCN).

Nguyen, D. T., Singh, J., Le, H. P., & Soh, B. (2009). A hybrid TDMA protocol based ultra-wide band for in-car wireless communication. Paper presented at the IEEE Region 10 Conference (TENCON).

Palattella, M., Faridi, A., Boggia, G., Camarda, P., Grieco, L., Dohler, M., & Lozano, A. (2014). Performance analysis of the IEEE 802.15. 4 MAC layer. *ZigBee Networks, Protocols and Applications*.

Pantazis, N. A., Nikolidakis, S. A., & Vergados, D. D. (2013). Energy-efficient routing protocols in wireless sensor networks: a survey. *IEEE Communications Surveys & Tutorials, 15*(2), 551-591.

Park, P., Di Marco, P., Fischione, C., & Johansson, K. H. (2013). Modeling and optimization of the IEEE 802.15.4 protocol for reliable and timely communications. *IEEE Transactions on Parallel and Distributed Systems, 24*(3), 550-564.

Park, P., Fischione, C., & Johansson, K. H. (2011). Adaptive IEEE 802.15.4 medium access control protocol for control and monitoring applications *Wireless Networking Based Control* 271-300.

Park, P., Fischione, C., & Johansson, K. H. (2013). Modeling and stability analysis of hybrid multiple access in the IEEE 802.15.4 protocol. *ACM Transactions on Sensor Networks (TOSN), 9*(2), 13.

Parthasarathy, D., Whiton, R., Hagerskans, J., & Gustafsson, T. (2016). An in-vehicle wireless sensor network for heavy vehicles. Paper presented at the IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA).

Peng, C., Qian, K., & Wang, C. (2015). Design and application of a VOC-monitoring system based on a zigBee wireless sensor network. *IEEE Sensors Journal, 15*(4), 2255-2268.

Pinelis, M. (2013). Automotive sensors and electronics: trends and developments in 2013. *Automotive Sensors and Electronics Expo, Detroit, MI, USA.*

Pollin, S., Ergen, M., Ergen, S. C., Bougard, B., Van der Perre, L., Moerman, I., Catthoor, F. (2008). Performance analysis of slotted carrier sense IEEE 802.15. 4 medium access layer. *IEEE Transactions on Wireless Communications, 7(9),* 3359-3371.

Qu, F., Li, J., Yang, L., & Talty, T. (2011). Measured channel capacity of SIMO-UWB for intra-vehicle communications. Paper presented at the 5th European Conference on Antennas and Propagation (EUCAP).

Qu, F., Wang, F.-Y., & Yang, L. (2010a). Intelligent transportation spaces: vehicles, traffic, communications, and beyond. *IEEE Communications Magazine*, *48*(11), 136-142.

Qu, F., Wang, F.-Y., & Yang, L. (2010b). Intelligent transportation spaces: vehicles, traffic, communications, and beyond. *IEEE Communications Magazine*, *48*(11), 136-142.

Rahman, M. A. (2014a). Design of wireless sensor network for intra-vehicular communications. Paper presented at the International Conference on Wired/Wireless Internet Communications.

Rahman, M. A. (2014b). Reliability analysis of zigbee based intra-vehicle wireless sensor networks. Paper presented at the International Workshop on Communication Technologies for Vehicles.

Rahman, M. A., Ali, J., Kabir, M. N., & Azad, S. (2017). A performance investigation on IoT enabled intra-vehicular wireless sensor networks. *International Journal of Automotive and Mechanical Engineering*, *14*, 3970-3984.

Rahman, M. A., Kabir, M. N., Azad, S., & Ali, J. (2015). On mitigating hop-to-hop congestion problem in IoT enabled intra-vehicular communication. Paper presented at the 4th International Conference on Software Engineering and Computer Systems (ICSECS).

Ramya, C. M., Shanmugaraj, M., & Prabakaran, R. (2011). Study on zigbee technology. Paper presented at the 3rd International Conference on Electronics Computer Technology (ICECT).

Ranjit, J. S., & Shin, S. (2013). A modified IEEE 802.15.4 superframe structure for guaranteed emergency handling in wireless body area network. *Network Protocols and Algorithms, 5*(2), 1-15.

Rao, V., & Marandin, D. (2006). Adaptive backoff exponent algorithm for zigbee (IEEE 802.15.4). Paper presented at the International Conference on Next Generation Teletraffic and Wired/Wireless Advanced Networking.

Rasheed, M. B., Javaid, N., Haider, A., Qasim, U., Khan, Z. A., & Alghamdi, T. A. (2014). An energy consumption analysis of beacon enabled slotted CSMA/CA IEEE 802.15. 4. Paper presented at the 28th International Conference on Advanced Information Networking and Applications Workshops (WAINA).

Rasouli, H., Kavian, Y. S., & Rashvand, H. F. (2014). ADCA: Adaptive duty cycle algorithm for energy efficient IEEE 802.15.4 beacon-enabled wireless sensor networks. *IEEE Sensors Journal*, *14*(11), 3893-3902.

Rault, T., Bouabdallah, A., & Challal, Y. (2014). Energy efficiency in wireless sensor networks: a top-down survey. *Computer Networks, 67*, 104-122.

Rawat, P., Singh, K. D., & Bonnin, J. M. (2016). Cognitive radio for M2M and internet of things: a survey. *Computer Communications, 94*, 1-29.

Rawat, P., Singh, K. D., Chaouchi, H., & Bonnin, J. M. (2014). Wireless sensor networks: a survey on recent developments and potential synergies. *The Journal of Supercomputing, 68*(1), 1-48.

Ross, N., & Schuhmacher, D. (2017). Wireless network signals with moderately correlated shadowing still appear poisson. *IEEE Transactions on Information Theory, 63*(2), 1177-1198.

Sadi, Y., & Ergen, S. C. (2013). Optimal power control, rate adaptation, and scheduling for UWB-based intravehicular wireless sensor networks. *IEEE Transactions on Vehicular Technology, 62*(1), 219-234.

Shen, W., Zhang, T., Barac, F., & Gidlund, M. (2014). PriorityMAC: A priority-enhanced MAC protocol for critical traffic in industrial wireless sensor and actuator networks. *IEEE Transactions on Industrial Informatics, 10*(1), 824-835.

Sheng, Z., Yang, S., Yu, Y., Vasilakos, A. V., McCann, J. A., & Leung, K. K. (2013). A survey on the ietf protocol suite for the internet of things: standards, challenges, and opportunities. *IEEE Wireless Communications, 20*(6), 91-98.

Shih, B.-Y., Chang, C.-J., Chen, A.-W., & Chen, C.-Y. (2010). Enhanced MAC channel selection to improve performance of IEEE 802.15. 4. *International Journal of Innovative Computing, Information and Control, 6*(12), 5511-5526.

Shih, B.-Y., Chen, C.-Y., Shih, C.-H., & Tseng, J.-Y. (2010). The development of enhancing mechanisms for improving the performance of IEEE 802.15. 4. *International Journal of Physical Sciences, 5*(6), 884-897.

Si, W., Starobinski, D., & Laifenfeld, M. (2018). A robust load balancing and routing protocol for intra-car hybrid wired/wireless networks. *IEEE Transactions on Mobile Computing, 42*, 1-16.

Singh, B., & Lobiyal, D. (2013). A MAC-layer retransmission technique for collided packets in wireless sensor network. *Wireless Personal Communications, 72*(4), 2499-2518.

Snigdh, I., & Gosain, D. (2016). Analysis of scalability for routing protocols in wireless sensor networks. *Optik-International Journal for Light and Electron Optics, 127*(5), 2535-2538.

Somani, N. A., & Patel, Y. (2012). Zigbee: A low power wireless technology for industrial applications. *International Journal of Control Theory and Computer Modelling (IJCTCM), 2*, 27-33.

Song, X., Li, X., Tang, W., & Zhang, W. (2016). A fusion strategy for reliable vehicle positioning utilizing RFID and in-vehicle sensors. *Information Fusion, 31*, 76-86.

Striccoli, D., Boggia, G., & Grieco, L. A. (2015). A markov model for characterizing IEEE 802.15.4 MAC layer in noisy environments. *IEEE Transactions on Industrial Electronics, 62*(8), 5133-5142.

Sun, Q.-b., Liu, J., Li, S., FAN, C.-x., & SUN, J.-j. (2010). Internet of things: summarize on concepts, architecture and key technology problem. *Journal of Beijing University of Posts and Telecommunications, 3*(3), 1-9.

Takayama, I., & Kajiwara, A. (2016). Intra-vehicle wireless harness with mesh-networking. Paper presented at the IEEE-APS Topical Conference on Antennas and Propagation in Wireless Communications (APWC).

Tavakoli, H., Mišić, J., Mišić, V. B., & Naderi, M. (2015). Energy-efficient cluster-head rotation in beacon-enabled IEEE 802.15.4 networks. *IEEE Transactions on Parallel and Distributed Systems, 26*(12), 3371-3380.

Tonguz, O., Tsai, H.-M., Saraydar, C., Talty, T., & Macdonald, A. (2007). Intra-car wireless sensor networks using RFID: opportunities and challenges. Paper presented at the IEEE Conference on Mobile Networking for Vehicular Environments.

Tonguz, O. K., Tsai, H.-M., Talty, T., Macdonald, A., & Saraydar, C. (2006). *RFID* technology for intra-car communications: a new paradigm. Paper presented at the IEEE Vehicular Technology Conference (VTC).

Toscano, E., & Bello, L. L. (2012). Comparative assessments of IEEE 802.15.4/zigbee and 6LoWPAN for low-power industrial WSNs in realistic scenarios. Paper presented at the IEEE 9th International Workshop on Factory Communication Systems (WFCS).

Tseng, H.-W., & Chuang, Y.-R. (2013). A cross-layer judgment scheme for solving retransmission problem in IEEE 802.15.4-based wireless body sensor networks. *IEEE Sensors Journal, 13*(8), 3124-3135.

Tuohy, S., Glavin, M., Hughes, C., Jones, E., Trivedi, M., & Kilmartin, L. (2015). Intra-vehicle networks: a review. *IEEE Transactions on Intelligent Transportation Systems, 16*(2), 534-545.

Tuohy, S., Glavin, M., Jones, E., Hughes, C., & Kilmartin, L. (2016). Hybrid testbed for simulating in-vehicle automotive networks. *Simulation Modelling Practice and Theory, 66*, 193-211.

Tuohy, S., Glavin, M., Jones, E., Trivedi, M., & Kilmartin, L. (2013). Next generation wired intra-vehicle networks, a review. Paper presented at the IEEE Conference on Intelligent Vehicles Symposium (IVS).

Uddin, M. F. (2016). Throughput analysis of a CSMA based WLAN with successive interference cancellation under rayleigh fading and shadowing. *Wireless Networks, 22*(4), 1285-1298.

Wadhwa, L., Deshpande, R. S., & Priye, V. (2016). Extended shortcut tree routing for zigbee based wireless sensor network. *Ad Hoc Networks, 37*, 295-300.

Wampler, D., Fu, H., & Zhu, Y. (2009). Security threats and countermeasures for intra-vehicle networks. Paper presented at the 5th International Conference on Information Assurance and Security.

Whitmore, A., Agarwal, A., & Da Xu, L. (2015). The internet of things: a survey of topics and trends. *Information Systems Frontiers, 17*(2), 261-274.

Xia, M., & Song, D. (2017). Application of wireless sensor network in smart buildings. Paper presented at the International Conference on Machine Learning and Intelligent Communications.

Yaala, S. B., & Bouallegue, R. (2016). On MAC layer protocols towards internet of things: from IEEE 802. 15.4 to IEEE 802.15.4e. Paper presented at the 24th International Conference on Software, Telecommunications, and Computer Networks (SoftCOM).

Yang, K. (2014). Wireless sensor networks. *Principles, Design and Applications*.

Ye, W., Heidemann, J., & Estrin, D. (2004). Medium access control with coordinated adaptive sleeping for wireless sensor networks. *IEEE/ACM Transactions on networking, 12*(3), 493-506.

Yu, B., Xu, L., & Li, Y. (2012). Bluetooth low energy (BLE) based mobile electrocardiogram monitoring system. Paper presented at the International Conference on Information and Automation (ICIA).

Yue, H., Zhang, C., Pan, M., Fang, Y., & Chen, S. (2012). A time-efficient information collection protocol for large-scale RFID systems. Paper presented at the IEEE Proceedings INFOCOM.

Zhang, T., Antunes, H., & Aggarwal, S. (2014). Defending connected vehicles against malware: challenges and a solution framework. *IEEE Internet of Things Journal, 1*(1), 10-21.

Zhao, X., Zhang, W., Niu, W., Zhang, Y., & Zhao, L. (2010). Power and bandwidth efficiency of IEEE 802.15.4 wireless sensor networks. Paper presented at the International Conference on Ubiquitous Intelligence and Computing.

Zhou, B., Cao, J., Zeng, X., & Wu, H. (2010). Adaptive traffic light control in wireless sensor network-based intelligent transportation system. Paper presented at the 72nd IEEE Vehicular Technology Conference (VTC).

Zhuo, S., Wang, Z., Song, Y.-Q., Wang, Z., & Almeida, L. (2013). iqueue-mac: A traffic adaptive duty-cycled mac protocol with dynamic slot allocation. Paper presented at the 10th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON).

Zulkifli, C., & Noor, N. (2017). Wireless sensor network and internet of things (IoT) solution in agriculture. *Pertanika Journal of Science & Technology*, *25*(1), 91-100.

LIST OF THE PUBLICATIONS

1. Jahan Ali, Munirul Hasan, Muhammad Nomani Kabir, Yasser M. Alginahi, "Assessment of Wireless Technologies for deployment in Intelligent Transportation System based on Internet of Things" on International Conference on Internet of Things 2017 (ICIT)" February 22-23, 2017, Maharashtra, India.

2. Md. Arafatur Rahman, Jahan Ali, Saiful Azad, Muhammad Nomani Kabir "A Performance Investigation on IoT Enabled Intra-Vehicular Wireless Sensor Networks" International Journal of Automotive and Mechanical Engineering 14 (2017): 3970-3984.

3. Abbas Ali MH, Jahan Ali, Md Arafatur Rahman, and Saiful Azad. "Comparative Investigation on CSMA/CA-Based MAC Protocols for Scalable Networks." In Computer and Communication Engineering (ICCCE), 2016 International Conference on, pp. 428-433. IEEE, 2016.

4. Md Arafatur Rahman, Muhammad Nomani Kabir, Jahan Ali, and Saiful Azad, "On mitigating Hop-to-Hop Congestion Problem in IoT Enabled Intra-Vehicular Communication," In Proc. of the 4th International Conference on Software Engineering & Computer Systems (ICSECS' 15), Kuantan, Malaysia, Aug. 19-21, 2015.

5. Jahan Ali, Md. Arafatur Rahman, Muhammad Nomani Kabir “Cyber-physical Autonomous Vehicular System (CAVS): A MAC Layer Perspective” (accepted in springer).

APPENDIX A
SAMPLE APPENDIX 1

NA

APPENDIX B
SAMPLE APPENDIX 2

NA