A Dual-Radio Self-Configurable Heterogeneous Area Network Architecture for Machine-to-Machine Communications

Dong Chen

B.Sc. M.Sc.

A thesis submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
School of Electrical Engineering and Computing

THE UNIVERSITY OF
NEWCASTLE
AUSTRALIA

February 2018

Statement of Originality

I hereby certify that the work embodied in the thesis is my own work, conducted under normal supervision.

This thesis contains no material that has been accepted for the award of any other degree or diploma in any university or other tertiary institution and, to the best of my knowledge and belief, contains no material previously published or written by another person, except where due reference has been made in the text. I give consent to the final version of my thesis being made available worldwide when deposited in the University's Digital Repository, subject to the provisions of the Copyright Act 1968.

Dong Chen

Abstract

Machine-to-machine (M2M) communications can be envisaged as an efficient means to provide automated data transmissions among low-power devices in large-scale geographical areas. The data from these devices from different systems such as the Internet of Things (IoT) and the Smart Grid must be accumulated and relayed to the cloud in a reliable manner. To do this, many networking technologies could be used to establish a heterogeneous networking environment, in which information exchange processes need to meet the Quality of Service (QoS) requirements for various M2M applications. This research focuses on heterogeneous area networks comprised of the IEEE 802.15.4 and IEEE 802.11g devices. The former has intrinsic shortcomings such as low throughput, high delays, the lack of end-to-end Internet Protocol (IP) connectivity and intra-network collisions, whereas the latter could cause inter-network collisions in a heterogeneous network when sharing the license-free band. As a result, mitigating the intra-and inter-cluster collisions and maintaining the QoS requirements for M2M applications are key challenges for the M2M communication network design. In addition, several M2M applications may need to support two-way communication links such as electric vehicles exchanging location and system information with charging stations. During this process, the downlink traffic mixed with the uplink traffic may experience traffic congestion, thus degrading the network performance.

To tackle these challenges, new simulation models, techniques, link designs and algorithms were proposed in this research. To enable the IP end-to-end connectivity from the devices to the cloud, a 6LoWPAN-based wireless area network architecture for M2M applications was first proposed. To investigate the proposed architecture, several OPNET simulation models were developed. These models ensure IPv6 connectivity and serve as a cornerstone for the following research. After that, to mitigate the intra-network collisions caused by beacons and data packets, a staggered link design was proposed to superimpose the incoming superframe on the outgoing superframe to schedule packet transmissions. A packet aggregation technique, combined with the staggered link design, was proposed to further decrease the number of the transmitted packets in the network. Both the techniques can significantly mitigate the intra-network collisions, thus increasing the packet delivery ratio and lowering the end-to-end delay for a homogeneous wireless area network. In addition, a heterogeneous area network was proposed to extend the transmission range over a large geographical area and to maintain the QoS requirements for different M2M applications. However, the heterogeneous area network can cause inter-network collisions, which degrades the network performance. To solve this problem, a novel algorithm named as Blank Burst was proposed to schedule 6LoWPAN packet transmissions to avoid the inter-network collisions in the heterogeneous area network. This algorithm was further enhanced to a lifetime-based algorithm that schedules the packet flows and differentiates them as per their lifetimes and priorities to maintain the QoS of different M2M applications.

Finally, to solve the downlink traffic congestion problem in the proposed heterogeneous area network, a congestion mitigation algorithm was proposed. The algorithm classifies the queue length into several intervals corresponding to different traffic flows and uses ACK packets to schedule the downlink traffic from the end device side. The main advantage of the proposed algorithm is that it can quickly detect the downlink traffic congestion, schedule the traffic and alleviate the network congestion. The simulation results showed that the proposed designs and algorithms can successfully tackle the above challenges and are superior to the existing solutions in the literature, especially in terms of mitigating the intra-and inter-network collisions while maintaining necessary QoS requirements for M2M applications.

Acknowledgement

First and foremost, I would like to express my deepest gratitude to both of my supervisors, Associate Professor Jamil Khan and Doctor Jason Brown. Without their guidance and assistance, I could not have entered the portals of research and learned how to become a researcher. Their continuous support, patience and inspirational discussions during our weekly meetings, as well as the time devoted to assisting me with my research problems, will always be remembered. I genuinely appreciate their technical and insightful advice and comments on my experiments and thesis writing, which significantly enhanced my capabilities to conduct research.

Secondly, I would also like to thank the University of Newcastle and the China Scholarship Council for offering me this precious opportunity to pursue my Ph.D degree in Australia. Without their financial support, I would not have been able to come to this land and explore the frontiers of scientific discovery.

I owe great gratitude to Trevor Nelson, the information officer in the faculty, who would always be there for me with my various strange software and hardware problems, even after hours. Although the learning curve of the simulation software was steep, he always had faith in me and thought I was getting there. Many thanks should also be given to Chanel Hopkinson and Jo Midwinter, whose invaluable advice and support were very constructive.

I would also like to acknowledge two fellow members, Wan Norsyafizan W.Muhamad, who shared her thoughts and experiences regarding the simulation tool and paper writing techniques, and Muhammand Awais Javed, who spent a lot time on my erroneous simulation models at my the early stages of the research. Thanks should be also extended to Doctor Lawrence Ong, who provided me with constructive advice on my poster and thesis.

I am very grateful for my friends, Xie Wei, Wenli Dong, Dunyu Liu, Jun Li, Jing Meng and Ke Ou. Thank you for your generous and selfless support when my life was stuck in the second gear. Without your company, it would have been more daunting and less rewarding when I was going through this long journey.

I am indebted to my parents, who always believed in me and supported me with endless love and encouragement. Without your love and support, I would not have been able to get through so many challenges and finalise the thesis. If heaven had a window, I wish my dad could look down, watch me and be proud of what I have achieved.

Lastly, I want to thank the examiners who review this thesis. The time and efforts they put in will be genuinely appreciated.

Table of Contents

List of Figures

List of Tables

List of Initialisms and Acronyms

AMI	Advanced Metering Infrastructure
ARP	Address Resolution Protocol
BO	Beacon Order
BI	Beacon Interval
BE	Back-off Exponent
BB	Blank Burst
BAN	Body Area Network
BPSK	Binary Phase-Shift Keying
CBR	Constant Bit Rate
CBT	Cooperative Busy Tone
CSS	Chirp Spreading Spectrum
CCA	Channel Clear Assessment
CAP	Contention Access Period
CFP	Contention Free Period
CTS	Clear to Send
CW	Contention Window
CCTV	Closed-Circuit Television Camera
CSMA/CA	Carrier-Sense Multiple Access With Collision Avoidance
CASAGRAS	Coordination and Support Action for Global RFID-related Activities and Standardization
DSSS	Direct Sequence Spread Spectrum
DHCP	Dynamic Host Configuration Protocol

DIFS	DCF Interface Space
DRR	Dual Radio Router
DSM	Demand Side Management
ETSI	European Telecommunications Standards Institute
EVSE	Electric Vehicle Supply Equipment
EPC	Electronic Product Code
FIFO	First-In-First-Out
FFD	Full Function Device
GTS	Guaranteed Time Slot
HAN	Home Area Network
HART	Highway Addressable Remote Transducer Protocol
H2H	Human-to-Human
H2M	Human-to-Machine
IP	Internet Protocol
ITS	Intelligent Transportation System
ICT	Information Communication Technology
ISA	International Society of Automation
IFS	Inter Frame Spacing
IETF	Internet Engineering Task Force
IEEE	Institute of Electrical and Electronics Engineers
IAACCA	Interference-Aware Adaptive Clear Channel Assessment
LTE	Long Time Evolution
LQI	Link Quality Indicator
LoWPAN	Low Power Wireless Area Network

LPWAN	Low Power Wide Area Network
M2M	Machine to Machine
MAC	Medium Access Control
MTC	Machine-Type Communication
MTU	Maximum Transmission Unit
MIMO	Multiple Input Multiple Output
MSDU	MAC service data unit
MFDRR	Multi-Frequency Dual-Radio Router
NAN	Neighborhood Area Network
NFC	Near Field Communication
NAV	Network Allocation Vector
NIST	National Institute of Standards and Technology
OPNET	Optimized Network Engineering Tools
O-QPSK	Offset Quadrature Phase-Shift Keying
PLC	Power Line Communications
PRACH	Physical Random Access Channel
RFD	Reduced Fraction Device
RTS	Request to Send
RED	Receive Energy Detection
RFID	Radio Frequency Identification
RSSI	Receive Signal Strength Indicator
SO	Superframe Order
SOA	Service Oriented Architecture
SNR	Signal to Noise Ratio

SAP	Service Access Point
SCADA	Supervisory Control and Data Acquisition
UWB	Ultra-Wideband
UCode	Ubiquitous Code
UMTS	Universal Mobile Telecommunications System
VBR	Viable Bit Rate
WAN	Wide Area Network
WSN	Wireless Sensor Network
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WiMAX	Worldwide Interoperability for Microwave Access
WCDMA	Wideband Code Division Multiple Access
WWBAN	Wearable Wireless Body Area Newark
3GPP	3rd Generation Partnership Project

Chapter 1

Introduction

1.1 Motivation

With the increasing use of distributed devices to support various industrial and ICT applications, the need for interconnecting the devices such as sensors, computers, and embedded processors is increasing. These devices are envisaged to form a network named as the Internet of Things (IoT) and play a key role in promoting information exchange and supporting advanced ICT services [1]. This change has led to the development of a new type of communication paradigm called Machine-to-Machine (M2M) communications. In other words, machine-type devices can autonomously generate and transmit data to other devices via communication networks without any human intervention. The benefits of this interconnection are threefold. Firstly, the connected machines can effectively and efficiently accomplish more complicated tasks than a standalone machine without human intervention and may significantly decrease operational costs. Secondly, various types of services could operate on these autonomous machines to enable ubiquitous communications. Thirdly, informed decisions can be made by analysing the collected information from the distributed devices [1].

To support communications between the distributed devices and different types of applications, wired and wireless networking techniques must be taken into account. Although wired technologies can guarantee necessary QoS in terms of the end-to-end delay and packet success rate, its applications are limited by significant infrastructure costs and requirements such as digging the ground, placing conduits and laying cables. In contrast, wireless technologies have shown their prevalence over the wired ones due to the lower infrastructure cost and less installation time to support a large number of mobile or stationary users. The wireless networks can be categorised as infrastructure-based and infrastructure-less networks. The infrastructure-based networks such as cellular networks are designed for mobile users to deliver multimedia data such as audio, video and recently some machine-type data. Cellular network links are generally asymmetric and support more data on the downlink. Infrastructure-less networks can be implemented using short-range networks, which may support a large number of scattered devices that generate a large volume of low duty-cycle traffic on the uplink. On the contrary, current generation cellular networks are not suitable to transmit M2M data because their uplink channels can be easily saturated. The infrastructure-less networks can be more effective than the infrastructure-based networks in supporting distributed applications due to its flexibility and low cost, especially in the transition from 4G networks to 5G networks. However, infrastructure-based IoT networks such as the Narrow Band IoT (NB-IoT) networks are currently under development and will be deployed under the 5G umbrella.

The use of different types of IoT devices poses real challenges to the development of M2M networks. This is because heterogeneous M2M devices have different functionalities and features [2]. For example, some nodes are responsible for environment monitoring, capturing and transmitting temperature and humidity data; whereas other applications need to support mobility, such as robotics for conducting rescue tasks under risky circumstances. Generally, M2M devices range from the ones with simple functionalities to the ones that are powerful and can handle more difficult tasks. Different IoT nodes can be designed using different hardware resources. As such, simple nodes can be battery-powered and deployed in order to implement easy tasks, whereas smart phones and robotics are less subject to energy constraints and can offer complex services.

Since M2M devices vary in terms of their hardware designs, capacity and functionality, the applications that can be supported by these devices are also different. For example, smart meters provide energy consumption information; remote control and fault diagnose functionalities for residential premises. Another example is the e-health, in which sensors are attached to a human's body, monitoring the heart rate and blood pressure and other physiological signals. Health reports are automatically generated and delivered to the doctors or medical servers. Vehicular networks also use the M2M devices to serve different applications. The European Telecommunications Standards Institute (ETSI) has proposed a new vehicular IoT communication architecture. Basic safety messages can be broadcasted by the safety sensors located on the road side, warning vehicles in the vicinity to keep a safe distance; integrated with the Intelligent Transportation System (ITS), traffic sensors can transmit congestion messages to drivers.`

To support different M2M applications, wireless networks must be properly developed to support the necessary QoS requirements of M2M applications. For example, smart meters can serve as a gateway to connect all the devices in a Home Area Network (HAN) and transmit energy consumption information in a cyclic or on-demand manner. E-health, by contrast, may need to support stringent delay requirements to support time-critical events such as a heart attack that triggers an alert generated by medical sensors to the medical center. In vehicular networks, basic safety messages can be broadcast by roadside sensors, which respond to traffic changes in a timely manner to deal with traffic congestion and accidents. This basic discussion indicates that the diverse nature of M2M traffic often results in complex traffic patterns in the backhaul network of M2M systems. M2M communications' advance has led to IoT system development, so the inter-connected systems can harness, transfer and process information from a large number of distributed devices. IoT systems can be deployed for both indoor and outdoor applications due to the diverse nature of traffic. To support such systems, it is necessary to develop advanced M2M network architecture that can adapt to support necessary QoS requirements of M2M applications.

1.2 Research Challenges

Though recent years have witnessed advances in M2M communications and a lot of research studies have been conducted, many fundamental networking problems still need to be explored and solved. In this section, several research challenges with respect to M2M communications are identified and discussed. M2M devices can generate different traffic patterns in a heterogeneous network. Each segment of the heterogeneous network may use a different networking protocol, thus causing interference for each other's operating environment. One example is that the short-range network standards such as ZigBee, Bluetooth, and Wi-Fi can be employed in a HAN. Therefore, interoperability between these networks is difficult to achieve. The transmission rates and medium access techniques of these networks can also significantly vary, so how to efficiently relay packets among the heterogeneous devices with low and medium transmission rates remains to be explored.

Many research studies have concluded that unlicensed short-range networks can better serve the needs of M2M communications by organising data devices into wireless area networks. Large numbers of M2M devices can form in a mesh or tree topology for large-scale deployment, and then these devices are connected via a gateway to a cellular network, which serves as a core network that can cope with aggregated traffic [3]. To cover a large area, a multi-hop wireless network with short-range network standards needs to be adopted. A large number of low-power devices could operate in the license-free 2.4 GHz band, so different types of packets can be transmitted on the same channel. Such a shared networking environment may cause the intra-network collisions, which can greatly degrade the network performance of the co-located subnetworks. For example, some control packets, such as beacons, can be lost due to the intra-network collisions, and thus packet transmissions can be affected. In addition, many low-power devices can be connected in multi-hop networks to forward packets from source nodes to a data sink. The network performances can exacerbate with high end-to-end delays and low packet delivery ratios when the number of hops increases. This is because packet losses and delays can accumulate with the increasing number of hops, so the sink node experience high packet losses and longer delays.

A large number of M2M devices use the current short-range wireless networking standards to operate in Instrumental, Scientific and Medical (ISM) unlicensed bands. Because of this, the performance of M2M networks may be subject to in-band collisions [4], which is one of the key concerns for the M2M and IoT network developers. The in-band collisions can be divided into intra-network collisions and inter-network collisions. The intra-network collisions refer to the packet collisions between homogeneous M2M devices, and the inter-network collisions denote the packet collisions between heterogeneous M2M devices. The intra and inter-network collisions can cause high power consumption for M2M devices, which limits the network lifetime and degrades the overall network QoS performance. Both the types of collisions pose specific challenges in terms of achieving network convergence among the heterogeneous devices. In addition, the access control mode of M2M devices varies in different wireless technologies. For example, Bluetooth uses a common clock and the same hopping sequence to synchronise in a TDMA type network, while ZigBee and Wi-Fi use the Carrier Sensing Multiple Access/Collision Avoidance (CSMA/CA) protocol to access the channel. As a result, coordination between the heterogeneous wireless networks is required to optimise the network performance.

M2M devices need to handle the bi-directional traffic for sensor actuator applications. Low power area networks have little uplink and downlink coordination, thus resulting in packet collisions or interference on these links. Bidirectional applications such as Demand Side Management (DSM) in the Smart Grid need to collect energy consumption data from consumers and regulate the energy demands to maintain the stability of the electrical grids. To implement a DSM system, the control packets transmitted on the downlink (from utility servers to residential premises via smart meters) need to compete for channel capacities with the uplink traffic. The uplink and downlink traffic together can result in traffic congestion on the relay nodes such as routers because they have limited capacities and suffer from packet losses on the uplink. Another challenge is that the packet prioritization mechanism for short-range networks is not well defined to differentiate the urgent and non-urgent applications. Downlink traffic flows such as DSM usually require a higher priority compared with many uplink applications. For this reason, the downlink packets with a higher priority must be protected from undue interference from the low priority traffic sources. Appropriate packet prioritization and congestion mitigation algorithms must be developed to maintain the QoS of the multiple M2M applications coexisting in the network.

1.3 Thesis Contributions and Organization

The main contributions of this thesis and its organization are described in this section. Chapter 2 review the related work on the Neighborhood Area Networks (NANs) and Field Area Networks (FANs) design techniques for M2M and IoT applications. Firstly, the IoT and its elements are explained in detail. The M2M and IoT standard organizations have recommended three classes of networks that constitute an IoT system: area networks, access networks and core networks. IoT applications are discussed in the context of three domains: the industry domain, the smart city domain and the health care domain. M2M communication technologies including wired and wireless solutions are then detailed. Among these solutions, short-range networks, which are widely adopted in the area networks, are reviewed. However, single standard-based short-range networks such as wireless sensor networks may not meet all the QoS requirements of different M2M applications, so heterogeneous network solutions are reviewed to explore the possibility of improving and maintaining the QoS requirements for various M2M applications [5-7]. Lastly, due to the complexity of the propagation conditions such as fading and path losses, interference management is reviewed because it is a key design task for the M2M communication platform. Latest research on the intra-network and inter-network collisions are also investigated [8, 9].

Chapter 3 considered a 6LoWPAN-based wireless area network architecture for IoT applications. The network architecture based on the 6LoWPAN standard is developed using a discrete event simulator OPNET. The chapter firstly presents a basic IoT network structure and implementation of the corresponding simulation model. The model is illustrated in a modular manner with the transition state machine, and algorithms are presented in flow charts. The chapter discusses the IEEE 802.15.4 standard and the associated protocols including the Carrier Sensing Multiple Access/Collision Avoidance (CSMA/CA) protocol, which is the key algorithm of many sensor and IoT networks. Secondly, since there is no 6LoWPAN simulation model available in the OPNET library, the chapter describes the model development techniques. In particular, the IPv6 header compression and restoration algorithms are implemented, and the simulation node models and process models are created and described.

Chapter 4 discusses the effects of the intra-network collisions in a homogeneous area network. In general, wireless area networks can experience significant intra-network collisions due to the overlapping periods of beacon and data packet transmissions. To solve this problem, a staggered-link design is proposed. The most important reason for this design is that the routers normally maintain two superframes: the incoming superframe and the outgoing superframe, so the two superframes need to be coordinated without generating overlapping transmission time. A packet aggregation technique including 6LoWPAN header compression and payload aggregation is proposed to further mitigate the intra-network collisions. However, increasing the number of hops can increase the end-to-end delay and lower the packet delivery rate. To solve these problems, a heterogeneous wireless area network combining the 6LoWPAN and IEEE 802.11g standards is considered. A dual-radio router (DRR) is proposed to extend the transmission range of the short-range 6LoWPAN network, reduce the end-to-end hop numbers and increase the transmission capacities of the routers.

Chapter 5 discusses the effects of the inter-network collisions in a heterogeneous area network, where the DRR can adversely affect the 6LoWPAN networks. M2M communications in general consist of many 6LoWPAN devices, so the inter-network collisions may lead to the degradation of network performance. To deploy a dense area network for IoT applications, a Multi-Frequency Dual-Radio Router (MFDRR) is proposed. The MFDRR employs two 6LoWPAN frequencies to increase the number of 6LoWPAN nodes and clusters in a given geographical area thus supporting a practical dense network architecture. To mitigate the inter-network collisions, a collision mitigation algorithm named as Blank Burst (BB) is proposed. The algorithm makes the 6LoWPANs pause for a short period, in which the WLAN interface of the MFDRR can aggregate 6LoWPAN packets into WLAN payloads and transmit. This period introduced by the BB algorithm prevents the 6LoWPAN packets from being adversely affected by WLAN packet transmissions. Since the WLAN interface has a much higher data rate and uses higher transmission power, the BB algorithm can effectively solve the problems discussed in Chapter 4 in the heterogeneous wireless area network. An aggregation factor is used to regulate the number of WLAN packets. The simulation results show the BB algorithm mitigated the inter-network collisions and improved the overall QoS of the M2M area network.

Chapter 6 further enhances the BB algorithm by proposing a new lifetime-based BB algorithm to tackle the inter-network collisions and maintain the QoS of the M2M area network. Specifically, the improved algorithm classifies the incoming packets into different traffic groups, each of which maintains the shortest lifetime of all the packets in the group. The algorithm obtains the lifetime value of each incoming packet and compares it with the current shortest lifetime value in the group. Different traffic groups are also compared to determine the shortest lifetime value in the network to trigger the Blank Burst algorithm. In particular, if a lifetime of the packet is less than the pre-defined guard margin, the packet is dropped to maintain the QoS of the applications. A packet prioritisation technique is introduced to guarantee the QoS requirements of a higher priority traffic group. Another contribution is a congestion mitigation algorithm for the sensor-actuator applications that may require bi-directional communications. The algorithm has four units: the congestion detection unit, downlink packet protection unit, congestion notification unit and inter-arrival rate adjustment unit. The simulation results confirm the effectiveness of the lifetime-based BB and downlink congestion mitigation algorithms in terms of packet delivery rates, end-to-end delays and packet loss ratios

Chapter 7 examines the performances of a large-scale area network involving multiple MDFRRs and a large number of 6LoWPAN devices with the proposed scheduling algorithms. This study aims to build a large-scale dense area network to support M2M applications. The inter-network collisions arise not only from the local area network as described in the previous chapters, but from the other area networks in the vicinity, which is inevitable especially when multiple area networks coexist for large-scale deployment. The simulation results prove the effectiveness of the proposed algorithms including the staggered link design, the aggregation factor-based BB, the lifetime-based BB and the downlink congestion mitigation algorithms. Even the inter-network collisions from the neighboring area networks can be minimized to improve the overall QoS of the large-scale heterogeneous area network

Chapter 8 concludes the study with the summary and future research.

The key contributions of this study are listed below.

- Investigated the key requirements of M2M area network design issues in Chapter 2.
- Proposed and developed a staggered link design and a packet aggregation technique to improve the QoS performance of a homogeneous IoT area network in Chapter 4.
- Evaluated the performance of low-cost license-free homogeneous area networks using the short-range 6LoWPAN-based wireless networking standard in Chapter 4.
- Proposed and developed a heterogeneous IoT network architecture combining the 6LoWPAN and IEEE 802.11g standards, which can be a low-cost solution for the Low Power Wide Area Network (LPWAN) in Chapter 4, 5 and 6.
- Comprehensively analysed the performance of the heterogeneous wide area network for dense M2M area network deployment in Chapter 7.
- Developed a full OPNET simulation model library to analyse the performances of the homogeneous and heterogeneous M2M area networks using the 6LoWPAN and IEEE 802.11g standards.

1.4 List of Publications

Book Chapter

[1] J. Y. Khan, D. Chen, “Low Power Wide Area Network’’, to be published by Pan Stanford Publishing Pte Ltd, www.panstandford.com in 2019

Refereed Journal Papers

[1] J. Y. Khan, ***D. Chen***, and O. Hulin, "Enabling Technologies for Effective Deployment of Internet of Things (IoT) Systems," *Australian Journal of Telecommunications and the Digital Economy,* vol. 2, 2014. pp [65.1]-[65.22]

[2] J. Y. Khan, ***D. Chen***, and J. Brown, "A Cooperative MAC Protocol for a M2M Heterogeneous Area Network," *Journal of Sensor and Actuator Networks,* vol. 5, no. 3 (2016): 12.

Refereed Conference Papers

[1] ***D. Chen***, J. Brown, and J. Y. Khan, "6LoWPAN based Neighborhood Area Network for a smart grid communication infrastructure," in *Ubiquitous and Future Networks (ICUFN), 2013 Fifth International Conference on,* 2013, pp. 576-581.

[2] ***D. Chen***, J. Brown, and J. Y. Khan, "Performance analysis of a distributed 6LoWPAN network for the Smart Grid applications," in *Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2014 IEEE Ninth International Conference on,* 2014, pp. 1-6

[3] ***D. Chen***, J. Y. Khan, and J. Brown, "An area packet scheduler to mitigate coexistence issues in a WPAN/WLAN based heterogeneous network," in *Telecommunications (ICT), 2015 22nd International Conference on,* 2015, pp. 319-325。

[4] ***D. Chen***, J. Brown, and J. Y. Khan, "An interference mitigation approach for a dense heterogeneous wireless sensor network," in *Signal Processing and Communication Systems (ICSPCS), 2015 9th International Conference on,* 2015, pp. 1-7.

Chapter 2

An Overview of Machine-to-Machine Communications Techniques

2.1 Introduction

With the advent of the Information Communication and Technology (ICT), embedded sensors, actuators and machines constituting a network to exchange information is named as the Internet of Things (IoT). IoT networks involve many technologies and applications, such as tracking and identification technologies, enhanced communication protocols, sensor and actuator networks, and intelligent automated devices [5]. To enable universal connectivity for the IoT, machine-to-Machine (M2M) communication networking infrastructures need to be developed [7]. M2M communications enables information to be exchanged between machines and intelligent devices without human intervention. The information is relayed via wired or wireless networks to a remote data centre, which processes the gathered information, evaluates the current status and then makes informed decisions and sends instructions to other machines. The technologies for M2M communications are therefore a cornerstone to achieving the large-scale deployment of control and monitoring infrastructures. M2M communications are a subset of the IoT system, which consists of many domains, such as the application domain, sensing and collecting domain. One of the typical M2M applications int the energy sector is the Smart Grid, which efficiently delivers electricity to consumers and improves the reliability, efficiency and security of the electricity grid.

2.1.1 Internet of Things Definition, Visions and Trends

The term ‘Internet of Things’ was first conceived by Kevin Ashton who envisaged that the physical world would be connected to the Internet by pervasive sensors and actuators that could transmit and process diverse information to improve the quality of life for people [2]. This concept was re-defined so that the IoT became as an infrastructure that links information, objects and people using the Internet [10]. The IoT enables the communication between smart devices or the objects separated and distributed in a large-scale area. Connected with each other, the devices share and coordinate information to automatically finish certain tasks. In this process, many technologies such as wireless sensor networks and pervasive computing play a significant role in enabling the communications. The IoT system can be divided into three layers [11]. The lowest layer consists of millions of smart devices such as machines, sensors and actuators that account for the significant number of the total devices. Tablets, computers and smart phones are in the middle layer and server as the main force connecting to the Internet. The third layer, the core of the IoT, is the cloud computing technology that abstracts the lower layer information, provide data analysis and perform services. It is envisioned that 212 billion IoT devices will be deployed around the world by 2025, leading to a huge market share of between $2.7 to $6.2 trillion [12]. Indeed, the increasing growth of the IoT devices benefits the related industries and applications, especially for manufacturers that upgrade traditional equipment and products to IoT devices. The realisation of the IoT requires interoperability between machines to machines, humans to humans, and machines to humans [13].

Before the concept of the IoT, the idea of embedding technologies led to ubiquitous computing in the late 1990s, and it was the predecessor of the IoT technology. With the proliferation of handheld devices such as smart phones and tablets, the world is becoming more informative and interactive. The smart environment, as proposed by Mark Weiser, the inventor of ubiquitous computing, is seamlessly connected by displays, actuators, sensors and computers that interweave a complex network [14]. In addition, the Internet can provide connectivity to all computers in the world, meaning that it has the potential to achieve ubiquitous computing by linking computers and other IoT devices. The concept of ubiquitous computing was further extended by Rogers who advocated human-centred ubiquitous computing that can increase human’s capacities to explore the world [15] and will be beneficial to corporations or organizations. Later, the features and components of ubiquitous computing were discussed by Caceres and Friday who pointed to two research fields: the IoT and cloud computing [16]. The latter is an emerging technique providing reliable data services for the next generation Internet by using virtual storage transparent to users. Cloud computing is one of the central pillars of the IoT, receiving data forwarded by a large number of sensors and processing these data from the background. Cloud computing also provides reliable data access, scalability to infrastructures and autonomous control of the devices. As a result, services can be customised by changing the parameters to maintain the QoS.

The rising interests in the IoT have attracted many standard organizations and research institutes to investigate this field with different visions. This is because research centres and standard organisations, driven by specific purposes and research interests, have different backgrounds and purposes, and look at the IoT from different perspectives. As new ideas come along, the IoT concept has evolved over time. In [5], three visions were proposed for the IoT: things oriented, internet oriented and semantic oriented. The first vision focuses on the basic elements of ”things”, which are sustainable, traceable and identifiable within the IoT system comprised of millions of wireless sensors, machines and actuators [17]. Several projects are underway, emphasising the ubiquity of accessibility to smart devices. It is expected that the smart devices will outnumber the population of the world in the near future [18]. The second vision, proposed by many consortiums such as Coordination and Support Action for Global RFID-related Activities and Standardisation (CASAGRAS) [19] have concentrated on the concept that the Internet connects all of the devices. In other words, the focal point has been shifted from “things” to the devices connected by the Internet and how they automatically connect and communicate with each other to benefit humans. As such, independent applications and services could be developed to support autonomous data acquisition, packet relay, and information processing, thereby improving the interoperability of devices in the context of the IoT. Another conjecture is to use the IP protocol to connect IoT devices. This is partly because the IP is a mature technology and has already connected a large number of devices around the world, so if IoT devices are added to the existing IP-based infrastructure, the IP protocol has the potential to support IoT applications. For that reason, to make IP more compatible with the IoT paradigm, a sensor network based on the 6LoWPAN standard has been proposed to adapt to the full deployment of IoT devices. The third vision is explained from a higher level than just physical objects [20]. The information abstraction on how to search, collect, store and represent data is important in the IoT because the information generated by a large number of IoT devices needs to be easily expressed and managed by the control centres.

The IoT system can connect the Internet and distributed physical devices such as refrigerators, microwaves and sensor networks capable of collecting and generating information. In other words, the devices that can generate data are allowed to connect to the existing network infrastructure and extend communication domains from human-to-human to human-to-machine or machine-to-machine. Therefore, devices can be integrated into internet-based systems to improve the communication range, efficiency and accuracy, and thus the devices must have several characteristics: (1) they have an identity that can uniquely identify the device within the network; (2) they can sense and process the information in the vicinity; (3) they should be equipped with communication modules capable of sending and receiving information; and (4) the information generated by the devices should be structured and easily readable by the higher layer entities. These features enable the devices to interact with other entities in the network, so the IoT is a distributed network system connecting a massive number of IoT devices.

In the context of the IoT, countless devices constantly collect information from the environment and change them into binary data. As such, some actions can be triggered to prevent malfunction when anomalies are detected. Several key problems should be considered before implementing an IoT system. A large number of heterogeneous devices pose a real challenge in terms of device management. As the system evolves, more objects will be added to the system, resulting in a scalability problem [5]; that is, how to facilitate new objects to smoothly communicate with the existing objects. Another concern about the IoT is that wireless networks will be adopted as communication mediums due to the ease and cost-effectiveness of installation, so many devices could use license-free spectrums for quick deployment. This may cause the scarcity of radio resources and lack of security. To solve these problems, it is important that synergetic efforts are required, including the design of hardware, software, protocols and algorithms.

To embrace the opportunities and challenges brought by the IoT, transmission platforms will be implemented to enable M2M communications, providing applications from many sectors such as transportation and logistics, smart environments, healthcare, etc. Standard bodies and research institutions have been working to advance IoT system capabilities, bringing humans a step closer to the realisation of the IoT. In this process, key enabling technologies play a vital part in achieving the ultimate design goals of the IoT, such as seamless connection between devices anywhere, anytime and from any medium [21]. Despite the development of the enabling technologies, research challenges and open issues remain to be explored.

2.1.2 The Elements of the IoT

To fully understand how IoT systems will behave in reality, the building blocks of IoT systems need to be investigated. IoT system operations can be divided into three phases: data collection, data transmission, and data process, management and analysis [22], As shown in Fig 2-1, each phase has different modules with different functionalities and purposes. The data collection phase aims at collecting the information generated by the sensors, actuators and machines at the lowest layer of the IoT. Several technologies are involved in this stage, and meanwhile, many other communication standards, such as IEEE 802.15.4 and IEEE 802.11, are also used to collect data. The data transmission phase focuses on delivering and relaying data to external applications and services, which need gateways that require heterogeneous technologies, such as routing and addressing, to access the network. The third phase is to process and analyse the data collected from the above two phases. The remainder of this section will explicitly explain how each phase works.

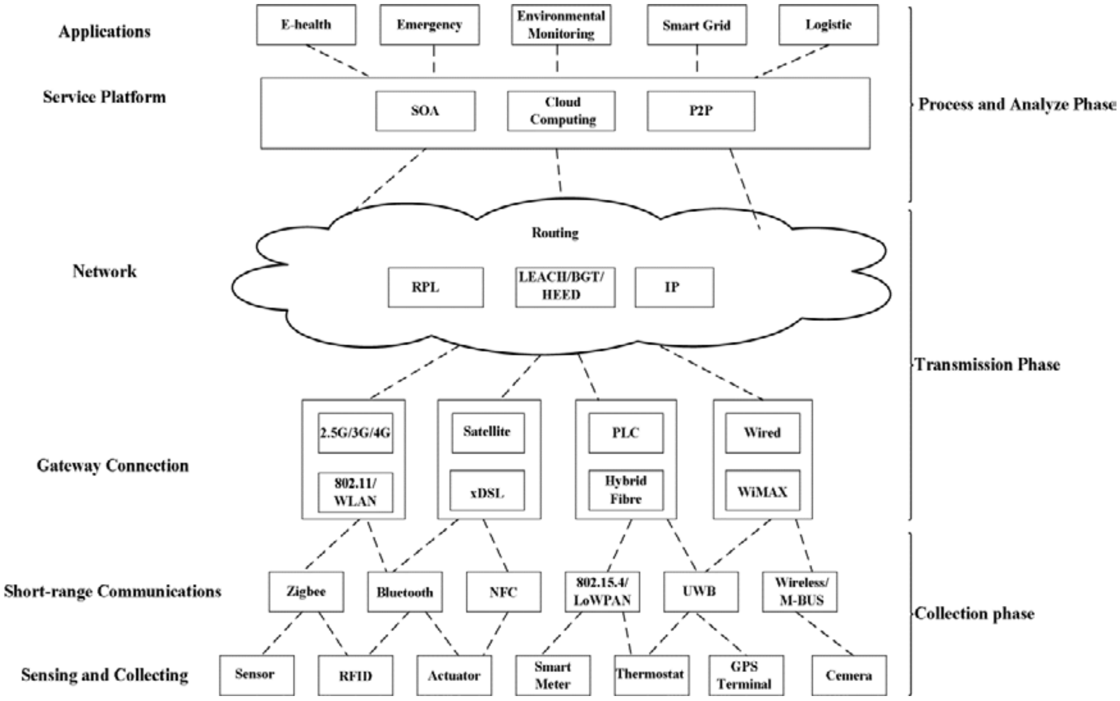


Fig 2-1 Representation of hierarchical communication architecture in the IoT

Data Collecting Phase

The distributed sensors, machines and actuators continuously sense the environment and collect the sensed data. Many technologies are involved in this process, and one of them is the RFID, which has two components: a tag and a reader. The tag is used to identify an object with an Electronic Product Code (EPC) or Ubiquitous Codes (uCode), while the reader reads from the tag and sends to the Internet [23]. In addition, two types of tags are involved in this process: the passive tag and the active tag. The passive tag is inexpensive, small and long-lasting, and does not have energy supply and uses the reader's energy to transmit data. However, the passive tag can only transmit a short distance of three meters [24]. Unlike passive tags, the active tags, equipped with a power supply, can transmit a longer range and do more complicated operations. Moreover, different frequency bands can be used to communicate between the tags and the readers. For example, the widely used frequency band ranges from low 125 kHz to high 915 MHz, with extra high frequencies up to 2.4 GHz. A further approach, similar to the RFID, is to use Near Field Communication (NFC) that enables wireless communications between two devices in the vicinity, including personal data such as video, audio and files. NFC is an improvement over the RFID and allows two-way communications between devices; that is, when two devices are close enough, e.g., less than 4 cm, the communication begins.

In addition to the RFID, Wireless Sensor Networks (WSN) are a key enabler for the IoT because they are applicable to many domains [25]. Sensors can be placed in any operating environment, such as an ocean, forest and cities, with applications such as intelligent agriculture and environmental monitoring. These sensor nodes are normally powered by batteries and have very basic computational capacities. WSNs consist of a large number of static nodes sensing several parameters, such as temperature, humidity and air pressure. All these sensor nodes are organised in a multi-hop fashion. In other words, the sensed data are forwarded via many hops before they reach to a data sink. The main communication standards adopted by WSNs are IEEE 802.15.4, ZigBee, 6LoWPAN and Wireless Highway Addressable Remote Transducer Protocol (HART). Most of these standards are generally operating at 2.4 GHz license-free bands and using 250kbps to transmit information [26].

WSNs have gradually attracted the attention of researchers in recent years, where much emphasis was put on routing, congestion mitigation, and MAC and Transport Layer protocols [26, 27]. However, a recent trend is to improve the energy efficiency of the WSNs deployed in some environments such as underwater or underground, in which replacing the energy source is difficult [28]. For that reason, low power networks are expected to be used in the IoT environment, and these devices could use the IEEE 802.15.4 standard to enable cost-effective wireless communications [29].

The IEEE 802.15.1 Bluetooth network is also a short-range candidate for the IoT and replaces wired communication between low-power devices [30]. In Bluetooth communications, the devices form a small-scale network named piconet where devices are classified into masters and slaves. The master polls each device and determines which device is allowed to access the channel. Similar to ZigBee and 6LoWPAN, the Bluetooth standard also uses the 2.4GHz license-free bandwidth with a data rate ranging from 1Mbps to 24 Mbps.

Table 2-1 Main characteristics of the short-range communication standards.

Technology	**Data Rate**	**Transmission range**	**Frequency**	**Reference Standard**	**Representative Devices**	**Application**
RFID	Up to 640kbps	3-10 m	125kHz to 2.4GHz	ISO/IEC 18000	Book/CD/DVD tag, passport, badge	Tracking, access control
NFC	106-424kbps	<10m	13.56MHz	ISO/IECI8092/ECMA-340 ISO/IEC21481/ECMA-352 ISO/IEC14443	Smart phone/parking meter/ticket stamping machine	Sharing/access control/contactless payment
WSN	20 to 250kbps	10-100m	2.4GHz/700-900 MHz	IEEE 802.15.4	Wearable sensors/monitoring sensors	Surveillance/Health monitoring
Bluetooth	1 to14 Mbps	5-30m	2.4GHz	IEEE 802.15.1	Wireless mouse/keyboard	Health care/helmet headset

Data Transmission Phase

In the second phase, after data are accumulated by the technologies previously mentioned, they are passed via networking processes to applications. As a large number of heterogeneous devices with different hardware and software exist in the data collection phase, the transmission network should use hybrid networks to form the backbone network [31]. In the case of the wired network standards, the first standard is IEEE 802.3 Ethernet that has been used for decades with transmission rates of up to 100 Gbps. The data are transmitted by means of coaxial cables, twisted pair and optical fibers, which prevent the network from being susceptible to interference and errors. Another wired standard is Power Line Communications (PLC) that use the electricity infrastructure as a transmission medium [32].

In the context of the IoT, the scalability of the wired network might become a concern when adding new devices and reorganising the network topology, so deploying large-scale wired networks to cater for the IoT is not an ideal choice. However, wireless networks show better flexibility than wired networks due to their “plug and play” characteristics. The IEEE 802.11 Wireless Local Area Network (WLAN) can either form a peer-to-peer network, where each device is equal and performs the transmission independently, or form infrastructure mode, in which devices connect to a central hub called an access point controlling the access to the channel. A WLAN normally operates on the 2.4 GHz/5 GHz band with the transmission rate ranging from 1 Mbps to 720 Mbps [33]. The WLAN also has many variants such as IEEE802.11a/b/g/e/n/ac that have been designed for different purposes. For example, 802.11n uses Multiple Input Multiple Output (MIMO) to increase throughput when sending and receiving at the same time.

Cellular networks are expected to be deployed in the IoT environment due to their design for video and audio transmission. For example, Long Term Evolution (LTE) is characterised as the high data rate and low latency network, providing connectivity for a dense networking environment and mobile devices. Satellite communications also serve as an ideal candidate for data transmission. It is useful to connect remote areas such as in oceans or on isolated islands where the cellular networks are difficult to be deployed.

Apart from the WLAN and Cellular networks, other technologies are also available for IoT data transmissions, such as wireless heterogeneous networks, cognitive networks and opportunistic networks. These technologies are emerging because so the temporarily free spectrums can be utilised to increase the efficiency of wireless transmissions. Cognitive networks dynamically distribute the spectrums that are not temporarily used by primary users, to secondary users [34], so the spectrum utilization is improved. In a cognitive network, carrier sensing and spectrum assignment play an important role as they greatly affect the QoS when sensing the channel and determining how to assign the available channel. There are still many challenges in dealing the vulnerabilities of cognitive networks. Opportunistic networks allow devices from different areas to carry and forward data within the transmission region. This is particularly useful in heterogeneous networks where spectrum efficiency can be optimized using the interoperability between the short-range wireless networks and the cellular networks [35]. For that reason, the combination of short-range, medium range and cellular networks could optimise the spectrum utilisation. It is therefore important that a heterogeneous network structure should be developed to handle IoT networks.

Table 2-2 Main characteristics of communication standards in the transmission phase.

Technology	**Standard**	**Frequency**	**Data Rate**	**Transmission Range**	**Transmission Medium**
Ethernet	IEEE 802.3 u/z	N/A	10Mbps to 100Gbps	100m up to 50-79km	Twisted-pair Optical fiber
xDSL	ADSL/ADSL 2+ VDSL		12-55Mbps (d) 1-20 Mbps(u)	Up to 6 km	Twisted-pair Coaxial cable Fibre
PLC	Home Plug AV, IEEE 1901	1-30 MHz	>100Mbps	Up to 1500 to the premises	Electrical power system
WLAN	IEEE 802.11a/b/g/n	2.4GHz/5GHz	1-54-600 Mbps	Up to 100 m	Wireless
WiMAX	IEEE 802.16/a/d/e/m	2-66GHz	Up to 70Mbps	Up to 50-80 m	Wireless
Cellular	GSM/GPRS/UMTS/ LTE-A	900-1800MHz 2100-1900MHz 800-2600MHz	9.6kbps, 56-114kbps 56Mbps (d)/22Mbps (u) 300 Mbps (d)/75 Mbps (u)	Macro/micro/pico/femto cells (10m to 30 km)	Wireless
Satellite	BSM./DVB-S/ DVB-TS	4-8GHz (C band) 10-18 GHz 18-31GHz	16kbps to 155kbps	GEO sat: 35786km MEO sat: 500-15000km LEO sat: 200-3000km	Wireless

Data Processing and Analysing Phase

The third phase deals with the data forwarded by the second phase and hands over to the application layer in the system. The upper layer service platform is responsible for analysing and abstracting all the features from the collected information. All information must be transparent to the lower layer in the system such that the data analysis and processing become easier. One effective way of achieving information abstraction is Service Oriented Architecture (SOA) [36]. The SOA is an architecture that allows communication protocols to provide services from the application layer to the lower layers using the Internet, and therefore has the potential to apply to the IoT scenario. The SOA normally includes three layers with different functionalities. The first layer aims to abstract objects and their functionalities and consider them as services, which can be accessed by semantics and procedures. The second layer manages these services and objects, and provides a means to automatically monitor the access and discover processes, and unveil their statuses. It also remotely maintains the communication between objects and services from other platforms. The third layer is responsible for all approaches to holistically managing the objects and services, and uses a repository to update the statuses of all the objects and services.

In addition to the service and application platform, cloud computing serves as the one of core platforms of the IoT. The cloud has a massive capacity in terms of storage and computation to deal with a huge amount of data, classifying, processing and analysing them after collecting from the transmission networks [37]. For example, a high volume of data need to be retrieved and handled in a real-time manner such that some applications running on the device can receive timely responses to tackle emergencies such as bush fires or burglary. To this end, large numbers of devices are connected to the cloud that can function as human brains do to handle complicated tasks.

2.1.3 Standard Organizations

As the IoT consists of the various technologies to support the three phases, it is necessary to generate a holistic plan that combines all of these technologies and deals with research challenges. Several significant issues such as the networking and addressing are discussed in this section. Due to a plethora of technologies developed for the IoT, it is difficult to reach a consensus that all of the components are compatible and interoperable. Developing a reference architecture, therefore, becomes important. Such momentum drives many universities, standard organizations and research institutes towards the realisation of the IoT. This section describes several representative architectures proposed by the Third Generation Partnership Project (3GPP), the European Telecommunications Standards Institute (ETSI), the Institute of Electrical and Electronics Engineers (IEEE) and the Internet Engineering Task Force (IETF).

The ETSI proposed a multi-tiered M2M communication architecture aimed at solving scalability and connectivity problems and providing seamless connectivity for a multitude of low-power devices [38]. The reference architecture was designed to bring one step closer to an IP-based network architecture that ensures end-to-end connectivity. This architecture has several advantages: (1) it is scalable to add new devices to the network; (2) all the devices run the IP stack, which reduces the complexity of the protocol translation; (3) it has unified interfaces and protocols; and (4) it is easy to extend other applications [39]. Fig 2-2 illustrates the hierarchical architecture consisting of the three network layers: area network, access network and core network.

Area Network

An area network consists of a large number of low-power devices and gateways. These devices generate and collect data from its operating environment, and then transmit to a remote server via the gateway. They either establish a straightforward communication link to the server or use the gateway to connect to the server. The gateway, with local processing and aggregating capability, acts as the translator to resolve the protocols from the area network to access network.

Access Network

This network aims to connect the gateways and the core networks, providing IP end-to-end connectivity. The access network corresponds to the second phrase in the IoT elements, and is responsible for collecting the aggregated data from the IoT devices. To do this, communication protocols play a critical role. Protocols such as WiMAX, LTE, ADSL and PLC can be used to ensure the connectivity.

Core Network

Applications reside on IoT devices and the servers connected via the access and core networks. The core networks connect many servers and field devices to enable IoT applications and middleware that abstracts and represents the information from the higher layer. One of the main functions of the core networks is cloud computing, which stores the gathered data and provides large capacity for computation and data processing.

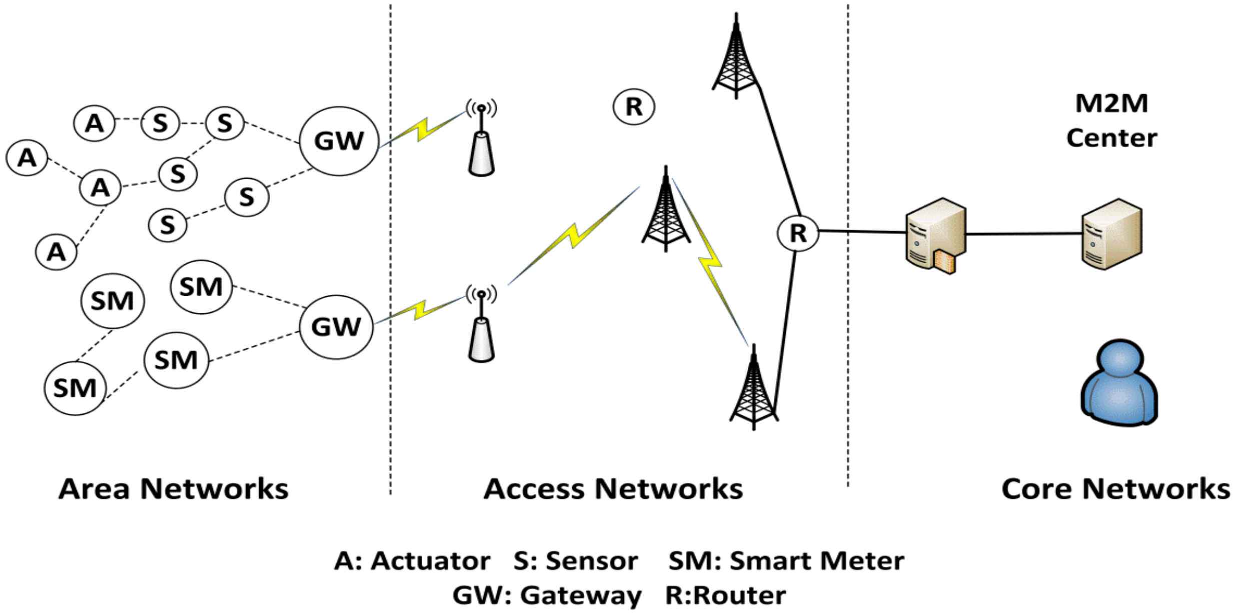


Fig 2-2 ETSI M2M communication architecture [39]

The 3GPP proposed an architecture aimed to increase the capacity of different types of services starting from basic sensing (e.g., temperature, humidity and speed) to multi-media (e.g., voice audio, video). One distinct feature of this architecture is that the 3GPP conceived the term Machine-Type Communication (MTC) suggested using cellular networks to support the MTC. In addition, Machine-to-Human (M2H) and Human-to-Machine (H2M) communication are also supported within this communication frame [40]. The principal cellular network adopted in the architecture is LTE, which is optimised by the 3GPP to support the MTC applications. The 3GPP architecture attempts to lower the operational costs in terms of energy consumption, extending the battery life of machine-type devices, improving the coverage of machine-type device groups and reducing the complexity of the signalling process [41].

IEEE launched the group-based approach to tackling M2M communications. Its main focus is on the IEEE 802.16 p amendment, which is used to support a large number of machine-type devices in a more efficient manner (e.g., low signalling overheads and low energy consumption). More precisely, it elaborates on device grouping so that the devices only communicate to other devices in the vicinity, and a concentrator elected from these devices wirelessly connects to a base station. Instead of making devices talk to the base station, this method ensures reliable connectivity and saves on the expensive signalling overheads [42, 43]. Three approaches are included in the grouping process. The first approach uses the same technique as the IEEE 802.16 m standard for all machine-types devices, relay stations and a base station. Instead of communicating to the base station directly, the machine-type devices communicate with a relay station that aggregates traffic first and then sends to the base station. In the second approach, a dual-mode relay station is used, which has two sets of transceivers. The dual-mode node uses the IEEE 802.16 standard to connect to the base station and uses the IEEE 802.11 standard or other short-range standards, to connect to the machine-type devices. This can save on transmission and processing power, boosts the channel efficiency and avoid interference. The third method uses one of the devices within a group to request radio resources and transmission power, and the other group members share the same radio spectrum and transmission power. The IEEE 802.16 m and IEEE 802.16 e standards also involved in the process, requesting the transmission power and radio resources from the base station. Despite the device grouping, signalling overhead is still high. Table 2-3 summarises and compares the features of the three standards.

Table 2-3 IEEE 802.16 grouping based solutions

Solutions	**IEEE 802.16 m**	**Dual radio required**	**Power consumption**	**Signalling overhead**	**Channel utilisation**
802.16m relay	Yes	No	Low	Low	Middle
Dual-mode group	No	Yes	Low	Low	High
802.16m/16e Grouping signalling	No	No	High	Middle	Low

2.1.4 Major IoT Applications

The IoT systems have the potential to apply for deployment in different application areas to facilitate information exchange. Current applications can be divided into three domains: the industrial domain, the smart city domain and the health domain, each of which can further be categorized into several groups, as shown in table 2-4. These applications have significant impacts on human lives, economies and societies. The remainder of this section describes the typical applications from the above three sectors.

Table 2-4 IoT application domains and applications

Domain	Major Applications
Smart City	Smart Mobility and Tourism: Road condition monitoring, smart parking Smart Grid: Load management, power generation and distribution. Smart Home: Lighting and energy management, access management
Industry	Logistics: Goods identification, product deterioration, warehouse management, inventory, smart payment Agriculture: Cattle monitoring, certification, irrigation control Industrial Processing: Vehicle Diagnostic, assistant driving, environmental monitoring.
Health Care	Medical Health Care: Remote monitoring, medical equipment tracking, entertainment tracking Independent Living: Elderly and disabled assistance, personal home mobile assistance.

Smart City Domain

In the context of the Smart City, the IoT can help cities to be more environmental-friendly and sustainable. More precisely, the main objective of the Smart City is to consume less energy, reduce carbon dioxide emissions and improve the quality of life.

Mobility

To support mobility on the road, vehicles equipped with radio transceivers that can dynamically receive information from other vehicles and road-side infrastructures to avoid traffic congestion and accidents. These modes of operations are referred as the so-called vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications [44]. Moving vehicles form an ad-hoc network, exchanging road information to maintain a safe distance between each other. Another application supporting mobility is the smart parking system, in which sensors guide the driver to car park according to different factors, such as personal preference and vacancies. Wrongly parked cars can also be detected by sensors. One example is that when the parking space reserved for disabled people is occupied by a regular car, the sensor can detect the inappropriate vehicle and trigger an alarm to inform tow trucks or parking rangers. An extension of this application is the smart payment system, where the driver, instead of using coins, uses the NFC and RFID technology to pay the fees [45].

Smart Building/Home

Buildings and homes are the places where people frequently visit and stay, so it is necessary to outfit IoT devices in both environments in order to optimise energy consumption and to improve the comfort of residents. Some of the building applications include security intrusion detection, video surveillance and building access management. All devices supporting these applications are connected to in-building IoT networks. Other applications, for example, facility maintenance, fault detection and entertainment systems aim to provide better services and improve the quality of life. Such a system allows residents of smart buildings to control their home appliances from remote places. For example, a resident can activate and turn the lights on before arriving home; the floor can be cleaned by cleaning robots and the kettle boils water. Such automation services could deliver services to people on time.

Industrial Domain

The IoT can benefit many industrial activities in achieving better performances. The RFID technology monitors and tracks products in logistics and supply chain management. By attaching RFID tags to products, it possible to accurately track them throughout the entire process as they are collected, transported and delivered [46]. In particular, the inventories of retailers and warehouses can be efficiently simplified and managed by using RFID [47]. In addition, easily perishable food such as fruits and vegetables can be monitored by real-time sensors and actuators that conduct the timely analysis and adjust the temperature and humidity to conserve and prolong the freshness of the food [1]. Another application is that smart shopping, in which the sensors can guide customers in the shopping centres and super markets and even recommend products to the customers as per their preferences.

Similarly, the IoT technologies can also be applied to agriculture. Animals such as cows, horses and chickens can be attached with sensors that continually monitor them in the event of losses or attacks by predators. The image sensors could identify abnormal behaviours of animals such that contagious diseases can be discovered immediately and the infected animals can then be isolated, preventing economic losses from happening [47]. In addition, sensors in farm areas will allow livestock to be automatically fed by adding food and water to a manger according to previous consumption and the needs of cattle. With the assistance of the IoT, farm management efficiency can be significantly enhanced, and food safety can also be ensured.

In the vehicle industry, IoT technologies can play a key role in remote vehicle diagnosis and maintenance. Sensors can measure parameters in the vehicle such as pressure, fuel, location, speed, etc [48]. These data will be stored inside the vehicle and then periodically transmitted to the remote centres. In a particular case, a mechanic can retrieve the data stored inside a vehicle so that the specific problem can be discovered, thereby providing tangible evidence for maintenance. The missing vehicle parts can be recovered by using the wireless networking technology. Another application is plant monitoring in freight where products are monitored by sensors. Any liquid and gas leak is detected and reported to the server systems such that alarms containing the composition of the liquids and gases can be triggered immediately. Therefore, the risky situations are quickly under control, and the safety of property and the rescue crew is guaranteed.

Health Care Domain

In the health care domain, the main applications are involved in sensing, monitoring, tracking and authentication. By using short-range standards such as ZigBee, Bluetooth, 6LoWPAN and WLAN, medical staff is expected to respond to emergencies in time when sensors attached on patients generate warnings. Similar in the industrial domain, a Body Area Network (BAN) formed by many sensors attached to patients allows nurses and doctors to remotely monitor the patients while they are not in the hospital. Parameters such as their heart rates, blood pressure, body temperature are remotely transmitted to the hospital so that whether the patient is healthy or not can be notified to doctors and nurses. Other beneficial applications include the storage of medical equipment that has smart labels attached. These labels effectively ensure the number of items and prevent them from going missing [49]. In addition, IoT sensors are useful in limiting access to only authorised personnel in the hospital in a seamless manner.

As for the personal health domain, the IoT has many benefits for human lives. Wearable sensors can monitor several physiological indicators from people who are walking, running and resting. Similar to the medical sensors, real-time data are collected by wearable devices that analyse and offer advice on how to keep a healthy life style. Senior citizens and disabled people can be constantly monitored by these sensors so that early symptoms and abnormal behaviours can be found. These sensors also engage them in the community, helping them to exchange ideas and opinions and enriching their lives [50].

With the growing popularity of smart devices, sensors with wireless communication functions generate many types of data such as location, orientation and speed. The software in the mobile devices reminds people of their current situations and provides advice for future activities. This is particularly useful in guiding people with impaired vision through road intersections. Indeed, well-being and health are the most important in a society. IoT-based applications have huge potential to improve the quality of life for people by gathering and analysing data from users' behaviours. For example, sensors can analyse walking distances and the amount of burnt calories, and make a detailed plan to inform exercisers. By using such applications, people become aware of the impacts they make on the environment, and, in turn, they will pay more attention to environmental protection.

2.2 M2M Communications

M2M communication architectures or platforms have been widely discussed in the literature. As depicted in Fig 2-2, the M2M communication architecture consists of area networks, access networks and a core network [3]. The area networks consists of many types of objects equipped with communication modules, such as wireless sensor networks, RFID, surveillance cameras and actuators are the focus of this study. All these devices are connected to the core network through access networks. Within the access networks, many gateways and routers relay messages from the area networks. To pass messages, the access networks adopt various communication technologies, such as Wireless Area Networks (WLAN), Long Term Evolution (LTE), Wideband Code Division Multiple Access (WCDMA) and the Ethernet. Due to the diversity of communication methods, the core network should be able to guarantee the reliability and QoS of the M2M traffic. Another reason for this guarantee is that although the traffic generated from one object or machine is small, the amount of traffic generated by a large number of devices is enormous, and thus it needs to be dealt with by the core network in a secure and sustainable manner. This huge amount of traffic comes from many types of applications running on heterogeneous hardware, and therefore, the traffic patterns are complex to handle. Given all these features, it is important that the M2M communication architecture be carefully designed and implemented.

2.2.1 M2M Communication Standards

M2M applications rely on networking standards and technologies to provide services. Given the complex nature of M2M communications, the available technologies can be divided into wired and wireless solutions. Wireless solutions can further be categorised into long-range and short-range solutions, as illustrated in Fig 2-3 Communication solutions for M2M networks are explicitly explained below.

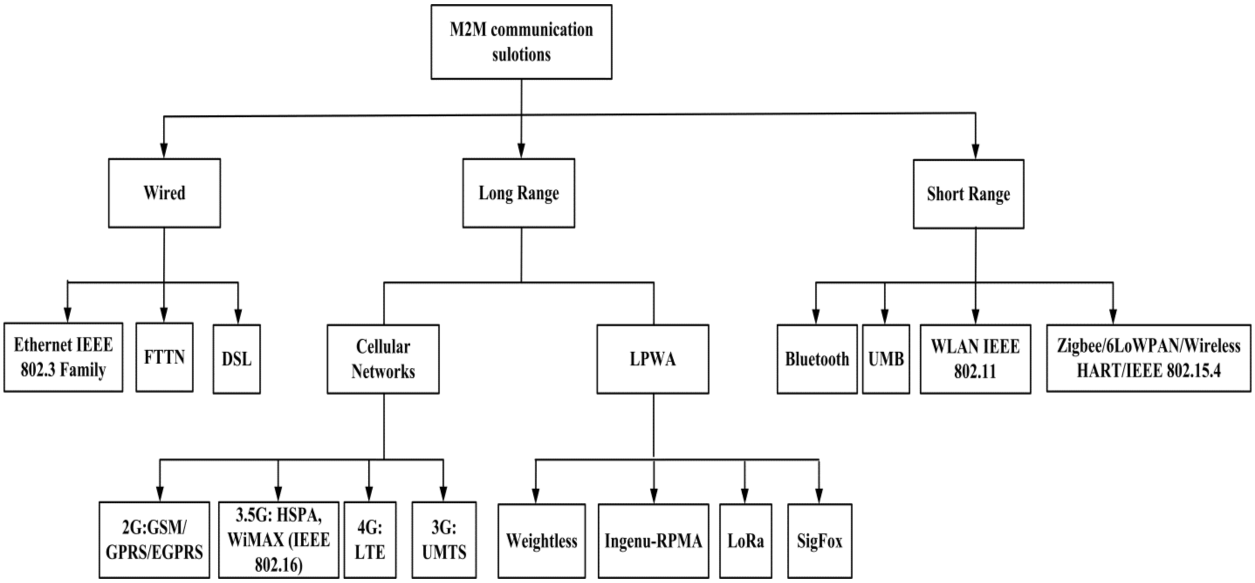


Fig 2-3 Communication solutions for M2M networks

Wired Network Solutions

In M2M communications, sensors, gateways, actuators and remote control centres are connected by dedicated cables such as the Digital Subscriber Line (DSL), Ethernet and the Fibre to The Neighbourhood (FTTN) to enable their transmissions. As such, wired solutions provide a low end-to-end delay, a high transmission rate and high security communications. It is difficult for a third party to access the information unless it is intercepted. Although wired networks have many advantages, they may not be suitable for M2M communications because they may not support thousands of M2M devices due to the interfacing issue, and new devices are always being added to the system. In particular, some of these devices are moving and placed in environments where it is difficult to deploy wired networks. For example, the Supervisory Control and Data Acquisition (SCADA) can be deployed to certain fields. In the context of M2M communications, the core network must be equipped with wired solutions to ensure the reliability, capacity and security of M2M communications. It is expected that wireless solutions will be more suitable for access and area networks considering the unique traffic characteristics of M2M communications.

Long-Range Solutions

The long-range solutions can be grouped into two groups: cellular networks and LPWANs as shown in Fig 2-3. Cellular networks refer to the 2G, 3G and 4G communication systems, which have been widely employed in the industry. Many standard organisations such as the ETSI and the 3GPP recommend that cellular networks should be adopted as one of the major networks for M2M communications. The cellular networks have many advantages. Firstly, cellular networks have a wide coverage of M2M devices, especially those devices deployed in areas inaccessible to humans. Secondly, cellular networks support roaming when M2M devices move from one place to another and the connectivity can still be maintained. For example, drones are used to monitor bush fires in rural areas, and need to communicate with a remote control centre while in flight. This is a typical case for M2M mobile applications. Thirdly, cellular networks can be easily deployed compared to wired networks. Wireless services can be accessed by installing a base station in the area. Most cellular networks use dedicated spectrums, so the communication efficiency can be improved. Another reason for the high efficiency of cellular networks is attributed to spectrum reuse, such that the same type of cellular network can cover a larger area. In the meter reading scenario, for example, remote areas and urban areas have different meter densities, so the network planner estimates the coverage as per the cell radius and capacity. The most prevalent long-range network solutions are summarised in Table 2-2.

Cellular networks have several disadvantages when used as an IoT network due to its original design to support symmetric traffic and support more capacity on the downlink. Besides, most of M2M devices use a lower duty cycle and stay in the sleep state to conserve energy, while cellular networks are required to exchange signalling information between M2M devices and the base station. This incurs additional delays as M2M devices switch from the sleep mode to active mode and reduce energy efficiency. In future, cellular networks are expected to be deployed as the access network connecting the gateway and the core network, whereas the short-range solutions are expected to be deployed in the area network.

To cope with the disadvantages of the long-range standard, 3GPP has developed a few new standards and solutions, such as Narrow-Band IoT, LTE Enhancement for Machine Type Communications (eMTC) and Extended Coverage GSM (EC-GSM) to cater for M2M applications, cutting the cost and complexity and prolonging the battery life [51]. The rationale behind these standards is to reuse the current infrastructure and the licensed spectrum. To be compliant with the LTE system requirements, the eMTC standard lowers the data rate from Category 1 to 0 and then to M. Half duplex operation is used in Category 0 to reduce costs, and bandwidth is reduced from 20MHz to 1.4 MHz in Category M. EC-GSM was released in 2016 and can support up to 50k devices with enhanced security and privacy. Signal process technologies and repetitive transmissions are used to improve the capacity and coverage of legacy GPRS. The NB-IoT standard was also released in 2016 and adopts a narrow-band technology to achieve low costs, a long coverage and low energy consumption. A software upgrade of the current LTE system can support NB-IoT.

LPWAN technologies have gained popularity recently. Several new LPWAN standards have emerged, such as LoRa, SigFox, Ingenu-Random Phase Multiple Access (RPMA) and Weightless Special Interest Group (SIG). LoRa is a low-power, low cost and long-range physical layer standard designed for IoT applications [52]. It uses a special chirp spread spectrum (CSS) technique as the modulation scheme and spreads the narrow band signal over a wide bandwidth to make the signal more resilient to noise and interruptions. LoRa also uses the frequency hopping technique to access available channels and mitigate interference. The data rate ranges from 300 bps to 37.5 kbps depending on the channel bandwidth and spreading factor (between 7 and 12). The transmission range supported by the standard is up to 15km with no clear line of sight communication. The LoRa Wide Area Network (LoRaWAN) is based on the LoRa standard and defines the upper layer of the LoRa standard. The MAC layer adopts the pure ALOHA protocol to avoid packet collisions on the same channel and only supports the star topology in which a LoRa device directly communicates to a gateway.

The SigFox standard uses the ultra-narrow band to achieve end-to-end connectivity with patented technologies [53]. The base stations use the cognitive software-defined transceivers to connect to the remote servers in IP-based network. The modulation scheme used in the physical layer is Binary Phase Shift Keying (BPSK) with a transmission band of 100Hz, which is an ultra-narrow band of the SUB-GHz ISM band. This makes the SigFox network less susceptible to interference and has high receiver sensitivity and lower energy consumption. However, the maximum throughput of the SigFox is only 100 bps. SigFox also supports bidirectional communications with the downlink communication ahead of the uplink communication. The number of the uplink messages is limited to 140 12-byte messages per day, while that of the downlink messages is only 4-8 byte messages per day. Since ACK packets are not used, Sigfox needs to retransmit the packets three times to ensure reliability.

Unlike SigFox, Ingenu RPMA uses the 2.4 GHz ISM channel and can achieve higher throughput because the maximum throughput is not regulated by in the U.S. and Europe [54, 55]. The Ingenu RPMA physical layer adopts the RPMA technology that allows several transmitters to share a single time slot. In fact, the RPMA technology is a variation of the Code Division Multiple Access (CDMA) technology. RPMA firstly increases the duration of a CDMA time slot, then adds a random offset delay to each transmitter and allows each transmitter to access the channel. This reduces the signal collisions and increases the SNR on each link. Two-way communications is supported, especially on the downlink where the base stations spread the signal to each end device and is broadcast by using CDMA. Ingenu RPMA can achieve -142 dBm as receiver sensitivity with a link budget of 168 dB, which is compatible with the IEEE 802.15.4 k standard.

The Weightless SIG has introduced three new standards: Weightless-W, Weightless-N and Weightless-P, which employ the licensed and license-free channels such as the cognitive radio and TV white space to access the channel as the secondary users and not to cause interference for the primary users [56]. Weightless-N is a UNB standard that uses the TV white space (470 to790 MHz) to support one-way communication. Weightless-W uses different modulation schemes such as 16-Quadrature Amplitude Modulation (16-QAM) and Differential-BPSK to support a data rate up to 10 Mbps. The end devices use this technology to transmit in a narrow band to the base stations. Weightless-P uses Gaussian Minimum Shift Keying (GMSK) and Quadrature Phase Shift Keying (QPSK) as modulation schemes that can achieve a data rate up to 100 kbps. However, this standard only supports unidirectional traffic.

Short-Range Solutions

The majority of M2M devices need to be energy-efficient and use low duty cycle, so they are suitable for the M2M area networks compared to the long-range networks. In other words, M2M devices are normally battery-powered and can operate for months or years without human intervention. They generally use the ISM license-free radio spectrum to form networks, which in turn decreases the deployment costs. Since a massive number of M2M sensors and actuators are deployed in many different operating environments, the licensed spectrum is not an ideal choice for the connection of area networks due to its high cost. Most of the short-range networks are based on the open standards that generally reduce the cost of system development, so the system design becomes relatively easy. The most popular short-range network solutions are explained as follows.

IEEE 802.15.4-based short-range network technologies have gained much attention in M2M communications [57]. With the IEEE 802.15.4 standard, many standard bodies and industrial alliances, such as the IETF and the ZigBee Alliance have proposed 6LoWPAN and ZigBee. These two standards define the Network and Application layer of the IEEE 802.15.4 stack, whereas the IEEE 802.15.4 standard specifies the Physical and Media Access Control (MAC) layer. The physical layer uses the ISM spectrums that include 868 MHz, 915 MHz and 2.4 GHz bands, and their corresponding data rates are 20 kbps, 40 kbps and 250 kbps. In particular, the 2.4 GHz band is widely used, while 868 MHz is used in Europe and 915 MHz is used in the US and Australia. ZigBee and 6LoWPAN based short-range networks have been extensively adopted in smart metering in the energy sector. The US has launched several projects and deployed smart meters in several cities.

IEEE 802.11 based Wireless Local Area Network (WLAN) is another standard, which can be used to connect M2M devices in the area networks. The WLAN is a protocol suite consisting of the IEEE 802.11 a, b, g, n, e and ac standards. A WLAN enables fast network access for users when forming either the infrastructure or the ad-hoc mode. Either of these two structures can support mobile and stationary applications. In addition, the WLAN offers reliable end-to-end connectivity, including authentication and encryption for industrial and residential applications. Due to the above two points, WLANs have been deployed in a variety of environments.

2.2.2 Smart Grid Communications

The Smart Grid is regarded as the next generation electricity grid, enabling the integration of energy storage, distributed and centralised generation, smart meters, and other relevant services and applications [32]. Customers will be offered more choices and incentives to change their consumption patterns and to overcome the disadvantages of the legacy power system. In addition, the Smart Grid intelligently delivers electricity to residential premises according to the needs; that is, when and where the power must be offered by utilities. The Smart Grid must be resilient to disturbances, such as overload, natural disasters and deliberate attack, must predict unexpected interruptions and can self-heal when disasters occur. All of these features are aimed at providing high security and the reliability of power supply.

To achieve the characteristics of a Smart Grid, communication technologies play an important role in realising the intelligent management of the power system. According to the IEEE 2030 standard [58] and the National Institute of Standards and Technology (NIST) [59], Smart Grid communication infrastructures can be divided into three classes: Home Area Networks (HANs); Neighbourhood Area Networks (NANs)/Field Area Networks (FANs); and Wide Area Networks (WANs), as shown in Fig 2-4. The WANs can spread up to over 100 kilometres to connect substations, microgrids and utilities. The NANs and FANs serve as the last-mile connection and join which can connect a large number of HANs, where all electric appliances are wirelessly connected to the smart meters that transmit all the information back to the utility servers via the NANs and FANs.

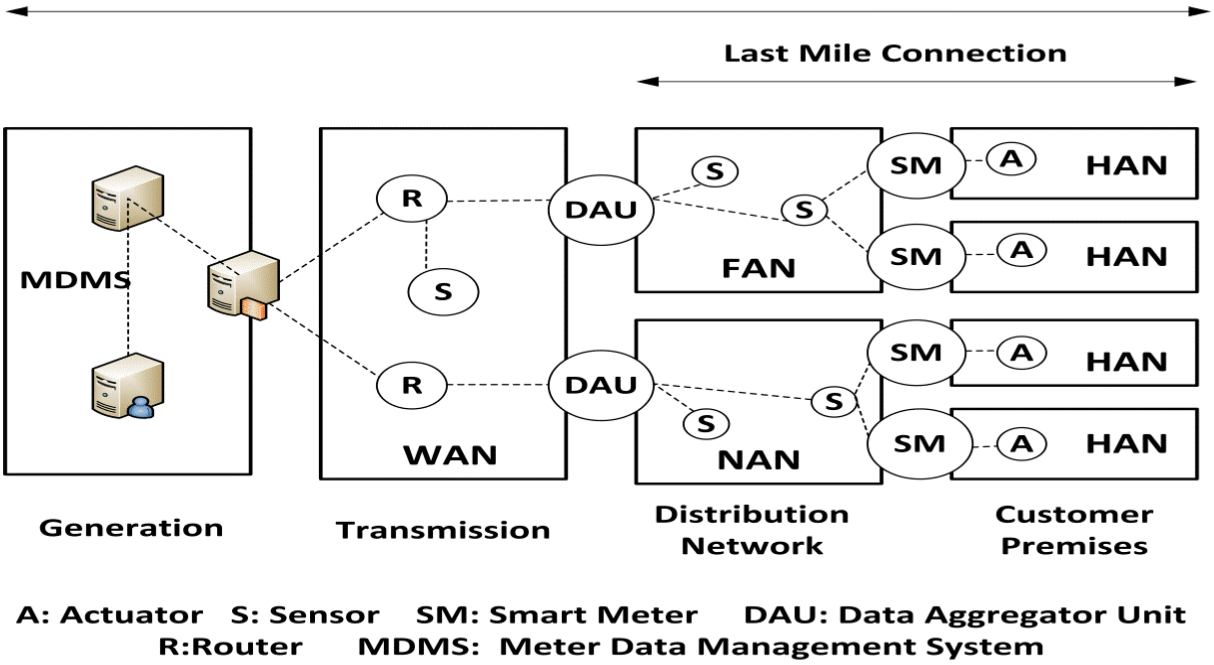


Fig 2-4 Smart Grid communication architecture

2.2.3 Traffic Characteristics of M2M Communication Services

M2M communications support applications that have different traffic characteristics compared to the conventional communication services. This section discusses the traffic characteristics of M2M communications. M2M communication requirements are quite complex, so the network heterogeneity and scalability must be considered. A reasonable approach is to analyse from different aspects. Energy consumption is a major issue due to distributed nature of the system where replacement of energy sources is very difficult, so energy-efficient approaches are needed to reduce the operational costs. M2M devices need to be self-reliant to achieve high level autonomy to adapt to different situations and respond to events. M2M applications have different characteristics and QoS requirements in terms of packet delivery ratios, end-to-end delays and packet burst sizes. For example, the requirements of environment monitoring and smart metering are quite different. Generally, environment monitoring applications have no strict delay requirements, whereas lower delay bound is extremely important for the smart grid.

Apart from the above issues, the privacy and security of M2M communication data is important to maintain data integrity [40, 60]. The security issues include remote cyber-attacks (such as

Denial of Service attack), failing to install security patches and eavesdropping, etc. The heterogeneity of the M2M devices interconnected with each other makes the security problems more complex than a homogeneous network, so the security requirements such as trust, confidentiality, authorization and authentication must be carefully considered in M2M networks.

In the three phases of the IoT network, the heterogeneous communication technologies can be used for local networks to connect with other underlying networks. It is noted that the interoperability among communication technologies is also important. Appropriate naming and addressing facilitate the interoperability feature. In a M2M network, a large number of devices access a gateway or a relay device, a priority scheme must be considered to differentiate services and applications as per their traffic requirements. For example, as one application is being served, another type of application traffic with a higher priority can preempt to get served. Also, some devices may be mobile, supporting seamless roaming is important in special scenarios. These devices operate in an on-and-off fashion to save on energy, so they must be supported by M2M communications to reduce the total energy consumption. Table 2-5 summarises and highlights some features of the M2M communications.

Table 2-5 M2M communication characteristics and application mapping

Characteristics	**Critical Aspect**	**Application**
Heterogeneous Network	Different networks such as wired wireless and cellular. Different access modes	Smart home, smart metering
Massive Device Transmissions	Concurrently access the same channel or a gateway	Surveillance and Security
High Reliability	Different network solutions have seamless connectivity towards devices	Demand response, health care, smart payment
Low power consumption	Energy efficient methods to reduce consumption	Environmental monitoring such as in a forest or in a building
Mobility	Mobility and roaming are supported	Smart parking
Addressing	Device identification, unicast, board cast and multicast.	Smart Grid, smart metering
Traffic Profile	Manage different traffic features such as continuous transmission, burst transmission, two-way communications	Smart home in which many devices have different traffic profiles.
Access priority	Differentiate the traffic type and allows urgent applications to transmit first	Surveillance and Security
Routing	Best route according to different needs	Smart Grid

2.3 Short-Range M2M Communications

In this section, the homogeneous and heterogeneous wireless solutions are analysed in order to study how the networking solutions can assist in achieving ubiquitous accessibility. Short-range networking solutions are preferable to connect a large number of M2M devices and provide seamless connectivity to them. Long-range solutions, in contrast, can handle aggregated traffic and support M2M device roaming. Short-range networks are suitable for access networks where a large number of low power and duty cycle devices are distributed over a large area. Due to the varying nature and requirements of the distributed devices, it may be necessary to design different access networks including homogeneous and heterogeneous networking techniques

2.3.1 Homogeneous Wireless Area Networks

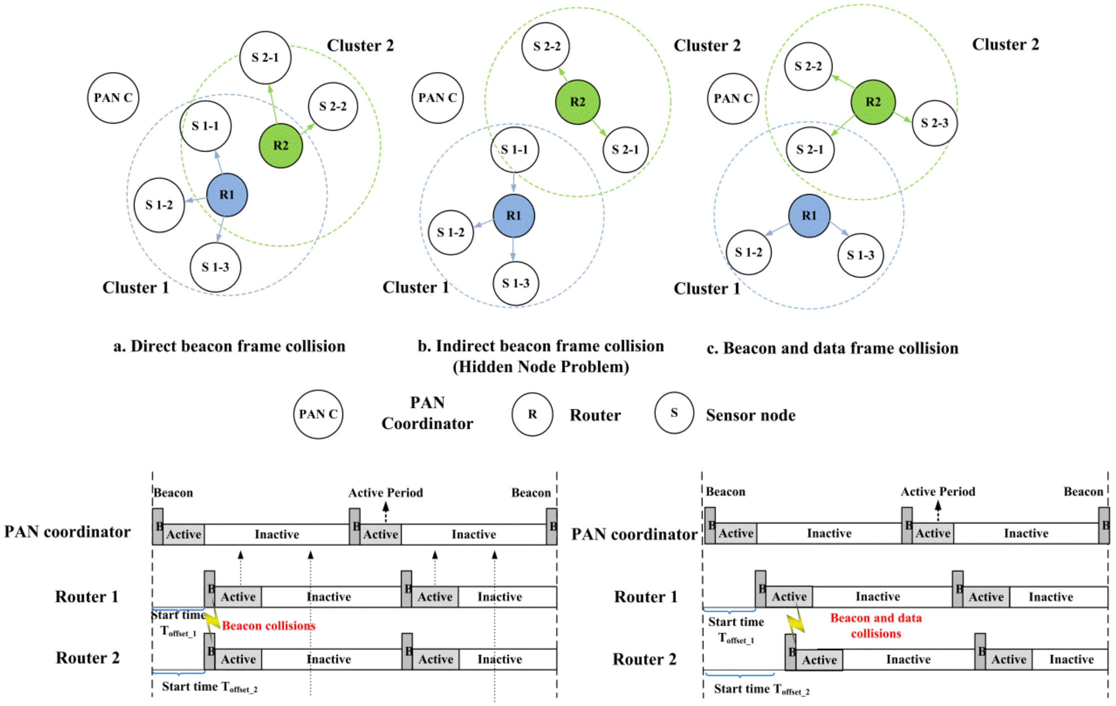
In general, a Smart City or Smart Grid scenario as shown in Fig 3-10 often covers a large geographical area [61]. An area network provides connectivity to M2M/IoT devices in the above application environment. If the area network coverage is large, a multi-hop sensor network can be used to relay data from distributed devices to a data sink located in a different segment of the network. As an example, one possible application of the area networks is the Advanced Metering Infrastructure (AMI) data communications where the bidirectional traffic is used to support smart meter readings, software updates and a data management function where information between the meters and utilities needs to be exchanged [62]. In such case, a multi-hop network plays an important role in supporting data flows within the Smart City and Smart Grid networks. The 6LoWPAN standard implements the layers above the data link layer, whereas the IEEE 802.15.4 standard defines the Physical and the Data Link layer. As shown in Fig 3-6, this standard supports three network topologies: star, cluster tree and mesh. In particular, there are nodes named the cluster head or router synchronised by the PAN coordinator using beacons in the cluster-tree topology, and then routers also can send beacons to their child nodes as a control signal.

One potential problem of a cluster-tree homogeneous wireless area network is that the network suffers from intra-cluster collisions including data packet collisions, beacon collisions and beacon-to-data collisions. The last two types of packet collisions can degrade the network performance with the beacon collisions being the worst case. More precisely, beacons could collide with one another or data packets sent from other nodes when they are not properly synchronized as shown in Fig 2-5. It is known that the network coordinator and routers may have overlapping transmission periods in which beacons collide. The two types of collisions can greatly impact on the system performance, thus adversely affecting the QoS of the M2M applications. If the nodes cannot receive beacon frames from their parents, they are disconnected from their own cluster heads without being able to receive any control information [63].

The IEEE 802.15.4-based WPANs may also be subject to other unreliability problems, such as scalability, QoS guarantee, energy efficiency and timeliness due to the lack of synchronisation [64]. These issues are attributed to the contention-based MAC protocol used for channel access. It was found that the network performance can be improved with appropriate parameter settings, but stringent timing requirements (e.g., meter reading on-demand requires an end-to-end delay of less than 15s) may not be met using the parameter setting method [65]. Collisions between the beacon frames have detrimental effects, particularly due to packet losses and retransmissions; hence it is necessary to solve the beacon collision problem in a dense network environment. The beacon collisions can be grouped into direct beacon collisions and indirect beacon collisions. The direct and indirect collisions are differentiated by the status of the routers.

Figure 2-5 a illustrates the direct beacon collisions where the cluster heads R1 and R2 can hear each other. It can be seen that routers R1 and R2 transmission ranges (as indicated by the dotted blue and green circles) overlap. Fig 2-5 b shows the indirect beacon collisions, where R1 and R2 cannot detect each other’s transmissions (the classical hidden node problem). It can also be seen that the blue dotted line does not cover R2, while the green dotted line does not cover R1. The reason is that no channel assessment is performed before beacon transmissions. As the transmission ranges of routers R1 and R2 overlap, the beacons can collide, so the associated sensor nodes lose track of the beacons and cannot send data packets. The direct beacon collisions tend to happen in a single WPAN, in which just one coordinator controls all of the routers, whereas indirect collisions may occur between different WPANs in which multiple PAN coordinators exist. The third type of beacon collisions under study is the collisions between the beacons and the data frames, as shown in Fig 2-5 c. For example, when R2’s direct sensor node 1 sends a packet colliding with a beacon frame coming from router R1, such collisions occur since

R2’s active period overlaps with R1’s active period. If this type of collisions occurs often, the synchronisation between sensor nodes 2 and 3, and router R1 will be lost, thus resulting in a more severe impact on the sensor nodes than the beacon collisions only.


a. Direct beacon frame collision

b. Indirect beacon frame collision (Hidden Node Problem)

c. Beacon and data frame collision

Fig 2-5 Three types of beacon collisions

The 2006 version of the IEEE 802.15.4 standard proposed a superframe-scheduling scheme that allows the superframe of the router to be scheduled with the other routers to avoid beacon collisions [66]. Specifically, the standard suggests that the timing of sending a beacon frame should be designed so that the routers must schedule their beacon transmissions in neighboring clusters’ sleeping periods to avoid collisions. In other words, routers receive superframes from their parents and use the sleeping periods of the superframes to send their own superframes to control child nodes. As can be seen in Fig 2-5, router 1 and 2 receive beacons from the PAN coordinator and need to transmit their own beacons to control the sensor nodes. However, the standard does not give any suggestions on how routers having the same parent (e.g., R1 and R2 are governed by the PAN coordinator) can mutually avoid the two types of beacon collisions.

Many studies proposed several methods to avoid beacon collisions. A multi-channel superframe scheduling approach was introduced in [67, 68], in which two channels are used on the routers (one set of transceivers with two channels), as shown in Fig 2-6. Specifically, when the adjacent routers are either parent or child, a parent or a child node cannot schedule their beacons simultaneously. Instead, nodes that are two hops apart can schedule their beacons using different channels simultaneously. For example, initially in the time slot $T_{1,}$ the PAN coordinator, R2, R4 and R6 transmit their own beacons using channel A, and meanwhile, R3 and R5 switch to channel A to receive the beacons from the PAN coordinator. In the next time slot T_2, R3 and R5 use channel B to schedule their beacons, and at the same time, R2, R6 and R4 switch to channel B to receive the beacons sent from their parents R3 and R5.

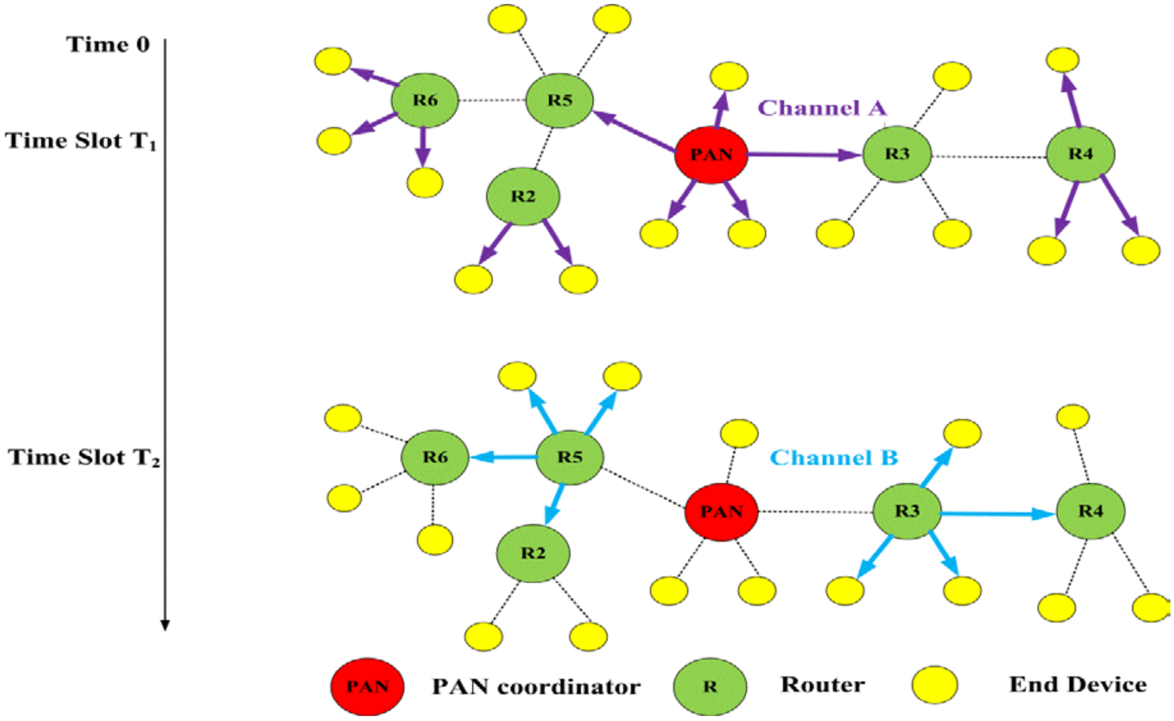


Fig 2-6 An example of how a multichannel WSN approach works [67]

Considering the beacon collisions caused by the limited number of available channels and a large number of nodes, a clean channel discovery mechanism called the multi-dimensional scheduling (MDS) algorithm was proposed by making the routers scan a free channel in the inactive period of the superframe [69]. The beacon collision avoidance algorithm is based on the idea that if the router senses beacon collisions, it reports itself to the PAN coordinator that can scan the available clean channels during the inactive period. As collisions occur, the PAN coordinator transmits a re-alignment command packet using the CSMA/CA mechanism, notifying the end device of a free channel. Upon receiving the control packet, the end device, which has been isolated from the PAN coordinator, begins the recovery procedure and switches to a new channel. Meanwhile, the PAN coordinator also switches to the same channel on which beacons can be retransmitted without collisions. However, the simulation results showed that it takes more time for an end device to recover from beacon collisions and consumes a significant amount of energy to support the signalling procedure. This approach is suitable to support multiple independent WPANs using different transmission channels. However, the proposed algorithm may not be suitable for a single WPAN covering a large-scale area with a number of clusters frequently switching channels because it might take a longer time to signal all the devices.

A mode-switching scheme operating between a beacon-enabled and a non-beacon-enabled cluster tree was proposed to ensure a low delay and a high packet delivery rate [70]. It was found that the cluster-tree topology tends to have a high end-to-end delay and a low packet delivery ratio, so it cannot provide a satisfactory QoS for specific delay-sensitive and high priority applications. In contrast, the non-beacon mode mesh topology transmit packets with stringent delay requirements, so this feature can be used to shorten the end-to-end delay required by applications such as real-time monitoring. Initially, the wireless sensor network used in this study was formed into a cluster-tree where the beacons were sent from the PAN coordinator to synchronise the whole network. Once an emerging event is detected by the sensor node, a de-construct request command (DRC) is initiated and transmitted to the PAN coordinator, which is called the upstream report of the deconstruction request command. Upon receiving the request, the PAN coordinator uses beacon frames to inform the sensor nodes to de-construct the cluster-tree topology. After the beacons have spread through the whole network, each router picks up the de-construction information to change the structure from the cluster-tree to the mesh topology. With the mesh topology, time-sensitive packets can be relayed with the aid of the mesh routing algorithm. The PAN coordinator monitors the traffic volume of the emerging events. Once the emerging events are finished, the PAN coordinator starts the cluster-tree reconstruction process by sending normal beacons in which a flag is used to inform the network nodes. The simulation results in this work have shown that this mode-switching scheme can maintain a relatively low mean end-to-end delays and high goodput when transmitting time-sensitive packets. However, the signalling packets could be lost due to interference or packet collisions between the end devices and the PAN coordinator. In case of signalling packet losses, these packets need to be retransmitted, leading to a longer end-to-end delay. Another limitation is that the transformation of the deconstruction and construction processes may not be completed due to losses of the signalling packets, so some of the end devices might be isolated and cannot perform the mesh routing.

Changing the timing of the beacon transmissions could be another solution to reduce the number of beacon collisions. This approach uses a time window denoted as the Beacon-Only period that is reserved at the start of a superframe and dedicated for beacon transmissions [71]. Specifically, a contention-free time offset is chosen by each router so that the beacons do not collide with neighbouring beacons as shown in Fig 2-7. After the beacon transmissions, the active periods of different clusters can start at the same time so that the direct communication between different clusters is enabled. This is particularly useful in establishing a mesh network where the routers can send data packets to any neighbouring node, so two types of collisions including beacon-to-beacon and beacon-to-data frames are avoided. However, the superframe structure is completely different from the standard one defined by the IEEE 802.15.4 standard, so the modification of the superframe structure must be made. The direct communication due to the share of the active period could cause more collisions between data and GTS packets in each WPAN, and it is difficult to calculate the duration of the beacon-only period for a given WPAN since the parent-child relationship between the PAN coordinator and the routers takes time to settle.

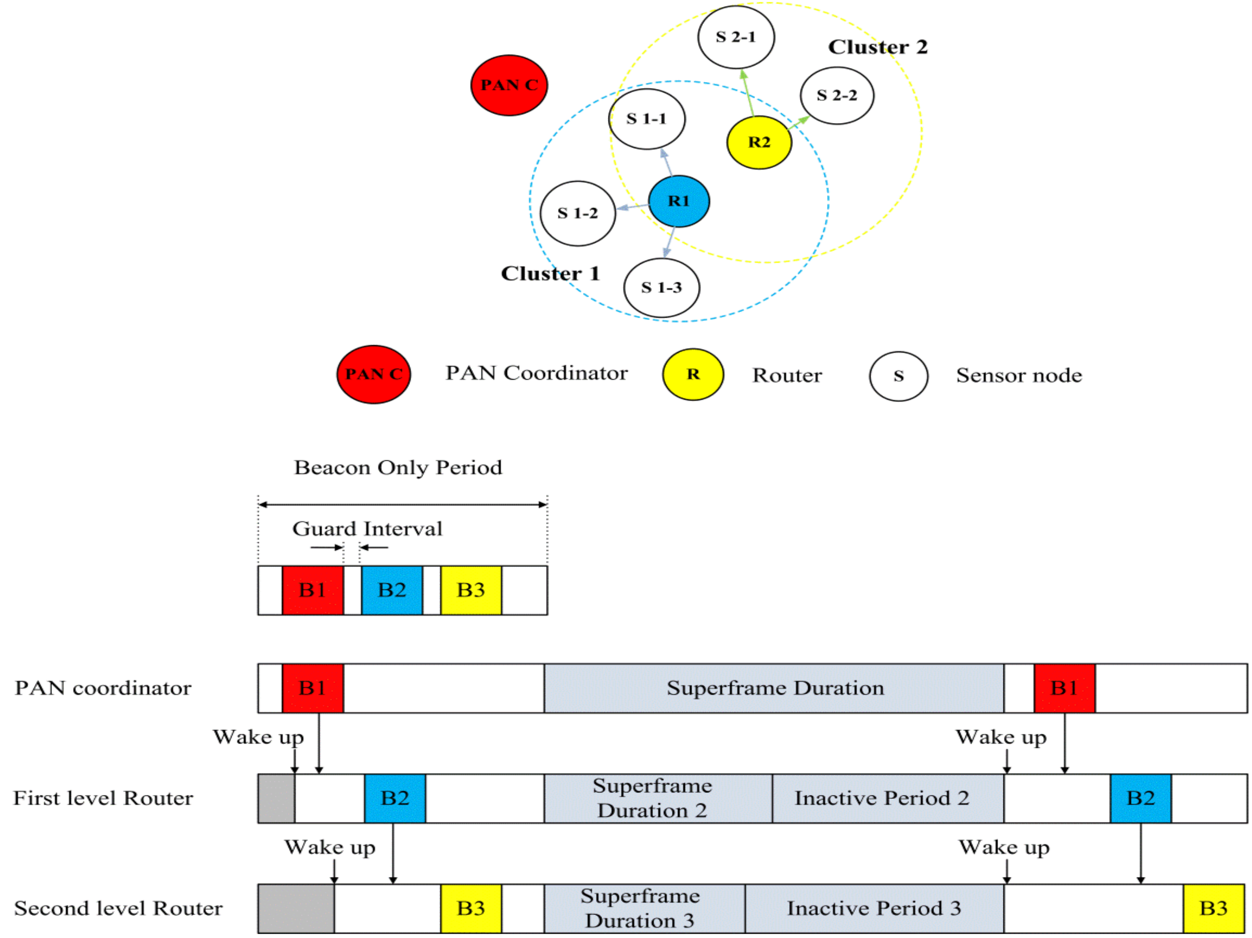


Fig 2-7 The beacon-only period approach [71]

2.3.2 Heterogeneous Wireless Area Networks

Using homogeneous wireless area networks in M2M communications is not realistic due to the intrinsic shortcomings including the high end-to-end delay and low packet delivery ratio. This is because an M2M communication platform consists of different components, such as sensor nodes, actuators, machines, etc. To interconnect all of these components and provide seamless connectivity, a homogeneous wireless area network may not offer sufficient capacity in a cost-effective manner, so multiple wireless networking standards can be used to form a heterogeneous area network to provide a reliable M2M communication networking paradigm. However, the heterogeneous area network with a large number of devices forming a dense M2M and IoT communication network using an unlicensed band could cause in-band interference. This interference is in fact the inter-network collisions that are the packet collisions between two different types of wireless networks sharing the same spectrum.

The IEEE 802.15.4 standard provides three features suitable for M2M communications methods: (1) dynamically selecting a clean channel, (2) use of a lower duty cycle and (2) transmitting packets with low transmission power. In addition, according to the recent literature, research on inter-network collisions, especially the ones between the IEEE 802.15.4 and IEEE 802.11-based networks are divided into three categories as shown in Fig 2-8: (1) inter-network collision analysis, (2) adaptive collision mitigation techniques and (3) non-adaptive mitigation techniques. These categories can be further divided into several other sub-classes.

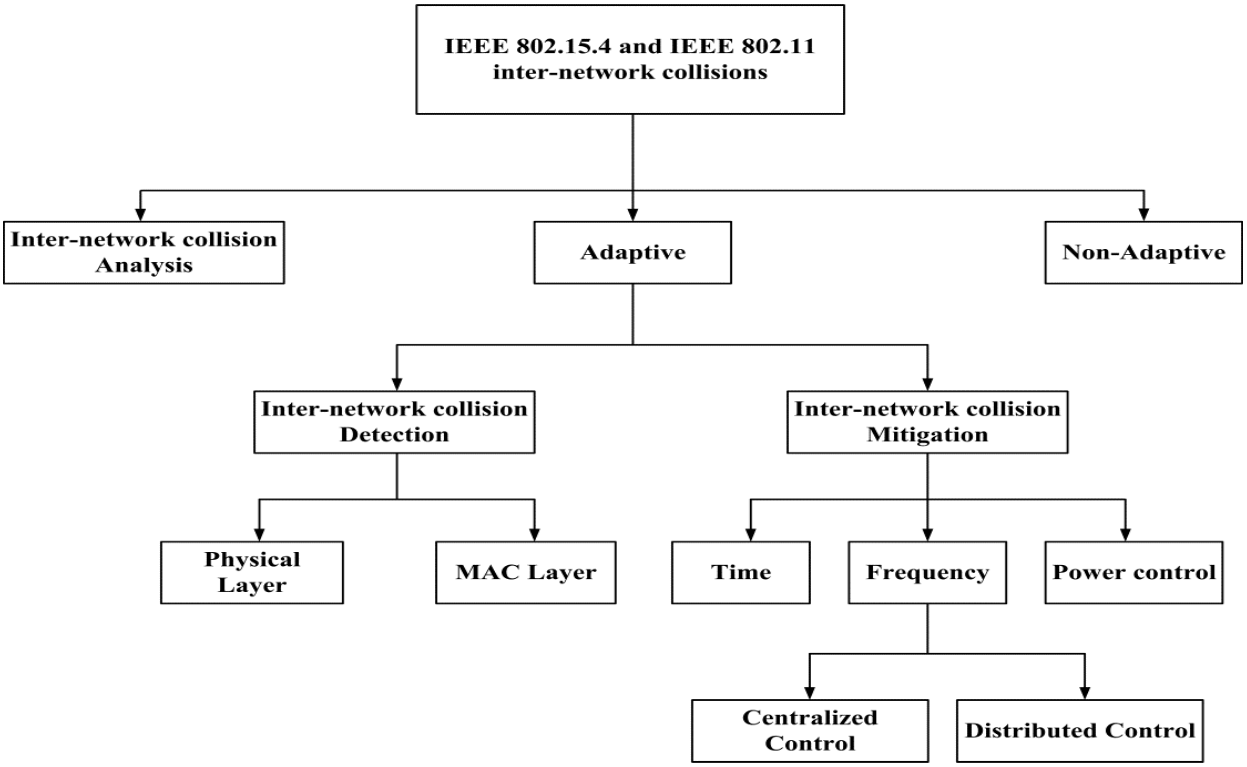

IEEE 802.15.4 and IEEE 802.11 inter-network collisions
Inter-network collision Analysis
Adaptive
Non-Adaptive
Inter-network collision Detection
Inter-network collision Mitigation
Physical Layer
MAC Layer
Time
Frequency
Power control
Centralized Control
Distributed Control

Fig 2-8 Taxonomy of Inter-network collisions mitigation approach

Inter-Network Collision Analysis

The first category is the analysis of inter-network collisions. A number of research works have investigated the effects of inter-network collisions and analysed the effects of collisions on all component networks. The main purpose of the inter-network collision analysis is to study how this type of collisions occurs and their effects on the other networks. Leopoldo Angrisani et al.

[72] performed testbed experiments involving a pair of Wireless Sensor Network (WSN) nodes and a pair of WLAN stations to find out how the inter-network collisions affected each other. The authors performed testbed experiments involving a pair of Wireless Sensor Network nodes and a pair of WLAN stations to find out how the inter-network collisions affected each other. In particular, when the WLAN node was the victim, the packet loss rate of the WLAN node did not decrease in the presence of the IEEE 802.15.4 (WPAN) devices. On the contrary, when the WPAN node was the victim, the WLAN stations exerted a detrimental impact on the WPAN nodes. An example of the adverse effects can be seen at the beginning of the WLAN operation, where the WPAN packet loss rate increased up to 70%. The work is an important one which is used as a reference model to propose the network resource allocation techniques in this work. Axel Sikora et al.[73] conducted a similar experiment to show how WLANs, Bluetooth devices and microwave ovens impact on the WPANs. Since the above networks use the same 2.4 GHz ISM transmission band, the WLAN devices with higher transmission power can adversely affect the WPANs, causing significant packet losses. In contrast, the impact of Bluetooth devices and microwave ovens on the WPANs was not as significant as the WLANs. In this case, the average observed packet error rate in the WPANs was around 10%. Since the IEEE 802.15.4 channels 25 and 26 are not interfered with by the channels frequently used by the WLAN channels, it was suggested that these interference free channels must be used to avoid the inter-network collisions.

Research work conducted by Mohamed Rihan et al. [74] studied the above issues. The work found that the blind coexistence of ZigBee, Bluetooth and WLAN nodes can degrade the performance of the ZigBee nodes. To study the effects of the WLAN inter-network collisions, several metrics such as the packet error rate, the Receive Signal Strength Indicator (RSSI) and the Link Quality Indicator (LQI) were used to study the WLAN’s adverse impacts on the IEEE 802.15.4 devices. Another work presented by Jo Woon Chong et al. [75] was to analyse the adverse impacts on ZigBee devices using a real testbed and an analytical model. The saturated ZigBee throughput was derived using the theoretical model to compare with the simulation results, confirming that the ZigBee network throughput reduces when interfered with by WLANs.

Adaptive Mitigation Techniques

The second category is the adaptive mitigation technique comprised of two stages: the collision detection stage and the collision mitigation stage. More precisely, the inter-network collisions can be detected from the physical layer using indicators such as the RSSI and the packet error rate. After that, at the second stage, various adaptive methods including time scheduling, frequency selection or redistribution, and transmission power control are used to mitigate the inter-network collisions. Yong Tang et al. [8] proposed an interference-aware adaptive clear channel assessment (IAACCA) technique to reduce the ZigBee packet loss rate. In this approach, as the WLAN transmissions interfered with the ZigBee transmissions, a ZigBee node constantly monitors the channel to determine the length of an idle period that is long enough to successfully transmit a ZigBee packet without WLAN interference. If the length of the idle period is not long enough to transmit a ZigBee packet, the ZigBee packet size is correspondingly reduced to adapt to that short idle period. In the worst case scenario, if the current channel is busy and the ZigBee nodes cannot send a ZigBee packet, they switch to a free or less-affected channel to continue operation. A similar method was proposed in [76] that used the ZigBee inactive period to transmit the WLAN packets. The system used the WLAN PCF period to transmit the ZigBee packets. To detect inter-network collisions, the packet error rate is used as a metric to determine when the ZigBee nodes switch to a free channel.

The authors of [76] proposed another method to mitigate the inter-network collisions in [77]. The work used a dual-radio node equipped with the WLAN and the ZigBee radios to serve as a mediator; that is, the ZigBee part of the dual-radio node only communicates with the ZigBee node and the WLAN part of the dual-radio node only talks to the WLAN nodes. To measure the inter-network collisions, the ACK packets between the PAN coordinator and the ZigBee devices are monitored by the dual-radio node. As the number of the ACK packets received by the PAN coordinator decreased, the measurements indicated that the ACK packets go missing due to inter-network collisions. The dual-radio node activates the collision mitigation procedure when the channel is found to be busy. In this process, the WLAN part of dual-radio node uses a virtual sensing technique to schedule the WLAN packet transmissions, so the ZigBee devices are not affected by the inter-network collisions. The difference between the dual-radio node in this study and the dual-radio node proposed in this study lies within the fact that the latter has data flows between two networks, whereas the former does not. Essentially, the system in their work had two separate networks, while the system in the thesis had one heterogeneous network.

Zhipeng Wang et al. [78] studied the reason for the lost ACK packets in the inter-network collision detection stage. The work found that ACK packets are affected due to inter-network collisions immediately after a data packet is successfully received. To solve this problem, the ZigBee coordinator measures N successive RSSI values for 16μs. If the mean of the N values is below the energy detection threshold P_{th} , then the ACK packet is sent to avoid inter-network collisions. As the ACK packet is only 11 bytes long, the successful delivery rate is high once a channel is found to be idle due to the short transmission time.

Aside from the lost ACK packet measures, Narjes Torabi et al.[79] found that the beacons can be corrupted due to inter-network collisions. Beacons can be corrupted when interfered with by inter-network collisions due to WLAN packet transmissions. Once the channel is detected to be busy, the collision mitigation procedure is triggered. As the Zigbee channel 25 as shown in Fig 5-1 is not affected by the inter-network collisions, so the broadcast channel can notify the Zigbee nodes to switch to a free channel. This work uses a time slot within the CAP period as the alarm slot and uses another time slot within the CFP period as the switching slot. In the collision mitigation process, when an end device detects a number of corrupted beacons, it sends a short alarm message in the alarm slot to inform the PAN coordinator about the interference using channel 25. Upon receiving the alarm message, the PAN coordinator searches for a new channel from the list of available channels, then it sends a broadcast message back to end devices via channel 25. As a result, upon receiving the message, the end devices all tune to the new channel assigned by the PAN coordinator to avoid inter-network collisions.

Apart from employing the beacon and ACK packets as the metric, Xinyu Zhang [80] proposed a different approach named the cooperative busy tone (CBT) in which a central ZigBee controller emits a strong signal that makes the WLAN nodes back off for a period of time while the ZigBee node’s transmission can proceed. The central ZigBee controller then simultaneously schedules a busy tone signal with the transmission of the ZigBee network, enhancing the visibility of the ZigBee network to the WLAN. Every time a ZigBee device wishes to transmit, the ZigBee controller hops to an adjacent channel, sending a strong signal to force the WLAN nodes to back off. This scheme significantly improves ZigBee’s throughput in the presence of WLAN inter-network collisions. One drawback of this approach is that the energy consumption of the network will increase to support transmitting strong signals from the Zigbee controller. The network size and the frequency of the CBT signal will determine the energy efficiency of the approach. The strengths and weaknesses of the adaptive mitigation techniques are listed in Table 2-6.

Table 2-6 Strengths and weaknesses of the adaptive collision mitigation technique

Adaptive Collision Mitigation Technique	**Strengths**	**Weaknesses**
Channel switching [8] [76]	Easy to operate Fast to avoid inter-network collisions	Free channels run out in dense networks with multiple WLAN stations
Zigbee inactive period transmission and WLAN PCF [79]	Easy to implement ZigBee and WLAN operate in a TDMA fashion does not generate inter-network collisions	Inactive periods are occupied and cannot be used for multi-hop networks to avoid intra-cluster collisions
WLAN CTS and RTS [77]	CTS and RTS are used to allow ZigBee devices and WLAN stations to operate separately	Long delay if many WLAN stations are used Not suitable for dense networks
Measuring RSSI reading [78]	Effective in protecting ACK packets Inter-network collisions can be abated to some extend	Cannot tackle long periods of strong inter-network collisions. A high packet loss rate in a dense networks
Busy tone [80]	Improve the visibility of an 802.15.4 network in the presence of WLAN inter-network collisions. Medium capturing is used by sending a fake CTS signal.	The fake CTS signal consumes more energy in dense and multi-hop networks than traditional ZigBee networks WLAN networks may have longer delays.

Non-Adaptive Mitigation Techniques

The third category is the non-adaptive mitigation techniques employed in scenarios where the WLAN and ZigBee networks are located close to each other and the inter-network collision level is high. In this case, the adaptative mitigation techniques might not be effective due to the high level of the inter-network collisions. The non-adaptive collision mitigation techniques attempt to reduce the inter-network collisions in a fixed manner. Kunho Hong et al. [81] proposed a stop-and-wait algorithm, making WLAN devices stop sending packets while the ZigBee network is transmitting. The algorithm controls the WLAN traffic flow and ensures that the imposed delay is tolerable to the ZigBee network, while the WLAN network can still maintain high throughput. The algorithm allows WLAN devices to wait for a short period of time and thus sacrifices the WLAN throughput to enable the ZigBee network to transmit in an interference-free mode. Another technique based on distance was proposed by Dae Gil Yoon et al. [82]. This technique analysed the impacts of the WLAN devices on the WPAN transmissions in terms of the Packet Error Rate (PER) and the collision time duration. The work used the PER to derive a safe transmission distance where the WPANs are placed four metres away from the WLAN devices. The study showed that the safe distance reduced inter-network collisions. A similar safe distance and a safe frequency offset were proposed by Peizhong Yi et al.[83]. To eliminate the inter-network collisions, it was found that it is better to switch to another free channel and position the ZigBee and WLAN networks in such a way so that the inference distance is at least four metres to reduce inter-network collisions.

Dual-Radio Heterogeneous Technique

In addition to the research studies on inter-network collisions on separate IEEE 802.15.4 and IEEE 802.11 networks, there are several other studies based on IEEE 802.15.4/IEEE 802.11 dual-radio heterogeneous networks. The notion of large-scale dual-radio wireless sensor networks was proposed by Anis Koubaa *et* al [84]. The energy-constrained large-scale sensor network is connected with WLAN networks, which have a high data rate and a longer transmission range. This two-tiered network can improve the real-time QoS performance, reliability and scalability. Specifically, the high data rate and the longer transmission range of the WLAN networks can allow the real-time transmissions of the sensor traffic with the required QoS. WLANs are less susceptible to the inter-network collisions than the sensor nodes, so the WLAN networks can be used as the back-bone networks. Wireless sensor networks often need to increase the number of nodes to cover a wide area, so the WLANs can be used as back-bone networks to achieve longer transmission distances by forming WLAN mesh networks. However, the work in [84] only provided a conceptual design without detailed results. Similar ideas were also proposed in [85, 86]. A sensor network for IP-WSN gateway was developed in [87]. In this work, the IP-based sensor network was connected with WLAN networks to make the network globally accessible to the Internet in a fast and cost-effective manner. Although this work implemented a hardware platform using the TI CC2520 devices, but did not provide test plans or simulation results either.

A dual-radio network was used in the building blocks [88]. This work implemented a WiFi-ZigBee hybrid build area network to tackle the problem of efficiently deploying AMI with heavy network loads and in a difficult radio propagation environment. To further investigate the performance of the hybrid network, a case study was conducted. The simulation results showed that the round trip time for demand response applications was 0.6s and that the one-way time transmission for smart metering is around 9s. ZigBee nodes connect to a dual-radio node using only one hop. The work did not report if the ZigBee network could be affected by the WLAN transmissions.

Jun Wang et al [89] proposed a heterogeneous ZigBee/Wi-Fi network and compared the performance of this network with that of ZigBee networks in terms of throughput, packet loss rate, packet loss ratio and average end-to-end delay using the OPNET modeler . It was found that the hybrid approach outperformed the ZigBee network, offering a good performance at lower traffic loads. However, the hybrid approach adopted a star topology and did not consider the inter-network collisions. Another study used a ZigBee-Wi-Fi dual-radio node to form a multi-tier multi-hop heterogeneous network monitoring transportation networks such as trains and truck platoons [90]. Specifically, sensors nodes were organised into clusters and wirelessly connected with other nodes in the same cluster using the ZigBee radio. The communications between the clusters was enabled by a ZigBee/Wi-Fi gateway with a Wi-Fi radio. The work used the OPNET simulation model and the simulation results were compared with the theoretical analysis, but the Wi-Fi and the ZigBee radios used two different channels to avoid the inter-network collisions. A dual-radio network based on the IEEE 802.11 and IEEE 802.15.4 standards was proposed in [9] to extend the transmission range of the IEEE 802.15.4 multi-hop network. It was expected that this extension might create inter-network collisions in the IEEE 802.15.4 networks. As a result, an adaptive aggregation approach was proposed to reduce the number of IEEE 802.11 packets, thus mitigating the inter-network collisions. To fully take advantage of the IEEE 802.11 payload, 25 IEEE 802.15.4 payloads were aggregated into one IEEE 802.11 packet. Reducing the number of IEEE 802.11 packets proved to be effective in mitigating inter-network collisions.

2.3.3 QoS Provisioning

Given the complex traffic characteristics of M2M communications, providing sufficient QoS for different M2M applications is difficult, and there are no one-size-fits-all solutions for M2M applications [51]. This is because the IoT is a complex paradigm, so heterogeneous networking technologies must be used to offer some minimum required QoS for the corresponding applications. For example, some technology needs to support delay-tolerant applications such as meter reading in the Smart Grid context, while it also needs to support home security applications such as alarms. This results in the coexistence of different networking technologies and applications. In some case, several networking technologies can work collaboratively support one application.

However, not many studies specifically have focused the QoS issue before, and most of them only discussed the collecting phase of the IoT to classify the traffic characteristics and QoS requirements for M2M applications. A majority of M2M applications are located within the area networks, offering different services to users. To differentiate these services and guarantee QoS requirements, M2M communications must support a wide range of applications from non-real-time meter reading to urgent alarm notifications. For example, meter reading can be categorized into several classes: (1) meter reading on demand, which is triggered when needed by utilities; (2) scheduled interval, which is planned for 4 to 6 times per day; and (3) bulk transfer, which transmits the accumulated meter information to utilities 2 to 3 times per day. The three groups of metering are required to finish transmission within 15 seconds, 4 hours and 2 hours, respectively.

In contrast, medical sensors are used to monitor the parameters of the human body, such as blood pressure, temperature and breathing activity. The collected information will be aggregated and transmitted to the medical centre for further analysis. This allows the medical staff to perform remote monitoring and take prompt action when the health condition deteriorates. As a result, this type of application requires responses in seconds [32]. Another related medical application is personal wearable sensors in the portal devices (e.g., smart phones and watches) that can track walked steps, burned calories and performed exercises, thus providing personal health advice to enhance lifestyle. This application may require less time-critical packet transmissions, but still need to be satisfied within less than half an hour or several minutes [57]. As for environmental monitoring, a large number of fixed and wireless sensors are expected to be deployed in difficult terrains such as deserts, oceans and forests. The sensors are required to transmit the information promptly, preventing any harmful effects (flood and bush fires). In addition, these sensors are normally distributed in a large-scale area, and the data sink may not be able to maintain a high packet success rate due to interference, which is difficult for sensors to maintain a satisfactory QoS requirement. This study proposes a heterogeneous area network model to maintain the QoS requirements for the short-range networks.

2.4 Conclusion

In this chapter, the IoT, M2M and Smart Grid communications networking techniques were reviewed, and the IoT applications were discussed, followed by a comprehensive survey of the important IoT elements, standard bodies and applications. The key pillars and elements of M2M communications were introduced. Then the communication standards with wired or wireless solutions were provided. Specifically, Smart Grid acting as one of the applications of M2M communications was also introduced. This was followed by the traffic profile, including the traffic characteristics and QoS provisioning. To meet the QoS requirements of M2M applications and to make the end-to-end connection stable and reliable, short-range networking solutions including the homogeneous and heterogeneous networks were discussed. The heterogeneous wireless networking technologies can be suitable for communications in the area networks. The underlying problems regarding the homogeneous and heterogeneous networks were narrowed down to the intra-and inter-network collisions, which are the major problems to be discussed in the following chapters.

Chapter 3

Low-Power Wireless Area Networks for M2M Applications

3.1 Introduction

With the increasing number of low-power devices deployed for M2M applications, the need for a new distributed computing architecture is on the rise, so energy efficient network architecture is needed to meet the above needs. For some applications, traditional WANs are used to support connectivity in a large geographical area. The WANs are often implemented with 3G and 4G standards such as UMTS and LTE, which serve H2H or H2M communications with high data rate links. As these standards are designed for applications such as video, audio and multimedia for humans, they have the potential to maintain wireless connectivity between base stations and M2M devices to some extent.

However, 3G and 4G networks may not be able to offer seamless wireless connectivity among machine-type devices. A large number of machine-type devices generating small-size packets in a sporadic manner may result in network congestion or even the collapse of a cellular network [91]. This is because signalling traffic, such as the control and management packets generated by these devices, can overwhelm the control channels of a base station. Cellular networks are designed to handle a moderate number of users with a large amount of traffic, so the signalling overhead caused by the users is not very high. A concrete example is where a sudden traffic surge caused by concurrent access to a base station by a large number of M2M devices could give rise to the overload of the Physical Random Access Channel (PRACH) in the LTE cellular system [92]. This overload will subsequently lead to the contention of the channel and, in turn, the degradation of the system’s performance. This occurs especially when a large number of machine-type devices concurrently wake up, requesting connections to the same base station.

In addition, traditional cellular networks are susceptible to spatial or temporal fading when covering a large-scale area with machine-type devices. In other words, the traditional cellular networks require either a LoS or NLOS wireless connection to obtain a sufficient Signal-to-Noise-Ratio (SNR) to decode signals [93]. For example, a vehicle can obstruct the connectivity between a cluster of static machine-type devices and a base station, so the data connection can be affected. H2H and H2M communications, however, can avoid such a risk by simply moving to a different location with sufficient SNR. M2M communication networks are featured as infrequent data arrival rates, low energy consumption and minimum overheads. Traffic asymmetry in the M2M networks (uplink more than downlink) is quite opposite to H2H and H2M traffic, so how to use traditional cellular networks to handle the asymmetry of M2M traffic is still an open issue [94].

Due to the above reasons, traditional cellular networks may not be an ideal candidate for M2M communications. As mentioned in Chapter 2, many standard organizations and research institutes such as ETSI, IEEE and 3GPP have proposed different types of architecture for the realisation of M2M communications. It can be observed that M2M communication architecture is divided into many segments. For example, ETSI proposed a type of architecture comprised of access networks, area networks and core networks, whereas the Smart Grid communication networks consist of Home Area Networks (HANs), Neighbourhood Area Networks (NANs) and Wide Area Networks (WANs). The different networks play different roles in each transmission stage, so it may be difficult to use single architecture to satisfy all of the requirements of the M2M applications. For example, data source and destination are sometimes located in different geographical areas, and an application data packet may transverse from HANs via NANs and WANs to a data sink.

This chapter focuses on the area network design for M2M communications as mentioned in Chapter 2. Short-range wireless standards can effectively be used to develop an access network for M2M communications, so this chapter presents a 6LoWPAN-based network architecture to support M2M and Smart Grid applications, as well as offering IP end-to-end connectivity. The main focus of this chapter is the development of a 6LoWPAN-based area network model that supports multi-service traffic. The remainder of the chapter is organized as follows: Section 3.2 introduces fundamentals of the IEEE 802.15.4 standard and describes the slotted CSMA/CA algorithm and its performance. Section 3.3 analyses the underlying network topologies that can be used in M2M communications and explains the 6LoWPAN OPNET model development in detail. The developed OPNET 6LoWPAN model can be used for the proposed scheduling algorithms Section 3.4 concludes the chapter.

3.2 An Overview of the IEEE 802.15.4 Standard

Short-range wireless networks can be seen as one of central pillars of M2M communications, particularly for the area networks. As shown in Table 2-1, many short-range standards and communication protocols are available, such as the Wireless HART, ISA 100.11a, ZigBee, Bluetooth, NFC and IEEE 802.15.4-based Networks. Some of the standards support the IPv6 protocol for machine-type devices to realise IP end-to-end connectivity, so this study uses the 6LoWPAN standard to develop a wireless area network and reduce the operational costs of M2M communications in terms of installation, data transmission requirements and battery life [95] while maintaining a flexible network architecture. Most of the nodes in the area networks are energy-constrained devices with small antennas and low computational abilities, so the energy may deplete depending on applications and network algorithms. For this reason, the IEEE 802.15.4 standard can be used and allow the machine-type devices to operate in an on-and-off manner to save energy, which is cost-effective for M2M applications to use the license-free spectrum, compared to other standards that require the network to be constantly operating.

3.2.1 The IEEE 802.15.4 Physical Layer

The physical layer plays an important role in transmitting and receiving data packets with the aid of the modulation techniques used over a wireless channel. This layer uses the Direct Sequence Spread Spectrum (DSSS), which is resilient to interference. The physical layer operates at three different frequencies with various data rates: 868MHz (20 kbps) for Europe, 915MHz (40kbps) for North America and 2.4 GHz (250bps) for global use. These frequencies totally support 27 sub-channels with one between 868 and 868.6 MHz, ten between and 902MHz and 928 MHz, 16 between 2.4 GHz and 2.4835 GHz. With a lower frequency, the coverage is larger, and vice versa. Table 3-1 shows the frequency ranges and data rates of IEEE 802.15.4 standard, and Fig 3-1 illustrates the operating frequency sub-bands arrangements.

Table 3-1 Frequency bands and data rates of the IEEE 802.15.4 standard

Phys (MHz)	**Frequency Band (MHz)**	**Chip Rate (kchip/sec)**	**Modulation**	**Bit-rates(kb/sec)**	**Symbol Rate(ksymbols/sec)**	**Symbols**
868	868-868.6	300	BPSK	20	20	Binary
915	902-928	600	BPSK	40	40	Binary
2450	2400-2483.5	2000	Q-BPSK	250	62.5	16-aryorthogonal

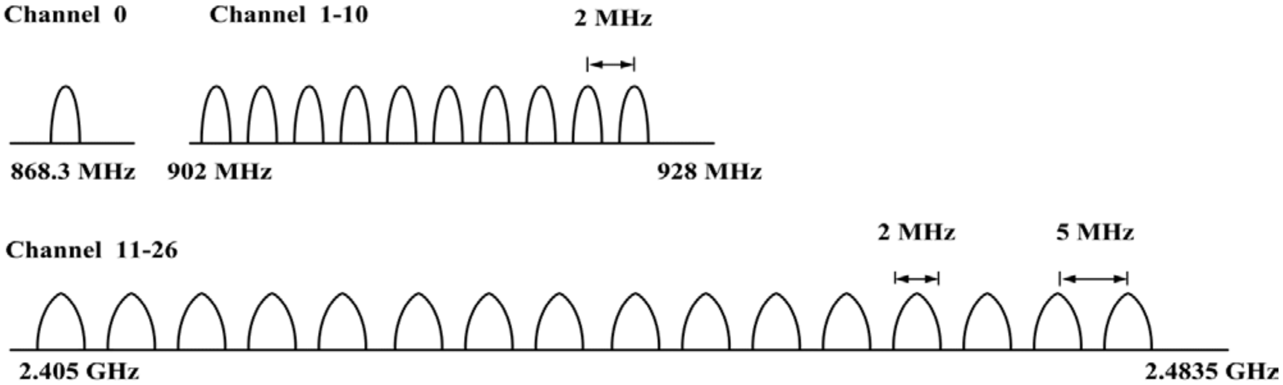


Fig 3-1 IEEE 802.15.4 Physical layer carrier bands.

The 802.15.4 standard has been developed with many variants for different countries and purposes over time. The 2003 version defined two primitive physical layers with one being 2.4GHz and the others being 915 and 868 MHz The 2006 version released four physical layers with three for the lower frequencies 915 and 868 MHz and one for the high frequency 2.4 GHz. More precisely, two physical layers, with lower frequency bands 915 and 868 MHz use the DSSS approach but adopt different modulation schemes: binary phase-shift keying (BPSK) and offset quadrature phase-shift keying (O-QPSK), respectively. The third physical layer in sub-GHz bands at 915 and 868 MHz employs the Parallel Sequence Spread Spectrum (PSSS) with Binary Phrase-shift keying (BPSK). The fourth physical layer with high frequency 2.4 GHz adopts the DSSS and O-OPSK.

The IEEE 802.15.4 a standard released two additional physical layers using the Ultra-Wideband (UWB) and the Chirp Spreading Spectrum (CSS) techniques. The former is a for low energy consumption and short-range communications with wide bandwidths ranging from 1 to 10 GHz for high-rate PAN transmissions, while the latter uses a wideband linear frequency modulated sinusoidal signal as the modulation scheme where the signal frequency varies over time.

Another standard IEEE 802.15.4c released three new ranges of spectrum for China: 779 to 787 MHz, 430 to 434 MHz and 314 to 316 MHz Similarly, IEEE 802.15.4d uses the 950 to 956 MHz spectrum for Japan. IEEE 802.15.4c uses the O-QPSK and MPSK techniques operating in the frequency band of 779 to 787 MHz. The IEEE 802.15.4d standard uses the Gaussian Frequency-Shrift Keying (GFSK) and BPSK modulation schemes. The IEEE 802.15.4e standard is an enhanced version of the 2006 standard, including the frequency hopping technique to withstand channel interference and multi-path fading.

In particular, the IEEE 802.15.4g standard was released for the Smart Utility Network (SUN). As mentioned earlier, a Smart Grid is usually comprised of HANs, NANs and WANs, the IEEE 802.15.4g standard is designed for NAN communications [96]. The rationale behind this is that NAN communications are becoming proprietary and the utilities are calling for vendors that can provide the best service. Vendors, utilities and equipment manufacturers have joined together to develop the IEEE 802.15.4g standard, which offers four fundamental and distinctive features: (1) the available frequency ranges at 868 MHz, 915 MHz and 2.4 GHz; (2) data rates are more flexible, ranging from 40kbps to 1000 kbps; (3) the physical PPDU size has been augmented to 1500 bytes to accommodate either an IPv4 or IPv6 MTU without having to fragment the packet; and (4) co-channel interference has been mitigated when the IEEE 802.15.4g network coexists with other networks such as IEEE 802.11 WLAN and IEEE 802.15.1 Bluetooth. More precisely, a multi-PHY management (MPM) approach is adopted, allowing a potential coordinator to use a different PHY layer to discover an operating network. The MPM scheme coupled with the CCA mechanism can be used to mitigate the inter-network collisions. This is because the IEEE 802.15.4 standards do not provide any error correction services in the PHY layer, and if the network suffers inter-network collisions, it is difficult to restore the corrupted packets. As such, IEEE 802.15.4g is a timely standard and a key enabler for NAN communications. However, this standard is in its infancy and lacks a proper means to evaluate its system performance [97].

Apart from the above features, the IEEE 802.15.4 physical layer offers other important functions, such as the Link Quality Indication (LQI); Receive Energy Detection (RED); activation and de-activation; and Channel Clear Assessment (CCA). These four functions are explained in detail below.

Link Quality Indication (LQI)

LQI, computed from the received packets, represents the signal strength on a wireless communication link. The LQI is represented by an 8-digit value, which is confined between 0x00 and 0XFF corresponding to the lowest and highest detected signal strength as per the standard. The LQI is forwarded to the MAC layer using PHY Data. Indication primitive (PD-data. indication) to determine the causes of the packet corruption due to either insufficient signal strength or due to interference.

Receiver Energy Detection (Receiver ED)

Receiver ED aims to estimate the received signal strength used by the network layer algorithm responsible for selecting the channel to form a PAN. The average time for a Receiver ED is 8 symbols times. Receiver ED is an indispensable step in CCA that determines the channel status without using a decoding procedure and signal identification. Specifically, an 8-bit integer chosen from 0x00 to 0xff is reported from the PHY layer to the MAC Layer Management Entity (MLME) using the PHY Layer Management Entity-Energy Detection.confirm (PLME-ED.confirm) primitive.

Activation and De-Activation on the radio transceiver

The physical layer takes the responsibility of changing the receiver and transmitter state when operating on a certain channel once receiving a signal from the MAC layer. This process, often referred to as the turnaround time, takes no more than 12 symbols according to the standard.

3.2.2 The IEEE 802.15.4 MAC Layer

The IEEE 802.15.4 MAC layer interfaces the physical layer with the higher layer and governs the data transmissions from the MAC layer Service Access Point (SAP). Fig 3-2 presents the MAC layer data frame mapping through the SAP in the Physical layer. The MAC service data unit (MSDU) consists of many components, such as frame control, sequence number, addressing files, auxiliary security header and data payload. The first three fields are referred to as a MAC header (MHR) with a MAC footer header in the end. After passing from the MAC layer to the Physical layer, the MSDU becomes a PSDU with a Synchronization Header (SHR) and a Physical Header (PHR). The standard defines the maximum size of the PSDU as 121 bytes (6 bytes the PPDU header deducted from 127 types), so the minimum payload size of the MSDU is 82 bytes.

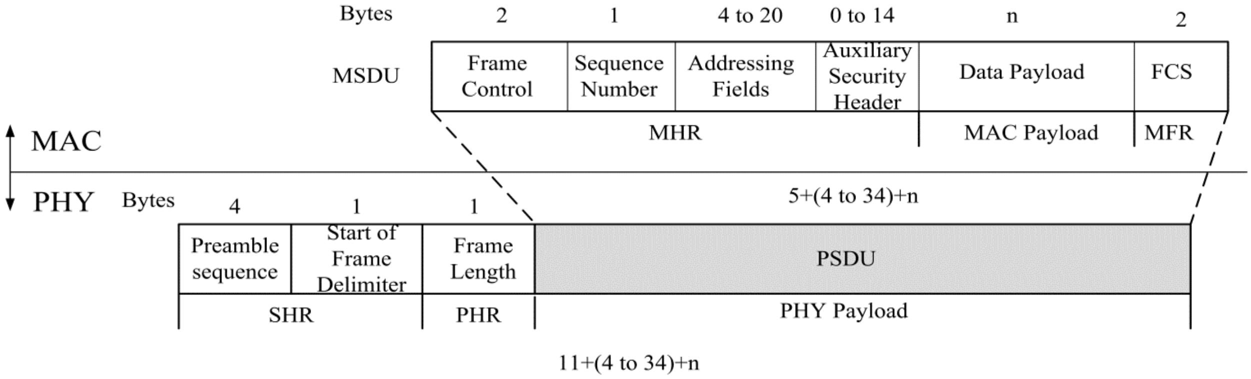


Fig 3-2 IEEE 802.15.4 MAC data frame

The MAC layer normally coordinates the transmission using a control frame named beacon, which integrates the start and end time point of data transmissions. This transmission time can be divided into the contention period and contention-free period. The contention period is subject to use of the CSMA/CA algorithm using all the physical layer’s features such as LOI and RED to access the channel and execute the transmission and reception. The contention-free period uses dedicated time slots known as Guaranteed Time Slots (GTS) to provide a Time Division Multiple Access (TDMA) service. A packet transmission is followed by a reply from the receiver, and this acknowledgement from the receiver ensures a packet’s reception. The MAC layer also supports an operation mode without the beacon, so an unslotted CSMA/CA algorithm is used to access the channel. The 802.15.4 MAC structure is presented in Fig 3-3.

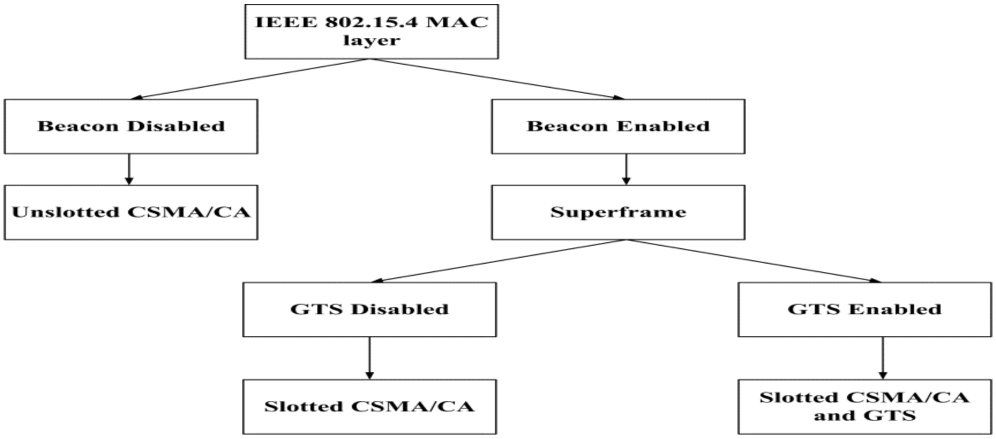


Fig 3-3 IEEE 802.15.4 MAC layer operation mode

Beacon Transmission

The 802.15.4 standard defines the duration between two consecutive beacons as a superframe, which defines the packet transmission services. As can be seen from Fig 3-4, the superframe starts with a beacon, indicating the beginning of a new transmission cycle. The transmission cycle is bounded by beacons. Specifically, the superframe is divided into two parts: an active period and an inactive period. The active period consists of 16 time slots used by all of the devices to access the channel in a contention model, whereas the inactive period is used to save energy when the devices are turned off. The active period can be further categorised into the Contention Access Period (CAP) and the Contention Free Period (CFP). The CAP allows all of the devices to compete for the channel using the CSMA/CA mechanism, whereas the CFP is used to allocate a particular number of time slots named as the Guaranteed Time Slot (GTS), which is dedicated to one or several devices and ensures the guaranteed channel access for real-time traffic.

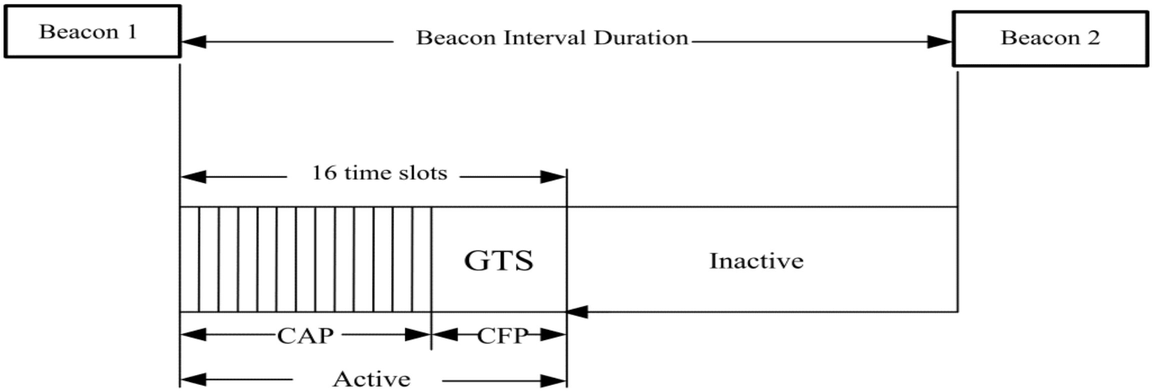


Fig 3-4 Superframe structure

The CAP period will be allocated with 16 time slots when the GTS is disabled. Within this period, any device attempting to transmit needs to commence their transmission in the first slot of the CAP and complete by the last slot of the CAP using the CSMA/CA mechanism.

If GTS is enabled, up to seven GTS slots can be allocated to guarantee direct access the channel dedicated to particular devices. The GTS allows devices to access to the channel without contending for the channel. For example, a device wishing to transmit real-time traffic is allowed to use these channels without colliding with other packets, resulting in the higher efficiency of the channel. Due to the limited available channels and the large amount of M2M traffic, the GTS is not adopted in the study.

In the inactive periods, no transmissions are allowed and the devices are turned off, switching to the sleeping mode to save energy. As such, energy can be saved to achieve the cost-effectiveness required by the standard. Meanwhile, the other devices not allocated with a GTS slot can still access the channel using the CSMA/CA mechanism. Any unfinished transmission either within the CAP or GTS period is deferred to the next superframe.

In this study, the beacon-based mode is preferred since it can reduce the probability of collisions within a network, allows devices to sleep between the coordinated transmissions to save energy, and reserves bandwidth to prolong the network lifetime. As a result, it is suitable for M2M/IoT applications in terms of energy efficiency and lifetime.

Non-Beacon Transmission

In contrast to the beacon mode, the non-beacon mode does not use either a superframe or a beacon. In other words, the devices in the network are not synchronised and do not go into the contention free period. Instead, they simply transmit packets when the channel is free so that they can generate a high level of collisions. This means that the nodes must sense the channel all the time, and this mode will use much more energy than the beacon mode. If the number of nodes is high, energy consumption is a concern. Accordingly, the non-beacon mode is normally used to handle light traffic with a small number of nodes. When the node number and traffic volume increase, the non-beacon mode may not be able to manage the nodes and tackle the increased traffic. Due to the above reasons, to better manage a large number of machine-type nodes distributed on a large scale, the beacon mode is adopted in the study.

Superframe Structure

Figure 3-4 shows that a superframe allows active transmission between two consecutive beacon frames. FFDs and RFDs can exchange data within this superframe. As per the standard, two important parameters impact on the structure of a superframe. One is the Beacon Order (BO), which defines the duration between two beacon frames, namely the Beacon Interval (BI), and as this frame varies the length of the duration between two beacons changes. The other parameter is the Superframe Order (SO), which regulates the length of the CAP period, and thus larger values contribute to a longer period. Accordingly, the correlation between the BI, BO and SO is explained as follows.

$$\mathrm{BI} = \mathrm{aBasesuperframeDuration} \times 2^{\mathrm{BO}}\ \mathrm{Symbols}, \tag{3-1}$$

$$\mathrm{SO} = \mathrm{aBasesuperframeDuration}\ \times 2^{\mathrm{SO}}\ \mathrm{Symbols}, \tag{3-2}$$

Where $0 \leq \mathrm{SO} \leq \mathrm{BO} < 15$.

According to the standard, the inactive period does not exist when BO=SO, and the superframe is comprised of the active period only. In contrast, if the BO is 15, the superframe does not exist as per standard, and therefore, the whole network operates as a non-beacon based model. In addition, the standard regulates the minimum duration of the superframe, which is equal to 960 symbols (15.36 ms). One time slot occupies 960/16 = 60 symbols (0.96ms). A beacon contains the control management information such as the start and end of a superframe, addressing information and the number of time slots allocated to the GTS. What follows the beacon is the CAP that begins at the start of a superframe and ends before the start of the CFP. With the CFP being disabled, the active part of a superframe is the CAP. The CFP, in contrast, can allocate up to seven GTS, in which the minimum length of the CAP is 440 symbols. This ensures that there is sufficient time to transmit the packets. Moreover, after a transmission, an acknowledgement for the received packet is sent back immediately to provide a reliable communication service in the MAC layer. A packet transmission needs to end within one Inter Frame Spacing (IFS). Otherwise, the packet will be deferred to the next superframe.

3.2.3 The Slotted CSMA/CA Algorithm

IEEE has released two operating modes: the slotted beacon-enabled mode and the unslotted beacon-disabled mode. These modes are based on the CSMA/CA algorithm, and the slotted beacon-based mode is discussed in this study. Before introducing the algorithm, there are several parameters that need to be mentioned.

The Back-off Exponent (BE) is an exponent used to calculate the number of back-off slots when a device wants to transmit, and it must check the channel status by performing a Clear Channel

Assessment (CCA) twice. This value is normally confined between macMinBE and macMaxBE, which are three and five by default, respectively. The number of Back-offs (NB) is that how many times a node experiences a back-off while attempting to transmit a packet. This value is fiv by default. The Contention Window (CW) refers to a back-off period when a device senses an idle channel. The value is initially set to two, and will be reset to two when the channel is sensed busy. In addition to these three variables, the number of retransmissions is recorded at each node.

The slotted CSMA/CA algorithm is described as the following steps as shown in Fig 3-5. Before a new packet arrives at the MAC layer, the NB, CW and BE are set to zero, two and three, respectively. The node backs off random time slots uniformly distributed from [0, 2^{BE}-1]. Afterwards, the nodes perform the first CCA and sense the channel. If the channel is sensed to be idle, the CW is decreased to one. Then if the CW is not zero, a second CCA starts. Once the channel is found idle again, the packet is transmitted.

If either of these CCAs fails, the BE and NB are increased by 1, and the CW is reset to two. A same back-off procedure is carried out again with new back-off time slots selected from the [0, 2^{BE+1}-1]. After the NB is greater than the macMAXCSMABackoffs, the algorithm ends with failure status and drops the packet.

According to the standard, the acknowledgment (ACK) is optional, so the CSMA/CA algorithm can either work in an ACK-enabled model or an ACK-disabled model. In the first mode, a packet can end up with a successful transmission or a collision, so it is easy to differentiate if a packet has been received or experienced packet collisions by using the ACK. In contrast, in the second mode, no ACKs will be replied to the sender irrespective of whether packet reception is successful or a packet Collison has occurred. In particular, in the ACK-enabled mode, when a packet is received at the receiver, the sender wait for L_{ack} time after the completion of a packet transmission; the receiver will respond with an ACK after a turnaround time that allows the receiver to change from the receiving mode to the sending mode. Meanwhile, the sender sets a time after a packet transmission, and if an ACK is not received within this time, the sender assumes a packet collision and a retransmission will start, so the number of retransmission *n* is increased by one. This packet can be transmitted for N=aMaxFrameRetries (3 by default) before being dropped, and a new packet transmission begins with the BE, CW, NB and *n* reset to their original values.

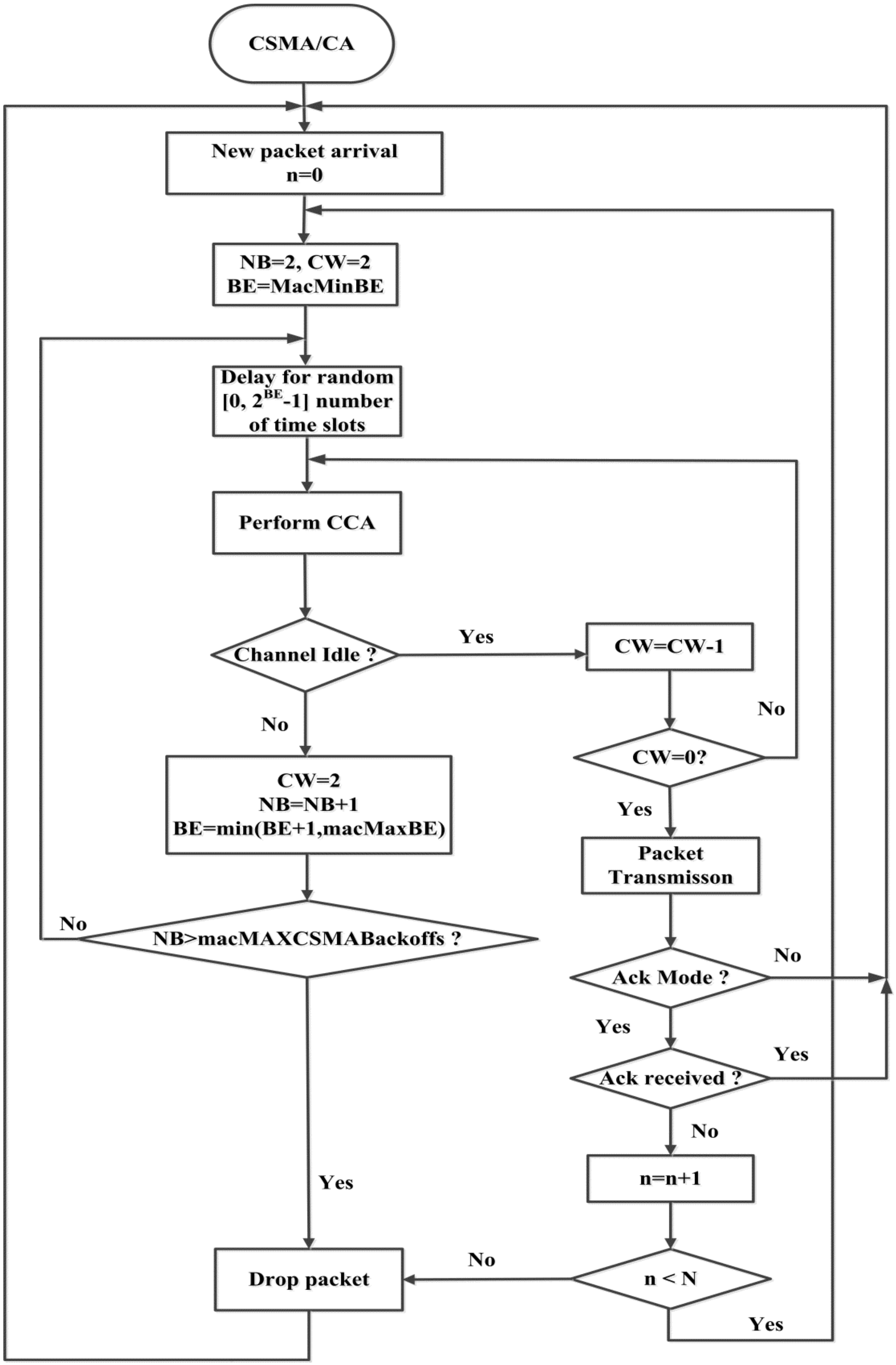


Fig 3-5 Slotted CSMA/CA algorithm [66]

3.2.4 The Topology of the IEEE 802.15.4 Standard

Two basic topologies are defined by the IEEE 802.15.4 standard depending on applications, as shown in Fig 3-6. In a PAN, all the devices are classed either as a Full Function Device (FFD) or a Reduced Function Device (RFD). The FFD executes the functions defined by the standard, while the RFD is equipped with limited functions. For instance, an FFD can communicate with all the RFDs and the other FFDs, but an RFD cannot communicate with the other RFDs and is only allowed to communicate with the FFDs.

In the star topology, the PAN coordinator directly establishes communications between devices and itself. The PAN coordinator, shaded in dark grey, is an FFD node that initiates the network, sends control packets and synchronises the other devices. Specifically, a PAN coordinator transmits messages, broadcasting the start-up of a network and allows other devices wishing to associate with the PAN coordinator. After the association, the PAN coordinator distributes an identification field named the PAN ID to these associated devices, claiming that these devices belong to this PAN. In addition, the star topology has been widely used in industry, home automation and medical science because it is easy to be deployed and added with new nodes. In [98], A. Milenkovic proposed a Wearable Wireless Body Area Newark (WWBAN) architecture that employs IEEE 802.15.4-based device to constantly monitor a patient’s heart rate and breath in a real-time manner. Similarly, Timmons [99] presented an approach that sensors are implanted underneath the skin, maintaining the transmissions in a non-beacon mode over a long period.

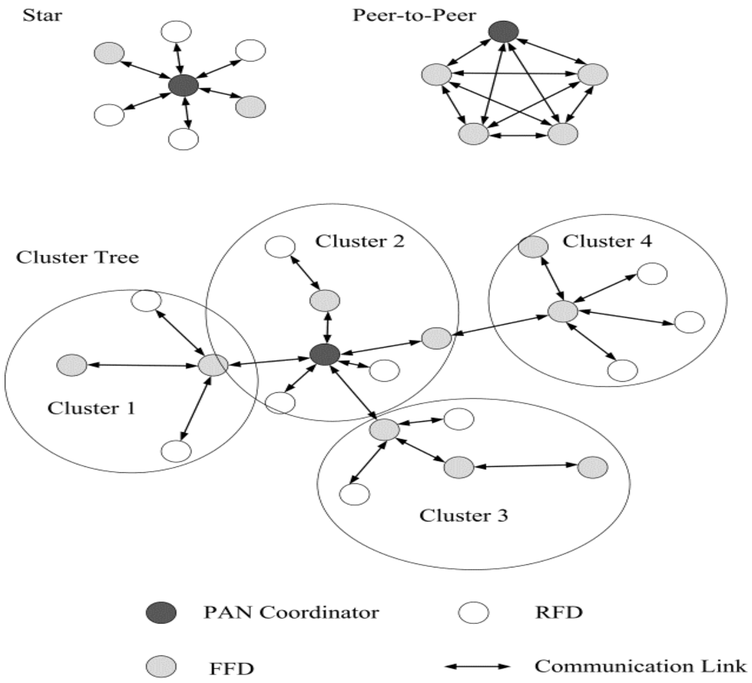


Fig 3-6 IEEE 802.15.4 topology

The peer-to-peer topology is a scenario where the FFDs are allowed to talk to each other as long as they are within communication range. The mesh topology, a more complex topology, can be formed to increase the reliability of a PAN; that is, if one link fails to relay the packets, the other links can bypass the failure and resume transmitting the packets. The peer-to-peer topology can increase the packet success ratio and make the network less susceptible to interference. Due to this feature, the peer-to-peer topology can be applied to many applications. A typical example is the Smart Grid, in which smart meters are interconnected in the peer-to-peer topology to achieve seamless connectivity, so a failed link can be bypassed [100]. As the meter reading is one of the M2M applications, the peer-to-peer topology can be deployed in other M2M applications such as home control and monitoring and industrial automation [101].

Although a peer-to-peer topology maintains good connectivity, it can only supports a small-scale area. To extend the coverage, the IEEE 802.15.4 standard defines a cluster-tree to enable the FFDs and RFDs to widespread into a large-scale area. In such a cluster, one cluster head controls the RFDs and meanwhile connects to the other clusters, as shown in Fig 3-6. In addition, despite many clusters, only one PAN coordinator is allowed to exist in a PAN. The cluster-tree topology can cover larger areas compared to the star and peer-to-peer topologies, but it has drawbacks such as the long delay caused by multi-hop wireless links; another drawback is that the packet success rate declines as the number of hops increases [102]. This poses a real challenge to large-scale deployments in M2M communications because machine-type devices may be spread in a distributed area and be interconnected by the cluster-tree topology. It is easy to support many M2M applications such as building monitoring, and facility management in small-scale [2]. A summary of advantages and disadvantages are shown in Table 3-2.

Table 3-2 Advantages and disadvantages of the IEEE 802.15.4 topologies

Topology	**Advantage**	**Disadvantage**
Star	Small-scale efficient transmission Easy deployment Easy to add new nodes to the network The coordinator can easily monitor and manage the whole network	Once the coordinator fails, the whole network breaks down. The network capacity relies on the coordinator's capacity. Small overage
Peer-to-peer	Nodes can communicate to each other directly Many routes to pass packets if one route fails	Small coverage Difficult to manage Relay nodes have to keep all the information of neighbors, and energy consumption is high Beacon is applied as no synchronization is required, any node can send packets to the nodes in the transmission range
Cluster tree	Large coverage Network divided into several segments that can be easily managed Once one segment fails, the other segments are not affected. High energy efficiency due to sleeping period in beacon mode	High latency Low packet success rate

3.2.5 Guaranteed Time Slots (GTS).

The Guaranteed time slot is a contention-free period in which a certain number of dedicated time slots in an active period of a superframe are assigned by a PAN coordinator and allows devices to access the channel without competing with other devices. To obtain a GTS slot, devices are required to transmit a GTS request to the PAN coordinator, but this process is still contention-based using the CSMA/CA algorithm [103, 104]. With the allocation of the GTS slots, real-time high priority traffic can be sent with relatively lower delay than the CAP period.

On the other hand, if the contention is fierce and the packet loss is high in the CAP, the PAN coordinator can withdraw an allocated GTS to end the transmission. As such, the IEEE 802.15.4

standard regulates that the number of GTS is restricted to seven, keeping enough slots remained for the CAP, and that a GTS can only happen between a PAN coordinator and a RFD. In addition, apart from the allocated GTS, the other devices without the allocated GTSs still can contend for the channel. With the CAP slots, a GTS request sent by a device could be rejected by the PAN coordinator simply due to insufficient GTS resources. The request usually contains network information such as starting slots, packet length and link direction. The link direction indicates whether a device is receiving or transmitting a packet in the CFP. The IEEE 802.15.4 standard defines an Interframe Space (IFS) depending on the packet length. If the packet length is smaller than 18 bytes, a Short Interframe Space (SIFS) is used; otherwise, a Long Interframe Space (LIFS) is adopted. It is important to note that losses of synchronisation could lead to the loss of an allocated GTS slot.

GTS Allocation

A device wishing to use the GTS service needs to send a GTS request to the PAN coordinator using a GTS command frame that is transmitted using the CAP slots. Fig 3-7 shows the GTS command frame specified in the standard. The GTS length is the number of slots required by a device. The GTS direction indicates whether it is transmitting (value 0) or receiving (value 1). The characteristic type specifies allocation (value 1) and de-allocation (value 0). Once receiving a GTS request, the PAN coordinator immediately sends an ACK to the device and checks how many slots are still available. If the PAN coordinator determines that the number of the requested slots is not beyond the remaining slots, the GTS slots starts to be allocated.

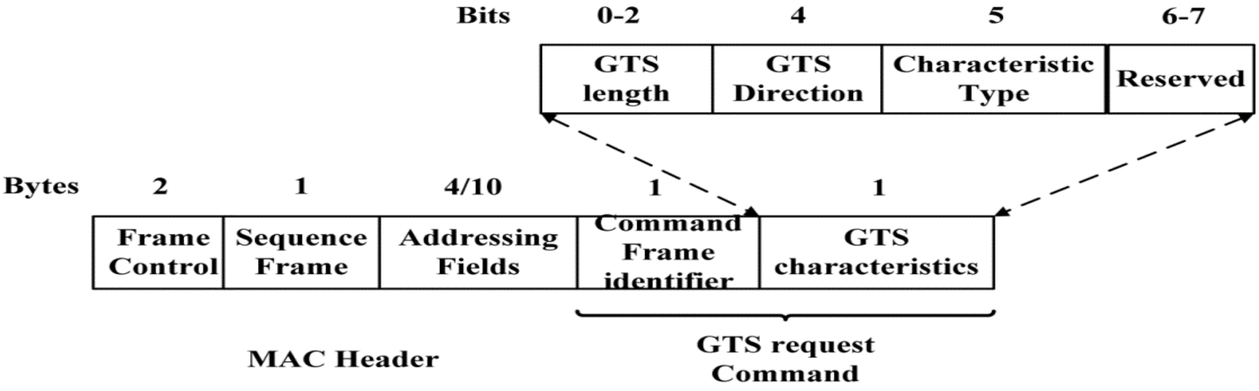
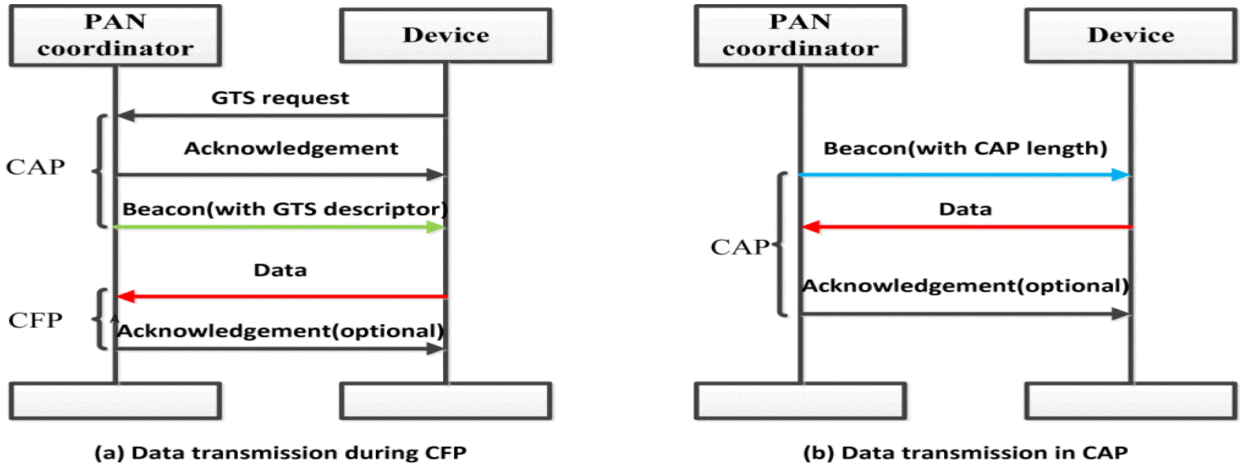


Fig 3-7 GTS request frame

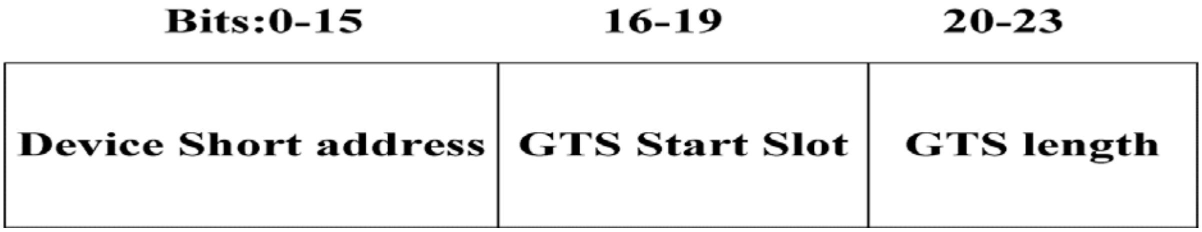
Figure 3-8 (a) illustrates the GTS allocation process. A PAN coordinator uses a First-In-First-Out (FIFO) queue to distribute the GTS slots. As mentioned earlier, if the remaining time slots are adequate in the CAP, an acknowledgement is replied to the device. It takes a time of four beacon frames to determine this GTS allocation, both the request and acknowledgement transmission occur in the CAP period using the CSMA/CA mechanism, as shown in Fig 3-8 (b). The device keeps tracking the four-beacon duration after the receipt of the ACK from the PAN coordinator until a beacon with a GTS descriptor including node addresses, the GTS Starting slot and GTS length arrives. After these interactions, the device starts to transmit to the PAN coordinator. On the other hand, if the GTS allocation fails, the GTS descriptor is assigned with a zero value to the starting time, and thus the device needs to resend another request to the PAN coordinator. Fig 3-9 demonstrates the GTS descriptor that can cause a reduction in the CAP duration because the GTS descriptor needs to integrate the updated information and occupies the space of the CAP. The GTS descriptor will be removed once the device receives the GTSDescPersistence superframe.



(a) Data transmission during CFP

(b) Data transmission in CAP

Fig 3-8 Data transmission process for the CFP and CAP



Bits:0-15	16-19	20-23
Device Short address	GTS Start Slot	GTS length

Fig 3-9 GTS descriptor

GTS De-allocation

Once a GTS slot has been successfully allocated and discovered by the Mac layer of a device, the device can immediately send packets at the start of the allocated time slot. To de-allocate a GTS slot, a device needs to send a request using the command frame and set the characteristic value to zero (de-allocation). On receipt of the request, an acknowledgement will be sent by the PAN coordinator that in turn checks whether the value of GTS characteristic in the request frame matches the existing stored GTS characteristics in the coordinator or not. If it fails to match the existing characteristics, the de-allocation occurs and the CAP length will be updated.

3.3 OPNET 6LoWPAN Model

This study present the design of an area network for different M2M applications using the short-range wireless standard 6LoWPAN and also cater for the QoS requirements. An area network with many sensors and actuators is interconnected by wired or wireless communication links. Therefore, it is necessary to design a network to support seamless connectivity between the M2M devices and the M2M gateways dealing with the various types of M2M applications such as the Smart Grid, health care monitoring and industrial applications. As IPv4 addresses are being depleted, IPv6 is a viable choice and can address countless machine-type devices. Identifying M2M devices in the M2M networks is important. This can be solved using the 6LoWPAN standard that can provide 2^{128} addresses for applications in M2M communications

To explicitly design an area network, an M2M area network architecture is proposed, as shown in Fig 3-10. 6LoWPAN end devices are distributed in a $250 \times 250\text{m}^2$ area. Most of these devices are connected to the routers relaying the collected information through many hops to a data sink. Due to the limited transmission range, the data collected from the devices needs to be transmitted through several hops, which may waste energy and experience packet losses. The distance between each 6LoWPAN device is approximately 50 metres, and the distance from R1 to the data sink is approximately 250 metres. This 6LoWPAN-based area network is one of many M2M area networks and chosen as a typical example for analysis, so an M2M device can be identified with the 6LoWPAN protocol.

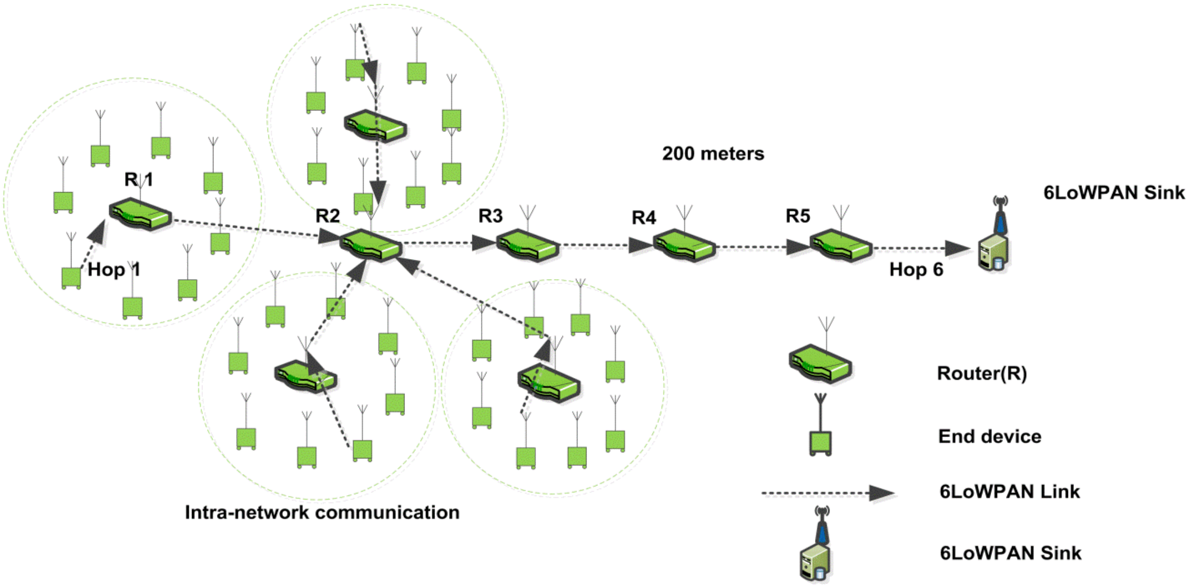


Fig 3-10 An M2M area network architecture

3.3.1 6LoWPAN Protocol Stack

To design an M2M area network and evaluate its performance using simulation, the 6LoWPAN protocol stack and its related features should be introduced. The 6LoWPAN working group has drafted two RFC files that explicitly explains how the IPv6 packets can be sent using the IEEE 802.15.4 physical layer [105, 106]. One file defines basic designs to enable the encapsulation and de-capsulation of IPv6 packets such as header compression, fragmentation and de-fragmentation. More precisely, the 6LoWPAN standard defines the upper layers of the IEEE 802.15.4 standard. The other file defines the IPv6 address stateless auto-configuration that regulates how to automatically generate IPv6 addresses from the IPv6 prefix and MAC addresses. Furthermore, an adaptation layer has been made to tackle the incompatibilities in many aspects. As IPv6 has the minimum MTU size of 1280 bytes, meaning that at least 1280 bytes are allowed to create a packet sent through the IEEE 802.15.4 link layer. However, as can be seen from Fig 3-2, the IEEE 802.15.4 standard only supports 127-byte packet size that leaves 81 bytes reserved for the payload. In addition, the IPv6 protocol assigns 128-bit IP addresses to all the M2M devices, but the IEEE 802.15.4 standard provides two options for the devices: global 64-bit extended addresses or local 16-bit addresses [107]. This, therefore, poses a real challenge for addressing. Another aspect is the routing. It is expected that a great number of M2M devices will be deployed in a large-scale area, and the packets must be routed from the area network to the core network using the global routable IPv6 addresses. For simplicity, since dynamical IPv6 routing requires the neighbourhood discovery mechanism, which the OPNET does not have, static routing was employed in the study due to time constrains, and will be explained in the following sections.

This study uses the 6LoWPAN standard to develop an M2M communication network. Fig 3-11 presents a 6LoWPAN protocol stack compared with the IP protocol stack. The 6LoWPAN has many features. Firstly, 6LoWPAN has an adaptation layer between the IP and MAC layer. The adaptation layer makes it possible for the IPv6 packets to transmit through the IEEE 802.15.4 physical layer with header compression and packet fragmentation techniques. Secondly, the TCP protocol is not used in 6LoWPAN because it not suitable for M2M applications [108]; instead, the User Datagram Protocol (UDP) can be adopted as the transport layer protocol due to its connectionless-oriented feature. Thirdly, the Internet Control Message Protocol v6 (ICPMv6) is used for the realisation of the routing and neighbourhood discovery messages [109]. The last feature is that 6LoWPAN applications have specific traffic requirements, so the network must be designed based on the specific demands and adhere to the low-power and low-rate requirements.

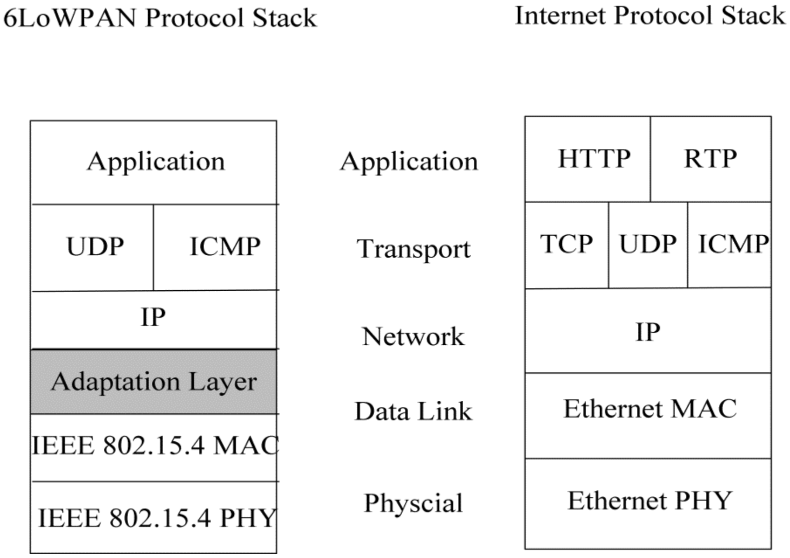


Fig 3-11 The 6LoWPAN and IP protocol stacks

3.3.2 Stateless Address Auto-configuration

In the M2M communication networks, a large number of M2M devices are normally distributed in a large-scale area, so traditional IP address configuration methods such manual configuration and Dynamic Host Configuration Protocol (DHCP) are not feasible in M2M networks. This is because manually configuring millions of devices is time-consuming; the DHCP requires an interaction between the devices and the DHCP server, which costs excessive energy and is not feasible either. Given these two constraints, IPv6 offers highly desirable solutions such as IPv6 address auto-configuration that can quickly assign either a link-local address or a global address to a machine-type device equipped with the IPv6 protocol stack. This is very useful for machine-type devices after their MAC addresses have been assigned by the manufacturer.

A 128-bit IPv6 address is divided into eight 16-bit fields, each of which is separated by a colon. It is understood that the second 64-bit section is known as the interface identifier, which adheres to the EUI-64 structure [107]. However, the IEEE 802.15.4 standard provides a 16-bit short MAC address that can be used to generate an IPv6 interface identifier. By using such an identifier and the prefix of an IPv6 address, a full IPv6 address can be presented. The full IPv6 address is presented in the following manner: Prefix :W : W : W : PAN_ID : 00FF:FE00: MAC. Prefix, W, PAN_ID and MAC occupy one 16-bit field, respectively. The last four fields (64 bits) are the interface identifier. For example, an IPv6 address can be expressed as 2000:0:0:0:1:0:0:23, where 2000 is the prefix; 1 is the PAN_ID; 23 is the MAC address; and the remainders are 0. In particular, 1:00FF:FE00:23 is the interface identifier.

The interface identifier can be generated using a PAN_ID and a MAC address. The generation process can be seen from Fig 3-12. A 16-bit MAC address and a 16-bit PAN_ID are both attached with eight zeros. After that, another two 8-bit hexadecimal values 0xFF and 0xFE are padded in between the augmented PAN_ID and MAC address according to [107]. This newly created 64-bit is the IPv6 interface identifier. Together with a prefix specified by the user, an IPv6 address is created. In a nutshell, once a prefix, a PAN ID and a MAC address are known by a machine-type device, either a link local IPv6 address or a global IPv6 address can be automatically generated without manual or dynamical configuration. Moreover, the adaptation layer plays a significant role in obtaining and generating IPv6 addresses. For example, on one hand, the adaptation layer needs to compute the MAC address and PAN_ID from an IPv6 address in the IP layer and transmit to the lower layer; on the other hand, the adaptation layer is also required to generate a corresponding IPv6 address to pass the IP layer using a prefix, a MAC layer and a PAN ID.

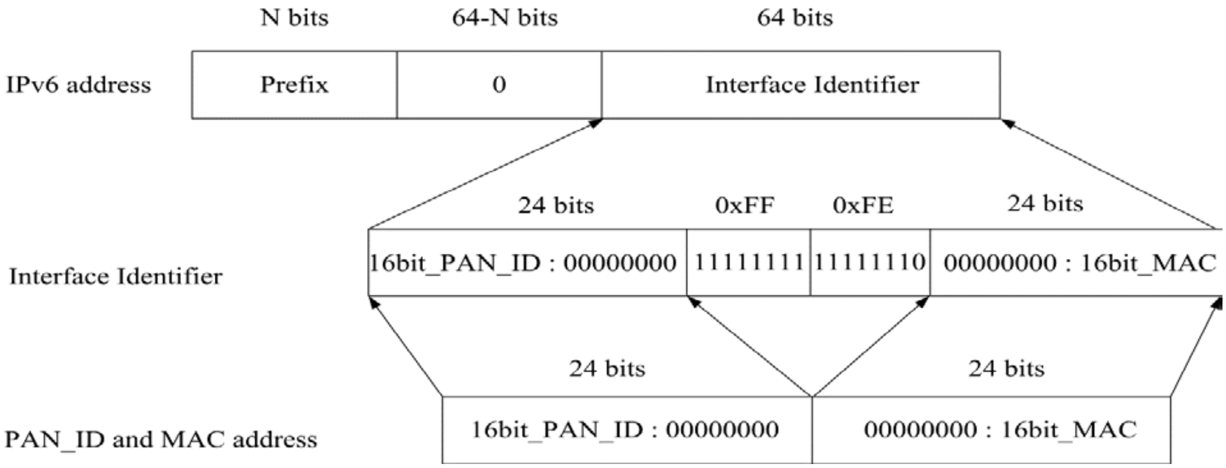


Fig 3-12 IPv6 address interface identifier generation process

3.3.3 IPv6 Header Compression and Restoration

One shortcoming of the 6LoWPAN protocol is the oversized header that limits the transmission of the IPv6 packets in the sensor network. An IPv6 header will occupy 50% of an IEEE 802.15.4 MAC payload and leaves only a small proportion of the payload size for actual data. Although small payloads can be transmitted using IEEE 802.15.4 packets, the channel utilisation tends to decline and batteries may drain fast because of transmitting small-sized packets. To solve this problem, the 6LoWPAN protocol introduces an adaptation layer. It not only receives the traffic coming from the MAC layer and relays it to the IP layer, but receives traffic sent from the IP layer and sends to the MAC layer. The adaptation layer does not generate packets itself, but it plays a significant role in connecting the IP and MAC layer functionalities. RFC 4944 describes how the IPv6 packets can be transferred through the IEEE 802.15.4 wireless link [105]. Due to the large IPv6 header and MTU size, header compression and packet fragmentation is required to be performed in the adaptation layer. With these two functions, an IPv6 packet can efficiently be transmitted using the IEEE 802.15.4 MAC layer.

The RFC 4944 defines three types of sub-headers to tackle the incompatibility between the IP protocol and the IEEE 802.15.4 MAC layer. The first is the mesh addressing sub-header that relays the MAC layer packets; the second is the compression sub-header that decreases the size of a large IPv6 header; the third is the fragmentation sub-header that fragments the IPv6 MTU and transmits it over several 802.15.4 packets. The sub-headers are shown in Fig 3-13. For simplicity, the mesh and fragmentation sub-headers are not considered in this work, and static routing is used because the mesh routing implementation is beyond the scope of this study. The fragmentation occurs when large-size payloads are required to be transmitted.

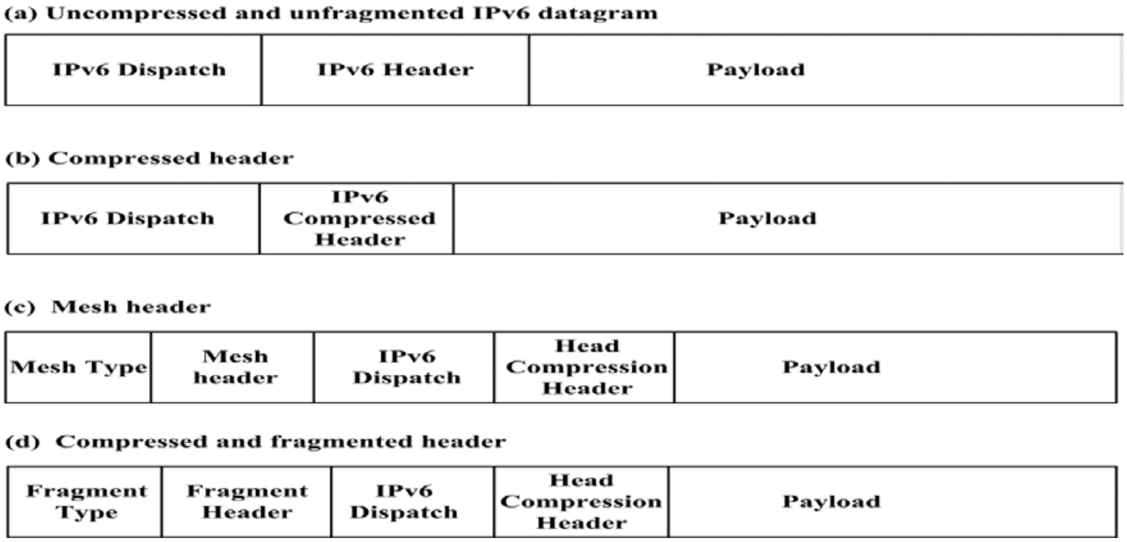


Fig 3-13 6LoWPAN sub-headers

There are two ways to compress the header: stateless header compression and context-based header compression [110]. The first is often used to compress link local IPv6 addresses, while the second is usually adopted to compress global IPv6 addresses. The reason for context-based header compression is because most IPv6 packets are transmitted to external nodes beyond the LoWPAN, so extra protocols from the higher layers such as UDP and application protocols are required. This research implemented the stateless header compression. The stateless IPv6 header compression follows a number of directives defined in [105]. To effectively explain how the IPv6 header compression works, it is necessary to understand the IPv6 header structure and the mapping process between the IPv6 original header and compressed header. Since multiple devices may share the same information within a PAN, it is possible to remove some of the fields in the IPv6 header. Fig 3-14 A depicts the IPv6 header with different fields. As such, IPv6 header compression can be accomplished in the following manner.

Version: this field should be omitted as it is IPv6 for all packets.

Traffic Class: this field is usually zero, so there is no need to transmit. Unless the field is required, it is transmitted with full eight bits.

Flow Label: this field is not transmitted unless told otherwise.

Payload Length: there is no need to transmit this field becaue it can be derived from other fields such as the MAC layer frame length.

Next Header: the possibilities for this field are the UDP, TCP and ICMPv6, so only two bits are needed to represent these three protocols. In particular, if other protocols are involved, this eight bits need to be sent through the network.

Hop limit: as the number of hops is important in recording how a packet traverses the network, it therefore cannot be omitted, and needs to be transmitted with full eight bits.

Source and Destination Addresses: whether these two addresses are compressed or not depends on the Source Address Encoding (SAE) and Destination Address Encoding (DAE) values as shown in

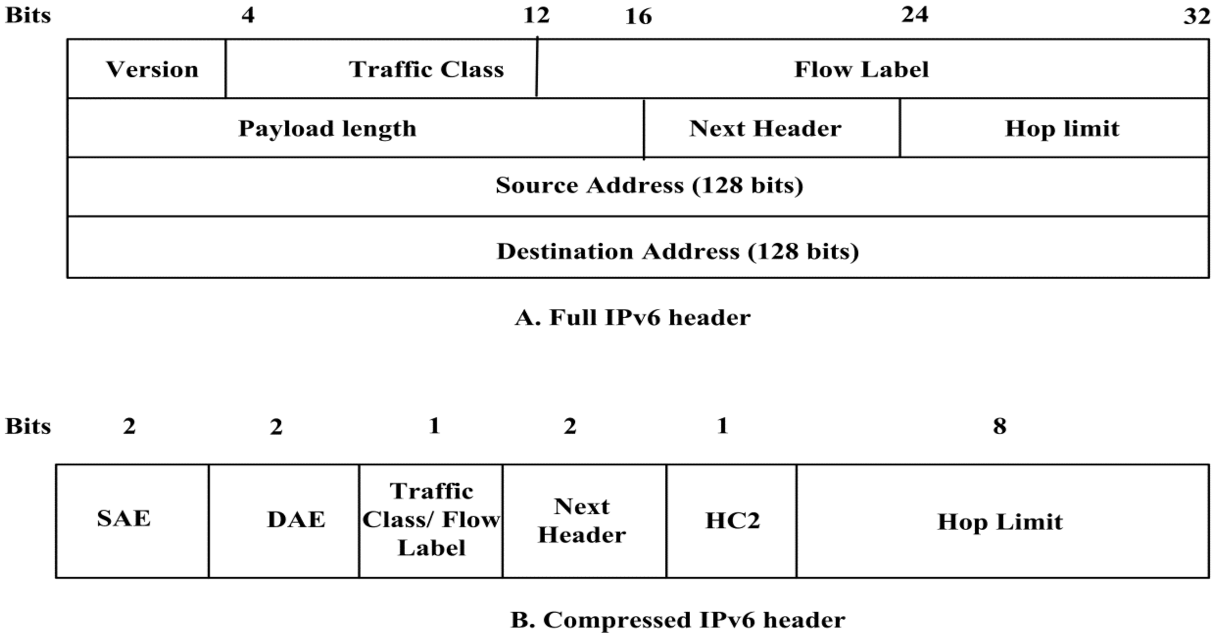
Table 3-3. Due to these two values, a complete IPv6 packet can be compressed. Once a full IPv6 packet has been received by the adaptation layer, the source and destination IPv6 addresses, as well as other fields, are retrieved so that a compressed IPv6 header can be made.

Table 3-3 Head compression SAE and DAE values

SAE or DAE value	Prefix	Interface Identifier
00	Sent in-line	Sent in-line
01	Sent in-line	Derived from MAC address
10	Link local FE80::/64	Sent in-line
11	Link local FE80::/64	Derived from MAC address

Following the above process, the 40-byte IPv6 header can be compressed to a two-byte header, reserving the hop limit and the compressed header. Fig 3-14 shows the compressed IPv6 header.

The number of bits indicates whether a field in a non-compressed IPv6 header needs to be compressed or not. For example, a zero in the Traffic Class and Flow Label field means this field should be compressed; otherwise, it should not be compressed.



A. Full IPv6 header

B. Compressed IPv6 header

Fig 3-14 IPv6 header structure and the compressed IPv6 header

The IPv6 header restoration is the reverse process of the IPv6 header compression. Once a packet is received by the adaptation layer, e.g., with a MAC header (the source and MAC addresses have been stored) being stripped off, a packet with a compressed IPv6 header will be retrieved by the adaptation layer, so that the SAE and DAE values, together with PAN IDs, are obtained. A prefix can be acquired from a local node once the node is in the same sub-net. With the prefix, the source and destination addresses and the PAN ID, a complete IPv6 header can be re-built. This IPv6 packet will then be forwarded to the IP layer.

A full IPv6 header compression is illustrated in Fig 3-15. There are two steps to pass the IPv6 packet through the MAC layer. In step one, upon receiving an IPv6 packet from the IP layer, the adaptation layer retrieves all the necessary information from the IPv6 header such as the source and destination IPv6 addresses, the PAN ID and the prefix. The source and destination MAC addresses can be obtained from the interface identifier from the IPv6 addresses. In addition, the value of each field in the compressed header should be filled to generate the compressed header.

For example, if both the IPv6 addresses need to be derived from the MAC addresses, the SAE and DAE values are filled with 01; if there are no higher layer protocols; the next header field is zero. In step two, the MAC header can be generated and attached to the compressed header by using the MAC addresses and the PAN ID.

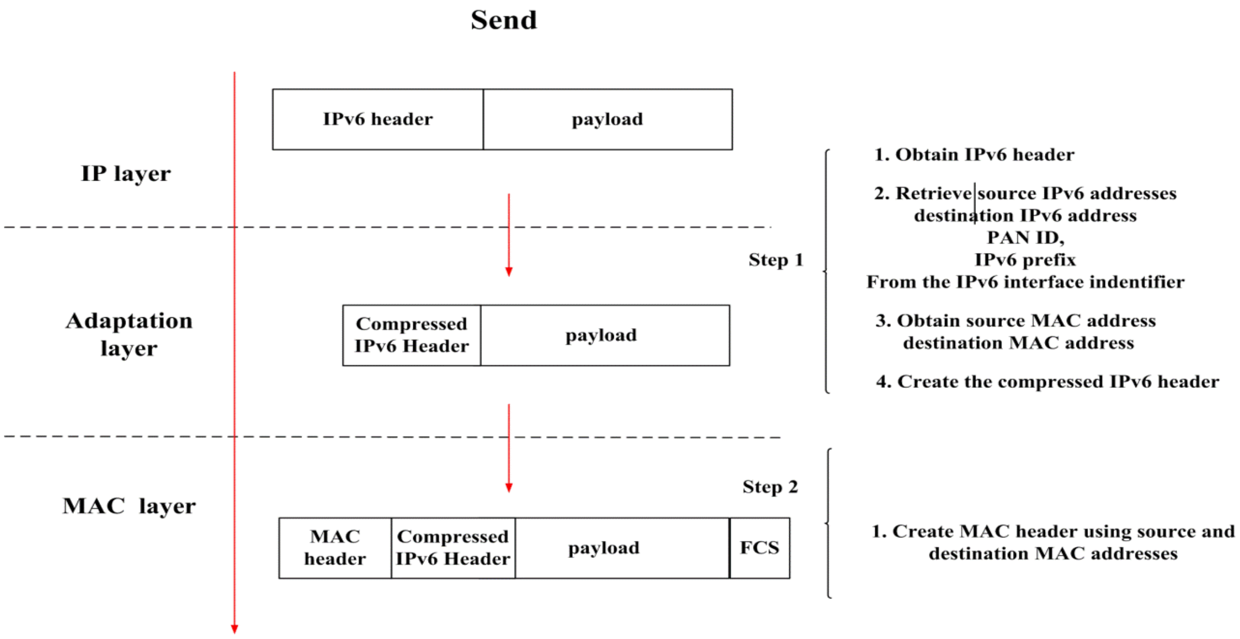

Send
IP layer
IPv6 header
payload
Adaptation layer
Compressed IPv6 Header
payload
MAC layer
MAC header
Compressed IPv6 Header
payload
FCS
Step 1
1. Obtain IPv6 header
2. Retrieve source IPv6 addresses destination IPv6 address PAN ID, IPv6 prefix From the IPv6 interface indentifier
3. Obtain source MAC address destination MAC address
4. Create the compressed IPv6 header
Step 2
1. Create MAC header using source and destination MAC addresses

Fig 3-15 IPv6 header compression

On the other hand, the header restoration process is presented in Fig 3-16. There are also two steps in this process. In step 1, after receiving the MAC frame, the source and destination MAC addresses, as well as the PAN ID, are obtained. This information will be passed to the adaptation layer to create the IPv6 addresses. In step 2, when the frame with the compressed IPv6 header is received by the adaptation layer, the fields of the compressed header are retrieved so as to restore the IPv6 header. For example, the MAC addresses and PAN ID are used to create the interface identifier. The IPv6 prefix is then obtained from the receiver itself since the sender and receiver are in the same subnet, so IPv6 addresses are created by combining the prefix and the interface identifier. Similarly, the whole IPv6 header can be restored by using the values of the fields in the compressed header. After the IPv6 addresses are generated, the traffic class, flow label and hop limit are used to recover the complete IPv6 header.

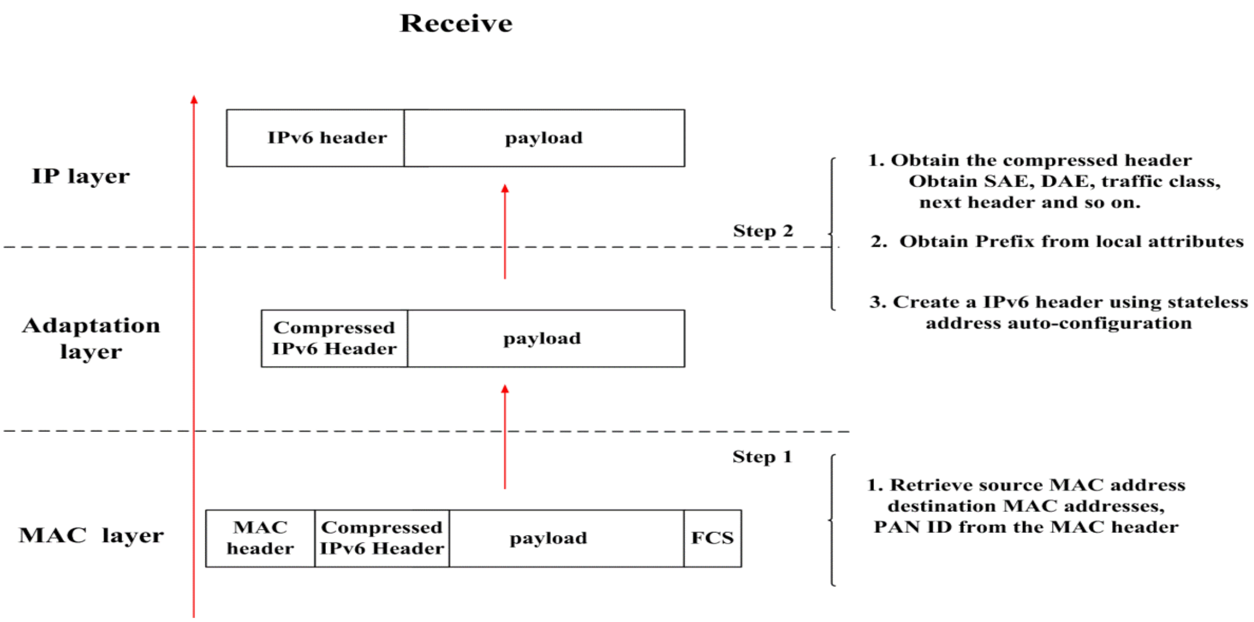

Receive
IP layer
IPv6 header
payload
Step 2
1. Obtain the compressed header Obtain SAE, DAE, traffic class, next header and so on.
2. Obtain Prefix from local attributes
3. Create a IPv6 header using stateless address auto-configuration
Adaptation layer
Compressed IPv6 Header
payload
Step 1
1. Retrieve source MAC address destination MAC addresses, PAN ID from the MAC header
MAC layer
MAC header
Compressed IPv6 Header
payload
FCS

Fig 3-16 IPv6 header restoration

3.3.4 Node Models

To evaluate the performance of the proposed 6LoWPAN network for M2M applications, a computer simulation is a cost-effective tool to evaluate the performance of proposed architecture and protocol. One widely accepted simulation tool is Optimised Network Engineering Tools (OPNET), which is a discrete-event simulation platform [111]. OPNET has been used by many scholars to obtain simulation results for performance analysis before deploying network devices in the real world. Specifically, the OPNET simulation is driven by the network events scheduled at points in time. As time goes by, the events set by the kernel procedure are triggered and executed. This process reflects how a real system performs if the configuration of the OPNET is in accordance with the specifications.

OPNET has been featured as a hierarchical modelling tool consisting of three domains: the network domain, the node domain and the process domain. The network domain regulates the topology in which the nodes and communication links are properly organized. The node domain represents the different nodes that are the basic communication entities in the network domain and allows packets to flow through different modules. The process domain is the lowest level of simulation, in which all the functionalities and connections are implemented in a Proto C language. A process model is comprised of finite state machines in which each state represents a logical operation carried out on data and each condition triggers the execution of code in each state.

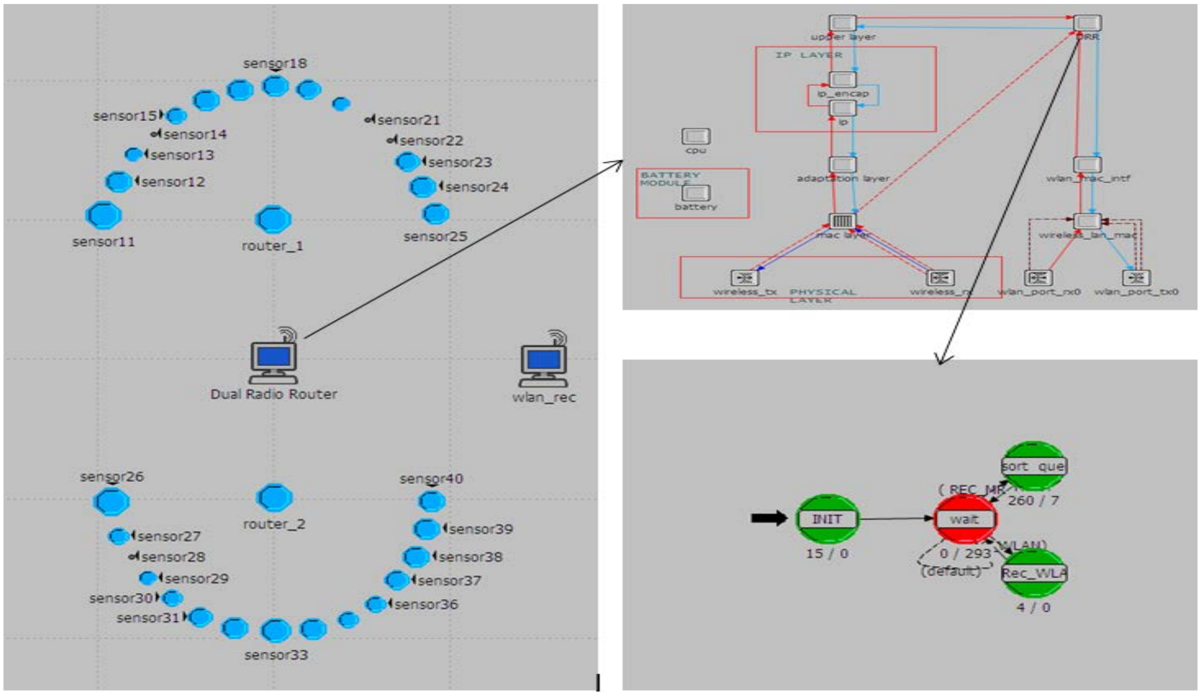


Fig 3-17 OPNET three domains

At time of model development, no 6LoWPAN model is available in the OPNET modeller library, so it needs to be developed. Thanks to the implementation of the IEEE 802.15.4 MAC layer of open-zb [112]. a new 6LoWPAN model was developed in this work using the open-zb model and other models from the OPNET model library. Open-zb, based on the IEEE 802.15.4 standard and ZigBee specifications, is open-source software, so employing it to develop the 6LoWPAN node is an ideal choice. The detailed node model development process is described below.

In addition, before implementing a 6LoWPAN node model, the internal model structures, such as the modules and packet streams, need to be carefully considered. As illustrated in Fig 3-18, the 6LoWPAN node model has been implemented according to the 6LoWPAN protocol stack (as shown in Fig 3-11) and combines two different node models. The first built-in IP layer model is truncated from an Ethernet node model named Ethernet_ip_station_adv from the standard OPNET library; the MAC layer model is obtained from the open-zb node model. The adaptation and the upper layer models were developed from scratch. In particular, since the IEEE 802.15.4 standard defines three types of devices (i.e., PAN coordinator, FFD and RFD), the corresponding devices (i.e., PAN Coordinator, Router and End Device) models were developed, complying with the 6LoWPAN protocol structure.

Numerous changes were made in the model to meet the requirements of the 6LoWPAN protocol stack requirement. Since the Ethernet model has an Address Resolution Protocol (ARP) layer located in the middle of a MAC and IP layer, how the ARP layer interfaces with the IP layer should be thoroughly investigated. Similarly, the open-zb node model has a network layer directly above its MAC layer, so it is necessary to understand how the Network layer interfaces with the IEEE 802.15.4 MAC layer. The two patterns reveal how an adaptation layer can be implemented as per the connection patterns in open-zb and the Ethernet node model. Moreover, the 6LoWPAN application layer node model is designed to interface with the IP layer and generate the different types of M2M traffic. The 6LoWPAN application layer implementation is referenced from the open-zb application layer model in terms of how to set the Interface Control Information (ICI) and traffic profiles. The open-zb application layer explains more details on how the open-zb node application generates traffic, thus this pattern can be applied to the 6LoWPAN node model sending packet flows to the IP layer.

The IP layer is the most complicated model in the OPNET library and consists of many functions such as TCP/IP protocol suite, dual-stack IPv4/IPv6, routing, ARP, fragmentation and Network Address Translation (NAT), as well as the routing policy and firewall filters. All these functions are integrated into these two modules sharing the same code operating in different modes. The OPNET document OPNETWORKS suggests that no modules should be added between the IP module and the ARP module; otherwise, it will be very difficult for debugging [113]. However, to interface the IP module with the open-zb MAC and PHY layer, the IP module needs to be separated from the ARP model as shown in Fig 3-18. This process proved to be extremely difficult, and the development process took a long time to connect the two modules in OPNET through debugging. More details about the model development are presented in Appendix C.

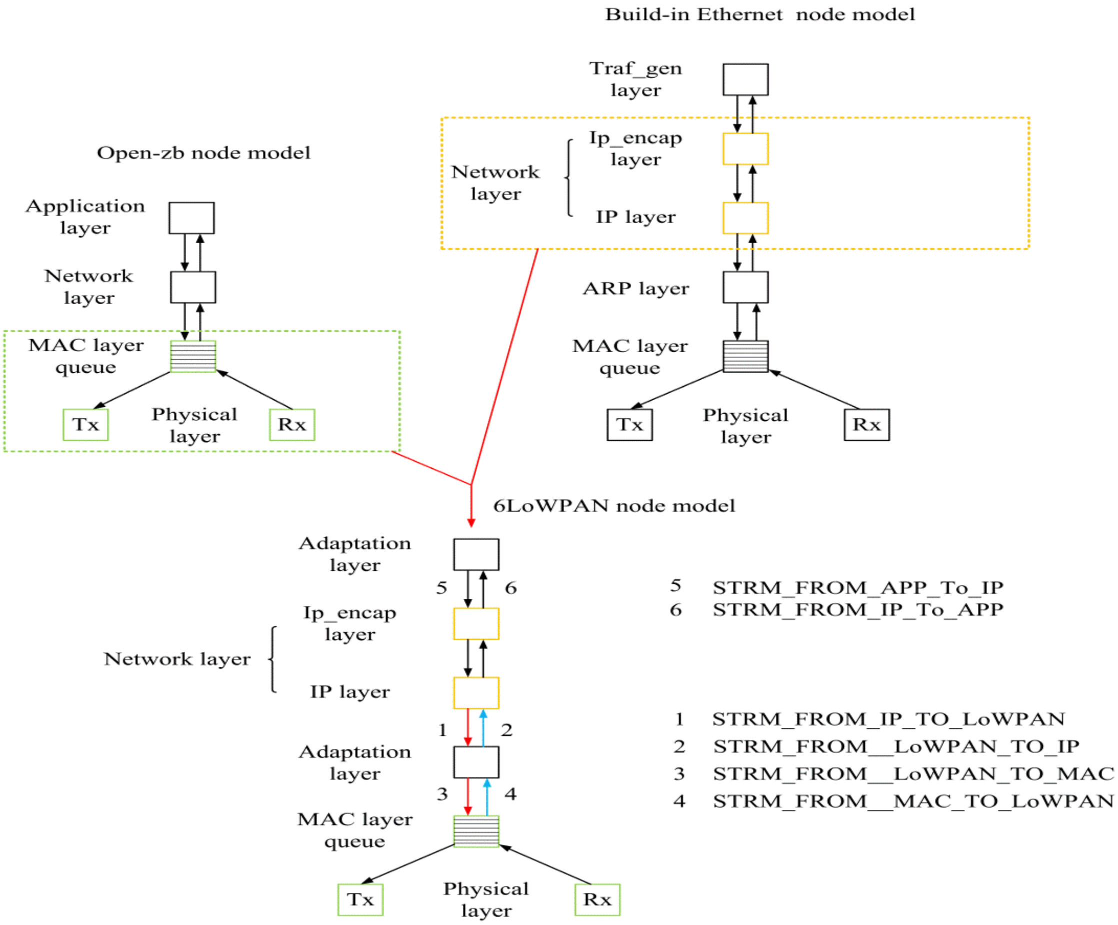


Fig 3-18 6LoWPAN OPNET node model and stream flows

Four packet streams for the adaptation layer are defined in the Header Block.

STRM_FROM_IP_TO_LoWPAN

STRM_FROM_LoWPAN_To_IP

STRM_FROM_MAC_To_LoWPAN

STRM_FROM_LoWPAN_To_MAC

These streams help transfer data packets between the IP and MAC layers. Another two packet streams connect the 6LoWPAN application layer and the IP layer, and provide communication between these two layers

STRM_FROM_IP_ENCAP_TO_ APP

STRM_FROM_APP_TO_IP_ENCAP

Moreover, the attributes have been created for the simulation configuration such that they can be promoted to the network level to enable multiple runs. For example, the open-zb node model supports the acknowledged and non-acknowledged traffic. To keep these functionalities, a corresponding change was made in the adaptation layer to control the ACK packets of the traffic. Many other attributes, such as IPv6 prefixes, were also integrated into the node model so that the stateless address auto-configuration can be used to generate the IPv6 addresses. A number of other modifications were also made to facilitate OPNET simulation, which are described below.

3.3.5 Process Models

According to the hierarchical OPNET modelling mechanism, all the functionalities and statistics in the simulation are driven by code in the process model [111]. The process mode contains all the code and is comprised of a series of finite state machines. To simulate a 6LoWPAN network where different node models are deployed in a distributed area, it is necessary to build different process models for the corresponding node models. This is because the RFD, FFD and PAN coordinator should operate as different entities, and the corresponding process models need to be developed to suit these needs individually. This section explains the implementation of the different 6LoWPAN process models in detail.

As mentioned before, to create 6LoWPAN models that interface with the IP layer, it is necessary to understand the techniques on how the IP model interacts with other layers. Some important fundamentals of interfacing the IP model were introduced in [114] especially regarding the lower layer and upper layer issues. The first critical procedure is that any process model wishing to connect to the IP model must register itself in a model-wide registry monitored by the IP model. The IP model, according to the OPNET official guide, is the most complex model in the model library because it integrates with other models and thus needs to be equipped with different network interfaces. As can be seen in Fig 3-18, the IP model consists of two OPNET entities: the ip_encap and ip model. These entities have two different functionalities [113]. The ip_encap creates the IPv6 header and is responsible for encapsulating upper layer packets and de-encapsulating lower layer packets, while the IP model searches a potential destination IP address in the routing table and forwards the packet from the ip_encap layer to the MAC layer. In addition, the IP model needs the upper and lower layers' model information before the simulation begins. This is because the IP layer requires information such as the number of physical layer interfaces in order to forward packets from the lower layer and be transportation layer protocols suitable for the specific applications. More details as to how to interface the IP model from the higher and lower layers can be found in Appendix A.

6LoWPAN End Device Process Model

The application process model is presented in Fig 3-19, and consists of five states: init, wait, traffic type 1, traffic type 2, traffic type 3 and receive packets. The functionalities of these states are explained below.

Init State: it mainly initiates the variables in the header block and registers this model in the model-wide registry used by the IP layer collecting the information from modules connected to the IP layer.

Wait State: it is a close-loop process and waits for a new packet arrival irrespective of where the packet comes from either the application layer or lower layer. Once a packet arrives, it either forwards it to the receive state or triggers a self-interrupt to generate traffic itself.

Traffic Type 1, 2 and 3: these three states can generate three types of traffic according to the specific traffic requirements. The traffic types can be configured in the OPNET node model and be obtained from the three states.

Receive State: this state deals with the packets received from the IP layer and records a number of statistics such as the number of packets received and the end-to-end delay.

In the process model, the IPv6 address generation and Interface Control Information (ICI) configuration are of great importance. To generate an IPv6 address and properly set the ICI value to meet implementation needs, modifying the IPv6-related files or attributes in the OPNET model library cannot be avoided. Two files, ip_addr_v4.ex.c and ip_addr_v4.h, have been used, containing sufficient functions to create IPv6 addresses and associate them with the ICI. The former is an IP address package and consists of several methods of generating the IPv4 and IPv6 network addresses, whereas the latter defines the prototypes and macros of the different addressing functions. In this process model, the function inet_address_create is used to create the IPv6 addresses, and it uses a MAC address to generate a corresponding IPv6 address, which is integrated with the ICI and sent down through the packet stream. Instead of transmitting an integer as an argument to inet_address_create to generate an IPv4 address, a structure is used as an argument to generate an IPv6 address.

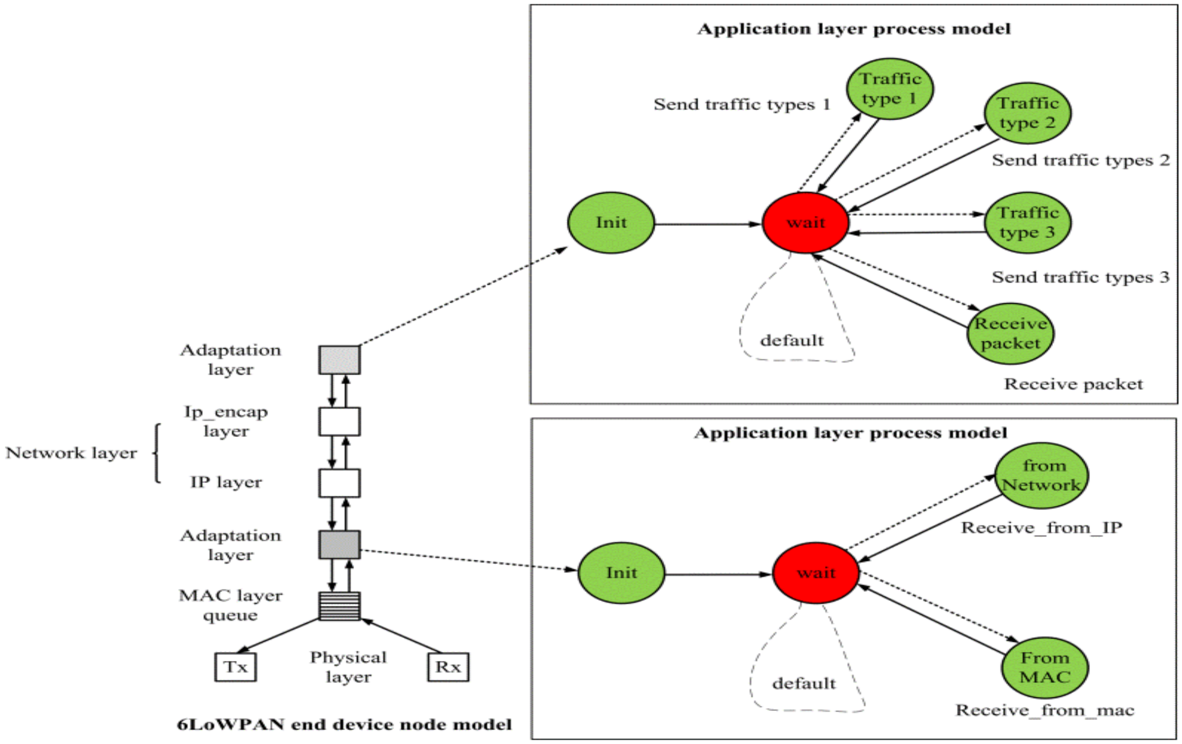


Fig 3-19 6LoWPAN OPNET end device node model with the application and adaptation layer process model

Fig 3-20 shows the flow chart of the 6LoWPAN application layer process model. As for the packet transmission, after the init state, the process model obtains the source and destination MAC addresses and traffic type from the attributes in the node model. Once the traffic type is determined, a destination IPv6 address and the ICI are generated using the OPNET kernel procedures. A payload size can be specified as per the traffic type. Afterwards, an IPv6 packet coupled with the ICI is sent to the IP layer. On the other hand, as for the packet reception process, upon receipt of a packet, the ICI information is obtained by a kennel procedure, indicating whether this is a right packet for this module or not. After that, the number of the received packets is counted before dropping the packet. Other statistics such as end-to-end delays are recorded in preparation for the performance analysis. The code can be found in Appendix D.

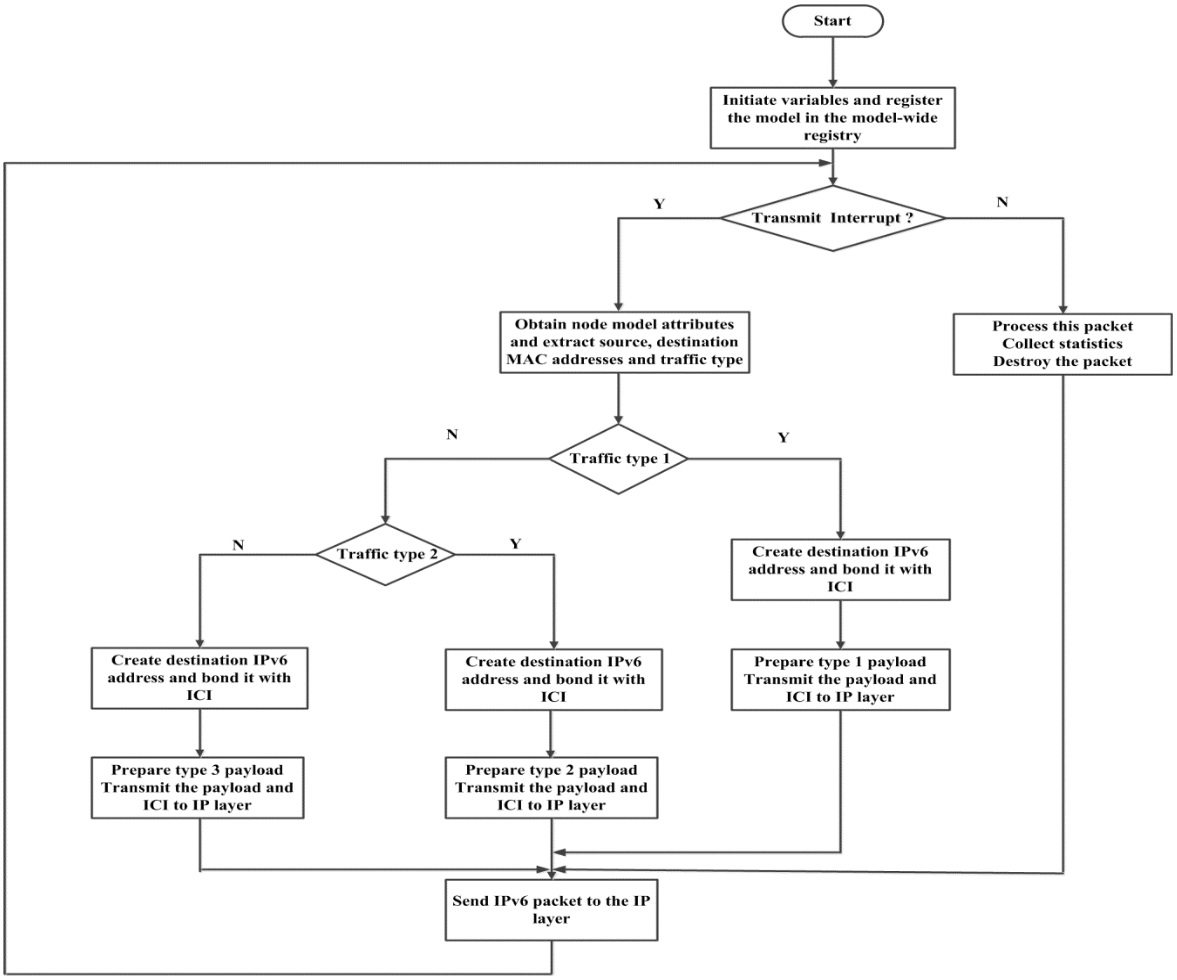

Start
Initiate variables and register the model in the model-wide registry
Transmit Interrupt ?
Y
N
Obtain node model attributes and extract source, destination MAC addresses and traffic type
Process this packet Collect statistics Destroy the packet
N
Traffic type 1
Y
N
Traffic type 2
Y
Create destination IPv6 address and bond it with ICI
Create destination IPv6 address and bond it with ICI
Create destination IPv6 address and bond it with ICI
Prepare type 1 payload Transmit the payload and ICI to IP layer
Prepare type 3 payload Transmit the payload and ICI to IP layer
Prepare type 2 payload Transmit the payload and ICI to IP layer
Send IPv6 packet to the IP layer

Fig 3-20 6LoWPAN application process model flow chart

In addition, the adaptation layer process model deals with more complex situations than the application layer process model. In other words, the adaptation process model not only receives the traffic coming from the MAC layer and relays it to the IP layer; but it receives traffic sent from the IP layer and re-sends to it the MAC layer. Unlike the application layer, the adaptation layer does not generate packets itself and connects the IP and MAC layer. The RFC 4944 describes how IPv6 packets can be transferred using the IEEE 802.15.4 wireless link. Due to the large IPv6 header and the MTU size, header compression and packet fragmentation techniques must be added to the adaptation layer. With these two functions, the IPv6 packet can efficiently transmit through the IEEE 802.15.4 MAC layer.

The adaptation layer process model has implemented the IPv6 header compression function and deals with two packet streams: the incoming stream and the outgoing stream. Therefore, the two functions, including the IPv6 compression and restoration, were developed from scratch. Once a packet is relayed to the adaptation layer, the first step is to determine if this packet is from the IP layer or the MAC layer. The function lowpan_receive_packet_from_ip is invoked when the packet is received from the IP layer; otherwise, the function lowpan_receive_packet_mac is invoked. The first function resolves the source and destination IPv6 addresses that calculate the source and destination MAC addresses, which need to be transmitted to the MAC layer, and then the IPv6 header is compressed. To efficiently convey the semantics between the two layers, ICI is also configured. Fig 3-21 describes how the IPv6 header compression is developed and how the compressed packet can be restored to an original IPv6 packet. For the IPv6 header restoration, once a compressed IPv6 is received from the adaptation layer, the corresponding information, such as the source and destination MAC addresses, is retrieved for the recovery of the IPv6 header. More precisely, the destination and source MAC addresses with the PAN ID are used by the stateless address auto-configuration mechanism to generate the IPv6 interface identifier. Combined with a prefix acquired from the node model attributes, a complete IPv6 header can be recovered, and it can successfully transverse the IP protocols stack. The information of restoring the IPv6 header is also used for the ICI between the adaptation layer and the IP layer.

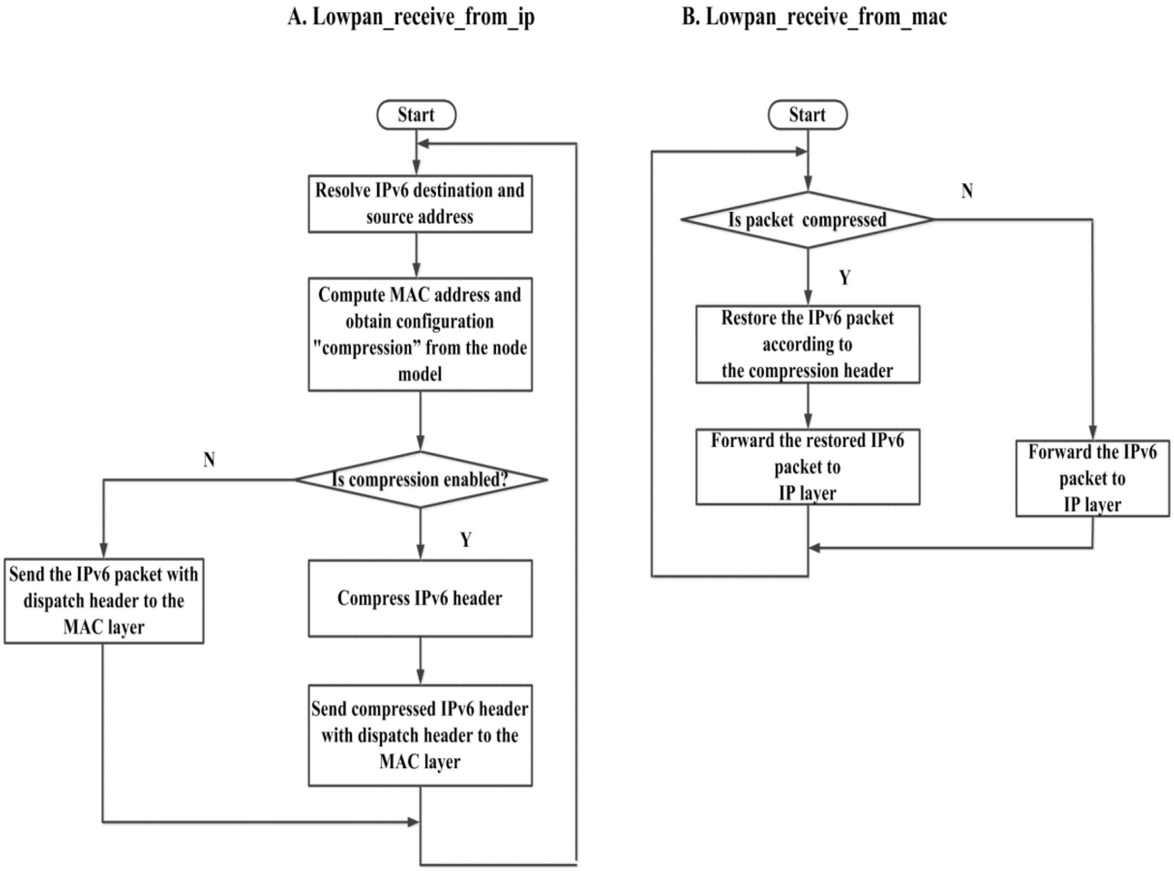

A. Lowpan_receive_from_ip
B. Lowpan_receive_from_mac
Start
Resolve IPv6 destination and source address
Compute MAC address and obtain configuration "compression" from the node model
Is compression enabled?
N
Y
Send the IPv6 packet with dispatch header to the MAC layer
Compress IPv6 header
Send compressed IPv6 header with dispatch header to the MAC layer
Start
Is packet compressed
N
Y
Restore the IPv6 packet according to the compression header
Forward the restored IPv6 packet to IP layer
Forward the IPv6 packet to IP layer

Fig 3-21 Flow charts of function lowpan_receive_from_ip and lowpan_receive_from_mac

3.4 6LoWPAN Model Validation

To validate the proposed model, a simplified network comprised of one 6LoWPAN node and one 6LoWPAN coordinator was developed as shown in Fig 3-22. The free space path loss model was used in the simulation where the packet inter-arrival rate varies from 0.5 to 2 pkt/sec. a basic analytical model is used to valid the initial simulation model. The 6LoWPAN simulation model is validated using a basic analytical model.

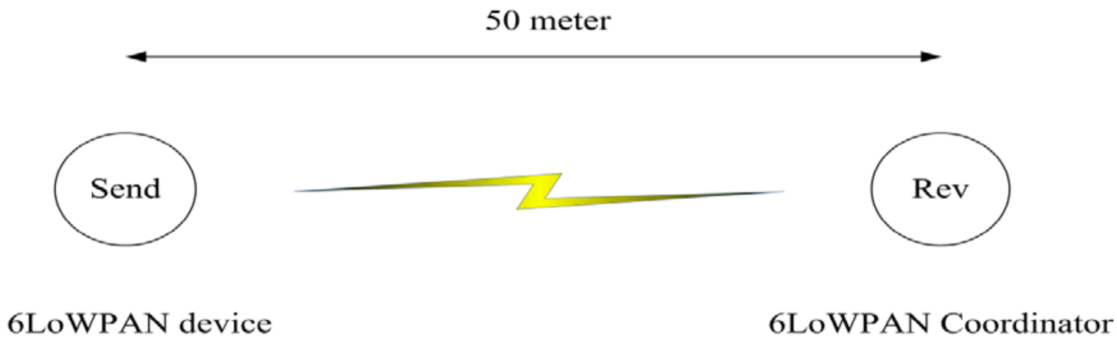


Fig 3-22 A simple network

The end-to-end delay is calculated in (3-3) :

$$T_{e2e} = T_{queue} + T_{backoff} + 2T_{CCA} + T_{data} + T_{ack\_wait} + T_{ack} + T_{LIFS} \tag{3-3}$$

According to the IEEE 802.15.4 standard, the MinBE is 3, so the number of number of backoff slots in the first time backoff should be within the interval (0, $2^3 - 1$). Since only one transmitter exists in the network, it always sends a packet successfully after the first backoff, so we consider the average number of backoff slots as 3.5. The cacluation is as follows.

Each backoff time slot is 20 symbols (80 bits), so $T_{backoff}$ is 3.5*80 bits/250000 bps =0.00112 s.

Each CCA is 8 symbols (32 bits), so $2T_{CCA}$ is 64 bits/250000 bps = 0.000256 s.

The packet size considered is 64 bytes, so T_{data} is 64*8 bits/250000 bps = 0.002048 s.

T_{ack_wait} is 216 bits/250000 bps = 0.000864 s.

T_{ack} is 88 bits/250000 bps = 0.000352 s.

T_{LIFS} is 160 bits/250000 bps = 0.00064 s.

As the model is expressed as an M/D/1 model by Kendall’s notation, T_{queue} is calculated as follows.

Table 3-4 Delay components of the end-to-end delay

Inter-arrival rate (pkt/s)	$T_{e2e\_simulation}$	$T_{e2e\_analysis}$	T_{queue} (ms)	$T_{backoff}$	$2T_{CCA}$	T_{data}	$T_{ack_{wait}}$	T_{ack}	T_{LIFS}
0.5	6.209	5.700	0.420	1.120	0.256	2.048	0.864	0.352	0.640
1	6.272	6.122	0.843	1.120	0.256	2.048	0.864	0.352	0.640
1.3	6.485	6.376	1.096	1.120	0.256	2.048	0.864	0.352	0.640
1.5	6.595	6.546	1.266	1.120	0.256	2.048	0.864	0.352	0.640
1.7	6.907	6.716	1.436	1.120	0.256	2.048	0.864	0.352	0.640
2	7.114	6.971	1.691	1.120	0.256	2.048	0.864	0.352	0.640

It can be seen from the table Table 3-4 that the analytical model results are close to the simulation data obtained from the OPNET model. The difference between the analytical and simulation results is due to use of number of backoff slots. In the simulation model the backoff window size varies randomly whereas in the analytical model the average value of 3.5 slots was used. The queuing delay slightly increases as the traffic load increases. The queuing, backoff and data transmission delays are the major components of the end to end delay.

3.5 Conclusion

This chapter introduced the 6LoWPAN standard adopted for M2M communications. It was shown that the IPv6 protocol can provide countless addresses and the routing mechanism for M2M devices. Since the 6LoWPAN protocol stack is built upon the short-range IEEE 802.15.4 standard, a comprehensive review of the 6LoWPAN standard was given including the Physical layer, MAC layer, topology and the access algorithm. The beacon-based mode and the cluster-tree topology were employed due to their potential for achieving a large-scale M2M area network. Further, due to the lack of the 6LoWPAN model and routing protocol in OPNET, these models had to be built from scratch, including the node models and process models. Meanwhile, the built-in OPNET IP module could be used first, and the other modules were developed based on it. To be in line with the 6LoWPAN standard and the RFC file 4944, the adaptation layer was developed, dealing with the packet header compression and stateless address auto-configuration. The process model contains the functions dealing with packet generation and packet receiving process, while the adaptation layer handles the IPv6 header compression and header restoration. Lastly, the model validation was presented. The analytical results agree with the simulation results, proving the effectiveness of the 6LoWPAN model. This chapter served as a cornerstone and paved the way for further performance analysis and algorithm development in the following chapters.

Chapter 4

Homogeneous and Heterogeneous Area Networks Design

4.1 Introduction

Chapter 3 introduced the IEEE 802.15.4 standard and the OPNET 6LoWPAN model. In this chapter, a 6LoWPAN-based M2M area network for IoT applications is proposed to serve M2M and IoT applications. Although 6LoWPAN networks can provide seamless IP connectivity for M2M end devices and achieve higher energy efficiency, the M2M area networks may encounter some intrinsic shortcomings of the IEEE 802.15.4 standard. One of the problems in an area network is that it cannot support higher traffic loads from a large number of connected devices. The previous studies on IEEE 802.15.4-based networks have found that the normalised throughput per node declines from in the star topology 0.15 to nearly 0.02 when the number of nodes increases from 10 to 45 in a cluster [115]. This decrease is due to the packet losses caused by intra-network collisions, which is an inherent feature of the CSMA/CA protocol [116, 117]. As for an efficient network design, the intra-network collisions discussed in Chapter 2 need to be managed to ensure the QoS requirements of M2M applications. The 6LoWPAN networks support short transmission distances, so multi-hop network architecture is needed when a longer transmission distance is required. The 6LoWPAN standard is part of the Low Power Wide Area Network (LPWAN) standard, where multi-hop networks will be more frequently used. In such a network, packet collision rates can rise due to the collisions between devices and between networks. In [102], it was found that the end-to-end throughput reduces from 140 kbps to 60 kbps as the number of hops increases from one to two hops, and it further drops to 20 kbps as the number of hops is increased to five.

In this chapter, a beacon-scheduling approach named the staggered link design based on the IEEE 802.15.4 standard was proposed to mitigate intra-network collisions. The staggered link design was first proposed in the IEEE 802.15.4 2006 standard. By using the staggered link design, the number of intra-network collisions can be reduced. During my research I found that the routers are the main bottleneck of the network where the contention level between the routers and the PAN coordinator is high. In order to reduce the contention level I developed two new packet aggregation techniques, to reduce the number of transmitted packets on the routers, thus further decreasing the level of intra-network collisions. Although the staggered link and packet aggregation techniques have been used and proposed separately by other researchers. In this work, I proposed a unique combined algorithm incorporating staggered link and packet aggregation techniques to minimise the collision level. This is combined algorithm is a novel approach not developed by any other researcher before

The rest of the chapter is organised as follows. Section 4.2 proposes the staggered link design and a packet aggregation technique, followed by the performance analysis of a multi-hop WPAN. Section 4.3 introduces a heterogeneous wireless sensor network and the analysis between a homogeneous WPAN and a heterogeneous WPAN is presented in terms of the end-to-end delay and the packet delivery rate. Section 4.4 concludes the chapter.

4.2 Intra-Network Collisions Mitigation

In this section, a staggered link design and a packet aggregation technique are presented. As mentioned, one of the challenges of an IEEE 802.15.4 multi-hop 6LoWPAN with the beacon-enabled mode is intra-network collisions, especially between beacons or between beacons and data frames. The collisions occur because beacon transmissions do not follow the CSMA/CA mechanism to access the channel, so if the beacons are not scheduled close to each other, then they could collide, thus corrupting beacons that cannot be decoded by routers or sensor nodes. As shown in Fig 4-1, it illustrates the two-hop 6LoWPAN with a cluster-tree topology used for mathematical analysis in the following sections. The 6LoWPAN coordinator has four clusters, each of which has a router responsible for synchronising eight sensor nodes. It can be seen that the routers have four collision zones; that is, the overlapping areas illustrated in red, green and blue dotted line. As routers 1, 2, 3 and 4 concurrently transmit beacon frames, so beacon collisions can happen, thus degrading the network performance. Specifically, each cluster has two collision zones that could lead to beacon collisions, data-to-beacon collisions and data packet collisions. The distance between the 6LoWPAN coordinator and the Router is around 50 metres, and the distance between each router and end device is also around 50 metres. The hidden node problem is also considered. Since there is no communication between the devices from different routers, the hidden node problem will not cause any negative impacts on the end devices. As for the routers, they are controlled by the PAN coordinator, so the staggered link design can schedule beacons to avoid the hidden node problem.

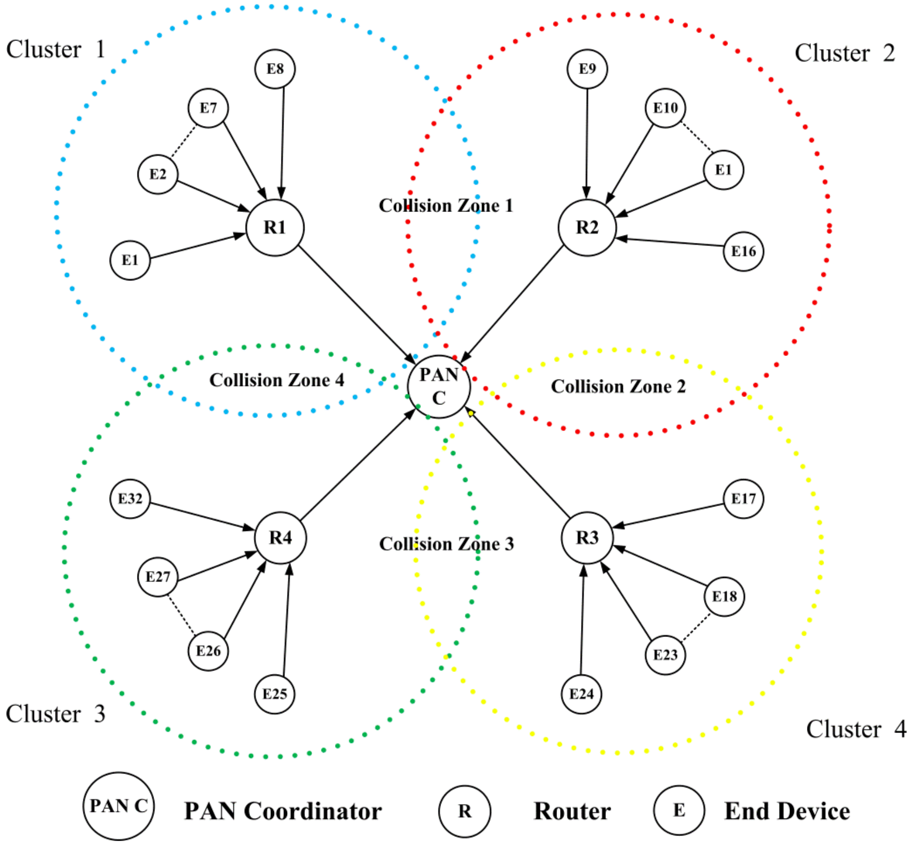


Fig 4-1 Intra-cluster collision zones in a cluster-tree WSN

4.2.1 Staggered Link Design and Packet Aggregation

As mentioned in Chapter 3, beacon-enabled IEEE 802.15.4 WPANs such as 6LoWPAN networks can adapt at least two system parameters, the BO and SO (defined in section 3.2), to determine the beacon interval (BI) and superframe duration (SD), as shown below.

$$\mathrm{BI} = \mathrm{aBaseSuperframeDuration} * 2^{\mathrm{BO}}, \tag{4-1}$$

$$\mathrm{SD} = \mathrm{aBase\ SuperframeDuration} * 2^{\mathrm{SO}}, \tag{4-2}$$

$$0 \leq \mathrm{SO} \leq \mathrm{BO} \leq 14.$$

When BO = SO = 0, BI = aBaseSuperframeDuration, which denotes the minimum number of durations in terms of the number of symbols (960 symbols). The CAP period consists of 16 time slots called aNumSuperframeSlots, as shown Fig 3-4. The duration of each slot is equivalent to $\mathrm{aBaseSlotDuration} \times 2^{\mathrm{SO}}$symbols, where aBaseSlotDuration is the smallest number of symbols in a time slot and equal to 60 symbols.

The proposed algorithm uses a time-division approach to assign suitable BO and SO values to the PAN coordinator and routers to avoid beacon collisions as shown in Fig 4-3. More precisely, the precise times of the beacon transmissions for the PAN coordinator and routers are calculated as follows. To ensure the transmission of the data packets from the routers, the BI of the PAN coordinator should be the round function of the packet inter-arrival time T_{inter} of the data packets. Let BO_{pan} be the BO for the PAN coordinator and N_{router} be the number of routers. Thus, BO_{pan} value can be calculated using ((4-3), where R_{data} denotes the symbol rate at 62500 symbol/sec, N_{super_slot} denotes aNumSuperframeSlots, which are 16 slots, and D_{basic} denotes aBaseSlotDuration, which is 15.36 ms/16 = 0.96 ms. To reduce the intra-network collisions between the PAN coordinator, routers and end devices, the number of routers from different depths can be obtained from ((4-4), where BO_{router} is the BO of the routers. It is obvious that the SD of a router is comprised of the length of a beacon (190 symbols) and the CAP, as shown in Fig 3-4.

$$\mathrm{BO_{pan}} = \left\lfloor \log_2\left(\frac{\mathrm{N_{router}} \times \mathrm{T_{inter}} \times \mathrm{R_{data}}}{\mathrm{N_{super\_slot}} \times \mathrm{D_{basic}}}\right)\right\rfloor, \tag{4-3}$$

$$\mathrm{N_{router}} = {}^{\mathrm{BO_{pan}}}\!/_{\mathrm{SO_{router}}} - 1. \tag{4-4}$$

$$\mathrm{SD_{router}} = \mathrm{CAP_{router}} + \mathrm{L_{beacon}}. \tag{4-5}$$

To use the time-division approach to scheduling the beacons of the routers, SD_{router} is equivalent to the BI of a router BI_{router} divided by the number of routers N_{router}, as shown in ((4-6). As a result, SD_{router} can be obtained by substituting CAP_{router} in ((4-5) with ((4-6), and thus (4-5 becomes into ((4-7). Since $\mathrm{SD_{router}} = \mathrm{N_{super\_slot}} \times \mathrm{D_{basis}} \times 2^{\mathrm{SO_{router}}}$, the value SO_{router} for routers can be obtained by ((4-8). Further, the SO and BO values for 6LoWPAN end devices are the same with routers.

$$\mathrm{CAP_{router}} = \frac{\mathrm{BI_{router}}}{\mathrm{N_{router}}} \tag{4-6}$$

$$= \frac{\mathrm{N_{super\_slot}} \times \mathrm{D_{basic}} \times 2^{\mathrm{BO_{router}}}}{\mathrm{N_{router}}},$$

$$\mathrm{SD_{router}} = \frac{\mathrm{N_{super\_slot}} \times \mathrm{D_{basic}} \times 2^{\mathrm{BO_{router}}}}{\mathrm{N_{router}}} + \mathrm{L_{Beacon,}} \tag{4-7}$$

$$\mathrm{SO_{router}} = \mathrm{Log_2}\left(\frac{2^{\mathrm{BO_{router}}}}{\mathrm{N_{router}}} + \frac{\mathrm{L_{Beacon}}}{\mathrm{N_{super\_slot}} \times \mathrm{D_{basic}}}\right). \tag{4-8}$$

Moreover, to use the time-division beacon scheduling approach, the IEEE 802.15.4 standard assumes a few basic conditions for a cluster-tree 6LoWPAN network that maintains time synchronisation between the PAN coordinator and the routers. In other words, there are two rules for the deployment of a beacon scheduling scheme. The first is that a router should maintain an incoming superframe and an outgoing superframe, which must not overlap with each other. The second rule is that any outgoing superframe coming from any router must not overlap when those nodes are within communication range. These two rules mean that the timing of these outgoing superframes should be accommodated within the length of one BI of the PAN coordinator without overlapping. The incoming and outgoing superframes are shown in Fig 4-2. It can be seen that the start time of the outgoing superframe is later than the incoming superframe.

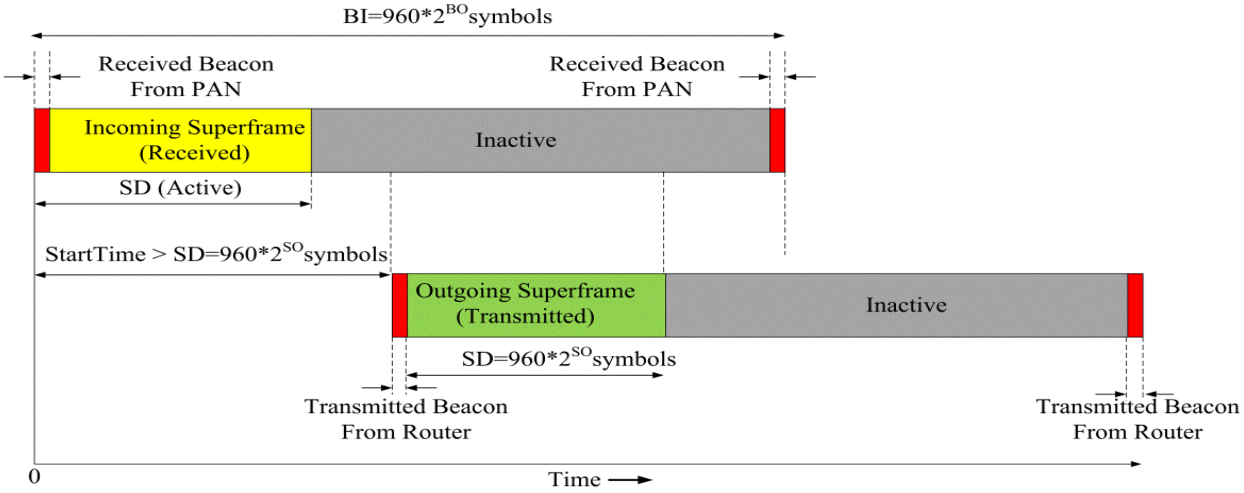

BI=960*2^BO symbols
Received Beacon From PAN
Received Beacon From PAN
Incoming Superframe (Received)
Inactive
SD (Active)
StartTime > SD=960*2^SO symbols
Outgoing Superframe (Transmitted)
Inactive
SD=960*2^SO symbols
Transmitted Beacon From Router
Transmitted Beacon From Router
0
Time

Fig 4-2 Incoming and outgoing superframe structures.

As such, it is possible to use the above rules to create a large-scale cluster-tree wireless sensor network. Fig 4-3 shows the time-division beacon scheduling structure of Fig 4-1 to adjust the precise time for the beacon transmissions. As can be seen in the figure, the different starting times of the beacon transmissions of the routers can be used to avoid beacon collisions using the above rules. Specifically, the starting time of each router including the PAN coordinator can be calculated as follows. Let $\mathrm{T_{offset\_pan}}$ and $\mathrm{T_{offset\_i}}$ be the starting time of the beacon of the PAN coordinator and the ith router, respectively. $\mathrm{T_{offset\_pan}}$ starts at the beginning of the superframe, while $\mathrm{T_{offset\_i}}$ is scheduled by（4-9）, where $\mathrm{SD}_{router_{i-1}}$ denotes the $(\mathrm{i}-1)$th routers node.

$$\mathrm{T_{offset\_i}} = \left\{\begin{array}{ll} \mathrm{T_{offset_{pan}}} + \dfrac{\mathrm{L_{beacon}}}{\mathrm{R_{data}}}, & \mathrm{i} = 1 \\ \mathrm{T_{offset_{pan}}} + \dfrac{\mathrm{L_{beacon}}}{\mathrm{R_{data}}} + \mathrm{SD}_{router_{\mathrm{i}-1}} & \\ & \end{array}\right\} 2 \leq \mathrm{i} \leq \mathrm{N_{coord}} \qquad (4\text{-}9)$$

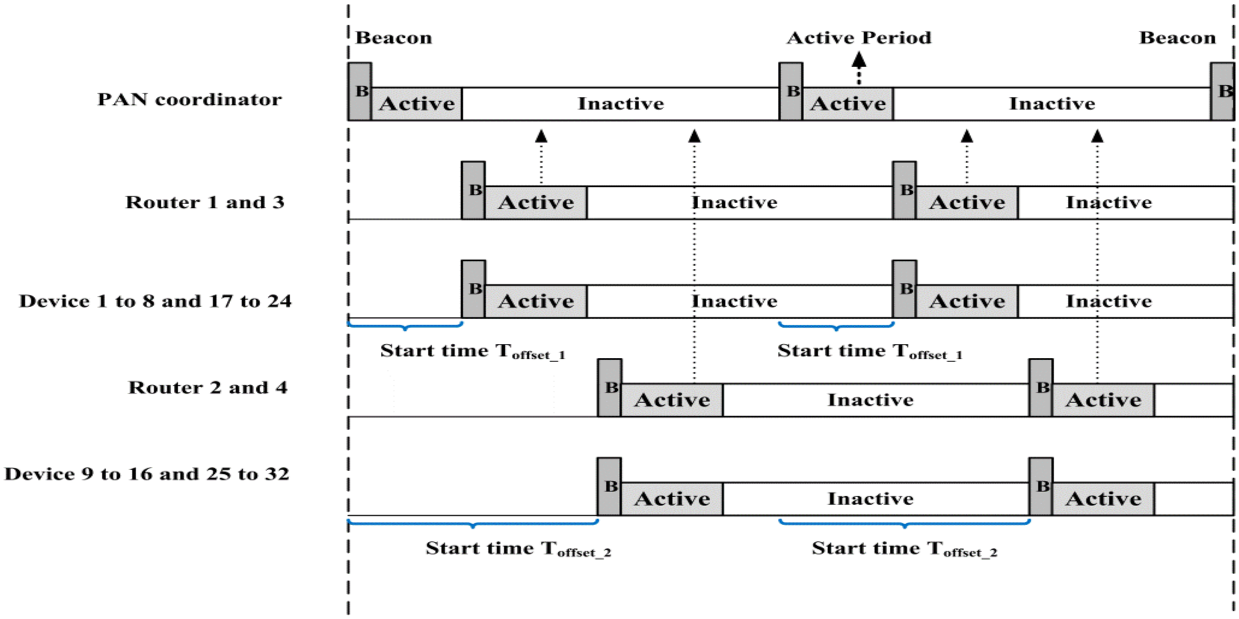

Beacon
Active Period
Beacon
PAN coordinator
B
Active
Inactive
Router 1 and 3
Device 1 to 8 and 17 to 24
Start time T_{offset_1}
Router 2 and 4
Device 9 to 16 and 25 to 32
Start time T_{offset_2}

Fig 4-3 Beacon scheduling for the four routers of Fig 4-1

These rules can be summarised into an algorithm describing how to assign a suitable value to the PAN coordinator and routers, as shown in Fig 4-4.

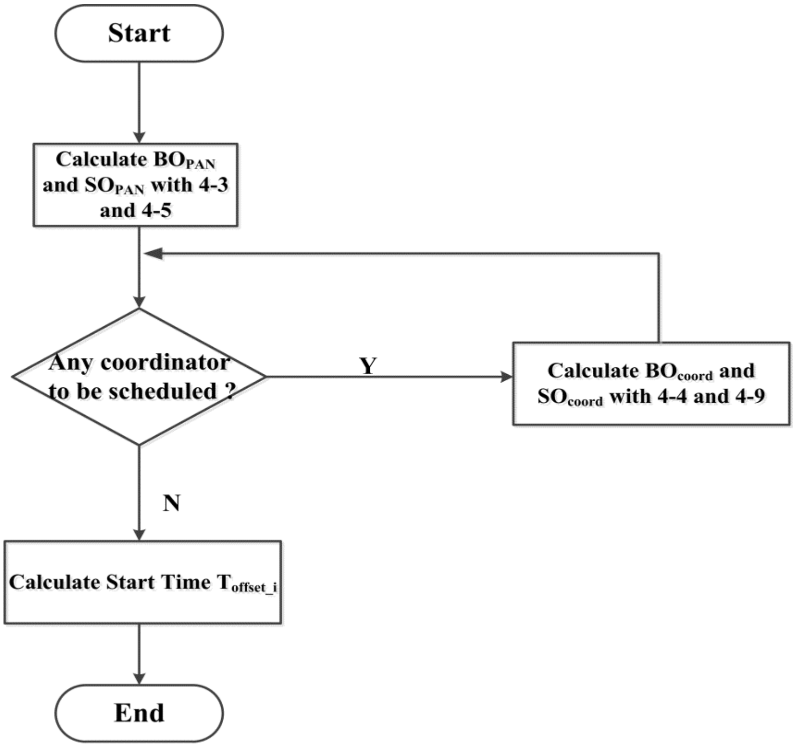

Start
Calculate BO_{PAN} and SO_{PAN} with 4-3 and 4-5
Any coordinator to be scheduled ?
Y
Calculate BO_{coord} and SO_{coord} with 4-4 and 4-9
N
Calculate Start Time T_{offset_i}
End

Fig 4-4 Beacon scheduling algorithm.

To further reduce the number of intra-network collisions, a packet aggregation technique is introduced. Aggregating small-size payloads into a large packet can reduce packet collision probability. Frame aggregation, or data fusion, plays a significant role in decreasing the number of packets and elevate channel utilization [118]. Since the 6LoWPAN standard has the option of using a header compress technique to reduce the 40-byte IPv6 header into 2 bytes, besides the 25-byte physical header and 21-byte MAC header, the remaining payload size is 81 bytes (the total packet size is 127 bytes). Since the payload size of certain M2M applications can be as small as 25 bytes, it is possible that three payloads can be aggregated into an IEEE 802.15.4 payload. As such, supporting more data in one payload with the aggregation technique could save more energy than constantly sending small-sized packets. In this work, the routers are used to aggregate the packets generated from the end devices. To do this, the aggregation algorithm is implemented in the adaptation layer of the 6LoWPAN router, as shown in Fig 4-5. In this section, the end device payload size used in the algorithm is 25 bytes, so the aggregated payload size in the router is 75 bytes.

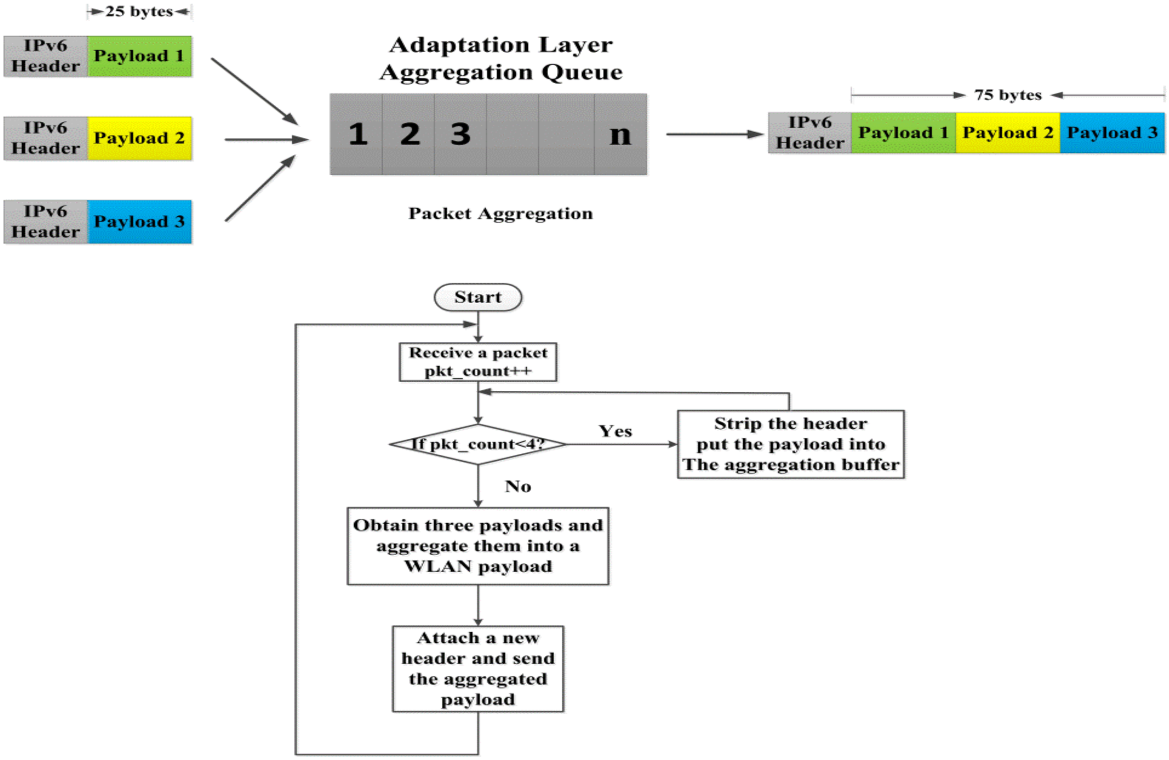


Fig 4-5 Flow chart of the packet aggregation algorithm

4.2.2 Simulation Setup

This section analyses the performance of the proposed staggered link design with a fixed packet aggregation technique. The simulation is performed in the OPNET Modeller 17.1 using the 6LoWPAN model as described in Chapter 3. In particular, the key parameters affecting the simulation performance, such as BO_{pan}, SO_{pan}, and SD_{coord} are calculated using (4-1） to（4-9）. As the R1 and R3 routers are far apart, it is possible to use the same BO and SO values. In other words, special reuse is considered to expand the communication coverage, so that the R1 and the R3 routers share the same starting time; also the R2 and the R4 routers share the same starting time. The key simulation parameters are listed in Table 4-1. The simulation model used multiple seed values for a single data point, and the simulation results are plotted with a 95% confidence interval.

Table 4-1 Key simulation parameters

Group Name	**Parameter**		**Value**
Network	Hop		3
	Number of nodes		32
	Standard		6LoWPAN
	Operating Frequency		2.4 GHz
Propagation model	Free space path loss		
PAN coordinator	BO		5
	SO		3
Router	BO		5
	SO		3
	Schedule Start time	R1	0.12289 s
		R2	0.24577 s
		R3	0.12288 s
		R4	0.24578 s
	Non-schedule Start time	R1	0.12290 s
		R2	0.12287 s
		R3	0.12288 s
		R4	0.12290 s
	Aggregated packet payload size		75 bytes
End device	Packet size		25 bytes
	Packet generation		Exponentially distributed
	Transmission Power		1 mw
	Packet inter-arrival rate		0.5, 1, 1.5, 2, 2.5 and 3 pkt/s

The simulation network is depicted in Fig 4-1. It can be observed that a two-hop wireless area network is used to simulate the multi-hop scenario with different traffic loads. Three scenarios are involved in the simulation. Scenario 1 does not include any proposed algorithms, meaning that the beacons are not scheduled. Links are intentionally arranged into beacon-to-beacon and beacon-to-data collisions to show that the intra-network collisions can degrade the network's performance. Scenario 2 uses the proposed staggered link design to mitigate the intra-network collisions. Scenario 3 combines the packet aggregation technique with the staggered link design to further reduce the probability of the intra-network collisions.

To explicitly show how the proposed algorithms decrease the number of intra-network collisions, scenarios 1, 2 and 3 are depicted in Fig 4-6. As mentioned before, the routers' outgoing superframe starting times are scheduled so that the packet transmission times do not overlap with that timing of the PAN coordinator. Moreover, these outgoing superframes cannot collide since the corrupted beacons cannot be decoded by the end devices. For this reason, scenario 1 arranges the router's start times in such a way: router 1 and router 3 are arranged into beacon-to-data collisions, and router 2 and router 4 are arranged into beacon-to-beacon collisions, as shown in Fig 4-6. In contrast, scenario 2 and scenario 3 use the proposed staggered link to shift the superframe durations backward in order to avoid intra-network collisions. In other words, the beacons and data packets from different routers will not collide.

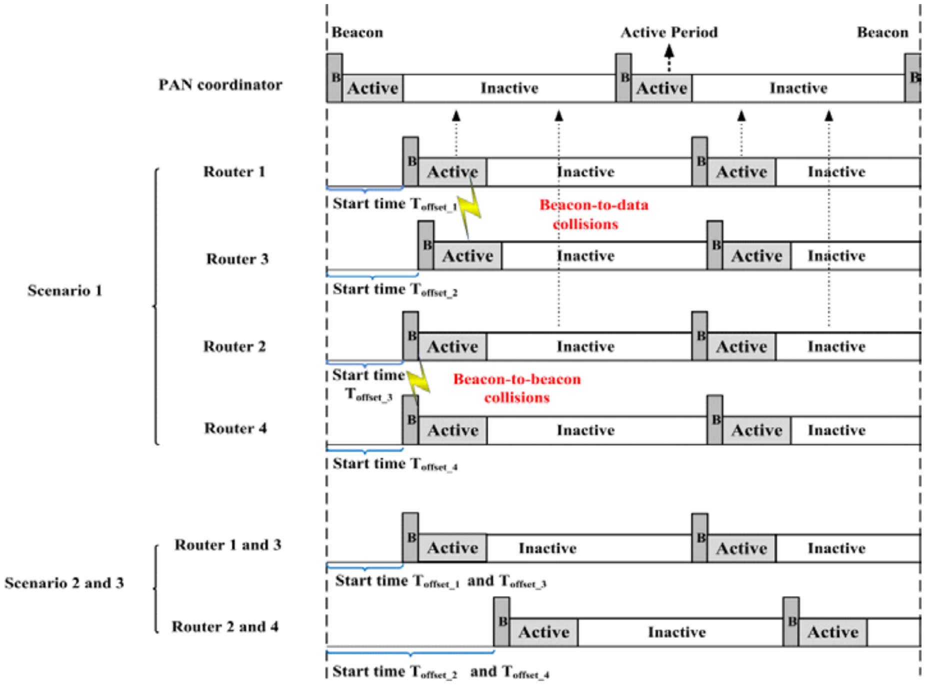

Beacon
Active Period
Beacon
PAN coordinator
B
Active
Inactive
Router 1
Start time T_{offset_1}
Beacon-to-data collisions
Router 3
Start time T_{offset_2}
Scenario 1
Router 2
Start time T_{offset_3}
Beacon-to-beacon collisions
Router 4
Start time T_{offset_4}
Router 1 and 3
Start time T_{offset_1} and T_{offset_3}
Scenario 2 and 3
Router 2 and 4
Start time T_{offset_2} and T_{offset_4}

Fig 4-6 Non-staggered and staggered links for simulation scenarios 1, 2 and 3

To evaluate the performance of the network and the proposed algorithms, the following several metrics are used.

- Packet delivery ratio: it is the ratio of the number of packets received by the PAN coordinator to the total number of data packets generated by all of the end devices. This metric indicates the reliability and the scalability of the data collection process.
- End-to-end delay: it is defined as the time difference between the time when an end device generates a data packet to the time when the packet is correctly received by the PAN coordinator. This metric represents the timeliness of the system.
- Number of packet collisions: it is defined as the total number of data packets experiencing collisions while contending the channel using the CSMA/CA protocol. This metric characterises the effectiveness of the CSMA/CA protocol. The hidden node problems are considered.
- Number of retransmissions per node: it is defined as the total number of retransmissions from the end devices and routers caused by data or ACK packet losses. This metric also measures the reliability of the network, and is in line with the IEEE 802.15.4 standard, which is set to three by default.
- MAC queuing delay: it is defined as the time difference between the instant a packet is inserted into the MAC queue to the successful transmission time of the packet. This metric represents the main component of the end-to-end delay.
- MAC queue length: it is defined as the average number of packets staying in the MAC queue waiting for transmission. This is a key indicator of network loading conditions.

4.3 Performance Analysis of the Proposed Algorithms

The following section analyses the simulation results and evaluate the effectiveness of the proposed techniques for a multi-hop wireless sensor network. Three scenarios are compared to show the effectiveness of the multi-hop network collision avoidance technique. The performance of the network is also examined for varying traffic loads and cluster densities.

4.3.1 Effects of Varying Traffic Loads

Packet Delivery Ratio

Figure 4-7 presents the packet delivery ratios for three scenarios: scenario 1 (red line staggered link-,agg-), scenario 2 (blue line staggered link+ agg-) and scenario 3 (green line staggered link+ agg+), among which ’+’ and ‘-’ means with or without the algorithm and technique and will be applied for the remaining chapters as well. It can be seen that network performance improved using the proposed staggered link design techniques as shown in scenarios 2 and 3 compared to scenario 1. Specifically, scenario 3 consistently had 33%, 157%, 339%, 496% and 571% improvement compared to scenario 1 at the incoming packet inter-arrival rate of 1 pkt/sec, 1.5 pkts/sec, 2 pkts/sec, 2.5 pkts/sec and 3 packets/sec, respectively. As the traffic loads increased, the packet delivery ratio in scenario 1 sharply dropped from 96.9% to 7.31% mainly due to collisions between data packets, beacons, and data packets and beacons which is indicated by Fig 4-10. In this case, many of the outgoing beacons from the routers were corrupted due to collisions between the beacons and data packets. As the beacons do not have the re-transmission mechanism, the end devices waiting for beacons needed to wait until they received a valid beacon in the next transmission round. On the other hand, the data packets were corrupted due to collisions causing a large number of packet losses despite re-transmissions.

It is worth noting that scenarios 2 and 3 had similar trends, gradually declining from 99.7% to 39.5% and 49.1%, respectively, with scenario 3 slightly higher than scenario 2. This minor performance gain was attributed to the packet aggregation reducing the number of collisions and the number of packet losses as indicated by Fig 4-12. As there were four routers in the network, the contention level is not high, so the aggregation technique does not show a sufficient advantage at low traffic loads lower than 2.5 pkts/sec. However, in scenario 3 with the aggregation technique had a 20% higher packet delivery ratio at 3pkt/sec than that of scenario 2. It confirmed that the aggregation technique offers an advantage at high traffic loads that are suitable for the M2M applications in a dense network scenario.

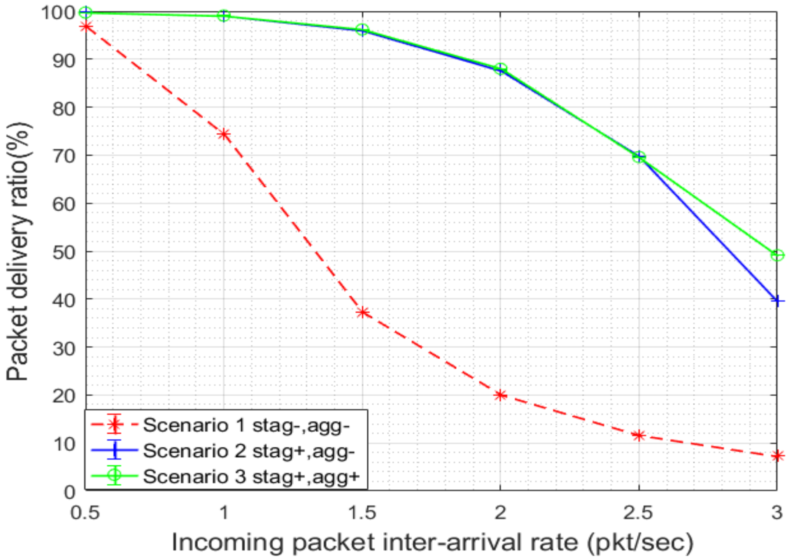


Fig 4-7 Packet delivery ratios for three scenarios

End-to-End Delay

The end-to-end delay, which records the total time required to successfully receive one packet from end devices, is shown in Fig 4-8. The delay consists of the medium access, buffering and packet processing delay. It can be seen that the end-to-end delays mildly rose as the traffic loads increased from 0.21s and 0.17s to 0.5s and 0.3s for scenario 1 and 2, respectively, and then quickly climbs 0.82s and 0.61s. As observed, scenario 3 presented a higher delay of 0.42s at the traffic load of 0.5 pkt/sec over the other scenarios. A higher delay in scenario 3 is attributed to the packet aggregation technique where payloads wait in the queue until a packet is generated. With traffic loads increasing, the aggregation delay decreases and becomes a minor component, while other delay component such as the MAC delay increases significantly. Fig 4-8 shows that at 3 pkt/sec, the end-to-end delays in scenario 1 and 2 significantly increases to 0.82s and 0.61s, respectively, whereas the scenario 3 end-to-end delay remained lower than 0.5s, offering an 18% lower value compared to that of scenario 2 and a 39% reduction compared to that of scenario 1. This clearly shows the advantages of the proposed staggered link design and packet aggregation technique.

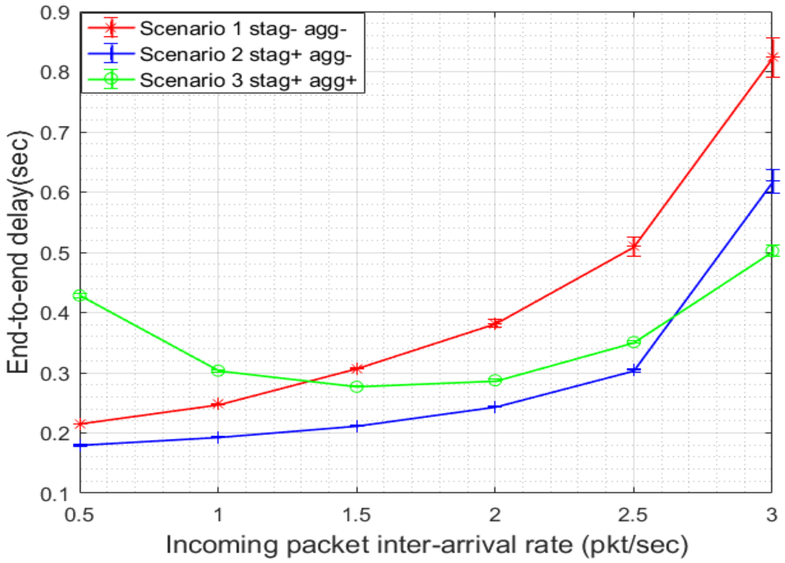


Fig 4-8 End-to-end delay for three scenarios

The end device-to-router delay is calculated using the follow components in (4-10).

$$T_{device\ to\ router} = T_{queue} + T_{backoff} + 2T_{CCA} + T_{data} + T_{ack\_wait} + T_{ack} + T_{LIFS} \quad (4\text{-}10)$$

The router-to-PAN coordinator delay is calculated using the follow components in (4-11).

$$T_{router\ to\ PAN} = T_{queue} + T_{backoff} + T_{aggregation} + 2T_{CCA} + T_{data} + T_{ack\_wait} + T_{ack} + T_{LIFS} \quad (4\text{-}11)$$

Where $T_{aggregation}$ is the packet aggregation delay and the other parameters are the same meaning as previously defined by (3-3) in Chapter 3. The end-to-end delay is calculated in (4-12)

$$T_{device\ to\ router} = T_{device\ to\ router}+T_{router\ to\ PAN} \quad (4\text{-}12)$$

$T_{device\ to\ router}$ is presented in Table 4-2 , and $T_{router\ to\ PAN}$ is presented in Table 4-3.

Table 4-2 End device-to-router delay components

Inter-arrival rate (pkt/s)	T_{queue} (ms)			$T_{backoff}$ (ms)			$2T_{CCA}$ (ms)	T_{data}	$T_{ack_{wait}}$	T_{ack}	T_{LIFS}
	Stag-agg-	**Stag+agg-**	**Stag+agg+**	**Stag-agg-**	**Stag+agg-**	**Stag+agg+**					
0.5	105.4	81.4	82.9	3.1	2.3	2.3	0.256	0.8	0.864	0.352	0.640
1	171.6	88.5	88.9	3.7	2.8	2.8	0.256	0.8	0.864	0.352	0.640
1.5	291.4	104.6	103.0	3.9	3.2	3.3	0.256	0.8	0.864	0.352	0.640
2	379.2	141.6	134.9	4.3	3.4	3.5	0.256	0.8	0.864	0.352	0.640
2.5	531.7	217.3	205.1	4.5	3.8	3.7	0.256	0.8	0.864	0.352	0.640
3	699.4	496.8	354.5	4.7	4.4	4.3	0.256	0.8	0.864	0.352	0.640

Table 4-3 Router-to-PAN coordinator delay components

Inter-arrival rate (pkt/s)	T_{queue} (ms)			$T_{backoff}$ (ms)			$\mathrm{T}_{\mathrm{aggregation}}$ (ms)			$2T_{CCA}$ (ms)	T_{data}	$T_{ack_{wait}}$	T_{ack}	T_{LIFS}
	Stag-agg-	**Stag+agg-**	**Stag+agg+**	**Stag-agg-**	**Stag+agg-**	**Stag+agg+**	**Stag-agg-**	**Sta+agg-**	**Stag+agg+**					
0.5	111.2	89.9	82.0	2.4	2.4	1.9	0	0	251.5	0.256	0.8	0.864	0.352	0.640
1	109.1	96.3	80.5	2.5	2.6	2.4	0	0	125.6	0.256	0.8	0.864	0.352	0.640
1.5	103.4	101.3	79.3	2.4	2.7	2.6	0	0	88.8	0.256	0.8	0.864	0.352	0.640
2	99.3	104.7	77.8	2.3	2.8	2.7	0	0	71.5	0.256	0.8	0.864	0.352	0.640
2.5	97.1	101.5	74.6	2.2	2.8	2.7	0	0	71.8	0.256	0.8	0.864	0.352	0.640
3	96.1	90.7	71.2	1.9	2.7	2.6	0	0	85.7	0.256	0.8	0.864	0.352	0.640

Analysing data from Table 4-2 and Table 4-3, we can see that the queuing delay is the major delay component of the end-to-end delay whose value increases with the increasing traffic load. In both the end devices and the routers, it can be seen that in the scenario 3 with the staggered link design and aggregation technique has the lowest queuing delay increasing from 82.9 ms to

354 ms, whereas for the same scenario, the aggregation delay decreases from 251.5ms to 85.7 ms due to the quicker arrival of data packets. When the queuing delays from the end devices and routers and the aggregation delay components are added, the end-to-end delay in scenario 3 shows a downward trend for packet arrival rates from 0.5 to 1.5 pkts/s. For the same scenario the end-to-end delay starts to increase as the device queuing delay starts to increase significantly.

Number of Packet Collisions

Figure 4-9 shows the number of collisions statistics. It is clear that scenario 1 had the highest number of packet collisions where the number of collisions increased as the traffic load increased. In contrast, scenarios 2 and 3 slowly rise to one half of the number of collisions in scenario 1 at the load 2 pkts/s and then quickly climb to be close to scenario 1. As indicated in the figure, scenario 1 included three types of intra-network collisions, whereas scenarios 2 and 3 avoided collisions between beacons and collisions between the beacons and the data packets by using the proposed staggered link design and packet aggregation technique. Notice that scenario 3 has a slight lower number of collisions than the scenario 2. This is because the packet aggregation technique has reduced the number of packets on the router-to-coordinator link, so the number of collisions is lower. These statistics firmly validates the effectiveness of the proposed staggered link design and packet aggregation technique when the traffic loads are moderate. However, it is noted that as the traffic loads continued to increase to over 2.5 pkts/sec, the data packet collisions became a dominating factor in the total number of collisions, which is a shortcoming of the CSMA/CA protocol.

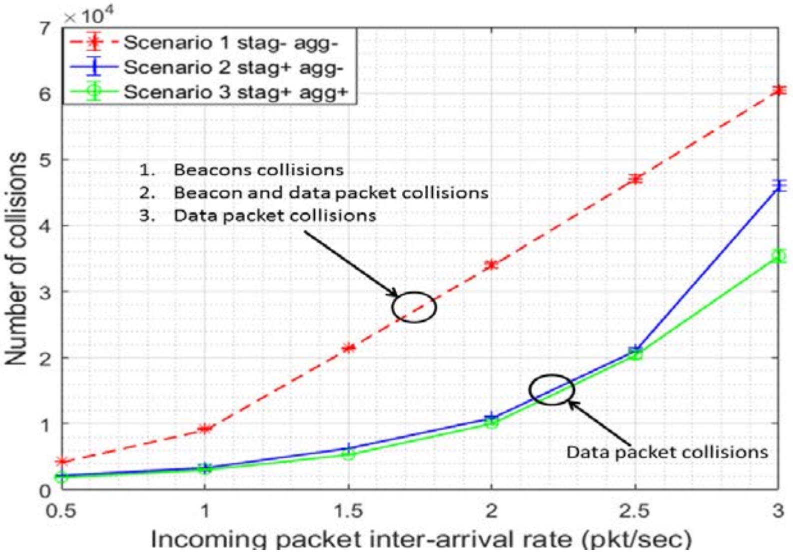


Fig 4-9 Number of Intra-network collisions

Retransmissions

As mentioned previously, a large number of beacons and data packets can collide if beacons are not scheduled in a proper manner. Retransmissions directly reflect the contention level in a network; that is, the retransmission numbers increase with the network contention level. In Fig 4-10, in comparison to scenario 1, scenario 3 showed significant reductions in the number of packet retransmissions. At the traffic load of 1.5 pkts/sec, only 11107 retransmissions were performed by the end devices in scenario 3, while scenario 1 had 40000 retransmissions. Such remarkable gains are a direct result of the proposed link design. Similar to the previous two figures, scenarios 2 and 3 showed similar patterns where the numbers of the retransmissions in these two scenarios were close to each other until the traffic load reached 2.5 pkts/sec. At the high load of 3 pkts/sec, the numbers of retransmissions of scenarios 1 and 2 were 97978 and 88098, respectively, while scenario 3 had a slightly lower number of retransmissions at 72895. The fundamental reason for this was because the data packets were colliding with the beacons due to a non-scheduled link in scenario 1. To compensate for the packet losses due to collisions, the end devices are required to increase the number of retransmissions. The proposed link design and the packet aggregation technique effectively reduced the number of collisions, thus requiring a lower number of retransmissions. Another reason for such a trend in scenarios 2 and 3 is that the aggregation was performed in the routers. In other words, the packet aggregation eliminates intra-network collisions between the routers and PAN coordinator, while the packet aggregation technique becomes effective at a higher contention level.

Figure 4-11 shows the router's retransmission statistics, which are quite different from the results in Fig 4-10. Scenario 1 had the number of retransmissions rising just over 2000 and then declines to 387 as the majority of packets had already been lost on the end device-to-router link due to intra-network collisions. Scenario 3 did not have any retransmission exceeding 3000 with the traffic loads increasing. In contrast, scenario 2 had the highest number of retransmissions, up to 9516, when the traffic load was 2 pkts/sec. In comparison to scenario 2, scenario 3 reduced the number of retransmissions by 73%, while maintaining low end-to-end delays and high packet deliver ratios. It is clear that the staggered link design alleviated the intra-network collisions on the end device-to-router link, and the packet aggregation technique reduced intra-network collisions on the router-to-coordinator link.

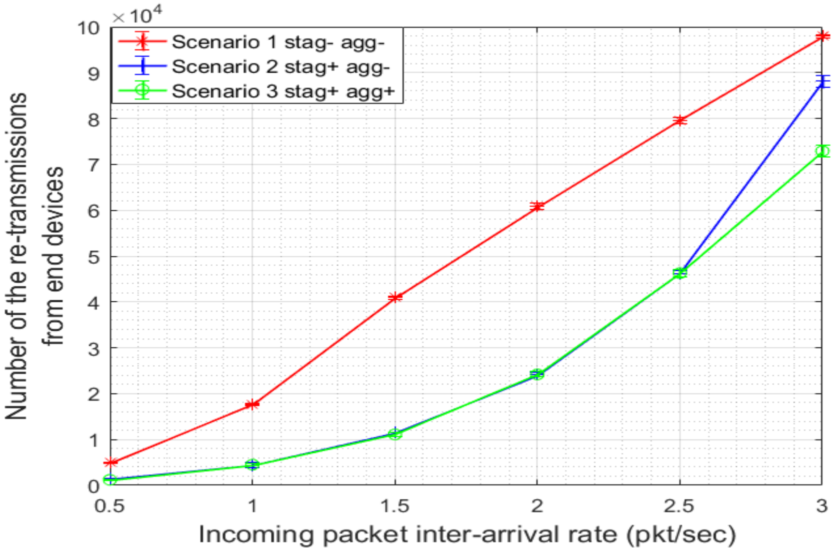


Fig 4-10 End device retransmissions in three scenarios

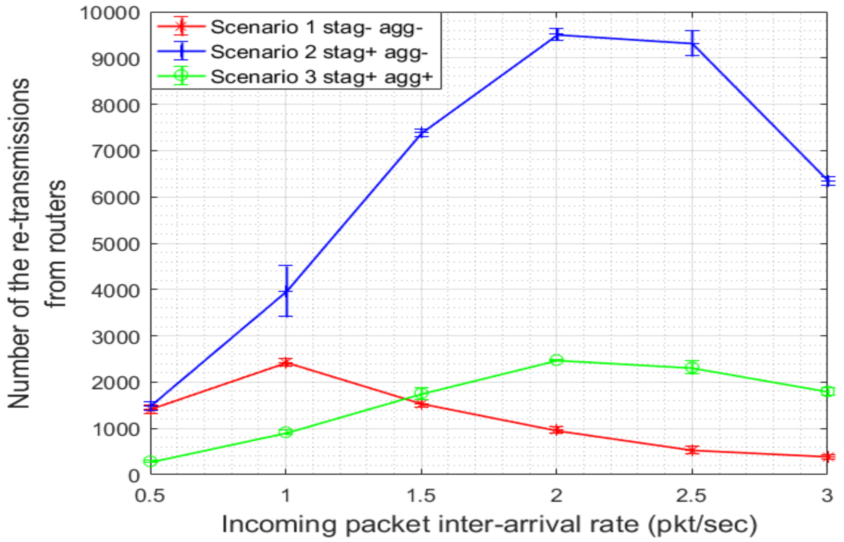


Fig 4-11 Router retransmissions in three scenarios

Packet Losses

Figure 4-12 shows the number of dropped packets in the MAC layer due to the limited number of retransmissions (three is allowed by the IEEE 802.15.4 standard). Compared to Fig 4-12, Fig 4-10 shows a similar trend in the end devices and routers, which validates the effectiveness of the proposed techniques. In Fig 4-12, scenario 2 and 3 show similar a trend. Both scenarios shows 85% lower packet losses compared to the scenario 1 at the traffic load of 2 pkts/sec. It is noted that scenario 1 experienced a linear increase in packet losses from 0 to 31467, whereas the other two scenarios 2 and 3 initially experienced a slow increase from 0 to 8400 at a low traffic load of 2 pkts/sec, then experienced a sharp increase to 22777 and 17272, respectively, at a high traffic load of 3 pkts/sec. It is clear that the proposed link design can reduce the packet losses at low traffic loads instead of at high traffic loads where the packet losses are getting close to other scenarios regardless the use of the staggered link. This means that the proposed link design may not fully mitigate the intra-network collisions when the traffic is beyond its capacity. It should also be noted that scenario 3 reduced packet losses by 24% at the traffic load of 3 pkts/sec, which means the packet aggregation technique effectively reduced packet losses even at a high traffic load.

Figure 4-13 shows the packet loss statistics for the routers. Most of the losses were due to data packet collisions. In other words, with the staggered link design, the collisions probability between beacons, and beacons and data packets have been reduced, so that the only one type of intra-network collisions left is the data packet collisions. As this type of collisions occurs, the data packets were corrupted so that they could not be decoded by the PAN coordinator, thus resulting in an expired ACK timer in the routers and in turn leading to data packet retransmissions. It can be seen that scenario 1 had the lowest number of packet losses since most packets were dropped at end devices. Scenario 2 has the most packet losses because the majority of the packets can survive intra-network collisions and be forwarded to the routers. In particular, comparing to scenario 2, scenario 3 reduced the packet losses by nearly 90%. At the load of 1.5 pkts/sec, scenario 2 had 60 lost packets, while scenario 3 had four lost packets. This was because the total number of transmitted packets has been reduced by 2/3, as shown in Fig 4-5, so the contention level was much lower. Note that scenario 2 experienced upward packet losses first and packet losses were reduced after the traffic loads passed 1.5 pkts/sec, which is the tipping point of network saturation. After 1.5 pkts/sec, the network went into the saturation state where less traffic arrived at the routers, thus leading to lower contention levels and lower packet losses. Recall that in Fig 4-7 scenarios 2 and 3 had the similar patterns of packet delivery ratios and scenario 3 had the lowest end-to-end delays; therefore, the packet aggregation technique enhances a network’s reliability and makes it more resilient in the presence of data packet collisions.

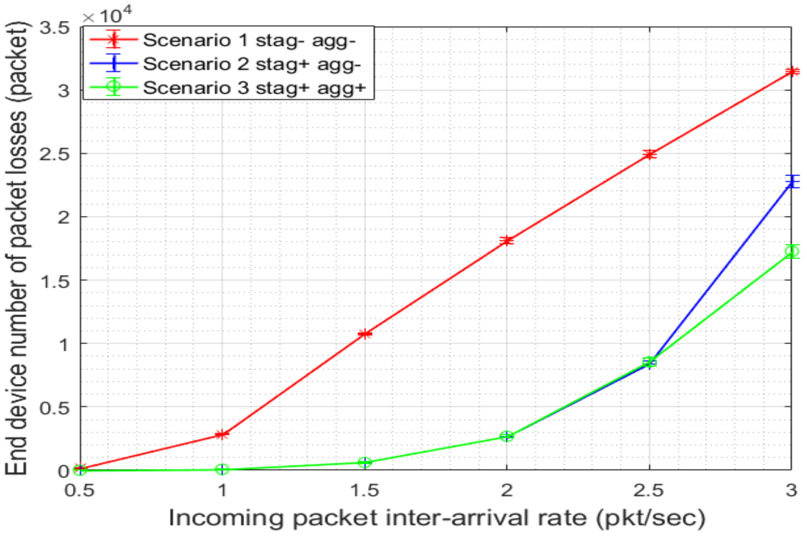


Fig 4-12 End device packet losses

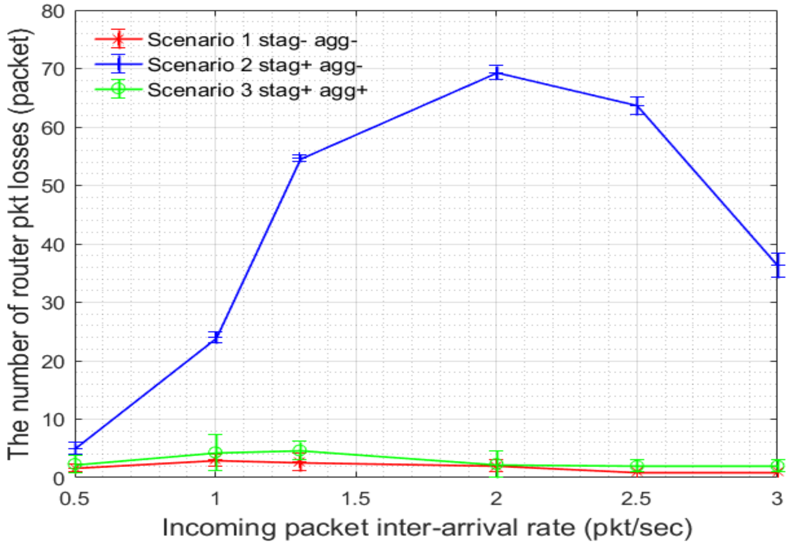


Fig 4-13 Router packet losses

As can be seen in Fig 4-14, the queue lengths of the end devices in the three scenarios are examined, which further confirms the performance improvement in the previous results. At low traffic loads from 0.5 pkt/sec to 2 pkts/sec, the queue lengths remain stable at one packet per second load. Then, the queue lengths then go up to 3 packets, 2.5 packets and 1 packet in scenarios 1, 2 and 3, respectively. Scenario 3 reduced the queue length by 60% compared to that of scenario 2 and by over 66% compared to that of scenario 1. The rationale for these results is that as the traffic loads increased, scenario 1 contention level increased much faster than in the other two scenarios, which had already been confirmed by the packet delivery ratios in Fig 4-7 and the end device packet losses in Fig 4-12. As contention flared, the end devices' packets are built up more quickly in scenario 1 than in the other scenarios. In contrast, Fig 4-15 shows the router queue length statistics. It can be seen that the queue length of scenario 2 was maintained at 2 packets as the traffic load increased from 1 to 3 pkts/sec. In contrast, scenarios 1 and 3 had a relatively low queue length of around one packet, but it had two different reasons. The first is that as for scenario 1, many packets were dropped in the MAC layer, so the routers could not obtain enough packets; the second reason is as for scenario 3 where all packets are aggregated so that the total amount of traffic is low.

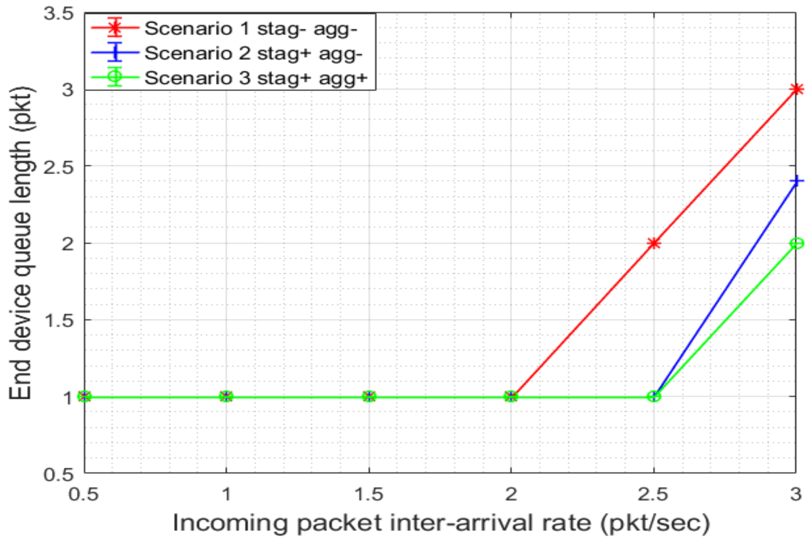


Fig 4-14 End device queue lengths for scenario 1, 2 and 3

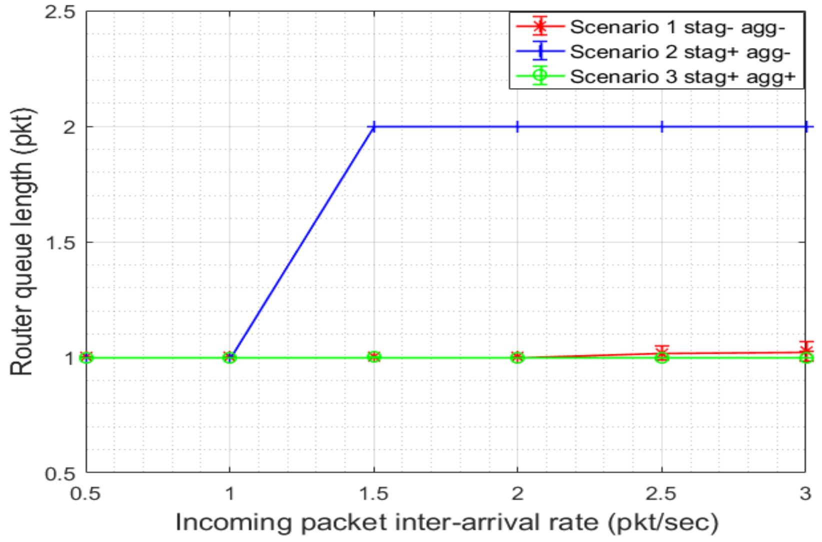


Fig 4-15 Router queue lengths for scenario 1, 2 and 3

4.3.2 The Effects of Varying Cluster Densities

In this section, the aforementioned metrics and coordinator's throughput are measured with different cluster densities. For this simulation, the packet inter-arrival rate of 3 pkts/sec/end device was used. The same three scenarios were used to compare the network performances for different cluster densities. Fig 4-16 shows the packet delivery ratios sharply dropped in scenario

1 from 93% to 5% as the number of clusters increased to four. In contrast, the packet delivery ratio started to go down from 95% to 30% for scenarios 2 and 3. With the aggregation technique, the packet delivery ratio in scenario 3 remained the same as in scenario 2. It should be noted that the network throughput for scenario 3 was only 1/3 that of scenario 2 because the number of packets had been reduced by 2/3 in scenario 3. It is obvious that the proposed algorithm improved the network's performance. For example, the packet delivery ratio with the proposed algorithm was increased by 200% compared to that of scenario without the algorithm for two clusters. The main reason of the lower packet delivery ratio in scenario 1 is due to the intra-cluster collisions causing a great number of beacon losses. Once the beacon losses occurs, the end devices lose synchronization with its parent router node, thus failing to send any data packets, resulting in the low packet delivery ratio.

Right-hand side of Fig 4-16 shows the PAN coordinator throughput. It can be seen that scenario 1 experienced a downward trend from 22 to 6.9 pkts/sec, whereas the scenarios 3 rose from 23.7 to 46.5 packets/sec. In particular, scenario 3 only had 1/3 of scenario 2 throughput due to the packet aggregation technique (three packets are aggregated into one 6LoWPAN payload) that greatly reduced the number of packets on the link and thus mitigates intra-network collisions.

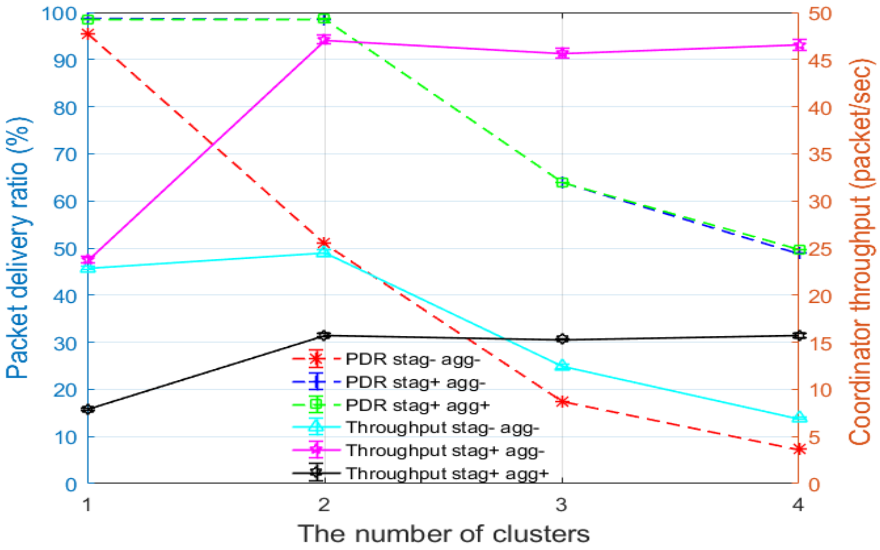


Fig 4-16 Packet delivery ratio vs the total coordinator throughput

Figure 4-17 and Figure 4-18 show the packet losses due to intra-network collisions in the three scenarios. As discussed earlier, packet losses affect the packet delivery ratios and end-to-end delays, and are the major contributor of these two metrics. Specifically, packet losses can lead to the low packet delivery ratio and rising queuing delay caused by the increasing number of packets to be re-transmitted by the MAC layer queue. This increased queuing delays and consequently led to high end-to-end delays. When comparing Fig 4-17 and Fig 4-18, it is clear that the end devices suffered much greater packet losses than the routers. This means that the majority of the 6LoWPAN packets were lost on the end device-to-router link. It can be seen in Fig 4-17 that there was a consistent 10000-packet loss gap between the scenario with the staggered link design and the one without. The reason for this is that beacon-to-data and beacon-to-beacon collisions caused more data packet losses than the scenarios with the proposed algorithm. In contrast, with the proposed algorithm, the packet losses are only due to data packet collisions. It can be seen that the number of data packet collisions are still very high, which indicates that the IEEE 802.15.4 MAC layer is well equipped for the high traffic loads and is not efficient in a multi-hop scenario. It is expected that packet losses will be even worse as the number of clusters increases.

Figure 4-18 shows the router packet losses, which was much fewer than that of the end devices presented in Fig 4-17 . This is because most of the packets were lost in the last hop, so not many packets reached the routers. It can be seen that the scenario without the proposed algorithm and the one with the proposed link design and packet aggregation have almost no packet losses. However, this is for different reasons. The latter is because the packet aggregation technique reduced the number of packets contending for the channel. It is interesting to see that that scenario with the staggered link design but without the packet aggregation technique had packet losses of up to 40 due to the channel contention. According to these results, the routers collecting packets from the clusters are regarded as the bottleneck in the network and tend to cause the packet losses. It is therefore necessary to decrease the number of outgoing packets using the packet aggregation technique.

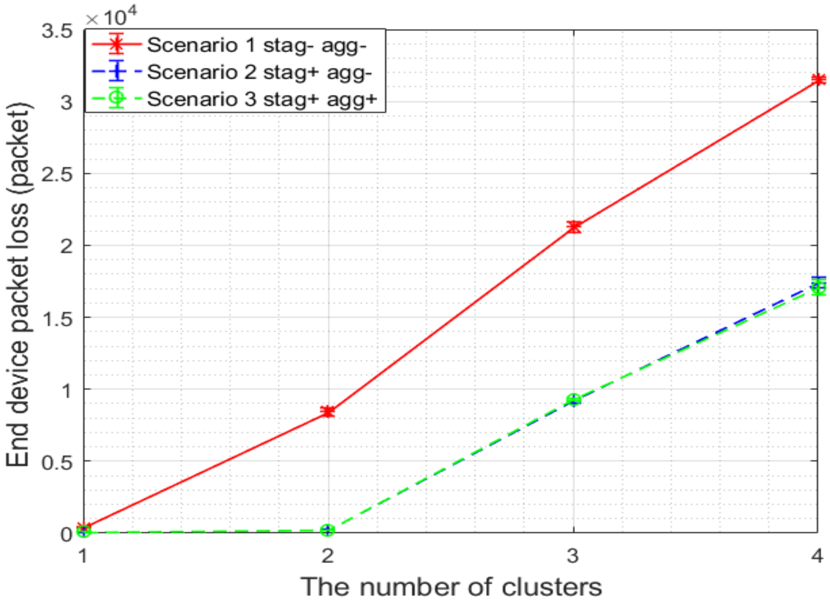


Fig 4-17 End device packet losses

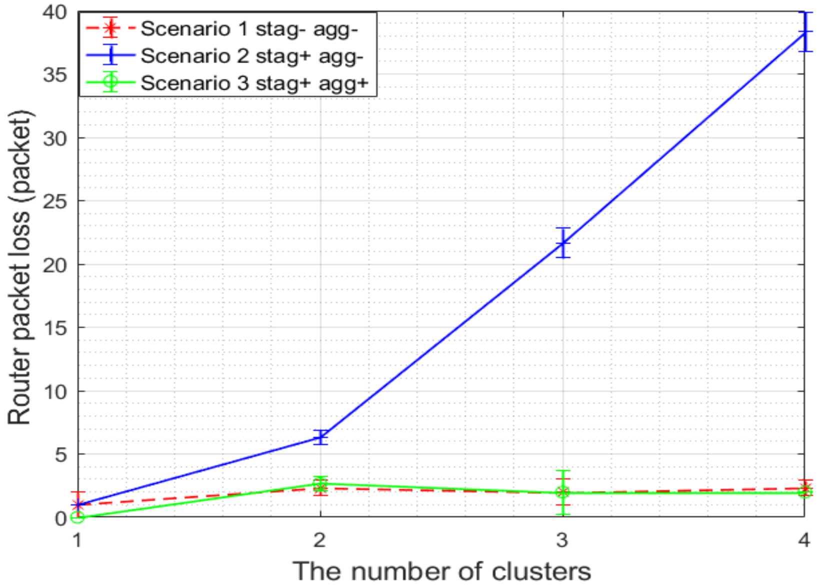


Fig 4-18 Router packet losses

Fig 4-19 depicts the end device queuing delays of the three scenarios. Given that packet losses are a major cause of the low packet delivery ratio and high end-to-end delay, the queuing delays are also affected. It can be seen from Fig 4-19 that the end devices experienced a longer delay compared to that of Fig 4-20 mainly due to intra-network collisions. It was proved that the proposed algorithm decreased the queuing delay by 50% from 0.8s to 0.4s, with four clusters. Although the proposed algorithm helped to reduce the queuing delay, it was still observed that its queuing delay rose from 0.1s to 0.4s due to the normal data packet collisions. It is understood that the end devices are the victims adversely affected by the intra-network collisions and they must be protected by the proposed link design in a multi-hop M2M network. For this reason, if the number of hops in the network is over three hops, the accumulated delay in each hop will be quite high at the sink and thus cannot meet requirements of some M2M applications.

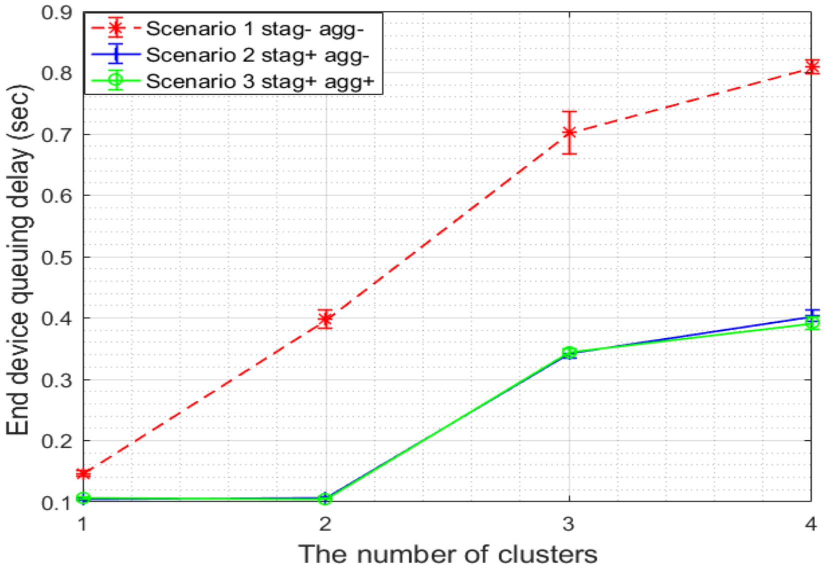


Fig 4-19 End device queuing delay

Fig 4-20 shows that the router queuing delays were declining as the number of clusters increased. This is because a large number of data packets were lost before reaching the router, so the rest of the packets could cause congestion in the router's MAC layer. Note that the scenario 3 with the staggered link design and packet aggregation technique had the lowest queuing delay reduced from 0.1s to 0.07s. This is because the router aggregates data packets that significantly reduced the number of data packets in the router's MAC layer. It is also noted that scenario 2 with the staggered link design had a slightly lower router queuing delay than scenario 1. It can be seen that the staggered link design may not be effective in decreasing the router queuing delay compared to the packet aggregation technique. This is because the staggered link design cannot reduce the number of transmitted packets on the link, but the packet aggregation technique can.

On the other hand, it is expected that the router queuing delay will increase as the number of clusters increases beyond four, which could cause congestion in router's MAC layer and increase the router queuing delay.

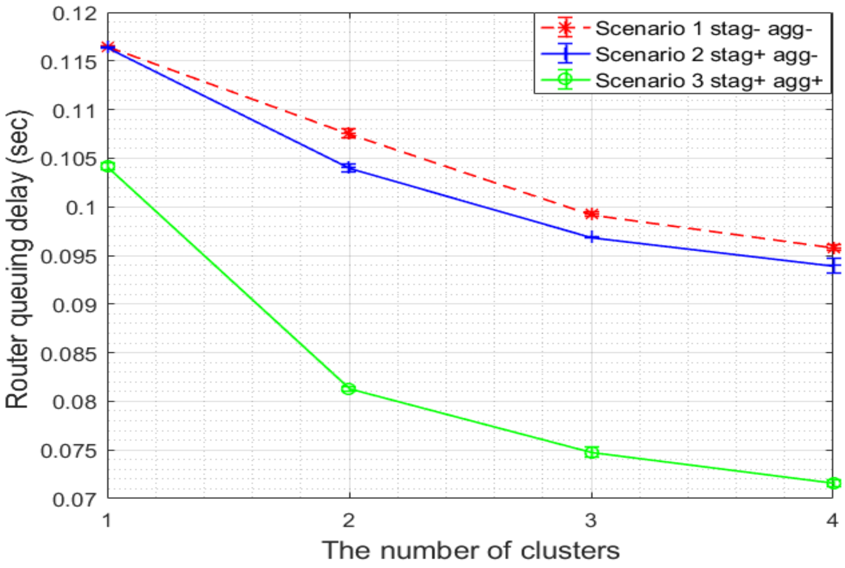


Fig 4-20 Router queuing delay

4.4 Heterogeneous Wireless Sensor Network

The proposed staggered link design and packet aggregation technique effectively decreases the number of intra-network beacon collisions. However, as the number of hops increases, the end-to-end delay increases, and the packet delivery ratio decreases. This is because the routers can cause long delays when packets are forwarded, and the packets colliding in each hop result in the accumulated packet losses at the sink node [119]. To solve these two problems, a heterogeneous area network combined with the 6LoWPAN and WLAN standards was proposed. It employs WLAN transmitters to increase the packet delivery ratio and reduce the end-to-end delay. The WLAN has a much faster transmission rate and larger coverage area than a 6LoWPAN transmitter, so a heterogeneous network can offer much better performances than a homogeneous 6LoWPAN network. The heterogeneous area network can compensate for the above two shortcomings.

As shown in Fig 4-21, it is a homogeneous 6LoWPAN network where the traffic converges at router 4 and then arrives at the sink node via routers 5, 6 and 7. Since the distance between router 4 and the sink node is 200 metres, it takes six hops for a 6LoWPAN packet to reach the sink node. Similarly, a beacon needs to be transmitted over six hops to the end devices. As the packets are transmitted via these hops, each packet needs to be buffered and uses the CSMA/CA protocol to transmit, so the end-to-end delay accumulates at the packets travelling through these hops.

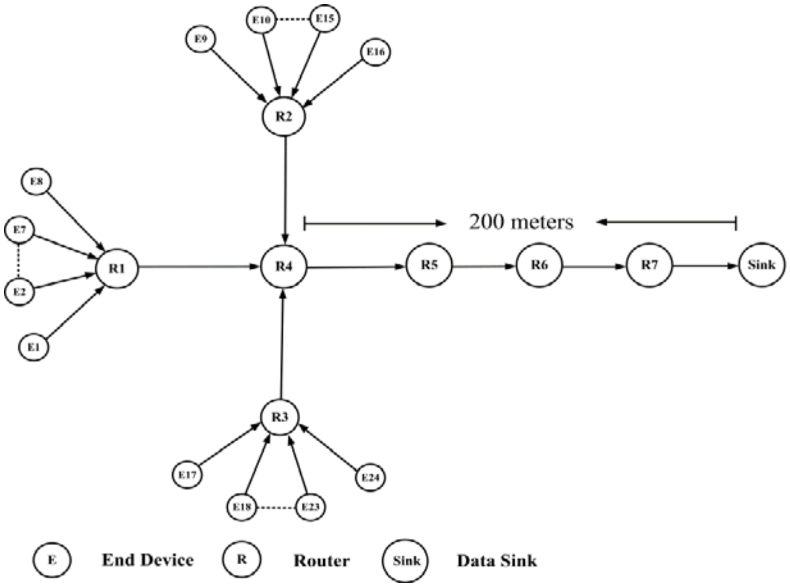


Fig 4-21 Multi-hop homogeneous area network

Therefore, some M2M applications such as demand management traffic, with stringent delay requirements may not meet the QoS requirements in a homogeneous network architecture. To tackle these problems for the higher priority traffic, a heterogeneous area network comprised of the 6LoWPAN and IEEE 802.11g standard was proposed to reduce the end-to-end delay and to improve the packet delivery ratio. The heterogeneous network reduces the number of hops by replacing router 5, 6 and 7 with a wireless WLAN link between a Dual Radio Router (DRR) and a WLAN sink. By doing so, the queuing and MAC delay can be reduced so that the total end-to-end delay can be reduced.

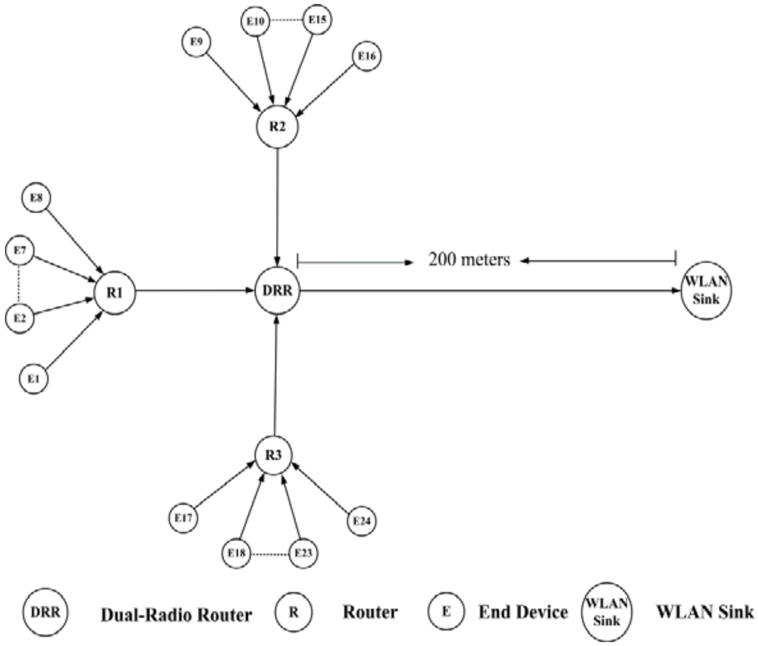


Fig 4-22 The proposed heterogeneous wireless sensor network

4.4.1 Heterogeneous Area Network Model

The heterogeneous area network includes the IEEE 802.11 and 6LoWPAN protocol stacks to develop the DRR to transmit packets to the data sink by converting the 6LoWPAN packets into IEEE 802.11 packets. The WLAN interface supports a much higher transmission rate than that of the 6LoWPAN network, so it takes less time to transmit packets from the end devices to the data sink, thus reducing the end-to-end latency. Since the WLAN can support larger payload sizes, the DRR can aggregate several 6LoWPAN packets into a single WLAN packet to transmit to a data sink. Fig 4-23 shows the protocol stack of the DRR comprised of the 6LoWPAN and WLAN protocol stacks. It can be seen that the 6LoWPAN packet is stripped of the 6LoWPAN header, and a WLAN header is added as the packet passes the protocol stack. However, there is no protocol stack in the OPNET model library, so an OPNET simulation DRR model was built. As shown in Fig 4-24, it is the DDR node model representing the components offered by the OPNET. As the DRR consists of the 6LoWPAN and WLAN stacks, the latter was obtained from the built-in OPNET model library and was connected with the former by packet streams. In addition, the DRR receives 6LoWPAN payloads from the 6LoWPAN application layer and forwards them to the WLAN application layer. The forwarded traffic is then transmitted via the transceivers of the physical layer of the WLAN to a remote WLAN sink. To compare with the previous homogeneous multi-hop network (as shown in Fig 4-21), a heterogeneous area network is presented in Fig 4-22, in which the DRR and WLAN sink replace several routers to cover the same distance.

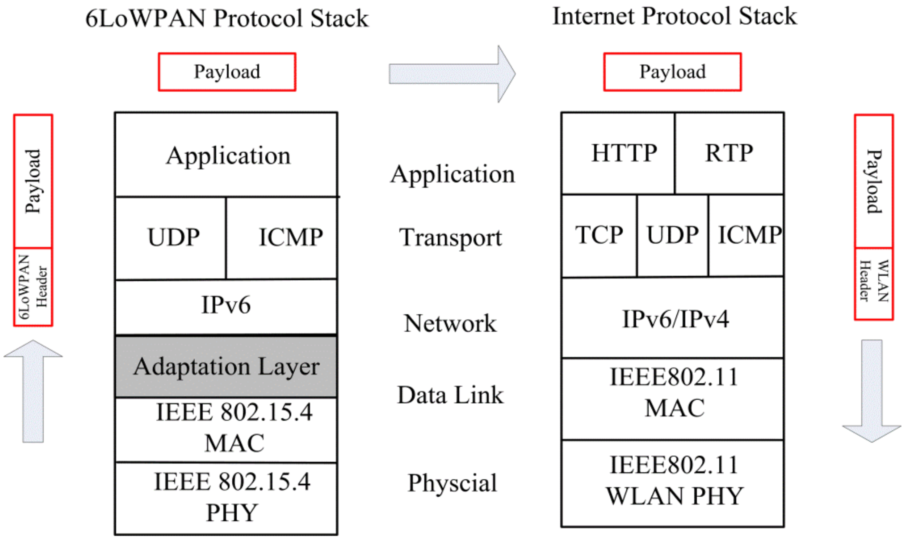


Fig 4-23 DRR protocol stack

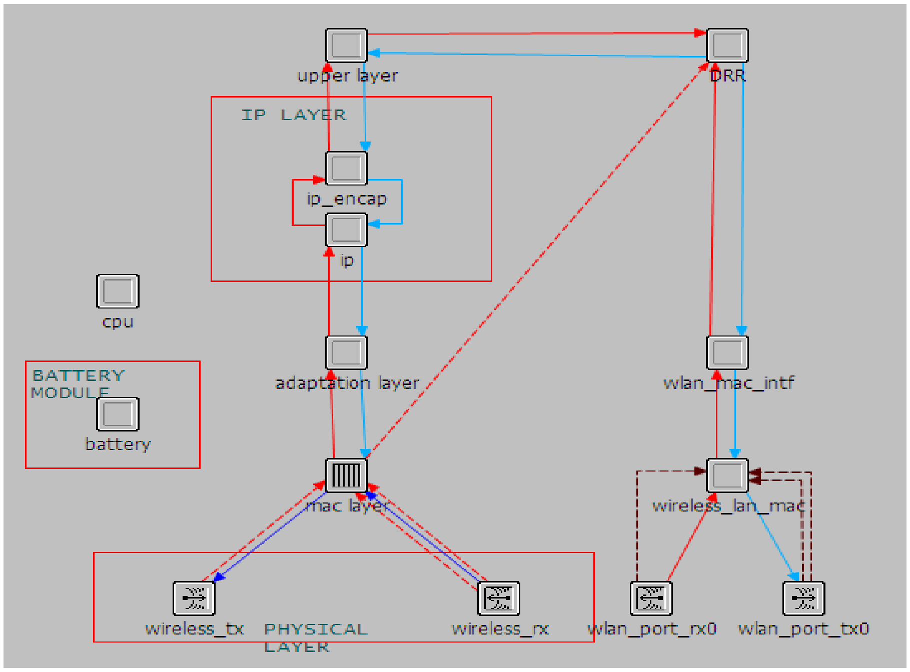


Fig 4-24 OPNET DRR node model

4.4.2 Performance Analysis of the Proposed Heterogeneous Wireless Sensor Network

To evaluate the performance of the proposed heterogeneous wireless sensor network, the scenario in Fig 4-21 and Fig 4-22 are compared. The packet delivery ratio and end-to-end delay are used as two key QoS metrics. Both scenarios use the staggered link design to avoid intra-network collisions. The only difference between the two scenarios is the 200 meters distance is covered by a WLAN wireless link in the heterogeneous wireless sensor network. The WLAN has a transmission rate up to 54 Mbps and has a larger transmission range up to 200 meters. Combing the WLAN with the 6LoWPAN networks can greatly improve the heterogeneous network throughput and reduce end-to-end delay. The key simulation parameters for the multi-hop homogeneous scenario and the heterogeneous scenario are listed in Table 4-4 and Table 4-5, respectively.

Table 4-4 Key simulation parameters in the homogeneous network

Group Name	**Paramter**		**Value**
Network	Hop		6
	Number of End Devices		24
	Standard		6LoWPAN
	Operating Frequency		2.4 GHz
	6LoWPAN channel		12
Propagation model	Free space path loss		
Router	BO		4
	SO		3 (R4, R5, R6), 2 (R1,R2 and R3)
	Schedule Start time	R1	0.1843231 sec
		R2	0.1228811 sec
		R3	0.1843232 sec
		R4	0.1228814 sec
		R5	0.1228813 sec
		R6	0.1228812 sec
		R7	0.1228815 sec
End device	Packet size		64 bytes
	Packet generation		Exponentially distributed
	Transmission Power		1 mw
	Packet inter-arrival rate		0.5, 1, 1.3, 1.5, 1.7, 2pkts/sec

Table 4-5 Key simulation parameters in the heterogeneous network

Group Name	**Parameter**		**Value**
Network	Hop		3
	Number of End Devices		24
	Standard		6LoWPAN, IEEE 802.11 g
	Operating Frequency		2.4 GHz
	6LoWPAN channel		12
	IEEE 802.11 g channel		7
Propagation model	Free space path loss		
Dual Radio Router (Gateway)	6LoWPAN	BO	4
		SO	3
		Transmission Power	1.8 mW
	WLAN	Transmission	100 mW
Router	BO		4
	SO		2
	Schedule Start time	R1	0.184323 sec
		R2	0.1828813 sec
		R3	0.1843232 sec
End device	Packet size		64 bytes
	Packet generation		Exponentially distributed
	Transmission Power		1 mw
	Packet inter-arrival rate		0.5, 1, 1.3, 1.5, 1.7, 2pkts/sec

Figure 4-25 shows the packet delivery rates achieved by the heterogeneous scenario and the homogenous scenario. The packet delivery rate of the heterogeneous scenario steadily descended from 95% to 73%, but was still much higher than that of the homogeneous scenario in which sharply plummeted from 72% to less than 10%. In particular, at the load of 1.5 pkts/sec, the heterogeneous scenario was 90%, which is much higher than that of the homogeneous scenario at 18%. As loads increased to 2 pkts/sec, the homogeneous scenario dropped down to less than 10%. The packet losses were due to buffer overflow and channel contention, which is explained below.

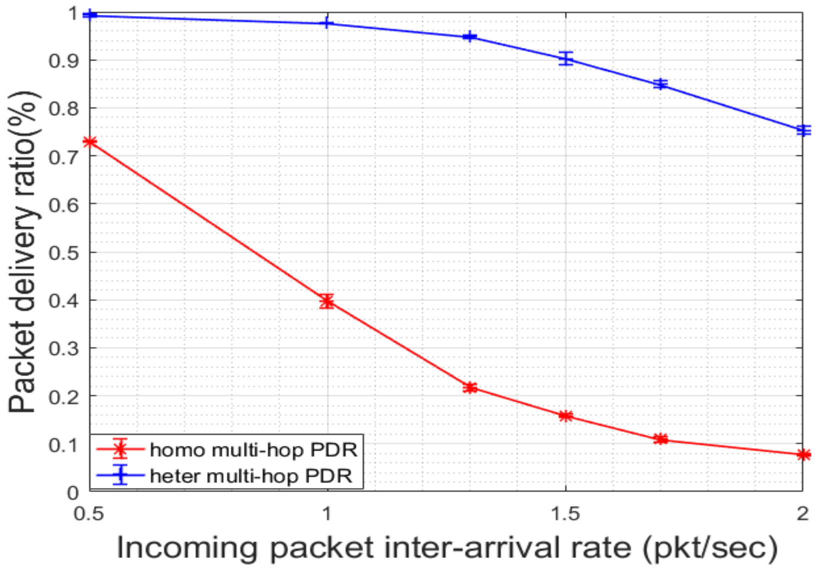


Fig 4-25 Homogeneous and heterogeneous network packet delivery rate

Figure 4-26 shows the end-to-end delay in the homogeneous scenario started to increase from a low value of less 5s to 160s as the loads increased from 1 to 2 pkts/sec, whereas for the heterogeneous scenario the delay remained less than 1s. This increase in end-to-end delay in the homogeneous scenario was due to the long queuing delay of the 6LoWPAN packets building up in router 4's MAC queue. It is clear that router 4 is the bottleneck in the homogeneous network because it received all the traffic from the other routers, which leads to router 4 buffer overflow as the traffic loads increased. In particular, the proposed heterogeneous scenario maintained a relatively high throughput at the traffic loads of 2 pkts/sec because the high transmission rate of the WLAN could tackle a large amount of traffic loads. For example, the 6LoWPAN transmission rate is 250 kbps, while the WLAN is 54 Mbps (216 times higher compared to the 6LoWPAN), so the DRR can increase the total network throughput and avoid MAC layer buffer overflow.

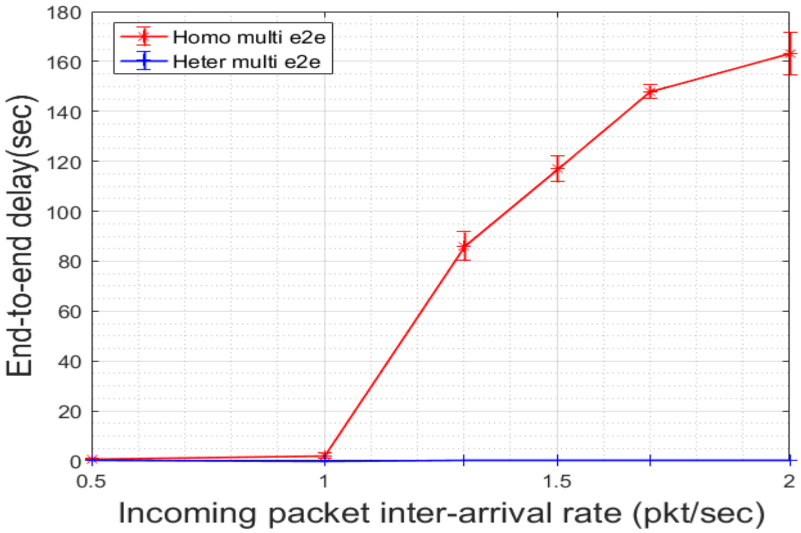


Fig 4-26 Homogeneous and heterogeneous

The spike in the end-to-end delay in the homogeneous scenario was caused by the long queuing delay as shown in Fig 4-27. The queuing delay showed a similar trend with the end-to-end delay in the same scenario. As router 4 was the bottleneck, the traffic loads can easily build up in the MAC layer queue, thus leading to MAC layer buffer overflow. In addition, router 4 experienced the highest amount of traffic, so it had the greatest number of packet losses due to channel contention. As shown in Fig 4-28, router 4 packet losses outnumbered the other routers' packet losses as the incoming traffic increased, as indicated by the blue line. It is noted that the number of packet losses in router 4 was up to 580 as the traffic was at 2 pkts/sec. In contrast, routers 1, 2 and 3 had the lowest number of packet losses as each of them sustained one-fourth of the total traffic. The red, blue, green and light blue lines overlap, showing that they are fewer than 50 pkts as the traffic loads increased. This proves that the heterogeneous area network is superior to the homogeneous multi-hop area network.

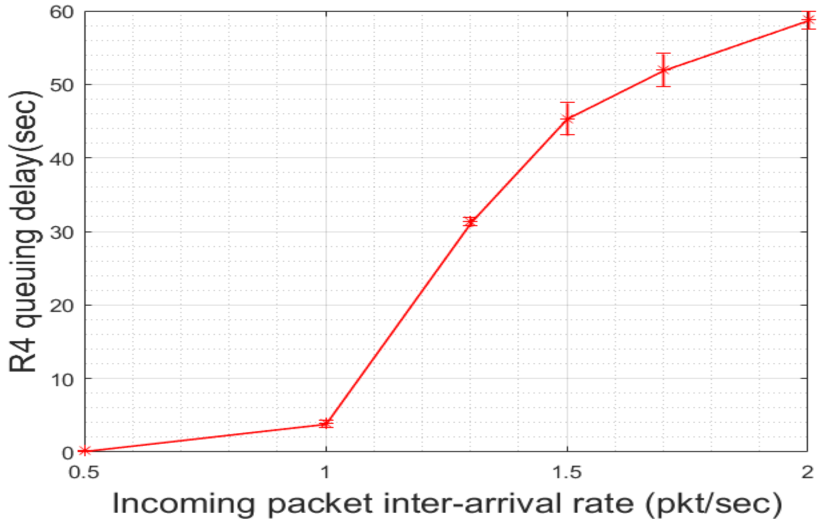


Fig 4-27 Router 4 queuing delay for the homogeneous scenario

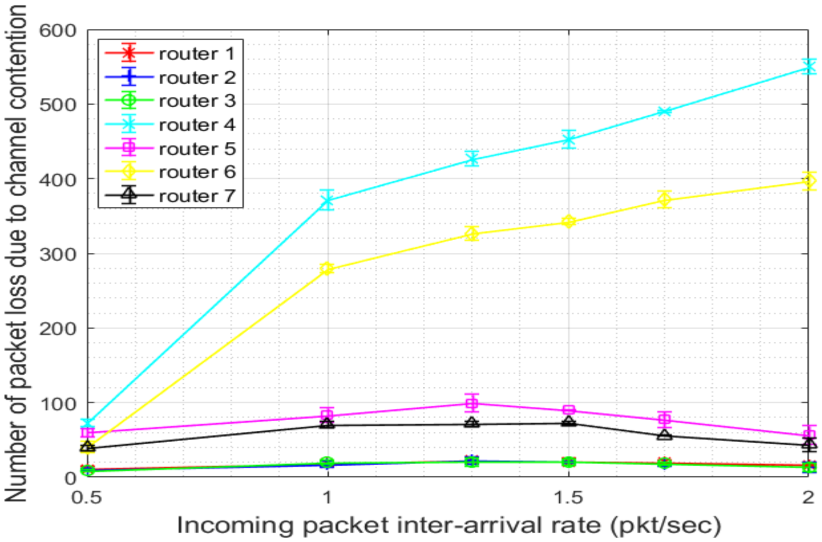


Fig 4-28 Router packet losses due to channel contention in the homogeneous scenario

4.5 Conclusion

Three types of intra-network collisions were investigated and analysed in this chapter. After the analysis, a staggered link design for a multi-hop 6LoWPAN was proposed to reduce intra-network collisions. The design uses the inactive period of a PAN coordinator’s beacon interval to accommodate the router’s active period, so the outgoing beacons from the router do not collide with the beacons or data packets from the other routers, thus reducing the possibility of intra-network collisions between the end device-to-router links. To further reduce the intra-network collisions between the routers, a packet aggregation technique was proposed. Three 6LoWPAN payloads were aggregated in the router's the adaptation layer forwarding the aggregate to the PAN coordinator. This technique greatly reduced the number of packets on the link, so the number of the intra-network collisions could be reduced. The simulation results demonstrated the benefits in improving the packet delivery ratio, end-to-end delay and packet retransmissions. However, the staggered link design may cause a long end-to-end delay and decrease the packet success rate in a multi-hop wireless sensor network. This is because packet losses either due to intra-network collisions or buffer overflow can occur on each hop of the network. To maintain the same distance that a multi-hop network can cover and to increase the packet delivery ratio, a heterogeneous area network consisting of the 6LoWPAN and WLAN protocols was proposed. One key component is the DRR, serving as a gateway to connect both the networks. The simulation results showed that the heterogeneous wireless area network is more suitable for the IoT and M2M applications.

Chapter 5

Interference Mitigation Techniques for Unlicensed-Band Networks

5.1 Introduction

Chapter 4 introduced the staggered link design and packet aggregation technique to reduce the number of intra-network collisions in the cluster-tree multi-hop area network. To cover a large-scale geographical area, the multi-hop area network may require multiple short-distance links that can cause the long end-to-end delay, as shown in Fig 4-26 . To reduce the number of short-distance links and the long end-to-end delay, a heterogeneous area network architecture was proposed for M2M and IoT applications, as shown in Fig 4-22. However, the heterogeneous area network with a large number of devices running on the unlicensed 2.4 GHz band in a dense IoT communication network could cause in-band interference. This interference is, in fact, the inter-network collisions that are the packet collisions between two different types of wireless networks sharing the same spectrum. As for the heterogeneous architecture, the 6LoWPAN coordinator was replaced by the DRR that includes the 6LoWPAN and IEEE 802.11 protocol stacks. The DRR instead connects a WLAN data sink to extend the transmission range of an IoT 6LoWPAN network. Therefore, the 6LoWPAN and WLAN packets tend to cause inter-network collisions in the proposed heterogeneous architecture.

The BB algorithm has been proposed to avoid the inter-network collisions as described on page 145. The BB signalling is a unique control signal architecture using beacon frames of the 6LoWPAN to propagate control information to all field devices. This is a unique and novel approach which employs the existing 6LoWPAN transmission structure to field devices with no additional control overhead and minimum transmission delay. To best of our knowledge, there is only one approach addressing the same issue using the packet aggregation method in [9]. We compared our performance of the BB algorithm with that of the existing one in [9] to show the uniqueness and originality of the BB algorithm. The unique signalling architecture improves the network performance in a deterministic manner; namely, it puts the network devices in the sleeping mode while the WLAN interface is used to transmit the aggregated 802.11 packets. As for heterogeneous networks, no other similar solutions exist to avoid the inter-network collisions. This original control signalling scheme was proposed by this research.

The work in this research proposed a method to mitigate the inter-network collision problem when using the DRR involving 6LoWPAN/IEEE 802.11g standards. To eliminate the inter-network collisions between the 6LoWPANs and the WLAN devices in this proposed network, a time slot based signalling mechanism is introduced, which is referred as the Blank Burst. In the proposed system, the WLAN packets are transmitted to a data server by silencing the WPAN devices using the Blank Burst (BB) signalling. During the WLAN transmission period, all of the 6LoWPAN devices go to the sleep state to alleviate the energy consumption requirements for a large area network. The proposed signalling mechanism is simple to implement, but can offer a effective method to eliminate the inter-network collisions. The algorithm has been further developed to offer higher network throughput in a dense networking environment.

The rest of the chapter is structured as follows. Section 5.2 presents the channel arrangements of both the IEEE 802.11 and IEEE 802.15.4 networks and analyses the effects of the inter-network collisions. Section 5.3 and 5.4 explains the design principle and the proposed Blank Burst algorithm. The performance analysis of the proposed algorithm is presented in Section 5.5. Finally, Section 5.6 concludes the chapter.

5.2 IEEE 802.15.4 and IEEE 802.11 Based Heterogeneous Network Design Issues

In this section, to understand how the inter-network collisions are generated, the IEEE 802.15.4 standard and the IEEE 802.11 standard are analysed. Due to the share of the 2.4 GHz unlicensed band by the two standards, the spectrum allocation is studied first to investigate the cause of inter-network collisions. Then the differences of the two MAC layers of the IEEE 802.15.4 standard and the IEEE 802.11 standard will be discussed. Finally, all the performance analysis will apply to the proposed heterogeneous area network.

5.2.1 Spectrum Allocation of IEEE 802.15.4 and IEEE 802.11 Standards

The IEEE 802.15.4 and IEEE 802.11 standards support multiple transmission frequency bands including the 2.4 GHz ISM band. This work focuses on the 2.4 GHz transmission bands where the transmission channels of the 6LoWPAN and DRR can overlap. The solutions proposed in this work can be extended to other frequency bands, particularly the 900MHz frequency band. Fig 5-1 shows the sub-channel arrangement of the IEEE 802.11 and IEEE 802.15.4 standards in the 2.4 GHz frequency spectrum. The 802.11b/g uses a 20 MHz transmission bandwidth, while the 6LoWPAN uses a narrow 2MHz transmission band. This figure shows that WLAN channel 1, 7 and 13 significantly interfere with four 6LoWPAN channels, in which each WLAN channel interferes with four 6LoWPAN channels. WLAN devices also tend to transmit in a much higher power level than 6LoWPAN devices, resulting in longer interference distances. In a dense networking scenario, the interference could be worse due to the co-location of many DRRs and 6LoWPAN devices.

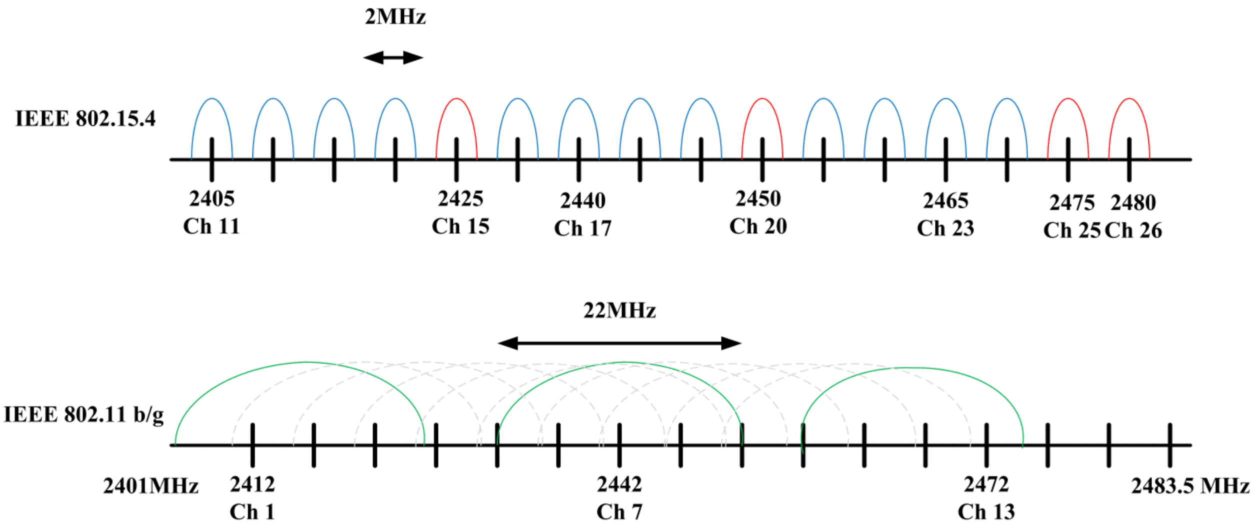


Fig 5-1 Transmission channels of the IEEE 802.15.4 and IEEE 802.11 standards in the 2.4 GHz band

5.2.2 IEEE 802.15.4 and IEEE 802.11 b/g MAC Protocols

The IEEE 802.11g standard defines the specifications of the physical layer and the MAC layer. The WLAN networks operate in the 2.4 GHz ISM band with 13 channels covering the allocated transmission band, in which each sub-band is 22 MHz wide. In this section, MAC protocols of the 6LoWPAN and WLAN networks are compared. As both the networks use the CSMA/CA random access protocol, the channel sensing and collision avoidance techniques have a significant impact on the QoS of these networks. The Distributed Coordination Function (DCF) is also discussed. Fig 5-2 shows the basic WLAN CSMA/CA algorithm. It has two carrier sensing approaches: physical carrier sensing and virtual carrier sensing. The former is performed in the physical layer by sensing the carrier signal energy on the transmission channel, whereas the latter is implemented in the MAC layer using the Network Allocation Vector (NAV). In this case, the NAV uses the duration field in the MAC frame to specify how long the frame will be transmitting and occupying the channel. With this information, the other WLAN stations will know the duration of the packet transmissions. Both the approaches are used to determine the channel status. If the channel is sensed busy, the station backs off for a random number of slots, which will be explained later in detail.

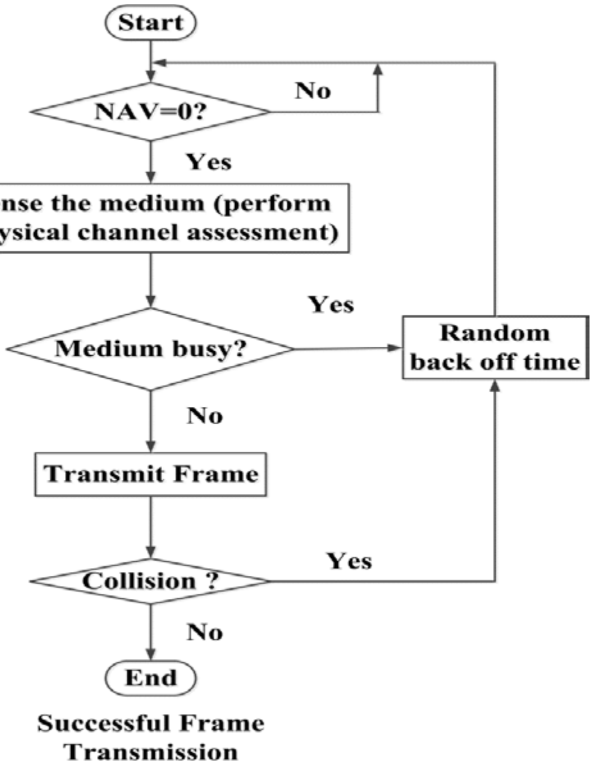


Fig 5-2 Flow chart of the IEEE 802.11 CSMA/CA algorithm [120]

Figure 5-3 shows the IEEE 802.11 CSMA/CA-based DCF packet transmission technique. The basic idea of the CSMA/CA algorithm is to listen before send. In other words, a station needs to sense the channel before starting its transmission in order to avoid packet collisions. As the channel is sensed busy, the station backs off for a random period of time and then senses the channel again; the process is repeated until the channel is found to be free.

Specifically, regardless of whether the channel is busy or idle, a station with a MAC Service Data Unit (MSDU) to transmit is forced to wait for a minimum duration of DCF interframe Space (DIFS). Following the waiting period, the sender can be in one of the two states. In the first case, the channel is found to be idle, and the sender has a pending packet to transmit. After the DIFS waiting period, the sender is allowed to directly transmit the packet, then waits for a Short Interframe Space (SIFS) until an ACK is returned. In the second case, after the DIFS period, as the channel is sensed busy, so the sender chooses a random number of time slots named the Contention Window (CW) to back off. The number of time slots is selected from a range uniformly distributed in a time interval [0, CW], where the CW falls within the range of [CW_{min}, CW_{max}]. After the first sensing, if the channel is found to be busy, the station repeats the above procedure until the channel is found to be idle with a successful transmission after the DIFS period. In addition, each WLAN node maintains a separate CW value indicating how many time slots it needs to wait before starting a transmission. The CW is initially set to be CW_{min}, and after an unsuccessful transmission (ACK not received or packet collision), the CW value is doubled, so the sender continues to back off with a lower chance of colliding with other WLAN packets. The upper bound of the CW is the CW_{max}, and the CW will be reset to the CW_{min} after either a successful transmission or the expiration of the retry limit.

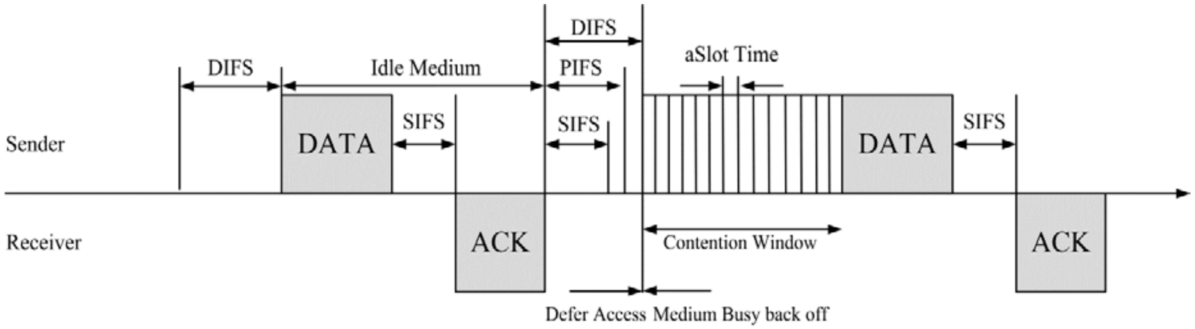


Fig 5-3 IEEE 802.11 WLAN Distributed Coordination Function

Figure 5-4 depicts how the contention window is incremented using the binary exponential back-off procedure, as shown in (5-1). Firstly, the CW is set to CW_{min}, which is the minimum value; the IEEE 802.11g standard uses 15 as the value of CW_{min}. More precisely, after an unsuccessful transmission, a re-try counter will be incremented, and a collided packet will be discarded when the re-try counter reaches its limit. It can be seen in Fig 5-4 that the CW is doubled several times due to collisions. The CW exponentially increases using (5-1), where the random $slot_{time}$ is the number of time slots in the CW and BE is the re-try counter.

$$\text{random slot}_{\text{time}} = 2^{\text{BE}} - 1, \tag{5-1}$$

where random $slot_{time}$ is a random backoff time, BE is the Backoff Exponent referred to as the number of retransmission attempts due to collisions.

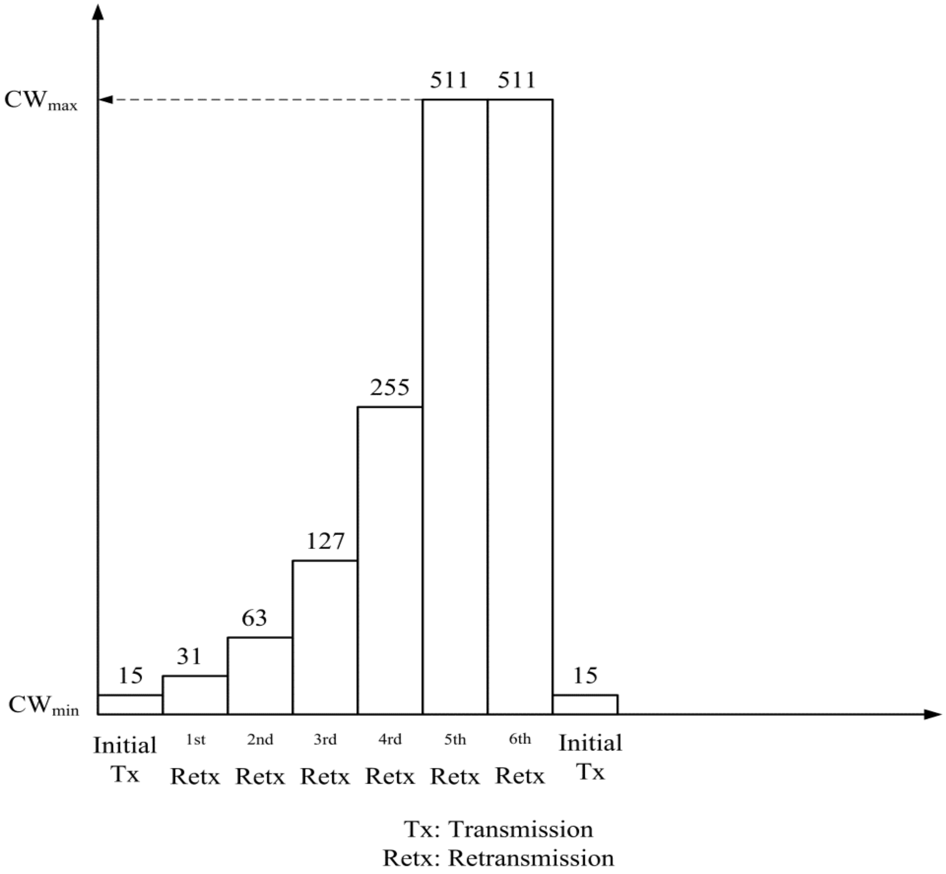


Fig 5-4 Binary exponential back-off

In contrast, the IEEE 802.15.4 MAC layer CSMA/CA procedure has been described in chapter 3. The CSMA/CA procedure is used with a CAP period followed by the inactive period as shown in Fig 5-5. For example, Fig 5-6 illustrates two cases when a sender has pending packets to transmit. The first case is after the random back off time, the channel is sensed to be busy; in the second case, after the random back-off, the sender performs two CCAs to transmit the pending data. The data is transmitted if the idle channel is detected by two consecutive CCAs. More precisely, the sender chooses a random number of back-off slots, which are called contention window in WLAN. After the back-off, the sender performs the clear channel assessment twice, and if any of those assessments fails, i.e., the channel is detected busy, the sender performs a binary exponential back-off to avoid packet collisions. On the other hand, if the two successive CCAs are successful, i.e., the channel is considered to be idle during the two CCAs, the sender immediately starts to transmit a packet. Specifically, if the channel is found to be idle, the CW of the IEEE 802.15.4 MAC is decreased by one. As the channel is detected to be idle again, the CW value is gradually decreased to zero, and then the packet is transmitted. If the channel is found to be busy twice, the CW is reset to two, and the sender continues to sense the channel using the mechanism, as shown in Fig 5-7. Upon receipt of a packet, the receiver waits for a Short Interframe Space (SIFS) or a Long Interframe Space (LIFS) period and then replies with an ACK packet.

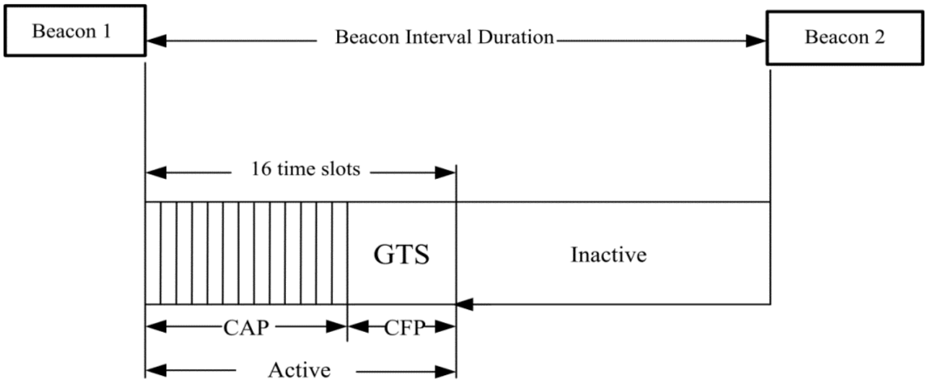


Fig 5-5 IEEE 802.15.4 superframe structure

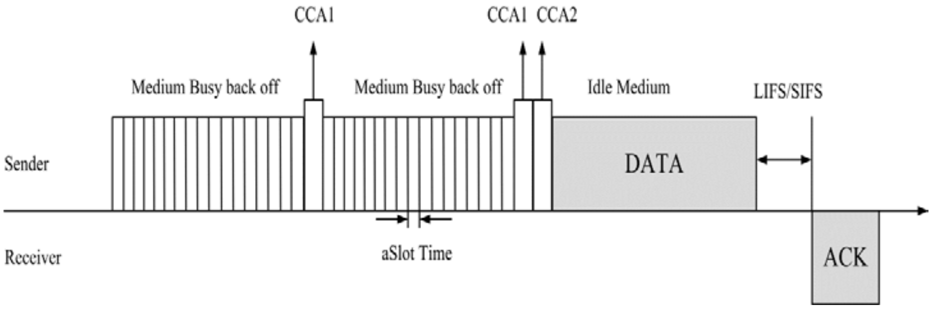


Fig 5-6 IEEE 802.15.4 CSMA/CA algorithm

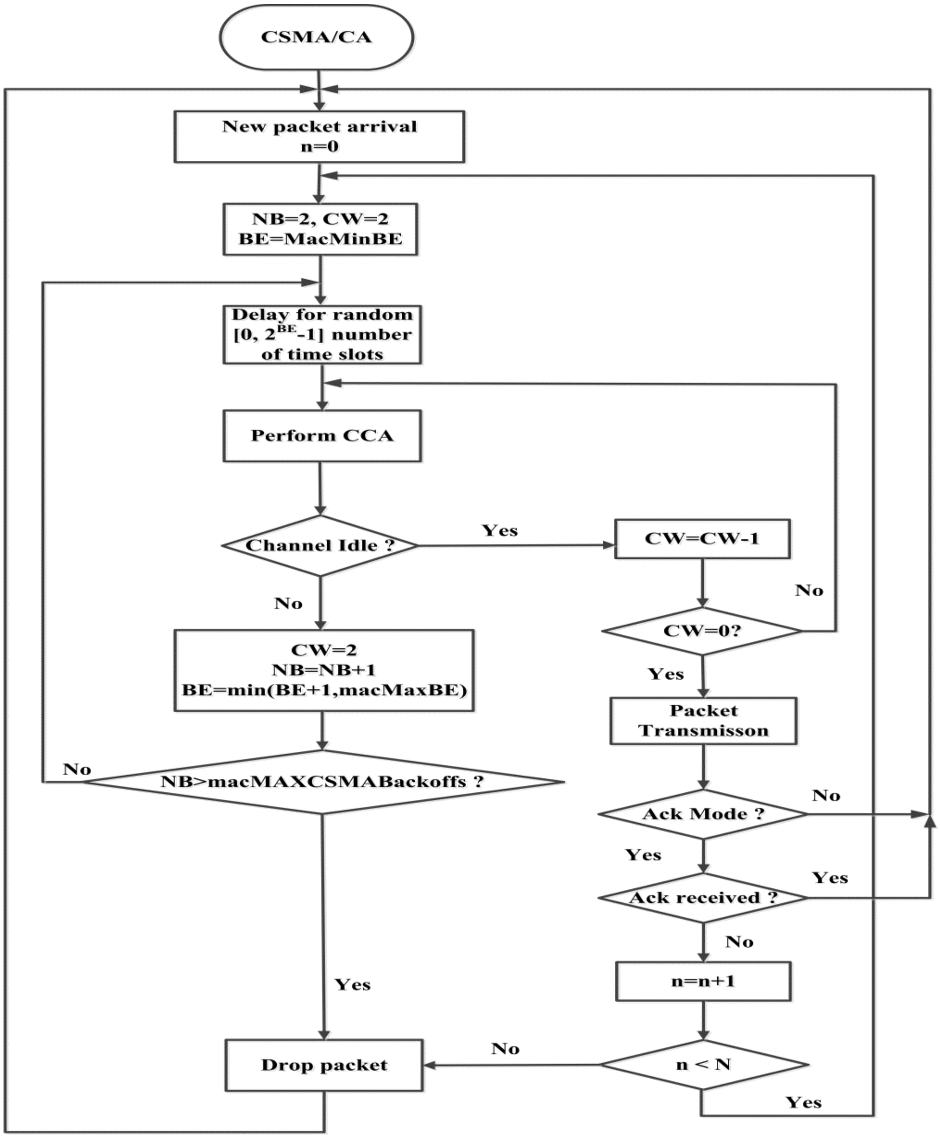


Fig 5-7 Flow chart of IEEE 802.15.4 CSMA/CA algorithm [66]

Although the IEEE 802.15.4 and IEEE 802.11 standards use the CSMA/CA MAC procedures to avoid collisions, there are distinct differences between them in terms of the back-off algorithm and the CCA procedure detecting the channel status. The main differences are: (1) IEEE 802.15. 4 network tasks such as back-offs, the CCA and channel access time is required to start at the boundary of time slots, while among IEEE 802.11 network tasks, only the back-off counter is related to time slots; (2) an IEEE 802.11 WLAN senses the channel after back-off, while an IEEE 802.15.4 network senses the channel after the back-off counter (two by default) decreases to zero; and (3) an IEEE 802.11 contention window refers to a number of back-off slots used to avoid collisions, while an IEEE 802.15.4 device does not use this number of back-off slots as the contention window; instead, the two CCAs' procedure is named as the contention window, which is reset to two when the channel is sensed busy. The other differences are listed in the Table 5-1.

Table 5-1 Differences between IEEE 802.15.4 and IEEE 802.11g WLAN

Parameter in Two MAC Protocols	**IEEE 802.15.4**	**IEEE 802.11g WLAN**
Transmit Power	-32dBm to 0 dBm	0 to 20 dBm
Receiver Sensitivity	-98dBm	-95 dBm
Bandwidth	2 MHz	22 MHz
CCA threshold	-85 dBm	-84 dBm
Back-off unit	320 μs	9 μs
SIFS	192 μs	10 μs
DIFS	N/A	28 μs
CCA	128 μs	N/A
CW$_{min}$	2	15
CW$_{max}$	N/A	1023
Center Frequency of the First Channel	2410 MHz	2412 MHz
Payload Size	80 bytes	1500 bytes

5.2.3 Inter-Network Collisions in the Proposed Heterogeneous Network

Given the characteristics of the IEEE802.15.4 and IEEE802.11 networks, it would be difficult for them to coexist under the same license-free 2.4 GHz band if both networks accidently share the overlapping channel. In a dense network scenario, where the 6LoWPAN nodes and the DRR coexist and share the same channel as shown in Fig 5-15, the DRR mode could give rise to inter-network collisions; that is, the WLAN side of the DRR will adversely affect the 6LoWPAN network. If the size of the network is small, switching to a free channel is possible to avoid inter-network collisions. However, if the size of the network is large and the number of DRRs is high, switching to a free channel to avoid inter-network collisions would become difficult, especially when multiple WLAN nodes contend the channel. As shown in Fig 5-1, three different 802.11g channel 1, 6 and 13 overlaps with most of the IEEE 802.15.4 channels, so it would be difficult for the 6LoWPAN network to change channels to avoid inter-network collision in a dense scenario.

Section 2.3.2 has summarised the traditional approaches to mitigating inter-network collisions and explained the factors impacting on the network performance. Most research studies analysed the inter-network collisions from three aspects: frequency, time and power. Firstly, as both the WLAN and WPAN networks use overlapping channels with a 2 MHz offset between the centre frequencies of the two networks, the frame error rate could rise up to 70% [121]. It is noted that in this study the frame error rate sharply dropped as the distance of two central frequencies increased. In particular, as it increased to 7 MHz, the frame error rate declined to zero. Using a larger IEEE 802.15.4 packet size might increase the frame error probability as a larger-sized packet experiences a longer collision duration. Secondly, the transmission power is an important factor. An IEEE 802.11g WLAN usually transmits power between levels from 1 mW to 250 mW, whereas an IEEE 802.15.4 network typically operates at 1 mW. These different levels of the transmission power can cause more inter-network collisions. The IEEE 802.15.4 network is therefore more susceptible to inter-network collisions. Specifically, the receive sensitivity of the IEEE 802.15.4 network is recommended as -98 dBm, whereas the IEEE 802.11g is -95 dBm depending on the modulation and coding scheme. Due to use of higher transmission power by the IEEE 802.11g networks, IEEE 802.15.4 networks may not successfully transmit packets. The IEEE 802.15.4 standard [66] has a section stressing the coexistence issues between other ISM standards and the IEEE 802.15.4 standard, and suggests an IEEE 802.11 WLAN should operate at a low transmit power to mitigate the inter-network collisions.

5.2.4 Inter-Network Model Analysis

To study the inter-network collisions, a heterogeneous 6LoWPAN/WLAN model is presented in Fig 5-8. The 6LoWPAN network collects data from the end devices, aggregates the data and transmits them to a sink located a distance from the end devices. Data are aggregated at the DRR that sends the aggregated packets via the WLAN link to reduce the number of hops between the end devices and the sink node. The IEEE 802.11g and 802.15.4 transceivers use an overlapping channel in a dense networking environment. The collision model for the heterogeneous area network is discussed below.

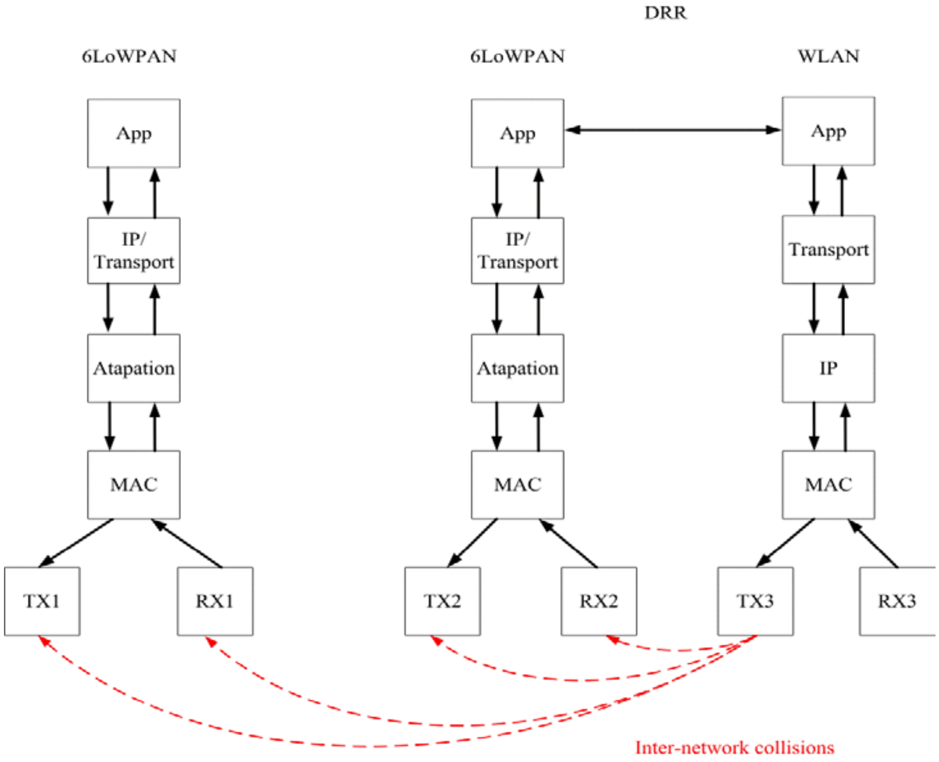


Fig 5-8 Dual-radio 6LoWPAN and IEEE 802.11 DRR inter-network collision model

Given the above reasons, the coexistence model demonstrates how inter-network collisions occur in two scenarios: a scenario in which the IEEE 802.15.4 and IEEE 802.11 transceivers can detect each other’s transmissions; and the other scenario, in which the 802.15.4 network can detect the 802.11network transmissions, but not vice versa.

Figure 5-9 presents two cases where the inter-network collisions occur. Both cases are illustrated in the overlapping area where the 6LoWPAN and WLAN packets are transmitted. The first case describes when the DRR cannot hear the 6LoWPAN devices two hops away. Due to the oversight of 6LoWPAN devices, the DRR could adversely affect the 6LoWPAN transmissions. This is because the DRR accesses the idle channel faster than the 6LoWPAN nodes because the back-off time slots for the DRR and 6LoWPAN node are 9 µs and 320 µs, respectively. Therefore, the inter-network collisions could affect the performance of the heterogeneous area network. The second case shows that the DRR replies to the 6LoWPAN node with an ACK packet. Since the ACK packet does not use the CSMA/CA protocol, they can be easily interrupted by the packets sent by the DRR. As the WLAN and 6LoWPAN transceivers are in the one node DRR, the inter-network collisions under this circumstance could be detrimental to the system.

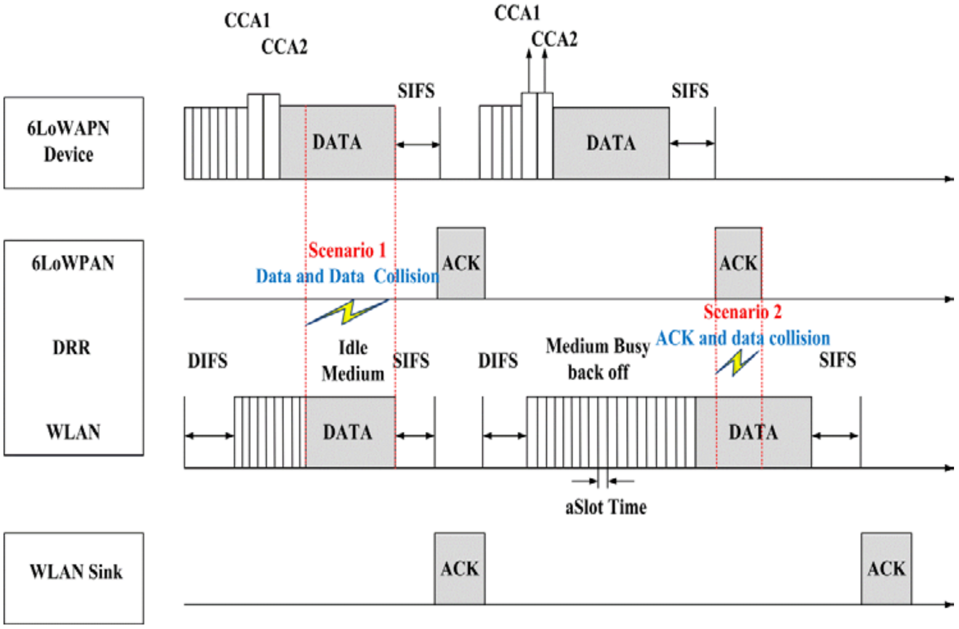


Fig 5-9 Two cases when inter-network collisions occur

5.3 Throughput Analysis for the 6LoWPAN Network with WLAN Inter-Network Collisions

5.3.1 IEEE 802.15.4 Markov Chain

The IEEE 802.11 Markov chain model has been modified into the IEEE 802.15.4 Markov chain model by adding two states indicating two Channel Clear Assessments (CCAs), as shown in Fig

1. Let s (t) be the stochastic process and represent the backoff stages [0,..m] for a given device at time t, where m is the number of backoff allowed for each packet; let b(t) be the stochastic process and represent the remaining backoff slots [-1, W_0-1] before the given device gives the first CCA. Then we let $b_{i,j} = \lim_{t\to\infty} P\{s(t) = i, b(t) = j\}, i \in (0, m), j \in (-1, W_i - 1)$, where $b_{i,j}$ is any given state shown in the Fig 5-10, $b_{i,0}$ and $b_{i,-1}$ are the states corresponding to the first CCA and second CCA time slots, respectively, and $W_i = W_0 \times 2^{min(i,\ BE_{max} - BE_{min})} - 1;\ \alpha$and β present the busy channel probability at the first CCA and at the second CCA, respectively. For simplicity, $b_{i,j}$ is expressed as (i, j) in the state of each circle.

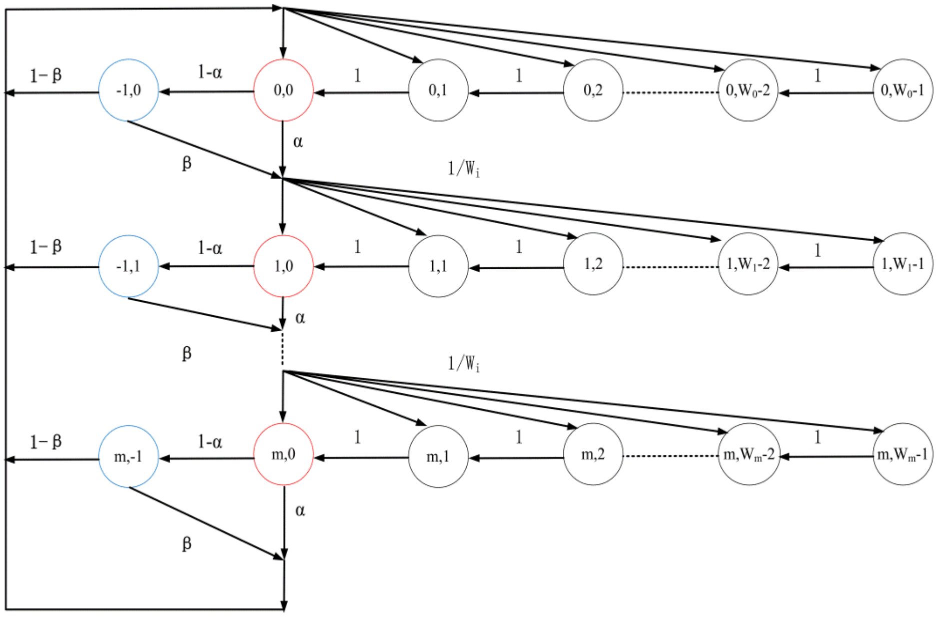


Fig 5-10 Discrete time Markov chain model for the IEEE 802.15.4 standard

The Markov Chain model has the following transition probabilities:

1. At the beginning of each slot time, the slot time is idle and the backoff counter is decreased by one.

   $p\{i, j|i, j + 1\} = 1 \qquad i \in [0, m] \qquad j \in [0, Wi - 2]$

2. After the backoff counter is decreased to zero, it starts the first CCA. If the first CCA is identified idle, the given device moves to the next time slot, beginning the second CCA. \

$p\{i,-1|i,0\} = 1-\alpha \qquad i \in [0,m]$

3. When the channel is sensed busy by the first CCA, the number of backoff increases and the new backoff counter is uniformly chosen in the range $[0, W_0 - 1]$,
   $p\{i,j|i-1,0\} = \alpha/W_i \qquad i \in [1,m] \qquad j \in [0, W_i - 1]$

4. When the channel is sensed busy by the second CCA, the number of backoff increases and the new backoff counter is uniformly chosen in the range.
   $p\{i,j|i-1,-1\} = \beta/W_i \qquad i \in [1,m] \qquad j \in [0, W_i - 1]$

5. When the channel is sensed idle by the second CCA, a device begins to send a packet, and a cycle begins.
   $p\{0,j|i,-1\} = (1-\beta)/W_0 \qquad i \in [1, m-1] \qquad j \in [0, W_0 - 1]$

6. When the number of backoff reaches the maximal value, which is four by default, and the channel is still sensed busy at the first CCA, the packet will be discarded.
   $p\{0,j|m,0\} = \alpha/W_0 \qquad j \in [0, W_0 - 1]$

7. When the number of backoff reaches the maximal value, which is four by default, and the channel is still sensed busy at the second CCA, the packet will also be discarded.
   $p\{0,j|m,-1\} = \beta/W_0 \qquad j \in [0, W_0 - 1]$

A packet can be transmitted successfully if the given device can finish two CCAs while the other devices are in the backoff states. Once the backoff counter is decremented to zero, a given device needs to go through following three steps: firstly, it reaches the sensing state $b_{i,0}$; secondly, it senses the channel using two CCAs with the probabilities $\alpha\ and\ \beta$; and thirdly, the packet is transmitted successfully with the probability P_{trs} without any collisions. The probabilities corresponding to these three cases are unknown and can be derived as follows. The probability that a given device is at the sensing sate can be calculated to further derive the system throughput. Let τ be the probability that a given device starts to perform the first CCA, at the state $(b_{j,0})$, out of all the backoff states.

$$\tau = \frac{\sum_{i=0}^{m} b_{i,0}}{\sum_{i=0}^{m} \sum_{j=0}^{W_i - 1} b_{i,j}} \tag{5-2}$$

$$= \frac{b_{0,0}(1 - (\alpha + (1-\alpha)\beta)^{m+1})}{\sum_{i=0}^{m}(W_0 2^{\min(BE_{\min}+i,\ BE_{\max})} - 1)(\alpha + (1-\alpha)\beta)^{i}} \times \frac{1}{1 - (\alpha + (1-\alpha)\beta)}$$

As n device contend the channel, each device sensing the channel with the probability τ, so at least one device transmit in a considered time with probability P_{tr}, which is given by the following:

$$P_{tr} = 1 - (1 - \tau)^{n}. \tag{5-3}$$

A packet can be successfully transmitted conditioned on the fact that only a given device transmits while the remaining $n - 1$ devices are in the backoff states and without WLAN packet collisions, so the probability P_{trs} at least one given device can successfully transmit is given by:

$$P_{trs} = \frac{n\tau(1-\alpha)(1-\beta)\gamma}{P_{tr}} = \frac{\tau(1-\alpha)(1-\beta)\gamma}{1-(1-\tau)^{n}}. \tag{5-4}$$

where γ is the probability that $\mathrm{n} - 1$ devices do not perform the first CCA and are interfered with by WLAN packet transmissions, which will be explained later. On the other hand, the throughput S is expressed as the ratio of the transmitted payload in a time slot to the length of the time slot.

$$\mathrm{S} = \frac{E[payload\ transmitted\ in\ a\ time\ slot]}{E[Length\ of\ a\ slot\ time]} \tag{5-5}$$

Where numerator denotes the number of payload size successfully transmitted in a slot time, and the denominator represents the average duration of a time slot, which can have three statuses: the slot is empty, the slot is sensed busy and the slot is used to transmit a packet irrespective of the packet success or collisions.

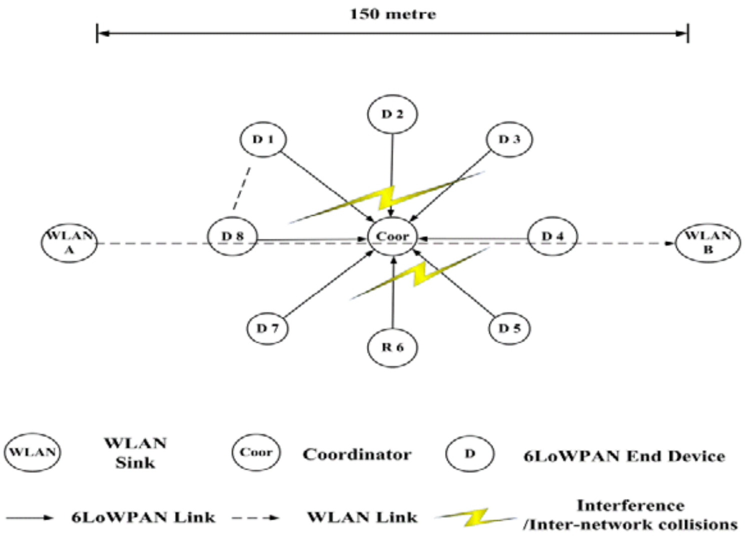


Fig 5-11 the 6LoWPAN network with a star topology under inter-network collisions

5.3.2 IEEE 802.15.4 Throughput under the Impact of WLAN

WLAN packets can adversely affect the 6LoWPAN devices, so the interference model can be simplified into a pair of WLAN devices and several 6LoWPAN devices in a star topology, as shown in Fig 5-11. The WLAN A is the sender, while the WLAN B is the receiver. The IEEE 802.11g standard and the WLAN are used interchangeably in this document. As the WLAN nodes start to transmit, the inter-network collisions occur between the 6LoWPAN and the WLAN devices. The derivation of the 6LoWPAN coordinator throughput under the influence of the inter-network collision is discussed in this section. We derive the first and second probabilities α and β in the Markov chain model where the WLAN inter-network collisions affect the 6LoWPAN devices.

The given 6LoWPAN device senses the channel busy at the first CCA and deters its transmission in two cases, as shown in Fig 5-12. (1) when a WLAN device is transmitting, a given 6LoWPAN device is about to transmit while the other 6LoWPAN devices are transmitting or not transmitting (period 1 and 2), and (2) the adjacent 6LoWPAN device transmissions affect the given 6LoWPAN device when the WLAN device is not transmitting (period 3). In period 4, the given device senses the channel idle at the first CCA.

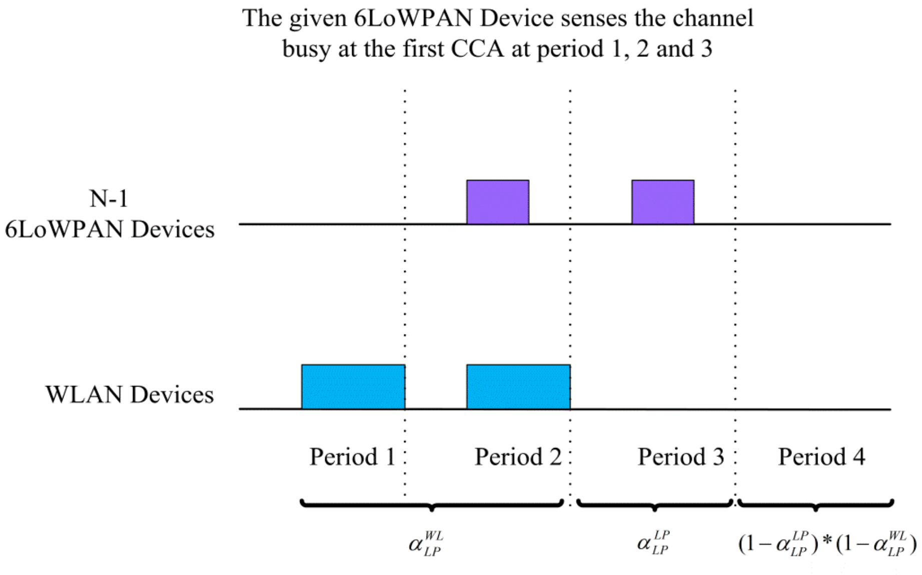

The given 6LoWPAN Device senses the channel busy at the first CCA at period 1, 2 and 3
N-1 6LoWPAN Devices
WLAN Devices
Period 1
Period 2
Period 3
Period 4
α_{LP}^{WL}
α_{LP}^{LP}
$(1-\alpha_{LP}^{LP})*(1-\alpha_{LP}^{WL})$

Fig 5-12 The given 6LoWPAN device senses the channel busy at the first CCA

Therefore, α can be expressed as follows:

$$\alpha = 1 - (1 - \alpha_{LP}^{WL})(1 - \alpha_{LP}^{LP}), \tag{5-6}$$

Where α_{LP}^{WL} and α_{LP}^{LP} denote the first CCA busy probabilities of the given device due to the WLAN only and 6LoWPAN only. We assume that the 802.11 g packet size is fixed and the packet arrives in a Poisson Distribution manner, so if the WLAN packet arrival rate is λ_{WL} and the packet size is L_{WL}, the α_{LP}^{WL} can be expressed as:

$$\alpha_{LP}^{WL} = \ exp(L_{WL}/R_{WL})\lambda_{WL} \tag{5-7}$$

On the other hand, α_{LP}^{LP} can be derived considering the impact of the 6LoWPAN and WLAN. Let P_{to}^{*} be the probability that at least one 6LoWPAN device out of $\mathrm{n} - 1$ 6LoWPAN devices performs the first CCA while the given device does not perform the CCA and the WLAN devices do not transmit packets in two following CCAs. P_{to}^{*} can be expressed as follows:

$$P_{to}^{*} = (1 - \tau)(1 - (1 - \tau)^{n-1})(1 - \alpha_{LP}^{WL})^{\left\lceil 2\lceil L_{CCA}\rceil \frac{T_u^{LP}}{T_u^{WL}} \right\rceil} \tag{5-8}$$

Where $\left\lceil 2\lceil L_{CCA}\rceil \frac{T_u^{LP}}{T_u^{WL}}\right\rceil$ means the WLAN does not transmit for two CCAs' time and L_{CCA}, T_u^{LP} and T_u^{WL} denote the 6LoWPAN's CCA duration in 802.15.4 unit backoff time, 6LoWPAN backoff unit in second and 802.11 backoff time in second, respectively. Next, let P_{so}^* be the probability that among the $\mathrm{n}-1$ 6LoWPAN devices, only one successful 6LoWPAN transmission occurs without any interference from the other 6LoWPAN and the WLAN devices. Thus, P_{so}^* can be derived as follows:

$$P_{so}^* = (n-1)\tau_{LP}^*(1-\tau_{LP}^*)^{n-1}(1-\alpha_{LP}^{WL})^{\left\lceil (2\lceil L_{CCA}\rceil + L_S)\frac{T_u^{LP}}{T_u^{WL}}\right\rceil} \Big/ P_{to}^* \tag{5-9}$$

Where $\left\lceil (2\lceil L_{CCA}\rceil + L_S^{LP})\frac{T_u^{LP}}{T_u^{WL}}\right\rceil$ means the 6LoWPAN device performs two consecutive CCAs and successfully transmit a packet with L_S^{ZB} length without the inter-network collisions. As a result, the α_{LP}^{LP} can be expressed as below:

$$\alpha_{LP}^{LP} = \frac{P_{to}^*(P_{so}^*T_{bs}^* + (1-P_{so}^*)T_{bc}^*)}{P_{to}^*(P_{so}^*T_{os}^* + (1-P_{so}^*)T_{oc}^*) + 1 - T_{os}^*} \tag{5-10}$$

Where T_{os}^* and T_{oc}^* represent the number of backoff slots for a successful 6LoWPAN transmission and a collision in the presence of the inter-network collisions. Parameters T_{bs}^* and T_{bc}^* denote the busy backoff slots out of T_{os}^* and T_{oc}^*. Specifically, $T_{os}^* = 2\lceil L_{CCA}\rceil + L_{LP} + \delta + L_{ACK}$ and T_{oc}^*=$2\lceil L_{CCA}\rceil + L_{LP}$; $T_{bs}^* = L_{LP} + L_{ACK}$ and $T_{bc}^* = L_{LP}$, where L_{ACK} and δ represent the ACK packet length in a time slot, respectively, and the ACK waiting duration in time slot. Substituting (5-7) and (5-10) into (5-6), then it becomes (5-11).

$$\begin{aligned} \alpha = 1 - (1 - exp(L_{WL}/R_{WL})\lambda_{WL}) \\ \times\left(1 - \frac{P_{to}^*(P_{so}^*T_{bs}^* + (1-P_{so}^*)T_{bc}^*)}{P_{to}^*(P_{so}^*T_{os}^* + (1-P_{so}^*)T_{oc}^*) + 1 - T_{os}^*}\right) \end{aligned} \tag{5-11}$$

Similarly, the second CCA busy probability of a given 6LoWPAN device in the presence of the WLAN's inter-network collisions and the other 6LoWPAN device packet collisions can be expressed as:

$$\beta = 1 - (1 - \beta_{LP}^{WL})(1 - \beta_{LP}^{LP}), \tag{5-12}$$

Where β_{LP}^{WL} and β_{LP}^{LP} are the second CCA busy probabilities of a given 6LoWPAN device due to only the WLAN and only the other 6LoWPAN devices. The β_{LP}^{WL} can be expressed as:

$$\beta_{LP}^{WL} = (L_{WL}/R_{WL}) \times \frac{1}{1 - \alpha_{LP}^{WL}}, \tag{5-13}$$

So β_{LP}^{LP}can be expressed as:

$$\beta_{ZB}^{ZB} = \frac{P_{to}^{*}(P_{so}^{*}T_{is}^{*} + (1 - P_{so}^{*})T_{ic}^{*})}{P_{to}^{*}(P_{so}^{*}T_{os}^{*} + (1 - P_{so}^{*})T_{oc}^{*}) + 1 - T_{os}^{*}} \times \frac{1}{1 - \alpha_{LP}^{LP}} \tag{5-14}$$

Where $T_{is}^{*} = 2\lceil L_{CCA} \rceil + \delta$ and $T_{ic}^{*} = 2\lceil L_{CCA} \rceil$, substituting (5-13) and (5-14) into (5-12), then β_{LP}^{*} can be expressed as:

$$\beta = 1 - (1 - exp(L_{WL}/R_{WL})\lambda_{WL}) \tag{5-15}$$

$$\times \left(1 - \frac{P_{to}^{*}(P_{so}^{*}T_{is}^{*} + (1 - P_{so}^{*})T_{ic}^{*})}{P_{to}^{*}(P_{so}^{*}T_{os}^{*} + (1 - P_{so}^{*})T_{oc}^{*}) + 1 - T_{os}^{*}}\right) \times \frac{1}{1 - \alpha_{LP}^{LP}}$$

From (5-2), (5-5), (5-6) and (5-12), the 6LoWPAN throughput in the presence of the inter-network collisions can be calculated as follows:

$$S = \frac{n\tau(1 - \alpha)(1 - \beta)\gamma L_{LP}/R_{LP}}{(1 - \tau) + \tau\alpha + 2\tau(1 - \alpha)\beta + \tau(1 - \alpha)(1 - \beta)(\gamma T_{os}^{*} + (1 - \gamma)\, T_{oc}^{*})} \tag{5-16}$$

Where γ denotes the probability that there are no 6LoWPAN CCA attempts and that when a 6LoWPAN packet is being transmitted, there is no WLAN transmission. The probabilities of the above two conditions are represented as $(1 - \tau_{LP}^{*})^{n-1}$and $\exp(1 - \lambda_{WL} * L_{LP} * \frac{T_u^{LP}}{T_u^{WL}}\ )$.

$$\Gamma = (1 - \tau_{ZB}^{*})^{n-1} * \exp(1 - \lambda_{WL} * L_{LP} * \frac{T_u^{LP}}{T_u^{WL}}\ ). \tag{5-17}$$

5.3.3 Results

To calculate the 6LoWPAN coordinator throughput S, a theoretical model was proposed to solve eight non-linear equations, in which eight unknown variables representing the corresponding probabilities from (5-1) to (5-17) were solved using the numerical method in MATLAB. S represents the 6LoWPAN coordinator throughput with the inter-network collisions. The key 6LoWPAN parameters are in table 1, and key WLAN parameters are in table 2.

Table 5-2 Key 6LoWPAN parameters

Name	Value	Description
$\boldsymbol{L_{LP}}$	12.8 slots	Length of the 6LoWPAN packet
$\mathbf{L_{LP}}$	1024	Length of the 6LoWPAN packet in bits
$\boldsymbol{L_{ACK}}$	1.1 slots	Length of the ACK packet
$\boldsymbol{T_{CCA}}$	0.4 slot	CCA duration
$\boldsymbol{\delta}$	1 slot	ACK wait duration
$\boldsymbol{T_u^{ZB}}$	320 μs	backoff duration in unit μs
$\boldsymbol{R_{ZB}}$	250	6LoWPAN data rate in kbps
minBE	3	Minimal backoff exponent
MaxBE	5	Maximal Backoff exponent
maxCSMABackoff	4	The maximal number of backoff times
$\boldsymbol{\lambda_{LP}}$	17	6LoWPAN packet inter-arrival rate pkt/sec
n	5, 10, 20	The number of 6LoWPAN devices

Table 5-3 Key WLAN parameters

Name	Value	Description
$\boldsymbol{T_u^{WL}}$	9	WLAN backoff duration in unit μs
$\boldsymbol{L_{WL}}$	1000	WLAN packet length in μs
$\boldsymbol{L_{WL}}$	750	WLAN packet length in bytes
$\mathbf{CW}_{\mathbf{min}}$	15	Minimum contention window size
$\mathbf{CW}_{\mathbf{max}}$	1023	Maximum contention window size
$\boldsymbol{R_{WL}}$	1	WLAN data rate in Mbps
$\boldsymbol{\lambda_{WL}}$	0, 16, 33, 50, 66, 83, 100, 116, 133, 150, 166	WLAN packet inter-arrival rate pkt/sec

The 6LoWPAN coordinator throughput under the influence of WLAN is presented in Fig 5-13. It can be seen that the throughput decreases with the increment of the input WLAN load. Without the WLAN load, the normalized throughput is 0.34, and it sharply drops to less than 0.01 as the normalized the normalized WLAN load increases to one. It was also found that as the number of 6LoWPAN end devices increases from 5 to 20, the 6LoWPAN coordinator throughput drops from 0.34 to 0.2 with no interference from the WLAN devices. It can also be seen Fig 5-13 that the throughput of 20 6LoWPAN devices is lower than that of 10 6LoWPAN devices. This is not only attributed to the inter-network collisions but attributed to the intra-network collisions.

The OPNET simulation results are presented in Fig 5-14. It can be seen that the 6LoWPAN throughput dropped from 80 pkt/sec to 3 pkt/sec with five 6LoWPAN nodes as the WLAN loads increased. The more 6LoWPAN nodes participated in packet transmissions, the more throughput dropped under the impact of inter-network collisions. The OPNET simulation results are added to Fig 5-13 as simulation results. Above all, the theoretical results agree with the simulation results, which have validated the theoretical model corresponding to Fig 5-10.

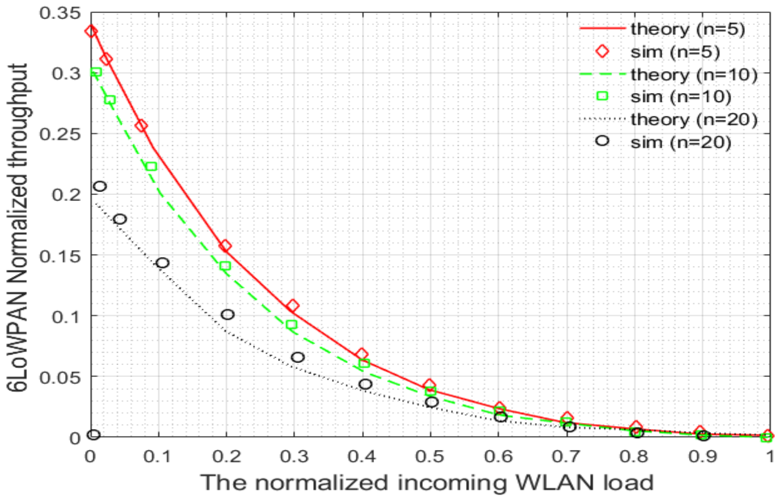


Fig 5-13 6LoWPAN coordinator throughput under the WLAN impact

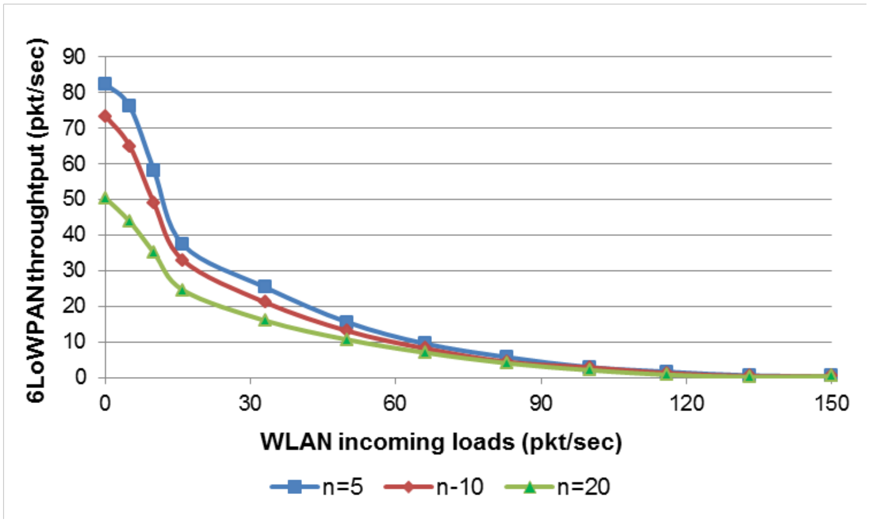


Fig 5-14 OPNET simulation results

5.4 Proposed Dense Heterogeneous Area Network Architecture

To extend the transmission range and increase the packet delivery ratio, a heterogeneous area network was proposed in Chapter 4. The proposed network can be used for smart city/smart grid applications as well as many other IoT applications as illustrated in Fig 5-15. The network is composed of 64 sensor nodes, in which are divided into eight clusters and each cluster has a 6LoWPAN router serving as the cluster head. The DRR discussed in Chapter 4 is converted into a Multi-Frequency Dual-Radio Router (MFDRR) as shown in Fig 5-16, so the dense heterogeneous network can be proposed in Fig 5-15. The MFDRR uses multiple IEEE 802.15.4 transceivers to communicate with the routers using different transmission channels, and Fig 5-15 shows the neighbouring routers using channel 11 and 12 to avoid intra-network collisions. The MFDRR with two transceivers can directly communicate with both routers. The network model shown in Fig 5-15 can reduce intra-network and inter-network collisions with the Blank Burst signaling technique.

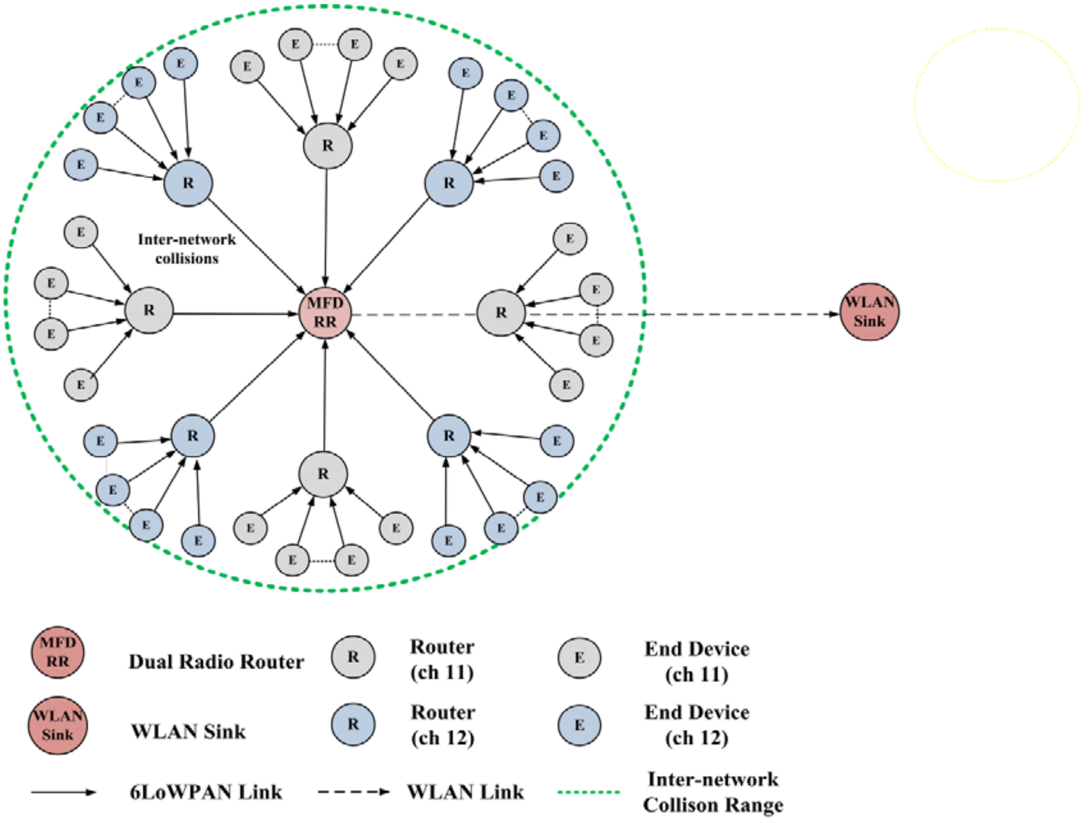


Fig 5-15 Proposed dense heterogeneous area network

Figure 5-16 shows the two protocol stacks of the MFDRR: the 6LoWPAN and WLAN stacks. The 6LoWPAN side of the MFDRR uses two MAC layers and two physical interfaces that can support two frequencies; the WLAN stack uses a fixed channel that overlaps with the two channels used by the 6LoWPAN devices. An aggregation buffer sits in the middle of the two stacks and stores the 6LoWPAN payloads for packet aggregation. In addition, the packet processing within the MFDRR begins in the following way: upon receiving a sensor packet from the 6LoWPAN MAC layer, the 6LoWPAN stack strips off the headers and forwards the payloads to the application layer. Subsequently, all the payloads are stored in the aggregation buffer that aggregates them into a WLAN payload for further transmissions.

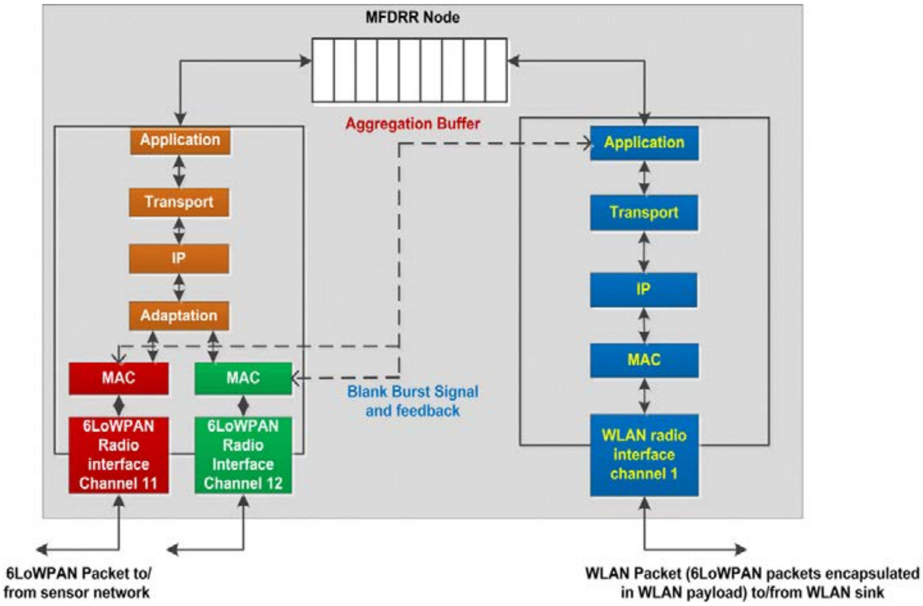

MFDRR Node
Aggregation Buffer
Application
Transport
IP
Adaptation
MAC
MAC
6LoWPAN Radio interface Channel 11
6LoWPAN Radio Interface Channel 12
Blank Burst Signal and feedback
Application
Transport
IP
MAC
WLAN radio interface channel 1
6LoWPAN Packet to/ from sensor network
WLAN Packet (6LoWPAN packets encapsulated in WLAN payload) to/from WLAN sink

Fig 5-16 MFDRR protocol supporting two 6LoWPAN transmission channels

5.4.1 OPNET Simulation Model

To measure the performance of the inter-network collision mitigation process, an OPNET model of the MFDRR was developed as shown in Fig 5-17. Based on the single-radio DRR OPNET model developed in Chapter 4, the model was further extended to a dual-radio 6LoWPAN model by adding two MAC layers at the bottom. To simulate the inter-network collisions, the OPNET pipeline stage was modified to enable the compatibility between the 6LoWPAN and WLAN models. The detail of the modification can be seen in Appendix B. The key part of the OPNET model is the MFDRR relaying packets from the 6LoWPAN devices to the WLAN sink. As can be seen in Fig 5-17, the MFDRR has two protocol models: the 6LoWPAN and WLAN models. The WLAN model connects the dual-radio 6LoWPAN model with two packet streams. The packet aggregation buffer was implemented in the module named DRR in the WLAN stack.

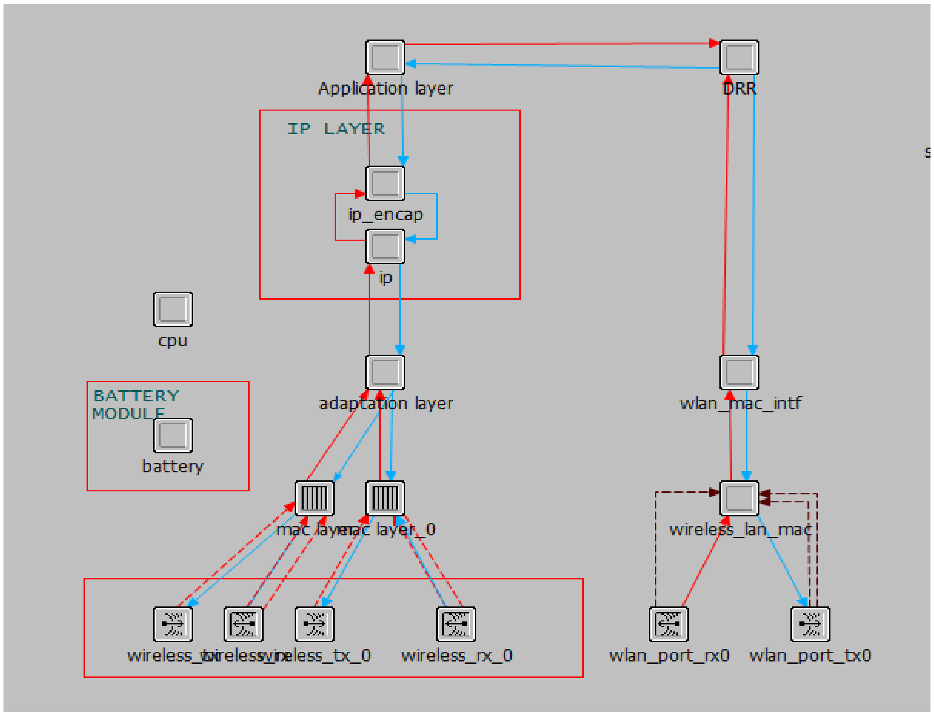


Fig 5-17 MFDRR OPNET simulation model

5.4.2 Effects of Inter-Network Collisions

In this section, the adverse impacts of inter-network collisions are evaluated in terms of the packet success rate, end-to-end delay and the throughput of the heterogeneous architecture. The network topology used for the performance analysis is shown in Fig 5-15. The key simulation parameters are listed in Table 5-4. Each simulation was run for 600 sec using multiple seed values, and the simulation results were plotted with a 95% confidence interval. In the initial simulation run, the MFDRR receives packets from the 6LoWPAN routers and then simply transmits the packet using the 802.11g transceivers to the data sink. Two scenarios are compared: (1) the 802.11g transceivers of the MFDRR share the same channel as the WPAN nodes and routers, and (2) the 802.11g transceivers of the MFDRR employ a non-overlapping channel.

Table 5-4 Key simulation parameters of the effect of inter-network collisions

Group Name	**Parameter**		**Value**
Simulation length			600 s
Network	Hop count		3
	Number of nodes		32
	Standard		6LoWPAN and IEEE 802.11g
	Operating frequency		2.4 GHz
	6LoWPAN channel number.		12
	IEEE 802.11g channel number		1
Propagation model	Free space path loss		
Dual Radio Router	6LoWPAN	BO	5
		SO	3
		Transmission Power	1.8 mW
	WLAN	Transmission Power	100 mW
Router	BO		5
	SO		3
	Start time	R1	0.122881 s
		R2	0.184325 s
		R3	0.122882 s
		R4	0.184324 s
		R5	0.122881 s
		R6	0.184325 s
		R7	0.122882 s
		R8	0.184324 s
	Transmission Power		1.8 mW
End device	Packet size		127 bytes
	Packet generation		Exponentially distributed
	Transmission Power		1 mw
	Packet inter-arrival rate		1, 1.2, 1.3, 1.5, 1.7 and 2pkts/s

Figure 5-18 shows the packet delivery ratio (PDR) of the heterogeneous network with or without inter-network collisions. In the presence of inter-network collisions, the PDR decreased from 90% to approximately 30%. This means that the 6LoWPAN devices experienced high packet losses as the traffic load increased from 0.5 to 2 pkts/s, while the PDR without the inter-network collisions gradually declined from 98% to 65%. The results show that inter-network collisions significantly reduce the network throughput due to a high level of collisions. As mentioned earlier, the WLAN packets can severely affect the 6LoWPAN devices.

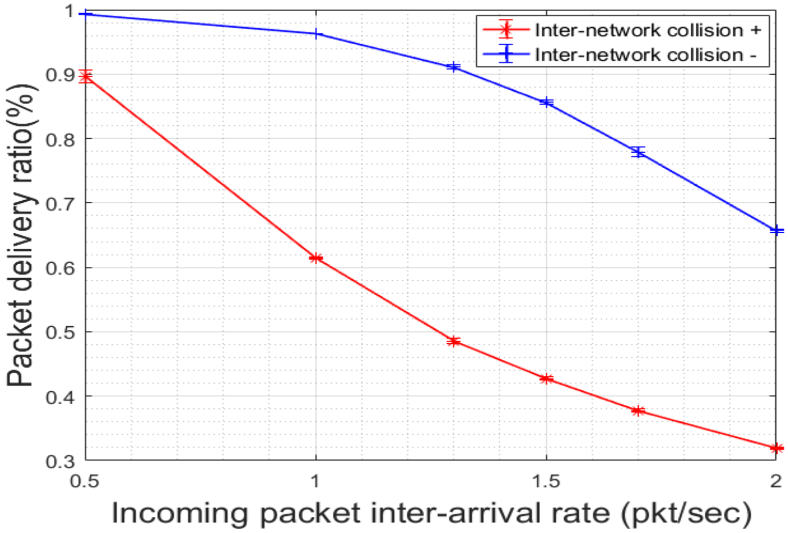


Fig 5-18 Packet delivery ratios with and without inter-network collisions with different traffic loads

The network performance is further indicated by the end-to-end delay as shown in Fig 5-19 for both collision scenarios. It can be observed that the end-to-end delay with inter-network collisions sharply rises from 0.28s to 0.75s, showing 2.67 times the delay rise as the traffic loads increased from 0.5 to 2 pkts/s. From the traffic load of 1.3 pkts/s and onwards, the delay reached a point from where the delay increased less rapidly as the network reached saturation point. In contrast, the case without inter-network collisions had a delay rising from 0.2s to 0.3s, which is a 50% increase with the increasing traffic loads. It is clear that inter-network collisions interrupted the 6LoWPAN transmissions, where the corrupted packets need to be retransmitted. With the increasing traffic load, the collision level grows as well, so more 6LoWPAN packets are held in the queue. The queuing time of the 6LoWPAN packets increases significantly, resulting in a longer end-to-end delay.

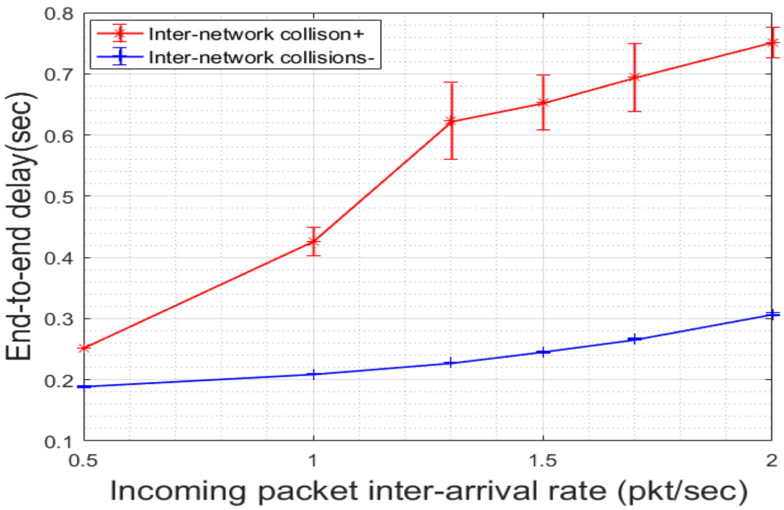


Fig 5-19 6LoWPAN end-to-end delay with and without inter-network collisions

The 6LoWPAN routers are the direct victims of the inter-network collisions. It can be observed from Fig 5-20 that the routers in the presence of inter-network collisions are losing more packets than those without inter-network collisions as the traffic load increases. Specifically, the number of 6LoWPAN packet losses soared from 1000 to 4000 as the traffic loads slightly increased from 0.5 to 1 pkts/s. As the traffic continued to increase from 1 to 2 pkts/s, the number of the 6LoWPAN packets loss fluctuated between 4000 and 4500 packets. The increase in 6LoWPAN packet losses from 1000 to 4000 reflects the adverse impacts of the inter-network collisions for the moderate traffic loads. Assuming that there are a large number of M2M devices, a WLAN station can easily interrupt the M2M device transmissions in the presence of inter-network collisions. At the high loads from 1 to 2 pkts/s, the number of 6LoWPAN packet losses remained stable as the network was saturated. In contrast, the number of packet losses without the inter-network collisions maintained at 300 packets. The gap between the two cases indicates that the inter-network collisions can be detrimental to M2M networks and applications.

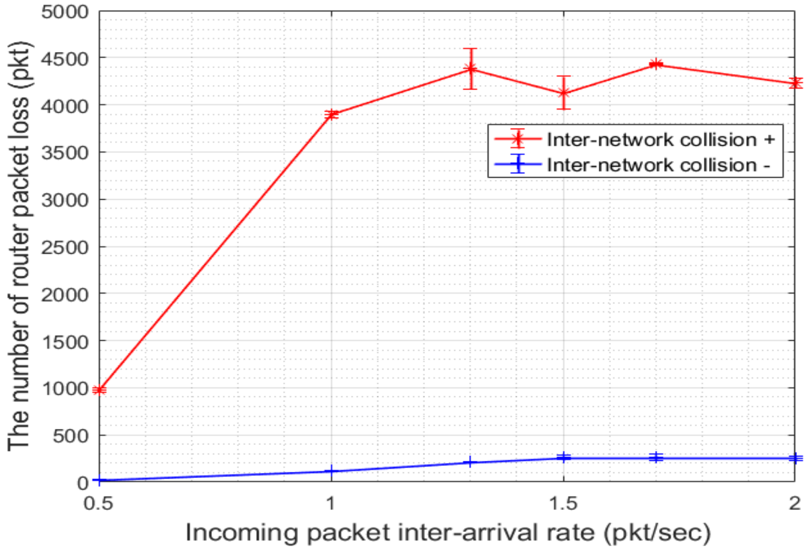


Fig 5-20 6LoWPAN router node packet loss with and without inter-network collisions

Figure 5-21 shows the number of router re-transmissions that indicate the collision statistics. This is because the packets are mostly lost due to the expiration of the packet retransmission threshold. The number of re-transmissions in the presence of inter-network collisions rapidly increases to 30000 and then stabilizes around 30000 as the load increases, whereas without inter-network collisions the number of collisions slowly rises to 15000, which is half of the previous case. Fig 5-22 illustrates the number of the end device re-transmissions. It can be seen that in the case of the inter-network collisions there were more re-transmissions than without internetwork collisions.

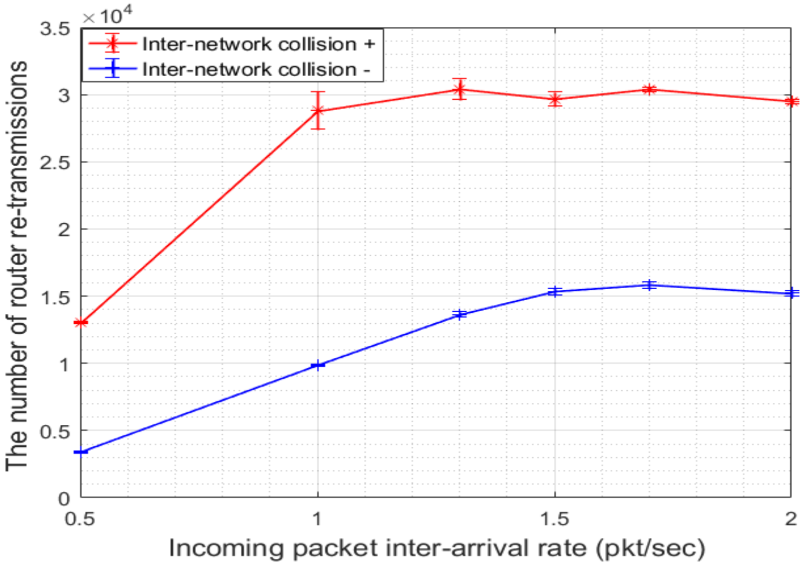


Fig 5-21 6LoWPAN Router retransmissions with and without inter-network collisions

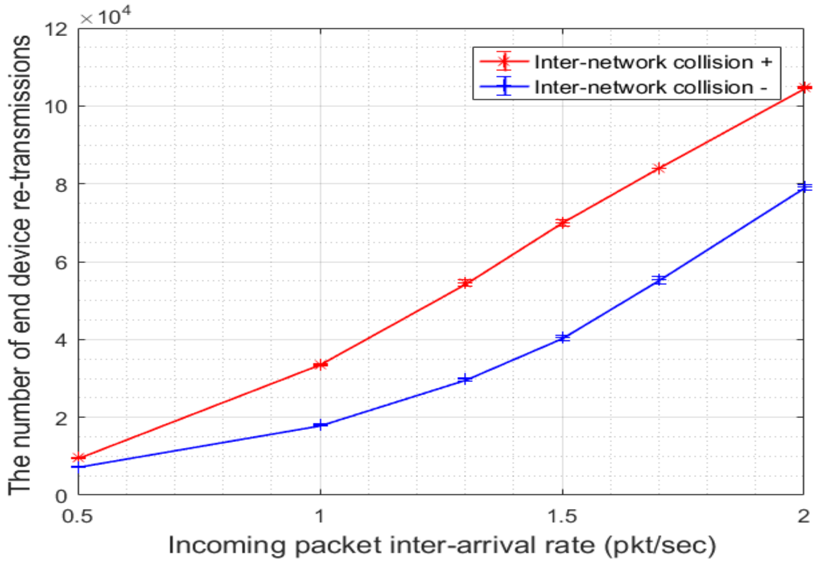


Fig 5-22 End device retransmissions with and without inter-network collisions

5.5 The Blank Burst (BB) Algorithm

The results from the previous section have shown that the WLAN transmissions adversely affect the 6LoWPAN transmissions due to inter-network collisions. To solve this problem, a micro silence period is proposed to suspend the 6LoWPAN transmissions when the WLAN packet transmissions start. Before the 6LoWPAN end devices stop transmitting packets, a Blank Burst

(BB) signal is piggybacked in a beacon, which is propagated to the end devices indicating that the devices suspend their transmissions for a short period of time. In doing so, the WLAN transceivers of the MFDRR use the silent period to transmit WLAN packets without interfering with the 6LoWPAN packet transmissions.

As shown in Fig 5-23, a BB signaling technique is proposed to solve the inter-network collisions. When the 6LoWPAN packets arrive at the buffer in the MFDRR as shown in Fig 5-16, they are aggregated into one WLAN packet. Once the number of packets in the buffer exceeds a pre-defined aggregation factor threshold, a BB signal request is triggered at time T1 and sent from the WLAN application layer to the 6LoWPAN MAC layer, prompting the 6LoWPAN MAC layer to prepare for the BB signal. At this time, the 6LoWPAN MAC layer can be in any status defined by the IEEE 802.15.4 standard such as backing off or sensing the channel, so the MAC layer needs to wait until the next beacon cycle begins and the beacon can be used to propagate a BB signal. Once the 6LoWPAN MAC layer is prepared to transmit a beacon, a BB reply is sent back to the WLAN application layer, informing that the 6LoWPAN MAC layer is about to transmit a beacon. After that, the BB signal is injected into the beacon packet and disseminated to the 6LoWPAN end devices as show in Fig 5-23.

Meanwhile, the MFDRR has a timer that records the time it takes to transmit the BB notification from the MFDRR to the 6LoWPAN end devices. Given the staggered link design described earlier, the duration for a beacon transmission time from the MFDRR to the end devices is fixed. Therefore, when the timer runs out, it means that the beacon has reached all the end devices at time T_2 via the routers. Upon receiving the beacon at time $T_{2,}$ the end devices extract the BB signal, read the T_{BB} field, and remain silent during this period, which is calculated in 5-18. The WLAN DCF technique is used to transmit the WLAN packets, where T_{DIFS} denotes the DCF inter-frame spacing; $T_{backoff\_min}$ denotes the minimum back-off delay; L_{agg} is one aggregated packet transmission time, including the headers and payloads; and T_{SIFS} denotes the short interframe spacing. T_{ACK} represents the acknowledgement packet transmission delay. N denotes the number of WLAN packets transmitted per BB duration, which depends on the aggregation factor. It is noted the back-off duration is the minimum back-off time because there is no other WLAN device completing the channel. In other words, after a WLAN packet is transmitted, the next packet can be sent without contending the channel. Meanwhile, the stored 6LoWPAN packets are aggregated into N WLAN packets, which in turn are transmitted via the WLAN sink during the T_{BB} period. After the completion of this Blank Burst at time T3, the 6LoWPAN end devices wake up and resume sending data packets, and then a new BB circle cycle begins.

$$T_{BB} = N \times (T_{DIFS} + T_{backoff\_min} + L_{agg} + T_{SIFS} + T_{ACK}) \quad 5\text{-}18$$

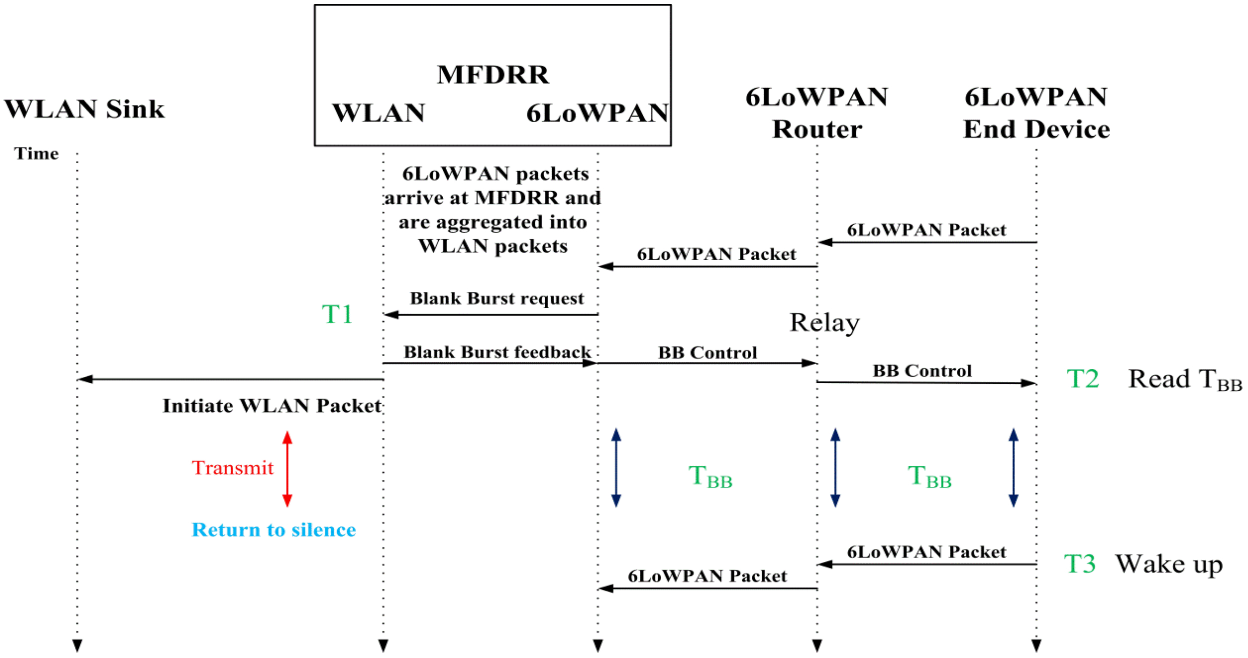


Fig 5-23 The Blank Burst process

As can be seen in Fig 5-24, the Blank Burst process can be illustrated in the algorithm. The collaboration between each entity is illustrated in the time-based flow chart. The algorithm is executed chronologically as signaled by the green arrow and explains the specific details of the tasks required by each type of the device. The algorithm is also driven by the aggregation factor, a pre-defined threshold allowing the 6LoWPAN packets to enter the buffer before triggering the BB algorithm. Once the 6LoWPAN payloads continue to enter the aggregation buffer and the number of the 6LoWPAN payloads reaches the aggregation factor agg_f, the BB algorithm is triggered. After that, a blank burst request is sent to the 6LoWPAN MAC layer of the MFDRR, which can be in any state, and thus the network needs to wait until the 6LoWPAN MAC layer is ready to send in the next round beacon. When the beacon are ready, the value of the BB period is wrapped in the beacon and transmitted to the end devices. Meanwhile, a reply is sent to the aggregation buffer to trigger the timer set for the WLAN packet transmissions. When the timer goes off, the WLAN packet transmissions begin, while the 6LoWPAN end devices receive the signaling beacon and remain silent for the BB period to avoid the inter-network collisions. The code of this algorithm can be found in Appendix D.

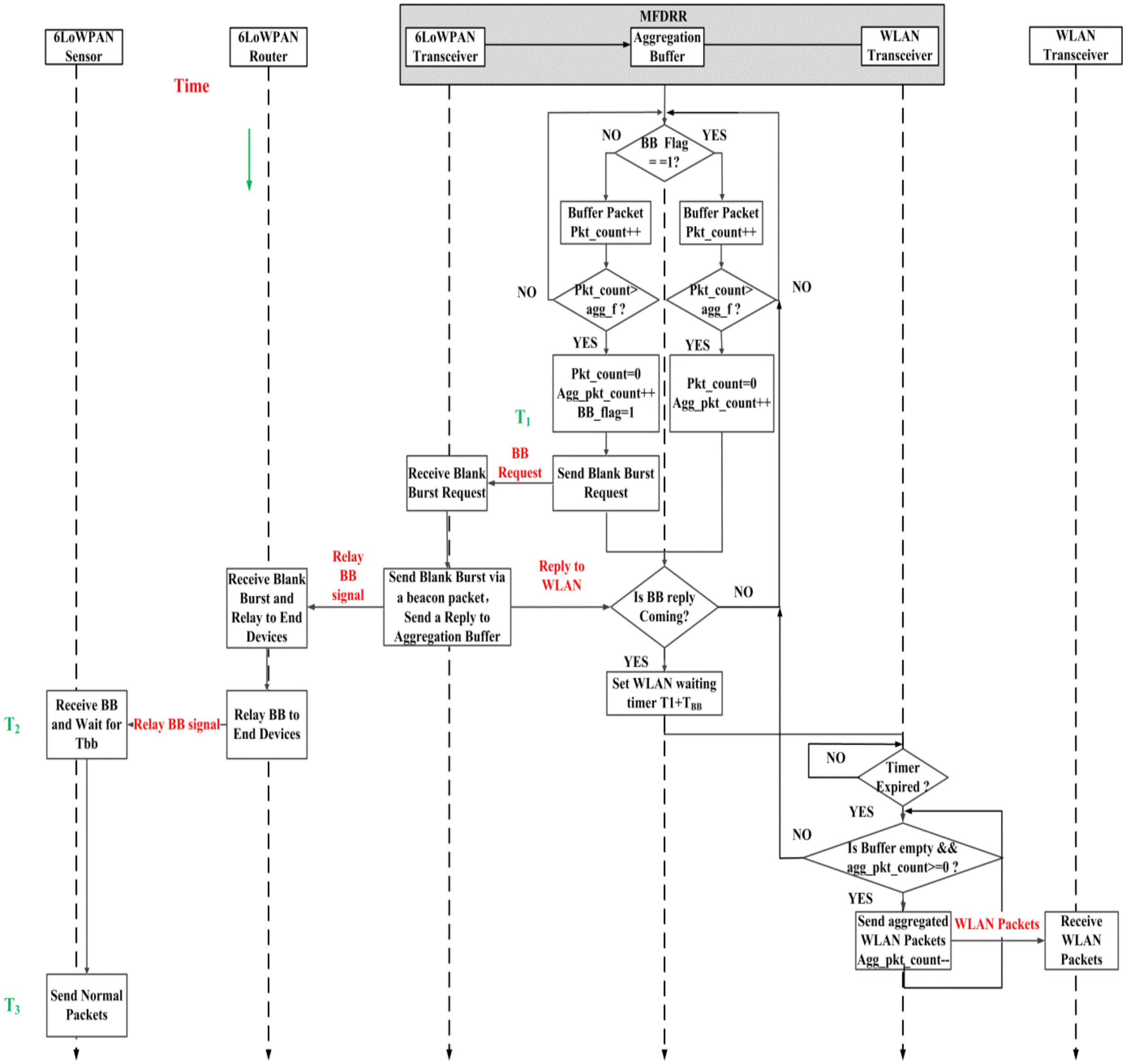

6LoWPAN Sensor
6LoWPAN Router
MFDRR
6LoWPAN Transceiver
Aggregation Buffer
WLAN Transceiver
WLAN Transceiver
Time
NO
BB Flag ==1?
YES
Buffer Packet Pkt_count++
Buffer Packet Pkt_count++
NO
Pkt_count> agg_f ?
Pkt_count> agg_f ?
NO
YES
YES
Pkt_count=0 Agg_pkt_count++ BB_flag=1
Pkt_count=0 Agg_pkt_count++
T1
BB Request
Receive Blank Burst Request
Send Blank Burst Request
Relay BB signal
Receive Blank Burst and Relay to End Devices
Send Blank Burst via a beacon packet, Send a Reply to Aggregation Buffer
Reply to WLAN
Is BB reply Coming?
NO
YES
Set WLAN waiting timer T1+TBB
T2
Receive BB and Wait for Tbb
Relay BB signal
Relay BB to End Devices
NO
Timer Expired ?
YES
NO
Is Buffer empty && agg_pkt_count>=0 ?
YES
Send aggregated WLAN Packets Agg_pkt_count--
WLAN Packets
Receive WLAN Packets
T3
Send Normal Packets

Fig 5-24 Proposed Blank Burst (BB) algorithm

5.6 Performance Analysis of the Blank Burst (BB) Algorithm

To evaluate the performance of the proposed BB algorithm, the key simulation parameters are listed in Table 5-5. The simulation has three scenarios: (1) the two sides of the MFDRR use two overlapping channels; (2) uses non-overlapping channels without the BB algorithm, and (3) the two sides of the MFDRR use an overlapping channel with the BB algorithm.

Table 5-5 Key simulation parameters of the BB algorithm

Group Name	**Parameter**		**Value**
Simulation time			300s
Network	Hop		3
	Number of nodes		64
	Standard		6LoWPAN IEEE 802.11g
	Operating Frequency		2.4 GHz
	6LoWPAN channel		12
	IEEE 802.11g channel		1
Propagation model	Free space path loss		
MFDRR	6LoWPAN	BO	5
		SO	3
		Transmit Power	1.8 mW
	WLAN	Transmit Power	100 mW
		Packet Size	1200 bytes
		Aggregation Factor	5，10，15， 20，25
	N_{min}		4
	N_{max}		18
Router	BO		5
	SO		3
	Schedule Start time Frequency 1	R1	0.12289 s
		R2	0.24577 s
		R3	0.12288 s
		R4	0.24578 s
	Schedule Start time Frequency 2	R1	0.12289 s
		R2	0.24577 s
		R3	0.12288 s
		R4	0.24578 s
End device	Packet size		64 bytes
	Packet generation		Exponentially distributed
	Transmit Power		1 mw
	Packet inter-arrival rate		1, 1.2, 1.3, 1.5,1.7, and 2 pkts/sec

Each simulation ran for 300s with multiple seed values, and the simulation results are plotted with a 95% confidence interval.

Figure 5-25 shows that the BB signalling technique has increased the packet delivery ratio in the system. There was a huge gap between the inter-network collision scenario and the scenario in which the BB signalling technique is used as the traffic load increased. Specifically, the packet delivery ratio in the first scenario (red line) dropped sharply from 90% to 30% due to the inter-network collisions. It is noted that as the traffic loads became more intense, more 6LoWPAN packets were absorbed into the MFDRR, which are transmitted via the WLAN interface. In contrast, the second scenario (blue line) and the third scenario (green line) performances almost overlapped, meaning that the BB algorithm can bring the packet delivery ratio closer to the point where there are no inter-network collisions. It can be seen that the packet delivery ratio improved by 95% at the load of 1.5 pkts/sec. The BB algorithm is effective in mitigating the inter-network collisions and improving the performance of the heterogeneous WPAN, in which a large number of energy-constrained devices are often involved and susceptible to the inter-network collisions.

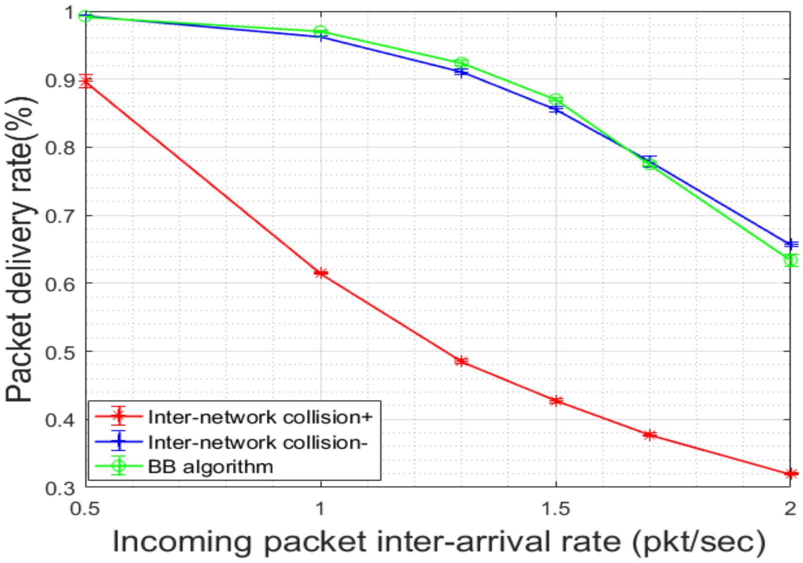


Fig 5-25 Packet delivery ratio in three scenarios

Apart from the packet delivery ratio, throughput is also another important metric to measure system performance. As can be seen in Fig 5-26, the throughput is affected by inter-network collisions that reduced the throughput to 40 pkt/sec compared to 83 pkts/sec in two other scenarios. In contrast, if no inter-network collisions exist, by using the BB signalling technique, the throughput is increased by 100% compared to that of the first scenario. Specifically, as the load increased from 0.5 pkt/sec to 2 pkts /sec, the throughput increased from 30 to 80 pkts/sec, before reaching to a plateau. If the traffic continues to increase, the throughput is expected to go down due to the intra-network collisions. The results show that the BB algorithm increases the throughput of the heterogeneous area network.

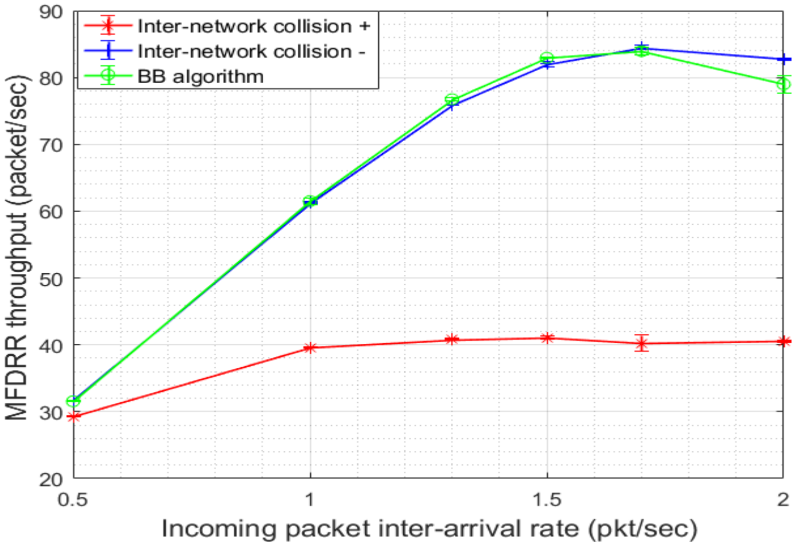


Fig 5-26 MFDRR Throughput in three scenarios

The end-to-end delay plays an important role in M2M networks, especially with the packets traversing through multiple networks. Fig 5-27 shows the end-to-end delays in the three scenarios. It is noted that the second scenario, without inter-network collisions, had the lowest end-to-end delay compared to the other two scenarios. A minor rise was observed in this scenario due to the intra-network collisions. In addition, the scenario under the adverse impacts of inter-network collisions showed a rising trend. The delays sharply went up from 0.25s to 0.63s as the incoming traffic loads changed from 0.5 to 1.3 pkts/sec. It then continued to rise with a slower pace from 0.63s to 0.75s. The scenario with the BB algorithm experienced a downward trend firstly from 0.62 to 0.55s and then steadily climbed to 0.62s. It is clear that the first scenario and the third scenario had a crossing point in the middle, and the third scenario reduced the delay by nearly 20% compared to the scenario with the inter-network collisions at a traffic load of 2 pkts/sec. However, the end-to-end delay of the third scenario was still as twice as that of the second scenario, as the latter has no aggregation delay. The BB algorithm sacrifices the latency in exchange for a high packet delivery rate, but the delay around 0.6s is tolerable for M2M applications such as e-health, lighting and energy management[19]. Due to the inter-network collisions, more packets need to be re-transmitted, and thus more incoming packets are stored in the MAC layer queue due to the re-transmissions, resulting in the long end-to-end delay. Similarly, the aggregation delay was added so that the total end-to-end delay was also increased but still less than that of the scenario with the inter-network collisions.

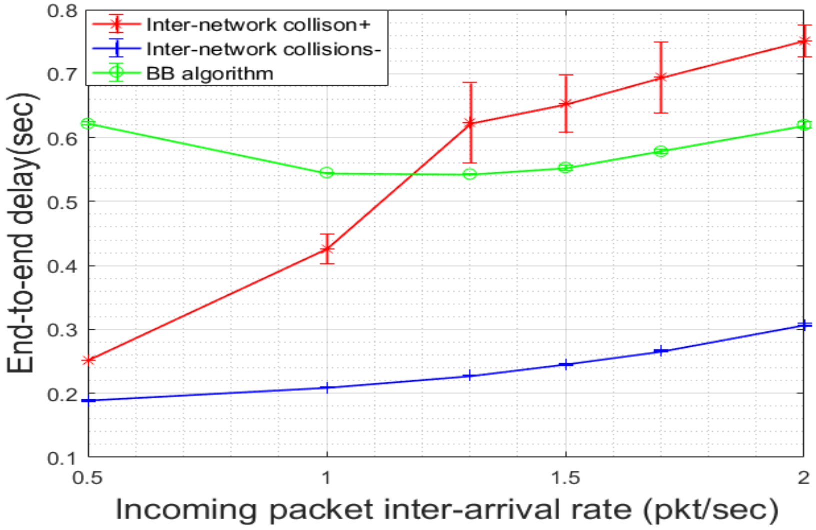


Fig 5-27 End-to-end in three scenarios

The end device-to-router delay is calculated using the components in (5-19) and presented in table Table 5-6. The router-to-MFDRR delay is calculated using the components in (5-20) and presented in Table 5-7. The MFDRR-to-Sink delay is calculated using the components in (5-21) and presented in Table 5-8.

$$\mathrm{T_{device\ to\ router}} = \mathrm{T_{queue}} + \mathrm{T_{backoff}} + 2\mathrm{T_{CCA}} + \mathrm{T_{data}} + \mathrm{T_{ack\_wait}} + \mathrm{T_{ack}} + \mathrm{T_{LIFS}}, \quad (5\text{-}19)$$

$$\mathrm{T_{device\ to\ MFDRR}} = \mathrm{T_{queue}} + \mathrm{T_{backoff}} + 2\mathrm{T_{CCA}} + \mathrm{T_{data}} + \mathrm{T_{ack\_wait}} + \mathrm{T_{ack}} + \mathrm{T_{LIFS}}, \quad (5\text{-}20)$$

$$T_{MFDRR\ to\ Sink} = T_{media\ access} + T_{aggregation} + T_{DIFS} + T_{data} + T_{SIFS} + T_{ack}, \quad (5\text{-}21)$$

where $T_{aggregation}$ is the packet aggregation delay, T_{DIFS} is DCF interframe space, T_{SIFS} is the short interframe space and the other parameters are defined as same as the previous ones.

The end-to-end delay is calculated in (5-22).

$$T_{device\ to\ router} = T_{device\ to\ router} + T_{device\ to\ MFDRR} + T_{MFDRR\ to\ Sink} \tag{5-22}$$

Table 5-6 The end device-to-router delay components

Inter-arrival rate (pkt/s)	T_{queue} (ms)			$T_{backoff}$ (ms)			$2T_{CCA}$ (ms)	T_{data} (ms)	$T_{ack_{wait}}$ (ms)	T_{ack} (ms)	T_{LIFS} **(ms)**
	Inter-collisions+	Inter-collisions-	BB algorithm	Inter-collisions+	Inter-collisions-	BB algorithm					
0.5	97.2	94.1	88.8	2.6	2.5	2.4	0.256	2.048	0.864	0.352	0.640
1	162.2	113.0	107.4	3.4	2.9	2.8	0.256	2.048	0.864	0.352	0.640
1.3	232.2	139.6	132.9	3.4	3.0	3.0	0.256	2.048	0.864	0.352	0.640
1.5	260.4	163.9	154.4	3.5	3.1	3.1	0.256	2.048	0.864	0.352	0.640
1.7	308.6	194.9	197.9	3.5	3.1	3.2	0.256	2.048	0.864	0.352	0.640
2	379.5	256.6	258.2	3.5	3.2	3.2	0.256	2.048	0.864	0.352	0.640

Table 5-7 Router to MFDRR delay components

Inter-arrival rate (pkt/s)	T_{queue} $(\mathbf{ms})$			$T_{backoff}$ $(\mathbf{ms})$			$2T_{CCA}$ (ms)	T_{data} (ms)	$T_{ack_{wait}}$ (ms)	T_{ack} (ms)	T_{LIFS} **(ms)**
	Inter-collisions+	Inter-collisions-	BB algorithm	Inter-collisions+	Inter-collisions-	BB algorithm					
0.5	170.9	122.5	126.7	3.3	2.6	2.6	0.256	2.048	0.864	0.352	0.640
1	348.9	129.3	135.2	3.4	2.8	2.8	0.256	2.048	0.864	0.352	0.640
1.3	403.4	133.5	139.2	3.4	2.8	2.9	0.256	2.048	0.864	0.352	0.640
1.5	361.3	134.7	139.3	3.4	2.9	2.8	0.256	2.048	0.864	0.352	0.640
1.7	418.1	133.9	137.8	3.4	2.9	2.9	0.256	2.048	0.864	0.352	0.640
2	321.0	132.3	133.1	3.4	2.9	2.8	0.256	2.048	0.864	0.352	0.640

Table 5-8 MFDRR delay components

Inter-arrival rate (pkt/s)	$T_{media\ access}$ **(ms) (T_{queue}+$T_{backoff}$)**			**$T_{aggregation}$ (ms)**			T_{DIFS} (ms)	T_{data} (ms)	T_{SIFS} **(ms)**	**T_{ack} (ms)**
	Inter-collisions +	**Inter-collisions -**	**BB algorithm**	**Inter-collisions +**	**Inter-collisions -**	**BB Agg factor =10**				
0.5	12.3	1.0	1.1		0	481.7	0.034	5.12	0.016	0.112
1	32.5	2.5	2.5	0	0	427.5	0.034	5.12	0.016	0.112
1.3	38.9	3.2	3.3	0	0	426.0	0.034	5.12	0.016	0.112
1.5	40.5	3.6	3.6	0	0	425.8	0.034	5.12	0.016	0.112
1.7	41.0	3.7	3.7	0	0	425.3	0.034	5.12	0.016	0.112
2	41.6	3.6	3.5	0	0	425.3	0.034	5.12	0.016	0.112

Analysing data from Table 5-6, Table 5-7 and Table 5-8, we can see that the queuing delay and the aggregation delay are the major delay components of the end-to-end delay whose value increases with the increasing traffic load. In both the end devices and the routers, it can be seen that in the scenario 1 under the inter-network collisions, the queue delays are increasing from 97.2 ms to 379.5 ms and from 170.9 ms to 321 ms, respectively. In contrast, scenario 3 with the BB algorithm has the lowest queuing delay increasing from 88.8 ms to 258.2 ms and from 126.1 ms to 133.1 ms in the end device and router, respectively.

The main delay component is the router queuing delay, as depicted in Fig 5-28. In the first scenario, the queuing delay increased up from 0.12s to 0.72s, while the other two scenarios maintained stability around 0.1s, as the traffic loads increased from 0.5 to 1.3 pkts/sec. Then, the delay under collisions dropped to 0.5s and further decreased to 0.43s with the increased traffic loads. As shown in Fig 5-26, the throughput of this scenario in the MFDRR was around 40 pkts/sec because many packets were lost due to the inter-network collisions. Gradually, the collision level went down and thus resulted in a lower router queuing delay. When the incoming loads was increased, the packets were held up in the router's MAC queue. In contrast, the delay in the scenario with the BB algorithm remained stable at 0.1s. The queuing delay was calculated by the queue length with a built-in function in OPNET according to queuing theory. Fig 5-29 shows the router average queue lengths in the three scenarios. Due to the inter-network collisions, the first scenario had a similar pattern as Fig 5-28; the queue length climbed to 6 pkts/sec and then slightly dropped to 4.6 pkts/sec. In contrast, the other two scenarios just remained at 2 pkts/sec as the traffic load increases.

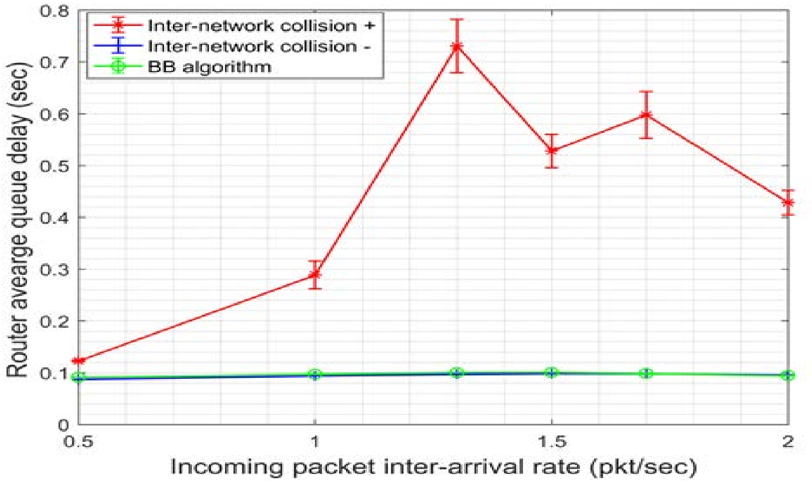


Fig 5-28 Router average queuing delay in three scenarios

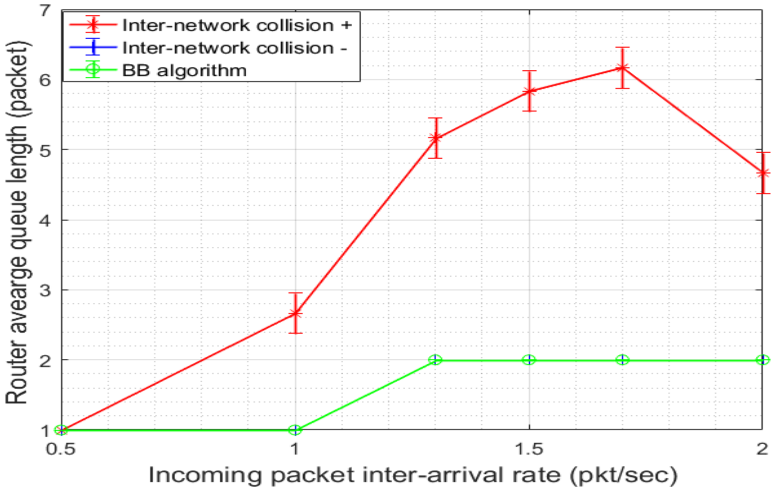


Fig 5-29 Router average queue length in three scenarios

Various aggregation factors contribute to the different end-to-end delays as shown in Fig 5-30. Five different aggregation factors are employed to evaluate the relationship between the end-to-end delay and the aggregation factor. As can be seen from the figure, the end-to-end delay ranges from 0.52 s to 0.97 s at the load of 0.5 pkt/sec. larger aggregation factors caused higher end-to-end delays. This is because packets need to wait in the MFDRR aggregation queue until the number of packets reached the value of the aggregation factor. In other words, the queuing time is fully dependent on the aggregation factor. Another issue to note is that the end-to-end delay slightly increased for all five aggregation factors as the incoming traffic loads increased. This is because intra-network collisions occur, so more packets were held up in the MAC queue, leading to longer queuing delays. In a nutshell, the aggregation delays are adjustable so that the aggregation factors can be changed to best suit specific M2M applications. The algorithm can be enhanced to estimate the amount of incoming traffic. For example, if the incoming traffic is not heavy, a small aggregation factor is used; otherwise, a large aggregation factor is used to control the traffic.

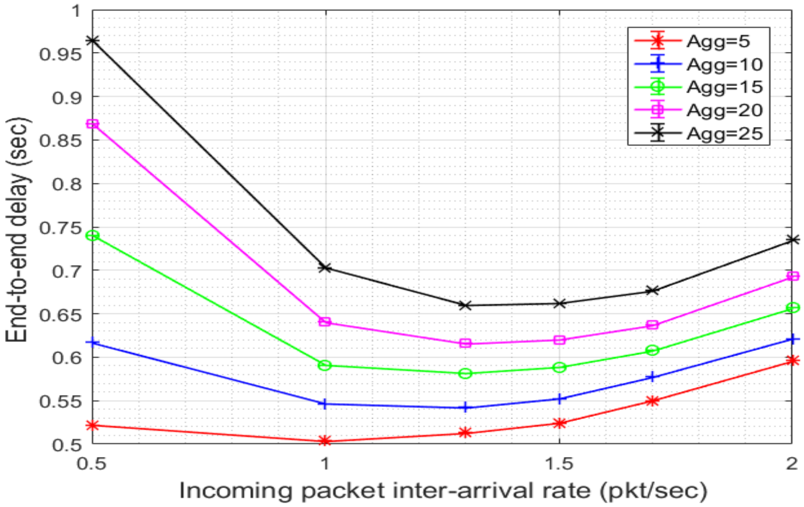


Fig 5-30 End-to-end delay for various aggregation factors with the BB algorithm

The main delay component of the end-to-end delay is the aggregation delay. Fig 5-31 represents the relationship between the aggregation factor and the aggregation delay in the MFDRR queue. It is clear from the results that the aggregation delay is a major component of the end-to-end delay. For example, at a load of 1 pkt/sec, the aggregation delay due to the aggregation factor 20 in Fig 5-31 was 0.53 s, which accounted for 75% of the total end-to-end delay (0.7s) in Fig 5-30. The aggregation delay had a similar pattern as the end-to-end delay; that is, the aggregation delay is decreasing with the increment of traffic loads. The lower aggregation factor resulted in a lower end-to-end delay. Although the BB algorithm reduced inter-network collisions, it introduces an additional end-to-end delay component due to the packet aggregation.

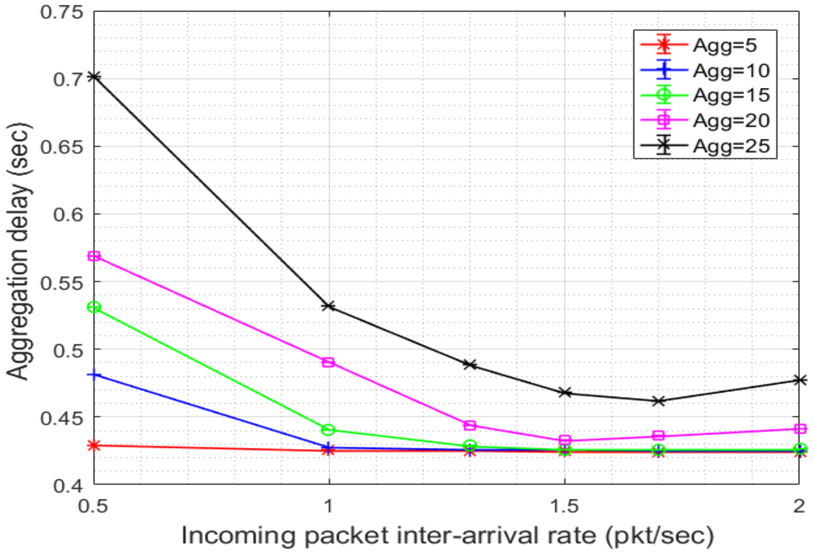


Fig 5-31 Aggregation delay in the MFDRR queue

Table 5-9 Aggregation delay for different aggregation factors

Inter-arrival rate (pkt/s)	**$T_{aggregation}$ (ms)**				
	Agg factor=5	**Agg factor=10**	**Agg factor=15**	**Agg factor=20**	**Agg factor=25**
0.5	429.3	481.7	530.9	568.9	701.7
1	425.4	427.5	440.8	490.5	532.0
1.3	425.1	426.0	428.9	444.0	488.6
1.5	424.7	425.8	426.1	433.0	468.0
1.7	424.3	425.3	426.0	436.1	462.0
2	424.3	425.3	426.5	441.4	477.5

It can be seen from Table 5-9 that the aggregation delays for factor 5 and 10 did not decrease much because the traffic arriving at the MFDRR with the low packet inter-arrival rate is already high and there is little waiting time in the queue. However, with a larger factor such as 25, the aggregation delay decreases with the quick arrival of 6LoWPAN packets. In the BB algorithm, the aggregation delay is the major delay component responsible for the end-to-end delay compared to the queuing delay. The reason is that the 6LoWPAN packets need to spend time waiting in the aggregation buffer before the BB algorithm can be triggered. The smaller the aggregation factor is, the more frequently the BB algorithm will triggered, thus less time the 6LoWPAN packets will spend in the aggregation buffer.

The number of collisions directly reflects the levels of intra-network and inter-network collisions. As can be seen from Fig 5-32, the number of collisions in the presence of the inter-network collisions linearly increases from 5000 to 25000 with the increased traffic loads. In contrast, the other two scenarios also saw an upward trend from 2500 to 19000. It is clear that the gap between the first scenario and the following two indicates the number of inter-network collisions. This means the BB algorithm alleviated the inter-network collision by 58% at the load of 1.3 pkts/sec. However, the intra-network collisions due to the use of the CSMA/CA mechanism are unavoidable despite using the staggered link design proposed in Chapter 4. It can also be seen that the BB algorithm reduced the numbers of the inter-network collisions to the limit, making the blue and green lines overlap.

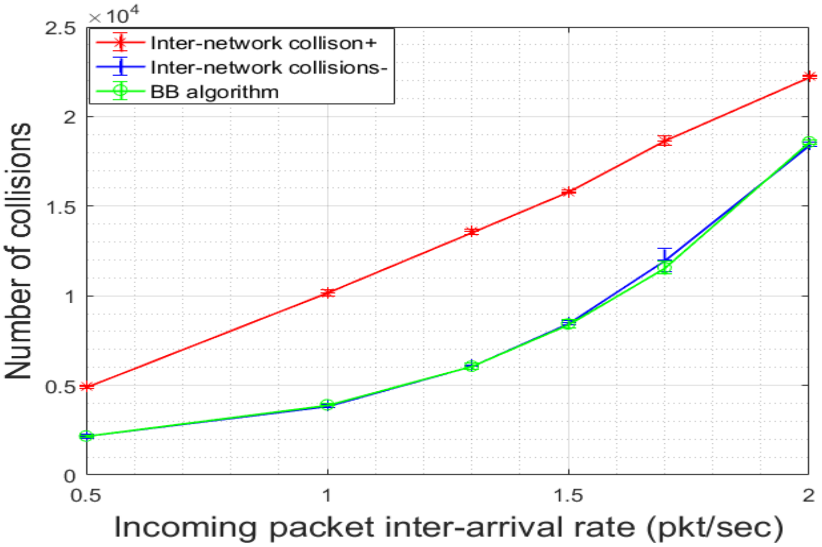


Fig 5-32 Number of collisions in three scenarios

Due to the inter-network collisions, the routers in the system need to re-transmit a packet that cannot successfully reach the MFDRR. Here the routers, the direct victims, are studied because the WLAN packets emitted from the MFDRR firstly impact on the routers. Fig 5-33 shows that the inter-network collisions caused much more packet losses compared to the other two scenarios. Specifically, the first scenario saw high packet losses, jumping from 1000 to 4300 packet losses and then stabilising between 4000 and 4500 packet losses, as the traffic was increased. In contrast, the BB algorithm maintained the number of packet losses at less than 500, which is close to the scenario in which no inter-network collisions occurred. The results show that the BB algorithm reduced the 80% number of losses in the presence of the inter-network collisions.

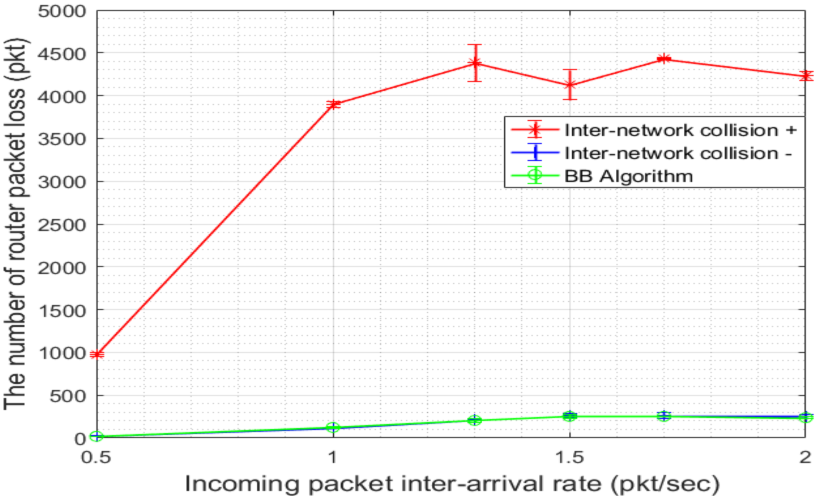


Fig 5-33 Number of packet losses in the MAC layer in three scenarios

Packet losses occur because a device has reached its re-transmission limit. Fig 5-34 illustrates the number of router re-transmissions in the three scenarios. It is clear that the BB algorithm reduces the half number of re-transmissions as a result of lower inter-network collisions. That is to say, the proposed algorithm reduced the number of re-transmission by 50% compared to the other scenarios. On the other hand, lowering the number of retransmissions can reduce the energy consumption of the whole heterogeneous network, which is important for M2M networks. After all, most of the M2M devices are battery-powered; however, energy consumption is not the focus of this study, so it is not discussed further here.

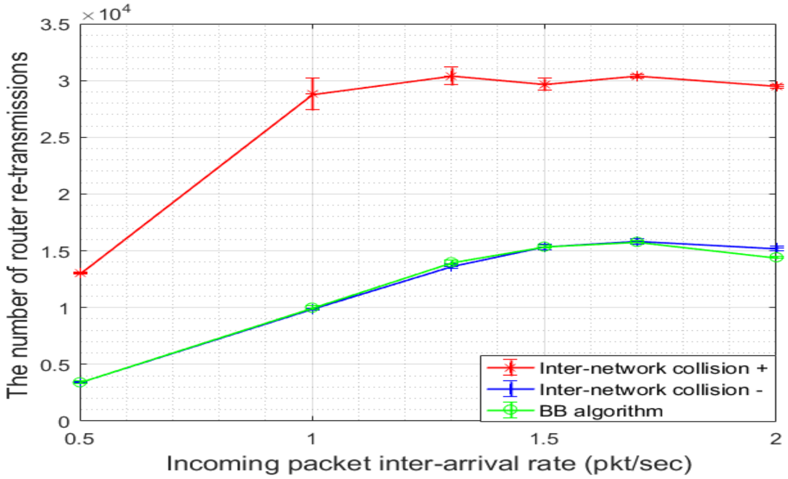


Fig 5-34 Number of 6LoWPAN router re-transmissions

To show effectiveness of the proposed BB algorithm, the proposed BB algorithm was compared with an simple aggregation algorithm presented in [9]. The algorithm proposed in [9] is the only study that can be compared with the proposed BB algorithm because it also studied the ZigBee/WLAN heterogeneous wireless sensor network while the other studies with respect to the inter-network collisions used two separate networks. Also, the existing algorithm [9] in the literature will be applied to a large-scale dense area network in Chapter 7. The work simply uses the aggregation factor of 25 to conduct the algorithm, which means that 25 ZigBee packets are aggregated into one WLAN packet. To meet the delay requirements for this one hop network with the star topology, the algorithm set a timer to 500ms between the ZigBee devices and the dual-radio node. Since it is easy to meet this requirement, the latency requirement is omitted in both algorithms. The proposed algorithm in the literature was employed in the area network as shown in Fig 5-15. The BB algorithm also used 25 as the aggregation factor. To simulate a super dense network, dummy 6LoWPAN packets are injected into the MFDRR, simulating a much more crowed 6LoWPAN network. Specifically, four 6LoWPAN inter-arrival rates 50, 100, 150 and 200 pkts/sec were used, which are correspondingly equivalent to 2, 4, 6 and 8 WLAN pkts/sec. The other simulation parameters are the same as in Table 5-5. The simulation consists of three groups: (1) without the dummy traffic and with the BB algorithm, (2) with the dummy traffic and with the BB algorithm and (3) with the dummy traffic and without the BB algorithm (referred to as the simple aggregation algorithm). The group one was used as a baseline to compare with the other two groups. The sensor traffic was used in the simulation.

Figure 5-35 shows the packet delivery ratios of the three groups. It can be seen that the packet delivery ratios of the BB algorithm and the proposed aggregation algorithm slightly declined with the increased incoming loads. The BB algorithm outperformed the simple aggregation algorithm. The performance gain was 22% when the number of the incoming dummy 6LoWPAN packets was 200. This is because the dummy 6LoWPAN packets created extra aggregated WLAN packets. Without the protection of the BB period, the simple aggregation algorithm is subject to much stronger inter-network collisions, resulting in a lower packet deliver ratio. This decline in the packet delivery ratio of the BB algorithm was attributed to the inter-network collisions.

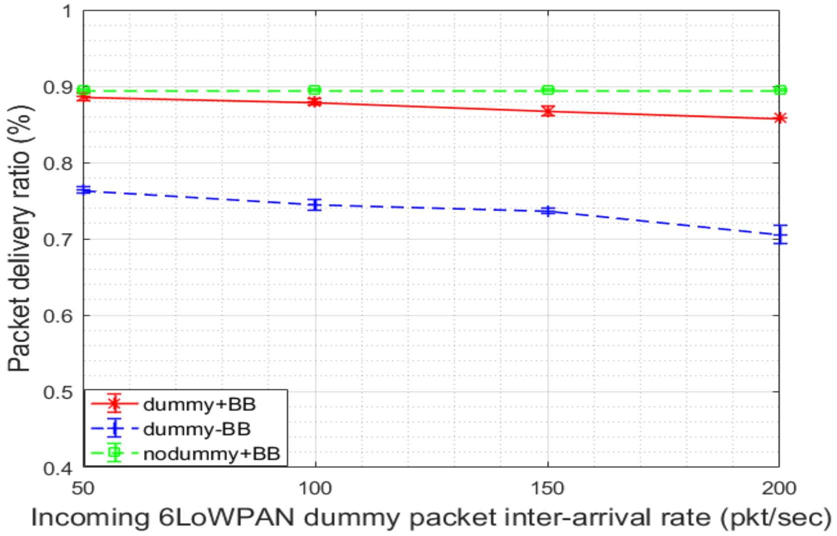


Fig 5-35 Packet delivery ratios for the BB and aggregation algorithms

Figure 5-36 presents the sensor traffic end-to-end delays. It can be seen that the delays of the simple aggregation algorithm and the BB algorithm gradually declined with the increased number of dummy packets. This was because the aggregation delay was reduced with the increased dummy packets. The inter-network collisions caused a longer queuing delay for 6LoWPAN packets, which is a main delay component of the total end-to-end delay. It is noted that the BB algorithm with dummy packets experienced a lower delay than the other two cases. For example, the delay of the BB algorithm with dummy packet decreased by 12% compared to the simple aggregation algorithm without the BB period at 200 dummy pkts/sec. This is because the number of dummy packets reduces the packet queuing time in the MFDRR, the frequency of the packet aggregation is faster and the execution times of the Blank Burst algorithm are also faster.

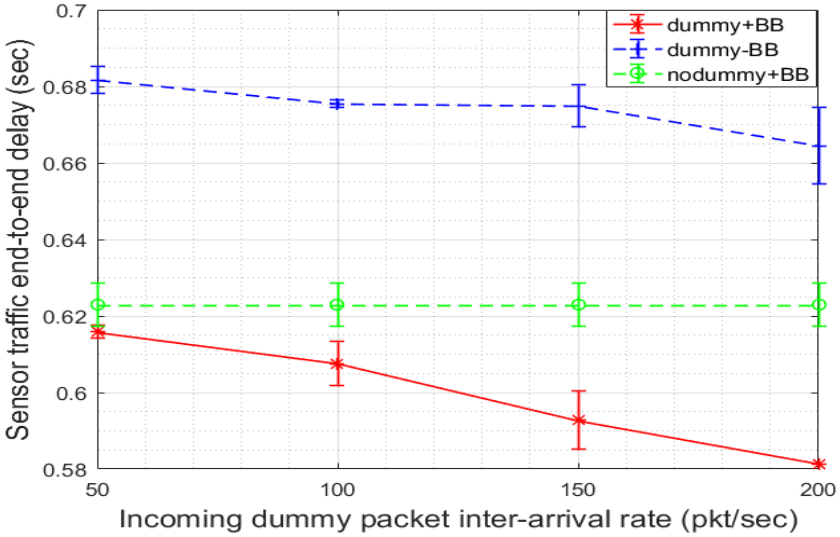


Fig 5-36 End-to-end delay for the BB and simple aggregation algorithms

Figure 5-37 and Figure 5-38 illustrate both the end devices and the routes packet losses. Overall, it can be seen that the end devices experienced the most packet loss compared to the routers. The main reason was that the BB period was scheduled at the end devices to protect them from being affected. Without the BB's protection, the number of packet losses went up from 1340 to 1700 packets as the incoming loads were increased. In contrast, with the BB's protection, the number of packet losses only increased from 583 to 791 packets. Without the dummy traffic, the number of losses remains stable, meaning that the BB period cannot completely avoid inter-network collisions, but can mitigate the adverse impacts to a large extent. As for the router packet losses, it can be observed that without the BB period, the routers had the lowest number of packet loss as the incoming dummy load increased. This was because the majority of the packets were lost on the end device-to-router link, so not enough packets were able to reach the router. However, for the group with dummy packets and the BB period, most of the 6LoWPAN packets were protected from the BB period, so more of the 6LoWPAN packets were lost on the router. It is also noted that without the dummy packets, the router with the BB algorithm lost more packets than the one with the BB algorithm and the dummy packets. The reason is that the group with the dummy packets and the BB algorithm lost more packets on the end device-to-router link due to inter-network collisions.

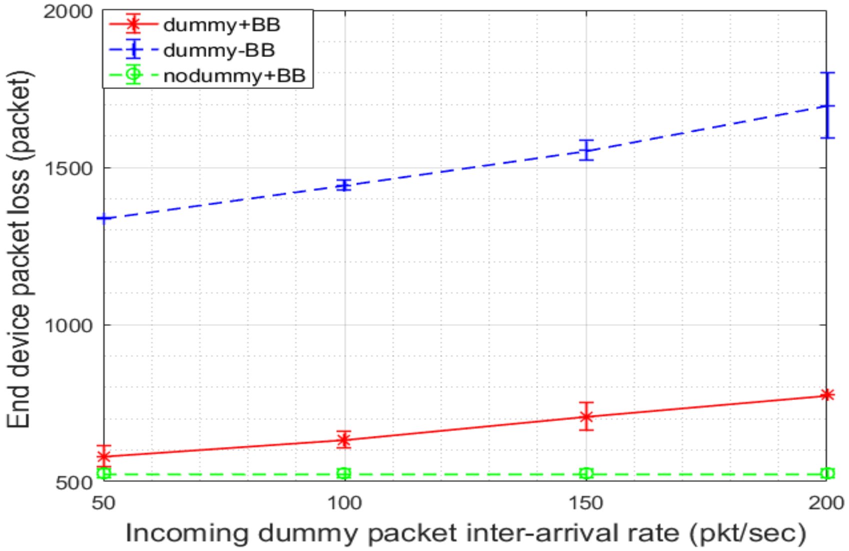


Fig 5-37 End device packet losses for the BB and simple aggregation algorithms

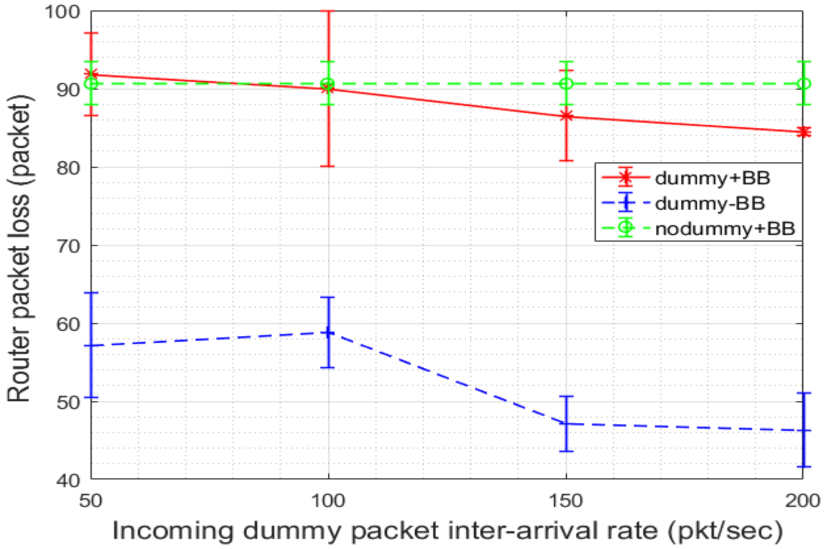


Fig 5-38 6LoWPAN Router packet losses for the BB and simple aggregation algorithms

Figure 5-39 and Figure 5-40 show the end device queuing delay and the router queuing delay, respectively. It can be seen that the end device delay increased from 0.19s to 0.202s with the dummy packets and without the BB algorithm. In particular, the delay was 52% higher than the group with the dummy packets and the BB algorithm and 67.5% higher than the group without the dummy packets and with the BB algorithm, respectively, for dummy load of 200 pkts/sec. In Fig 5-39, the increase in the delay of the end devices with dummy packets and the BB algorithm was due to the inter-network collisions causing most of the packet losses at the end devices. Accordingly, in Fig 5-40, the router delay with dummy packets and the BB algorithm were the lowest among the three groups as it had the lowest amount of 6LoWPAN packets reaching the router. It is also noted that the overall router queuing delays are lower than end device queuing delays. This can be attributed to the same reason that the majority of 6LoWPAN packets are adversely affected at the end device side, and thus not many arrive at the router.

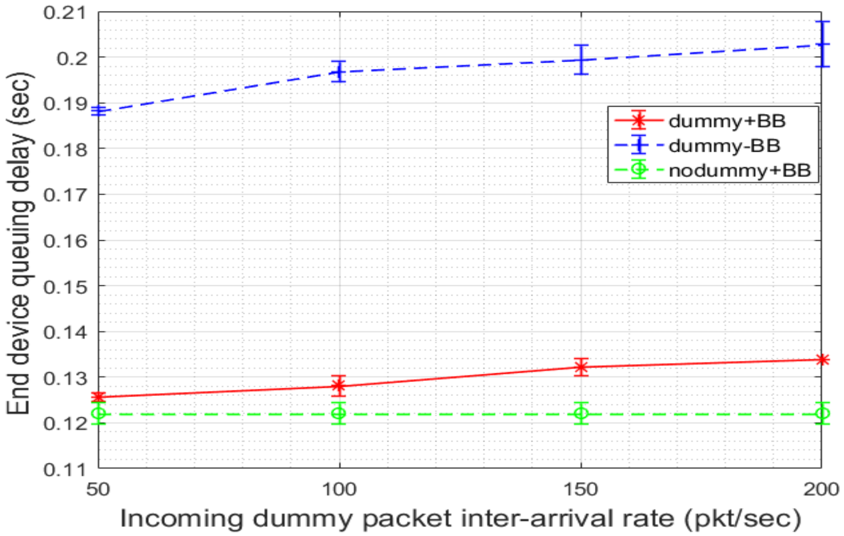


Fig 5-39 End device queuing delay

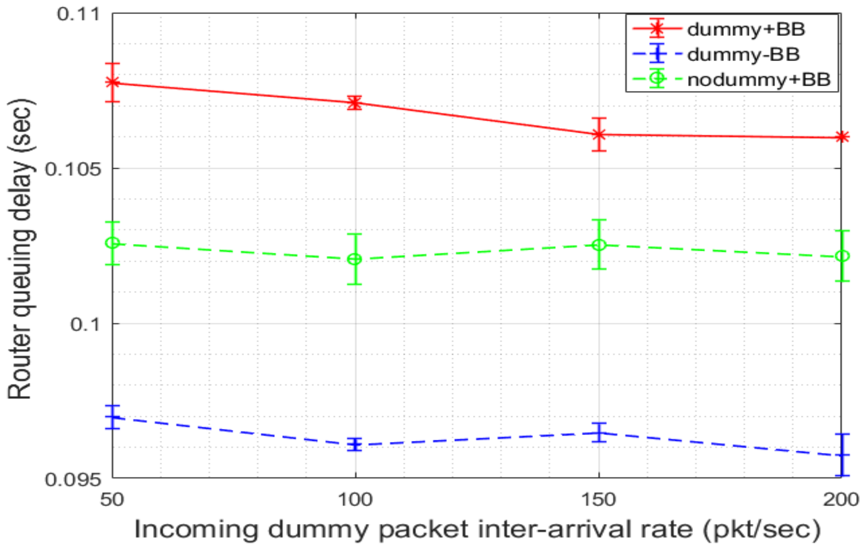


Fig 5-40 6LoWPAN Router queuing delay

Figure 5-41 shows the throughputs of the MFDRR for the three groups. To clarify, as the dummy packets are injected into the application layer of the 6LoWPAN, they are not regarded as the throughput. It is noted that the throughput steadily dropped from 80 to 74 pkts/sec as the number of dummy packets increased. In contrast, the other two groups maintained throughput above 90 pkts/sec, whereas the group with the BB algorithm slightly decreased from 94 to 92 packets/sec. In particular, the throughput of the group with the BB algorithm was increased by 24% when the number of dummy packets was 200 pkts/sec. It is understood that the reduction in throughput was due to the packet losses caused by the inter-network collisions, as previously discussed. The packet losses in the previous links resulted in the reduction in throughput at the MFDRR.

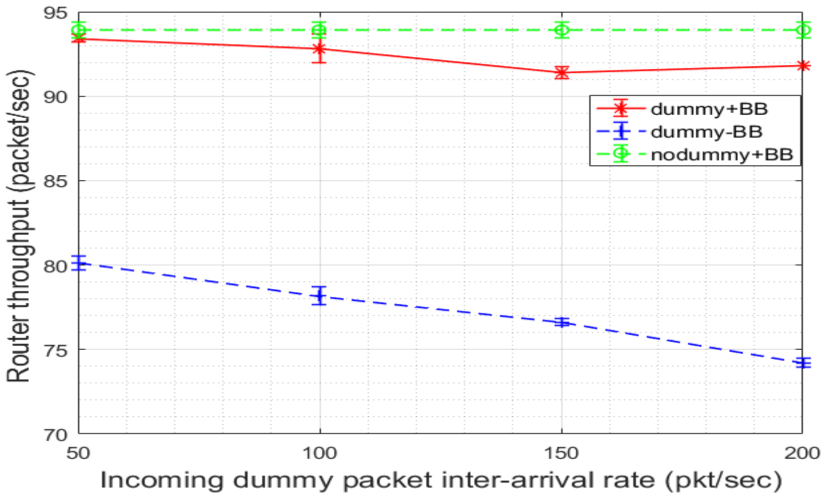


Fig 5-41 MFDRR throughput

Figure 5-42 shows the aggregation delays for the three groups. It can be seen that the aggregation delays of the groups with the dummy packets gradually declined, but the delay with the BB algorithm were much lower than that of the group without the BB algorithm. In particular, the delay was reduced by 15% when the number of the incoming dummy packets was 150 pkts/sec. It can be seen that the queuing delay is inversely proportional to the packet inter-arrival rate if the queue length is fixed. The BB algorithm outperformed the algorithm presented in the existing literature.

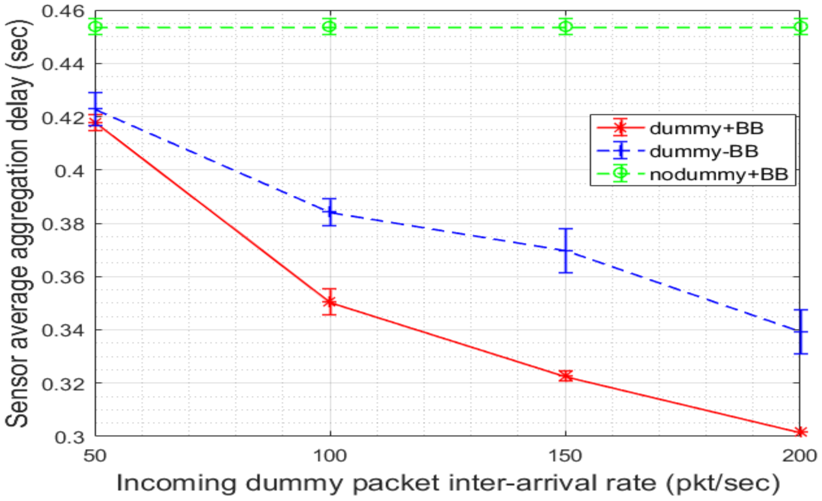


Fig 5-42 Sensor traffic aggregation delay in the MFDRR

5.7 Conclusion

In this chapter, the CSMA/CA packet transmission technique for both the IEEE 802.11 WLANs and IEEE 802.15.4 6LoWPANs were analysed. The proposed heterogeneous wireless area network architecture introduced stronger inter-network collisions due to close proximity of the two types of transceivers residing in the same MFDRR node. For this reason, the existing collision mitigation methods are not suitable for the proposed heterogeneous area network, hence the BB algorithm was proposed. The algorithm delays the 6LoWPAN transmissions for a short period of time so that the WLANs can finish transmissions without colliding with the 6LoWPAN packets. This algorithm employed the WLAN’s high transmission rate to reduce the air time of WLAN packets. The simulation results for a dense heterogeneous WPAN with realistic parameters proved the distinct advantages of the proposed BB algorithm. This chapter also compared the BB algorithm with an aggregation algorithm, which is the only study found in the literature. The simulation results showed that the BB algorithm outperformed the proposed aggregation algorithm in terms of the packet delivery ratio, end-to-end delay and throughput.

Chapter 6

QoS-Aware Heterogeneous MFDRR Design

6.1 Introduction

Chapter 5 introduced the BB algorithm to alleviate the inter-network collisions. The proposed algorithm suspends the 6LoWPAN packet transmissions for a short period of time, during which the IEEE 802.11g interface of the MFDRR forwards the aggregated 6LoWPAN packets to a data sink without being affected by the inter-network collisions. The algorithm uses a higher transmission rate of the IEEE 802.11g standard to burst data by accumulating a large number of small-sized 6LoWPAN packets, thus extending the traditional 6LoWPAN transmission range. The BB algorithm successfully alleviates the inter-network collisions in a complex scenario where the 6LoWPAN and IEEE 802.11g transceivers are housed in the same MFDRR node than the traditional scenario where the 6LoPWAN and IEEE 802.11g transceivers are used as two separate nodes operating within the network.

By using the BB algorithm, the packet delivery rate was increased by 104%. However, as a large number of machine-type devices serve various applications in the M2M scenarios, the QoS requirements of these applications in the proposed heterogeneous architecture must be considered. Generally, M2M networks forward the traffic to a remote data sink using the uplink, but some applications may require both the uplink and downlink traffic. For example, some control commands of the data sink need to be dispatched to a wireless sensor network to control actuators. In this case, the uplink and downlink packet streams travel in different directions on the same air interface, thus resulting in traffic congestion. To solve this problem, a congestion mitigation approach is proposed in this chapter to abate the level of congestion while maintaining the proper QoS for two M2M applications.

In M2M scenarios, applications are more on-demand than traditional ones. For example, sensors used in a fire alarm system are required to timely report a fire alert to actuators, so the actuators such as sprinklers will extinguish the fire within a certain time limit. It is therefore necessary to meet throughput and delay requirements for M2M applications. Networks with long delays and high packet losses rate will be suitable in delay-sensitive applications, whereas they may be tolerable for a ventilation system adjusting the temperature of an office. Metrics, such as the throughput, jitter, delay and packet success rates are used to measure the QoS of M2M applications [122]. A high throughput generally indicates a good system performance. An example of this is that camera sensors generating images for target tracking requires high throughput, so high throughput is important for the system. The end-to-end delay is the time that it takes for a packet to travel from a source node to a destination that includes the queuing, processing and propagation delays. A real-time system, such as a fire system, needs to finish the task within the time requirements. Jitter is defined as the delay variation caused by the different queuing delays of consecutive packets. The packet delivery ratio is a ratio of the number of successful packets over the total number of transmitted packets. This metric is another indicator of system reliability because a low packet delivery ratio may be attributed to congestion and packet errors.

M2M communications should support good connectivity for the uplink and downlink flows to enable remote servers to respond to the machine-type devices in the area networks. For example, the Smart Grid, serving as an M2M application, deploys smart meters to form the Advanced Metering Infrastructure (AMI) in which two-way communications are enabled between smart meters and the utility [123]. In [124], as there is a need for an information exchange between electric vehicles and the Electric Vehicle Supply Equipment (EVSE) to reserve charging slots. The energy consumption of the vehicle is processed and transmitted to the EVSE using wireless two-way communication links, so the EVSE can reserve suitable numbers of charging slots for a vehicle with a minimal delay. In addition to electric vehicles, the demand side management data is exchanged between the HANs and the utilities in the Smart Grid [125]. Demand Side Management (DSM) is used to shift the energy usage from peak times to off-peak times at late night or on weekends. As such, household residents must be able to receive messages from utilities to regulate energy usage, a case in which a bidirectional wired or wireless link should be established.

Two-way communications have been proposed for many years for M2M communications, but not many studies have investigated the underlying problems of M2M networks. Generally, M2M networks support asymmetric traffic flow with a higher volume of the uplink traffic than that of the downlink compared to traditional communication networks. In this chapter, the proposed heterogeneous area network in Chapter 5 is used to support two-way communications. It was found that when the uplink and downlink packets were transmitted at the same time, the traffic congestion could occur in the routers, which is a particularly problem for random access networks. As the congestion continued, packets were dropped in the MAC layer due to buffer overflow. Another issue is that the proposed network did not consider any mechanism to maintain the QoS of the high priority traffic. The downlink data flows such as demand side management packets usually have a higher priority than the other packets in the uplink, so the downlink packets should be offered a higher priority on the downlink. This chapter proposed a congestion mitigation algorithm that handles the congestion and offer different priorities to the selected M2M traffic.

The remainder of this chapter is organised as follows: Section 6.2 and 6.3 introduces a lifetime-based packet scheduling technique ensuring the QoS requirements of different M2M applications. This algorithm is an enhanced version of the BB algorithm and it includes several algorithms to schedule the packets in the MFDRR. Section 6.4 evaluates the performance of the proposed lifetime-based algorithm. Section 6.5 presents a two-way communication scenario in which the DSM data is sent back from a data sink. As the two-way communications can cause traffic congestion, a congestion-mitigating approach was proposed to ensure that demand management data can be received in time. Section 6.6 investigates the performance analysis of the multiple heterogeneous wireless sensor networks. A lifetime-based structure is also taken into account in this chapter. Section 6.7 concludes this chapter.

6.2 QoS-Aware Lifetime-Based Packet Transmission Technique

In this section, unlike using the aggregation factor as the triggering condition for packet transmissions, a lifetime-based algorithm is proposed in order to improve the performance of the BB algorithm and mitigate the inter-network collisions. To meet the stringent delay requirements of different M2M applications, it is necessary to deal with the packets with different delay budgets (or lifetimes) in the MFDRR. Specifically, each packet has its own lifetime and needs to be transmitted to the destination within the packet lifetime; otherwise, it must be dropped. Moreover, different packets are put into different queues, and specifically, three queues are used in the application layer of the MFDRR, differentiating the three types of traffic, as presented in Fig 6-1. Each queue maintains a timer recording its minimum lifetime representing the shortest lifetime of this queue. After a packet enters the queue, the lifetime value of each packet is retrieved and mutually compared to determine the minimum lifetime of the current queue. Since three queues have three minimum lifetime values, it must determine the shortest value to trigger the BB algorithm.

More specifically, as a new packet enters the queue, the scheduler takes two steps before triggering the BB algorithm. The first step is to compare the current minimum lifetime in the same queue. The second step is that a scheduler compares their minimum lifetime values computed from the three queues to determine the shortest lifetime among the three values. These two steps finally determine when to trigger the BB algorithm. In addition, since a large number of small-sized packets need to be transmitted, it is necessary to aggregate small packets into a IEEE 802.11g packet to improve channel efficiency. All of the packets in the three queues are packed into IEEE 802.11g payloads and transmitted using the BB algorithm. Additionally, given that the Maximum Transmission Unit (MTU) length is 2304 bytes, an aggregation factor is used to control the number of 6LoWPAN packets encapsulated in one IEEE 802.11g payload. For example, a large aggregation factor allows more 6LoWPAN packets to be packed in one IEEE 802.11 payload than a small aggregation factor. Given that a large aggregation factor generates fewer WLAN packets, so the channel utilisation is higher.

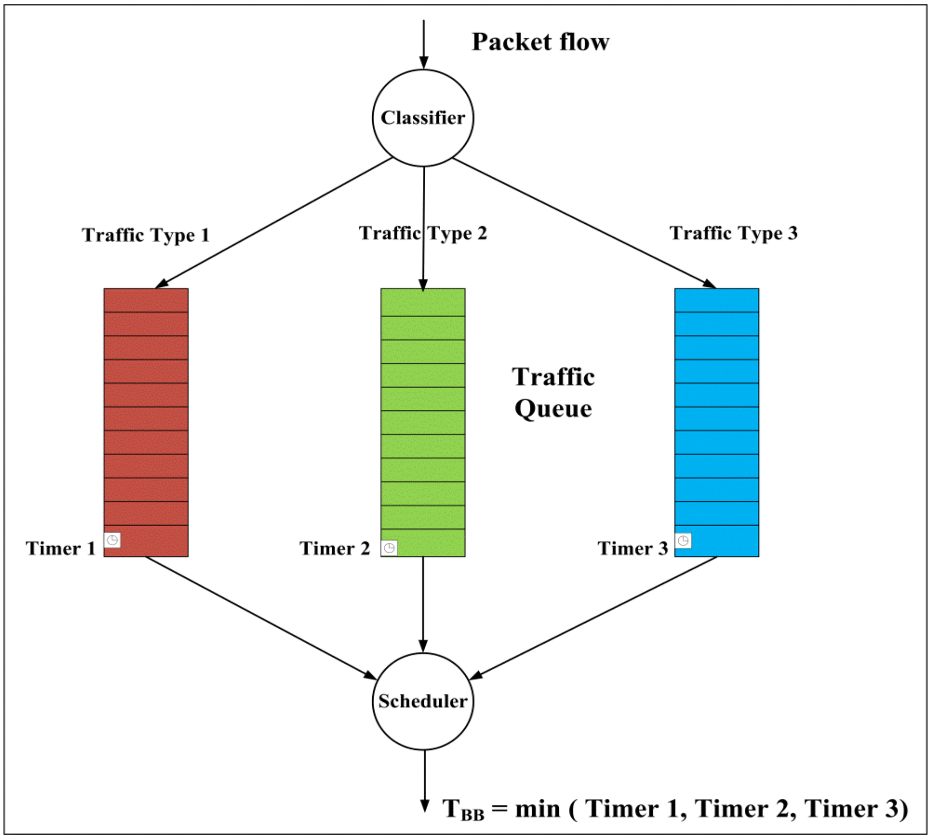


Fig 6-1 MFDRR application layer queue structure

Figure 6-2 shows three cases of the lifetime values. The blue, red and green blocks represent the lifetime value of an incoming packet T_2, the current absolute time is T_0 and the current shortest lifetime maintained by the queue is T_1. Another safety margin T_{margin} also needs to be set to avoid timeouts when the BB signal is being processed.

In case one, the new packet‘s lifetime is $T_2 < T_0$, meaning that the lifetime has expired so that this packet must be dropped. Also, if $T_0<T_2<T_{margin}$, the lifetime is longer than the current time, but smaller than the minimum time reserved for the Blank Burst triggering T_{margin}. In other words, since the BB signalling needs a margin area, falling behind this region means that this packet will expire before the Blank Burst algorithm is triggered, so this packet must be dropped.

In case two, if $T_0<T_{margin}<T_2<T_1$, it means that the new lifetime is shorter than the current lifetime, and thus the new lifetime should replace the current lifetime and become the newest lifetime. The previous timer should be cancelled. This case updates the timing to trigger the BB algorithm.

In the case three, if T_1<T_2, it means that current lifetime is the minimum lifetime, there is no need to update the current lifetime for this queue. Therefore, this packet should be stored in the queue.

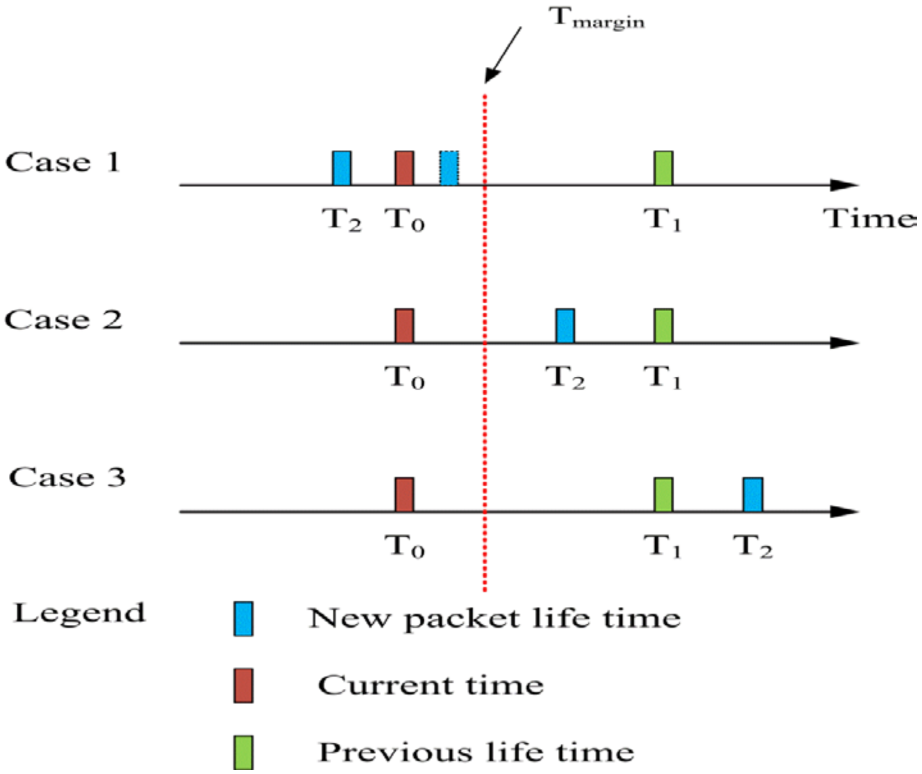


Fig 6-2 Blank Burst triggering based on lifetime

These three cases are used just for one type of M2M application, and each packet in the queue needs to maintain the current minimum lifetime, ensuring that an urgent request can be handled immediately. Before triggering the BB algorithm, it needs to determine the shortest lifetime among the three minimum lifetime values as the real minimum lifetime. To do this, the three minimum values in each queue are compared using a customised function, and the shortest one is used as the BB algorithm timer. In addition, the aggregation factors are used to regulate the number of packets wrapped in IEEE 802.11g packet payloads. Fig 6-2 shows the timing instants at which that the Blank Burst algorithm is launched. The BB algorithm may be triggered at any time, so the number of 6LoWPAN packets may not be an integer multiple of the aggregation factor, so at least two cases must be considered.

$$\mathrm{N_1} < \text{agg\_factor}, \tag{6-1}$$

$$\mathrm{N_1} \geq \text{agg\_factor}. \tag{6-2}$$

In the first case, $\mathrm{N_1} < \text{agg\_factor}$, the 6LoWPAN packets are packed into one IEEE 802.11g packet and the number of IEEE802.11g packets $\mathrm{N_2}$=1. In the second case, $\mathrm{N_1} \geq \text{agg\_factor}$, the 6LoWPAN packets are packed into several IEEE 802.11g packets. This case can be divided into two sub-cases: (1) $\mathrm{N_1} \bmod \text{agg\_factor} = 0$ and (2) $\mathrm{N_1} \bmod \text{agg\_factor} \neq 0$. The first case indicates that $\mathrm{N_1}$ is an integral multiple of agg_factor and the number of aggregated IEEE802.11g payloads is $\mathrm{N_2}$=$\mathrm{N_1}/\text{agg\_factor}$. In the second case, the number of aggregated IEEE802.11g payloads is $\mathrm{N_2}$=$\lfloor \mathrm{N_1}/\text{agg\_factor} \rfloor + 1$, meaning that the number of 6LoWPAN packets is an integer multiple of the aggregation factor; the remaining packets will be packed into one separate WLAN packet and then transmitted.

The combination of the packet lifetimes and the aggregation factors ensures that a packet can be transmitted in a timely manner and that high channel efficiency can be improved. In other words, a packet lifetime is used to guarantee the delay budget and trigger the BB algorithm, whereas the aggregation factor regulates the number of packets wrapped in an IEEE 802.11g payload. In this case, the BB algorithm is more complex than the previous one, which simply adopted the aggregation factor. Selecting the minimum lifetime from the three queues ensures that the urgent packets have the chance to be transmitted to the data sink to fulfil the QoS requirements. In addition, after the BB algorithm is triggered, the urgent packets must be transmitted, and thus that these queue needs to be emptied. The urgent queue needs to be emptied first, and if the blank burst transmission duration is long enough, the other two queues can also be emptied depending on the number of packets in those queues and the BB transmission duration.

6.3 Enhanced Blank Burst Algorithm

This section presents an enhanced algorithm that employs the packet lifetime to trigger the BB algorithm. The enhanced version of the algorithm is different from the previous one triggered by the aggregation factor as described in Chapter 5. The main differences are how to use the lifetime value to trigger the algorithm and how to use the aggregation factor to adjust the WLAN packet transmissions. Apart from these, the enhanced algorithm is the same as the previous one; that is, the BB signal is emitted from the MAC layer of the MFDRR, which is relayed to the 6LoWPAN end devices and suspends the 6LoWPAN transmissions, thus leaving this period for the IEEE 802.11g interface of the MFDRR. By implementing this algorithm, the 6LoWPAN and IEEE802.11g transmitters can corporately send packets without interfering with each other.

Figure 6-3 presents the three stages of the algorithm. The first stage is before the BB algorithm is triggered, as a packet comes into the application layer of the MFDRR, the packet is stored in a queue that stores the same type of packets by a classifier. Meanwhile, the lifetime of this packet is retrieved and compared using Algorithms 6.1 and 6.2. The second stage is the BB signal generation, in which the signal is embedded in one additional byte of a beacon packet, and then relayed to the 6LoWPAN end devices. The third stage is when the signal comes into play, when it stops the 6LoWPAN transmissions and allows the IEEE 802.11g transmissions with Algorithm 6.3. More precisely, the number of the aggregated WLAN payloads is calculated using the number of the 6LoWPAN packets and the aggregation factor. When these three queues are flushed, the queue with the minimum lifetime must be emptied first, and subsequently the second and third non-urgent queues are flushed to ensure the QoS of the M2M applications. To better explain the algorithm presented in Fig 6-3, three algorithms 6.1, 6.2 and 6.3 are explained in pseudo-code as these algorithms are repeatedly invoked within the improved BB algorithm, as shown in Fig 6-4, Fig 6-5 and Fig 6-6.

As shown in Fig 6-3, when a new packet enters the queue, the packet type is determined using the classifier. Algorithm 6.1 is used to identify the shortest lifetime of this queue by measuring all queued packets' lifetimes; Algorithm 6.2 uses the lifetime value to trigger the BB algorithm based on the results obtained from Algorithm 6.1, as shown in the blue rectangle. Once the minimum lifetime is obtained, the BB timer is set. This means the QoS of the system relies on this timer, and when it expires, the packets are transmitted using the enhanced BB algorithm, which means the QoS requirements of most stringent applications are met. In addition, after the expiration of the timer, the BB signal is emitted from the MFDRR MAC layer and forwarded to 6LoWPAN devices. Upon receiving the signal, the 6LoWPAN devices wait for a BB period of time for the IEEE 802.11g transmissions; as for the IEEE 802.11g part of the MFDRR, the IEEE

802.11g interface attempts to flush the three queues as per the packet priorities. The queue with the highest priority is flushed first. Combined with the aggregation factors, it can be seen in Fig 6-6 that Algorithm 6.3 in the green rectangle is repeatedly revoked to transmit different numbers of WLAN packets. After the end of the WLAN transmissions, the cycle begins. The code of the lifetime-based BB algorithm can be found in Appendix D.

The 6LoWPAN packet uses an optimum 21-byte header for the data packet, whereas the beacon uses a small header of 12 bytes containing various control fields. The 6LoWPAN nodes are controlled by the header bits of the beacon transmitted from the MFDRR. Only one byte is used in the beacon frame to represent the Blank Burst period, which is incorporated within the beacon structure. Specifically, the proposed algorithm evaluates the amount of aggregated packets to be transmitted, calculates the time that needs to transmit those aggregated packets using the WLAN interface and then writes the time value in the one-byte field. Upon receiving the time value wrapped in the beacon by end devices, they simply stop transmitting for that time duration. The proposed algorithms use one byte, which accounts for 7% length of the beacon frame and is the minimum additional signalling traffic, will not reduce the energy efficiency of the heterogeneous network compared to a standard Zigbee network. On the contrary, the proposed algorithms reduce the overall collision level in a network, thus improving the energy efficiency of the proposed heterogeneous network.

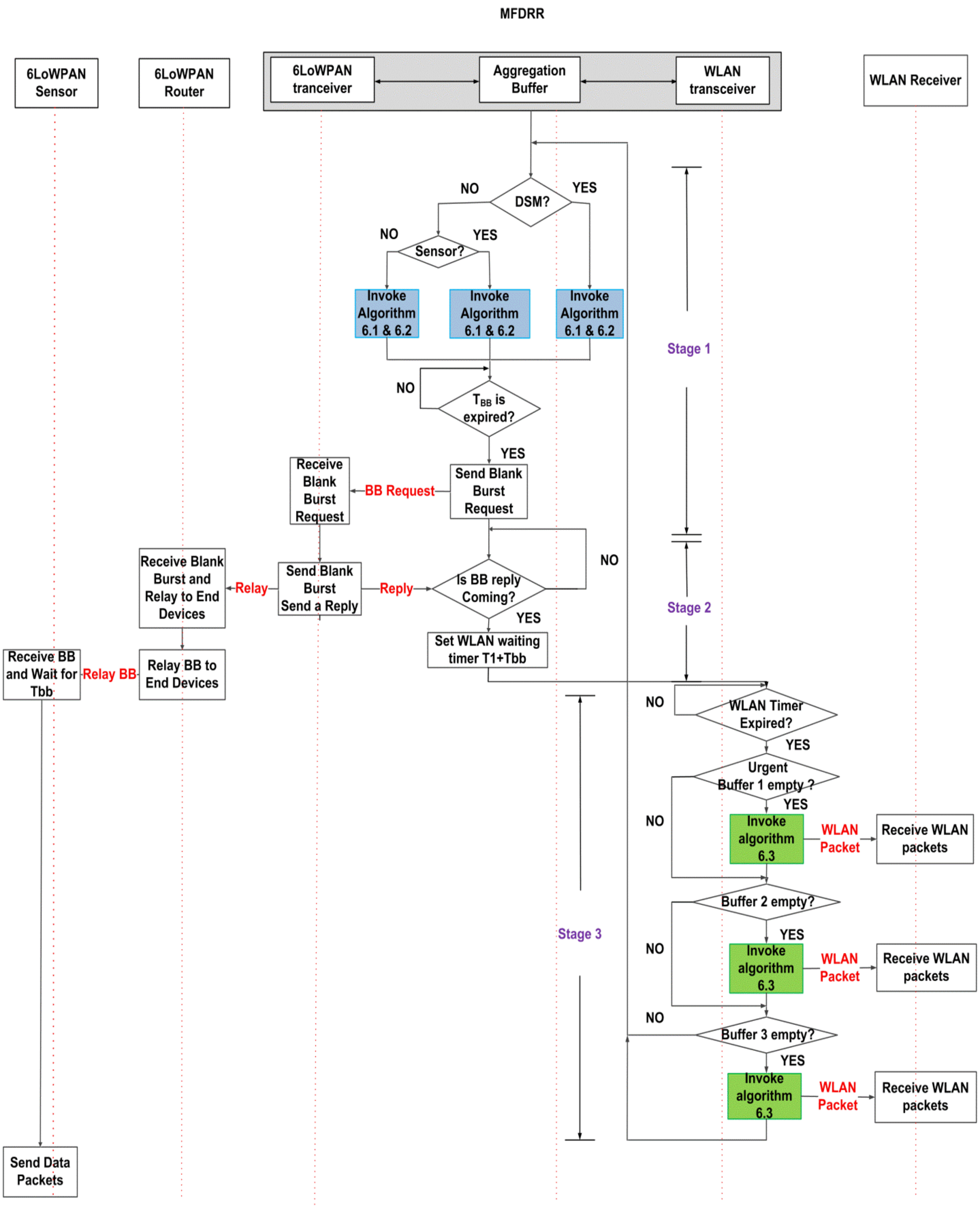


Fig 6-3 The flow chart of the lifetime-based Blank Burst algorithm.

Algorithm 6.1: Scheduler to identify the minimum lifetime value

```
Input: deadline_1, deadline_2, deadline_3
Output:BB_deadline
If deadline_1!=0 &&deadline_2!=0&& deadline_3!=0 Then
    If (deadline_1<deadline_2) then
        Return BB_deadline:=deadline_1;
    Else if deadline _2<deadline_1&& deadline_2<deadline_3
        Return BB_deadline:= deadline_2;
    Else
        Return deadline_3;
    End
Else if deadline_1==0 && deadline_2!=0  && deadline_3!=0 Then
    If  deadline_2<deadline_3 Then
        Return  BB_deadline:=deadline_2;
    Else
        Return BB_deadline:=deadline_3;
    End
Else if deadline_2==0 && deadline_1!=0&& deadline_3!=0 Then
    If deadline_1<deadline_3 Then
        Return  BB_deadline:=deadline_1;
    Else
        Return BB_deadline:= deadline_3;
    End
Else if deadline_3==0&&deadline_1!=0&&deadline_2!=0 Then
    If  deadline_1<deadline_3 Then
        Return BB_deadline:=deadline_1;
    Else
        Return BB_deadline:=deadline_2;
    End
Else if deadline_1==0&&deadline_2==0 && deadline_3!=0 Then
```

```
            Return BB_deadline:=deadline_3;
          End
    Else if deadline_2==0&&deadline_3==0 && deadline_1!=0 Then
          Return BB_deadline:=deadline_1;
          End
    Else if deadline_3==0&&deadline_1==0 && deadline_2!=0 Then
          Return BB_deadline:=deadline_2;
        End
    End
```

Fig 6-4 Algorithm 6.1

Algorithm 6.2: Lifetime Scheduling

```
Input: $T_2$, $T_0$, $T_{margin}$
Invoked by each packet queue to determine the newest minimum lifetime
If  Mutex==0 Then       // no Blank Burst signal has been triggered. Mutex is a signal,0 represents the Blank Burst signal is not triggered; 1 represents the Blank Burst signal is triggered.
    If deadline_1 ==0 Then //first time no values given to deadline_1
        If $T_2 - T_0 < T_{margin}$ Then
            Drop this packet;
        End
        If $T_2 - T_0 == T_{margin}$ Then
            Trigger Blank Burst (BB) algorithm and insert the packet into the queue;
        End
        If $T_2 - T_0 > T_{margin}$
            Deadline_1: = $T_2$ ;
            BB_deadline:= invoke Algorithm 6.1 (deadline_1, deadline_2, deadline_3);
            Set BB timer $T_{timer}$ =BB_deadline;// Obtain the new minimum lifetime
            Insert the packet in the queue;
        End
    Else If (deadline_1!=0) Then
        If deadline_1 < $T_2$ Then
```

```
            Insert the packet in the queue;
        End
        If deadline_1 > $T_2$ && $T_2 - T_0 == T_{margin}$
            Cancel the previous timer $T_{timer}$
            Trigger BB algorithm and insert the packet in the queue;
        End
        If deadline_1 >$T_2$ && $T_2 - T_0 > T_{margin}$
            Deadline_1: = $T_2$ ;
            BB_deadline:= invoke Algorithm 6.1 (deadline_1, deadline_2, deadline_3);
            Cancel the pervious timer $T_{timer}$
            Insert the packet in the queue;
            Set BB timer $T_{timer}$ :=BB_deadline;
        End
        If deadline_1 > $T_2$ && $T_2 - T_0 < T_{margin}$

            Drop this packet;
        End
    End
Else If Mutex!=0;  // a Blank Burst signal has been triggered
    Insert the packet into the queue
End
```

Fig 6-5 Algorithm 6.2

Algorithm 6.3. Count the number of the aggregated packets and sent them out

```
Input: pkt_count, agg_factor, agg_pkt_count
If  pkt_count $\leq$ agg_factor Then
    Remove packets from the aggregation buffer;
    Create an aggregated IEEE802.11g payload;
    Send the aggregated payload out;
Else if pkt_count $\geq$ agg_factor Then
```

```
        If $\mathrm{pkt\_count} \bmod \mathrm{agg\_factor} == 0$ Then
            agg_pkt_count:= pkt_count/agg_factor ;
            While agg_pkt_count !=0 do
            Obtain agg_factor packets from the buffer;
            Create an aggregated WLAN payload;
            Send this aggregated payload out;
            End
        Else
            agg_pkt_count:= $\lfloor \mathrm{pkt\_count}/\mathrm{agg\_factor} \rfloor$+1
            While agg_pkt_count !=0 do
            Obtain agg_factor packets from the buffer;
            Create an aggregated WLAN payload;
            Send this aggregated payload out;
        End
    End
```

Fig 6-6 Algorithm 6.3

6.4 Performance Analysis of the Lifetime-Based BB Algorithm

The network used in the simulation as shown in Fig 6-7. The performance of the lifetime-based BB algorithm is evaluated in this section, and the key simulation parameters are listed in Table 6-1. The simulation ran with multiple seed values and the results were plotted with a 95% confidence interval. Two types of application traffic were used: the sensor traffic and the meter reading traffic. Here, the sensor traffic has a delay requirement of 1s and the meter reading traffic delay limit is 900s. The entire performance analysis includes two steps. Step 1: one type of traffic is used to compare with Chapter 5 results; that is, the first scenario uses two overlapping channels; the second scenario uses two non-overlapping channels; and the third scenario introduces the enhanced BB algorithm. The lifetime-based BB algorithm is added to the fourth scenario to compare with the other three scenarios. Only the sensor traffic was used in this step. Step 2: the sensor and meter reading are introduced to test if the system meets the QoS requirements. The lifetime-based algorithm could guarantee the end-to-end delay and mitigate the inter-network collisions.

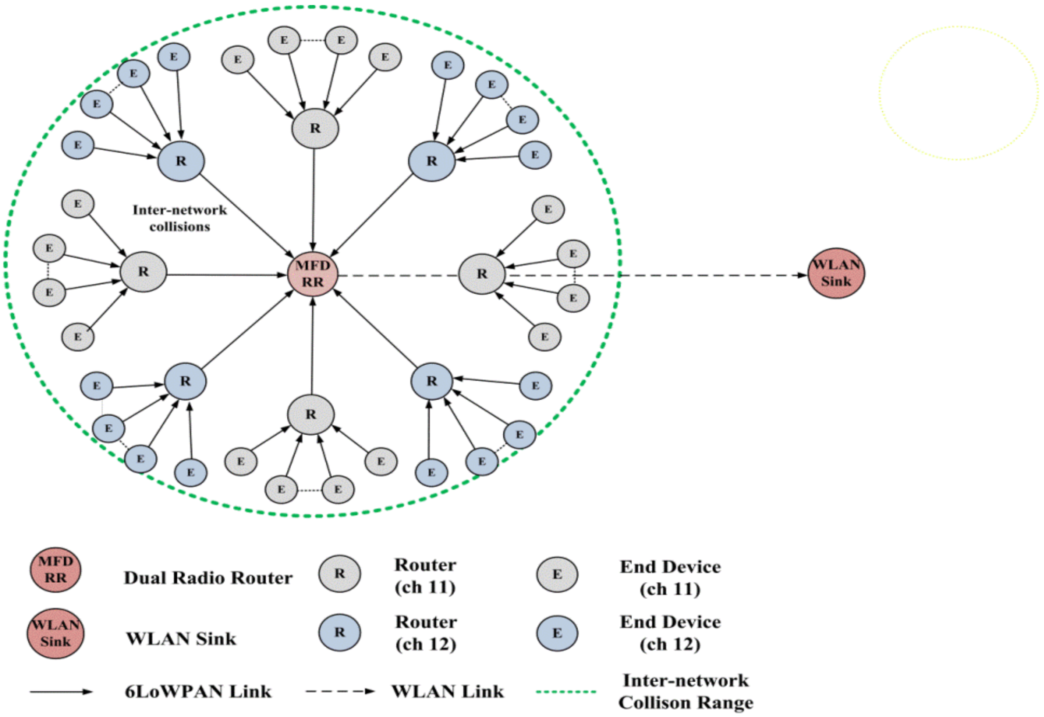


Fig 6-7 The heterogeneous area network

Table 6-1 The key parameters for the lifetime-based BB algorithm

Group Name	Parameter		Value
Network	Hop		3
	Number of nodes		64
	Standard		6LoWPAN IEEE 802.11g
	Operating Frequency		2.4 GHz
	6LoWPAN channel		12
	IEEE 802.11g channel		1
Propagation model	Free space path loss		
MFDRR	6LoWPAN	BO	5
		SO	3
		Transmission Power	1.8 mW
	WLAN	Transmission Power	100 mW
		Packet Size	1200 bytes
		Aggregation Factor	15
		Safety margin (sec)	0.2 sec
Router	BO		4

	SO	2
End device	Packet size	64 bytes
	Packet generation	Exponentially distributed
	Transmit Power	1 mw
	Packet inter-arrival rate	0.25, 0.5, 1, 1.3, 1.5,1.7, 2pkts/sec
Target Applications	Sensor end-to-end delay	1 s
	Meter Reading end-to-end delay	900 s

The packet delivery rate is initially evaluated, as shown in Fig 6-8. The packet delivery rate with the lifetime-based BB algorithm gradually declined from 98% to 65% as the traffic loads were increased, whereas the default scenario (red line) under the adverse inter-network collisions dropped from 90% to 32%. The result showed the lifetime-based BB algorithm (black line) offered a similar packet delivery ratio as the aggregation factor-based BB algorithm (green line, refer back to Section 5.4.1). In particular, at the traffic load of 1.3 pkts/sec, the enhanced algorithm improved the packet delivery rate by 89% compared to the scenario under the adverse impact of the inter-network collisions. Note that the packet delivery rate for the lifetime-based and aggregation factor-based algorithm are very similar because both the algorithms avoid the inter-network collisions. It is also noted that the two algorithms showed the same trend with the scenario where no inter-network collisions existed, meaning that both the aggregation factor-and lifetime-based algorithms can mitigate the inter-network collisions to the greatest extent.

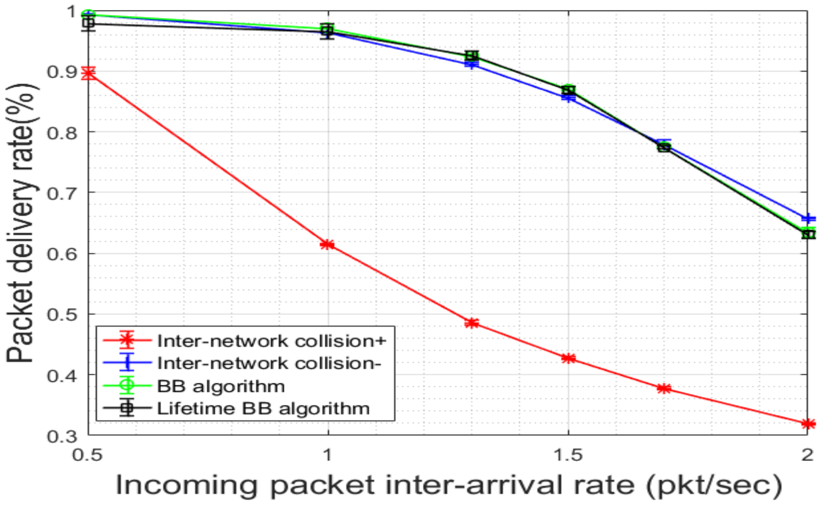


Fig 6-8 Packet delivery rate with the lifetime-based algorithm

Another metric is the end-to-end delay as illustrated in Fig 6-9. It can be seen that the lifetime-based BB algorithm's end-to-end delay remained constant at 0.58 s as the traffic loads increased. While due to the inter-network collisions, the packet delay slowly increased from 0.25s to 0.63s with the increasing traffic loads. As such, it is clear that the two scenarios meet the sensor's delay requirement at 1s, but this scenario under the impact of inter-network collisions suffered a relatively low packet delivery rate. One of the main components in the end-to-end delay accounts for the aggregation delay due to the small-sized 6LoWPAN payloads in the aggregation factor-based BB algorithm. Compared to the scenario in the presence of inter-network collisions, the lifetime-based BB algorithm reduced the end-to-end delay by 20%, which shows the feasibility of the large-scale deployment of the M2M devices.

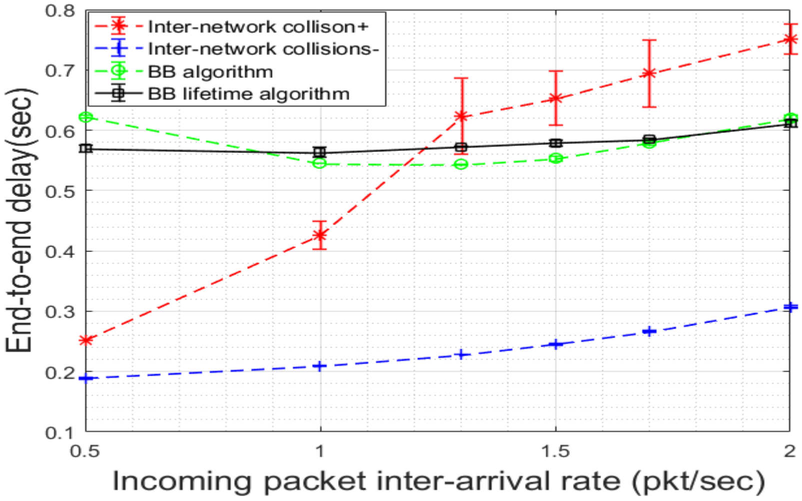


Fig 6-9 End-to-end delays with the lifetime-based algorithm

The lifetime-based BB algorithm drops the packets that fail to reach the WLAN sink with expired lifetimes. Fig 6-10 shows that the number of dropped packets due to the expired lifetimes in the MFDRR increased from 2 to 63 with the increasing traffic loads. This is because with the rising traffic loads, the network contention level increased, resulting in longer queuing delays and a higher number of expired packets. These packets in turn were dropped in the MFDRR to ensure the end-to-end delay requirement. In contrast, the aggregation factor-based BB algorithm does not have such mechanism in the MFDRR, meaning that some of the packets that arrive at the data sink have expired packet lifetimes. Therefore, the lifetime-based BB algorithm is better than the aggregation factor-based BB algorithm.

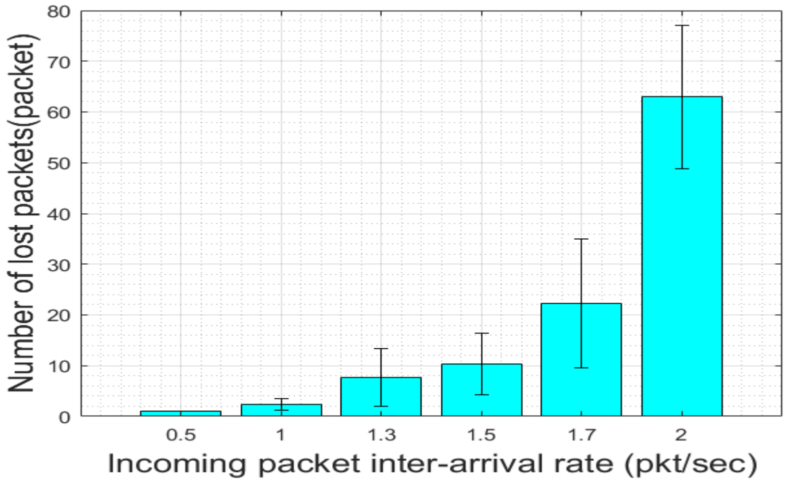


Fig 6-10 Number of dropped sensor packets in the MFDRR due to lifetime expiration

The 6LoWPAN router packet losses directly reflect the adverse impacts of the inter-network collisions. Fig 6-11 shows that the number of lost packets due to the inter-network collisions at the 6LoWPAN router for different BB algorithms. It can be seen that the number of the packet losses under the adverse effects of the inter-network collisions climbed from 1000 to 4000 packets then stabilised between 4000 and 4500 packets, whereas the lifetime-based BB and aggregation factor-based algorithms saw packet losses of fewer than 500 packets. This is because the BB period protected 6LoWPAN packets from the inter-network collisions. This confirms the effectiveness of the lifetime-based BB algorithm.

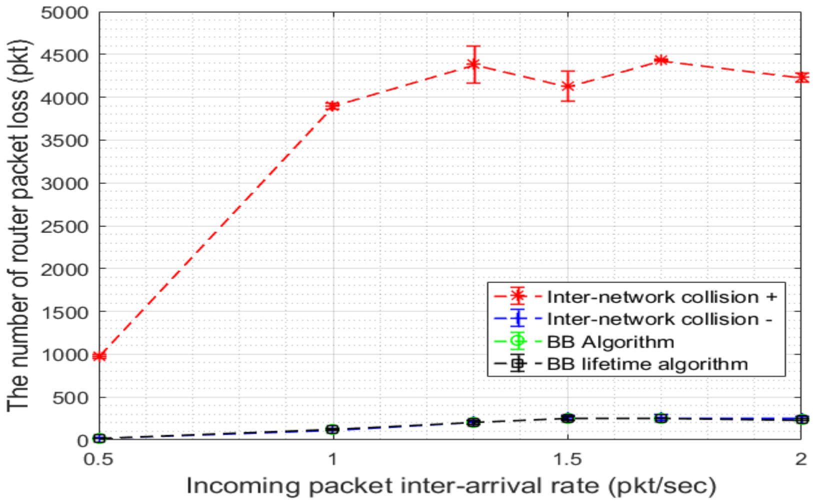


Fig 6-11 6LoWPAN Router packet loss due to inter-network collisions

Figure 6-12 shows that the number of packet collisions due to intra-and inter-network collisions. It can be seen that the scenario in the presence of the inter-network collisions had the highest number of collisions linearly increasing from 5000 to 23000. In contrast, the scenario without inter-network collisions and the scenarios with the lifetime-based BB and aggregation factor-based BB algorithms showed the low numbers of packet collisions, gradually rising from 2000 to 18000. It is clear that the gap between these scenarios is due to the inter-network collisions, while the lower three lines represent the intra-network collisions. From the intra-network collisions, we conclude the intra-network collisions cannot be completely avoided and are a main contributor to packet collisions despite the use of the staggered link design. As the traffic loads increased, this trend became more evident, as shown in the figure. For this reason, it is suggested that M2M network should operate at low data rates. For example, at the load of 1.3 pkts /sec, the lifetime-based algorithm reduced the number of collisions by 50%, showing a maximal gain for the proposed lifetime-based algorithm.

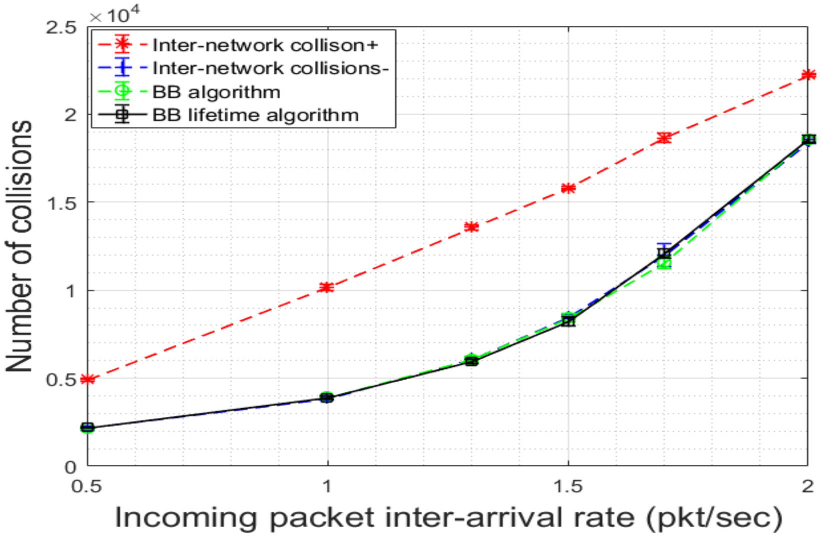


Fig 6-12 Number of collisions due to intra and inter-network collisions

In the second step, two types of traffic were introduced to test the performances of the proposed lifetime-based BB algorithm. Specifically, the sensor traffic and smart metering traffic were examined so that the QoS of the traffic could be guaranteed. The sensor traffic is bounded by the end-to-end requirement of 1s for M2M applications such as smoke detectors, while the meter reading traffic delay requirement is 900s. In the simulation, 32 out of the 64 6LoWPAN nodes are sensor nodes, while the other 32 nodes are meter reading nodes. The performance analysis of the lifetime-based BB algorithm is presented below.

The packet delivery rates of the sensor traffic and meter reading traffic are presented in Fig 6-13. The sensor traffic packet delivery rate gradually dropped from 98% to 60% as the traffic loads increased, while the meter reading packet delivery rate remained stable at nearly 99% over the simulation time. The difference lies within the fact that the sensor traffic, due to its higher packet inter-arrival rate, had a higher chance of colliding with the WLAN packets. The results also reveal that the access networks such as 6LoWPAN and WLAN networks tend to experience more packet collisions when traffic loads increase. Therefore, the network must maintain lower traffic loads to meet the QoS requirements of M2M applications.

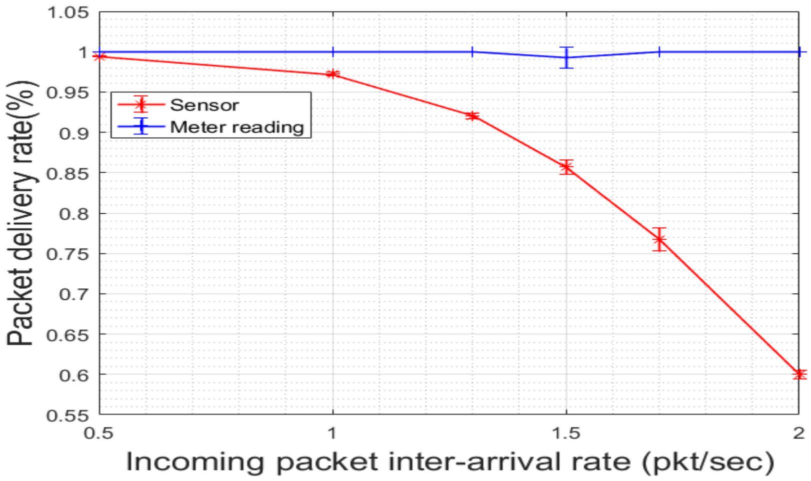


Fig 6-13 Packet delivery rate with two types of traffic

The end-to-end delays for the two types of traffic are illustrated in Fig 6-14. Both delays were quite stable around 0.56s to 0.6s even at traffic loads of 2 pkts/sec. The meter reading traffic load was not high, so the end-to-end delay levelled at 0.6s. Although the end-to-end delay of the sensor traffic was not high, it experienced packet losses at the high traffic loads due to the intra-network collisions. These results prove that the proposed heterogeneous network meets the end-to-end delay requirements of the basic M2M applications.

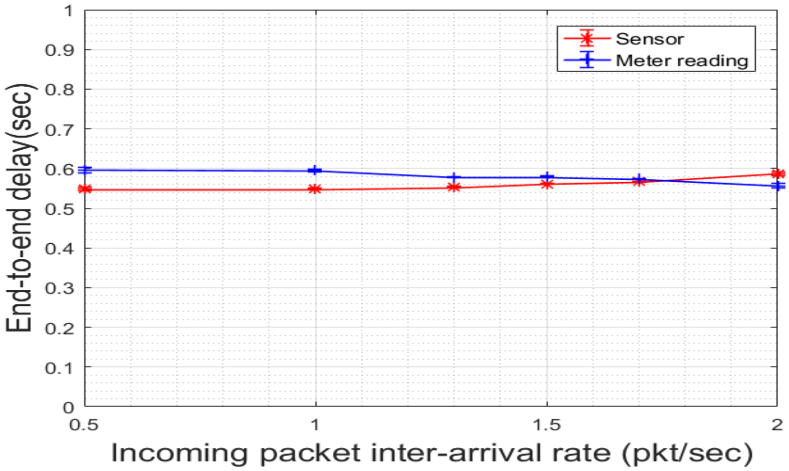


Fig 6-14 End-to-end delay with two types of traffic

The number of packet losses for the sensor and meter reading traffic for the lifetime-based algorithm is depicted in Fig 6-15. It can be seen that the sensor packet losses increased from zero to ten packets as the traffic load increased, whereas the meter reading loss is always zero. This is because the increased sensor loads slightly increased the queuing delay of the sensor traffic, so a small number of packets, which have exceeded their lifetime, were dropped by the MFDRR. In contrast, the meter reading traffic losses were low because the meter reading loads were low compared to the sensor traffic. The result shows that these two types of traffic can be well supported by the proposed MFDRR.

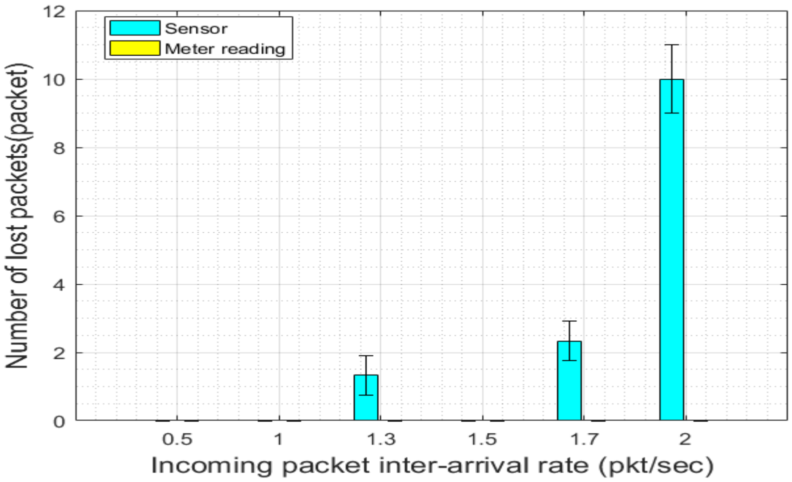


Fig 6-15 Sensor and meter reading packet losses using the lifetime-based BB algorithm

6.5 Two-Way Communications in M2M networks

Two-way communications play a key role in supporting M2M networks because applications need both uplink and downlink data exchanges between the field devices and data servers. One example is that electric vehicles need to dynamically obtain the location of the charging stations by communicating to the server, which in turn replies to the vehicles with the precise locations [124, 126]. Another example is that the Smart Grid, which connects many distributed renewable energy generators exchanging information with the remote server, so two-way communications are required.

6.5.1 Potential Problems in Two-Way Communications

M2M communication networks often involve the uplink and downlink traffic transmissions. As mentioned before, the uplink of the M2M network has more traffic than its downlink, so the downlink might cause traffic congestion when both the uplink and downlink traffic shares the same transmission medium using the random access protocol. Supporting bidirectional traffic is important in many networks including M2M and Smart Grid communication networks. Not many studies have focused on the problems of bidirectional data communications in a random access-based sensor networks. -

To deal with the above issues, a two-way communication network was proposed by using the proposed heterogeneous network model to support bidirectional sensor traffic flows. In this model, all the bidirectional data are generated by the end devices and forwarded to the distant data sink, which in turn transmits a packet on the downlink for every received uplink packet. The downlink traffic adds to the uplink traffic, so the routers that include the bidirectional and unidirectional traffic could experience traffic congestion. In general, when the networks generate event-based traffic burst in the uplink, they could become congested with a large number of concurrent packets in the queue. The congestion can be divided into two classes: node level congestion and link level congestion [127]. The node level congestion is commonly seen in traditional wireless networks and caused by peak traffic arrivals. The many-to-one traffic pattern in wireless sensor networks allows the traffic to travel from widespread sensor nodes to routers then to one or several sink nodes [128]. In this case, as shown in Fig 6-16 a, the relay node may not have a high transmission data rate link, so the MAC queue could grow, resulting in buffer overflow. The link level congestion is caused by packet collisions, and thus the throughput is reduced. Many sensor networks use the CSMA/CA protocol to access the channel, so packets can collide when the nodes attempt to seize the channel. As such, the end-to-end delay is increased, and the overall throughput and link utilisation are reduced. Collectively, these two types of congestion adversely impact on the QoS and energy efficiency of wireless sensor networks. In a multi-hop network, a relay node needs to compete with many sensor nodes. This is called one-to-many transmission, as shown in Fig 6-16 b. In this case, the downlink traffic adds to the uplink traffic, so the total volume of traffic may exceed the capacity of the relay node. Therefore, the relay node may also lose the downlink traffic due to packet collisions with other sensor nodes. In this case, the downlink traffic can have more congestions than that of the uplink. Losing high priority downlink packets could seriously affect the network QoS.

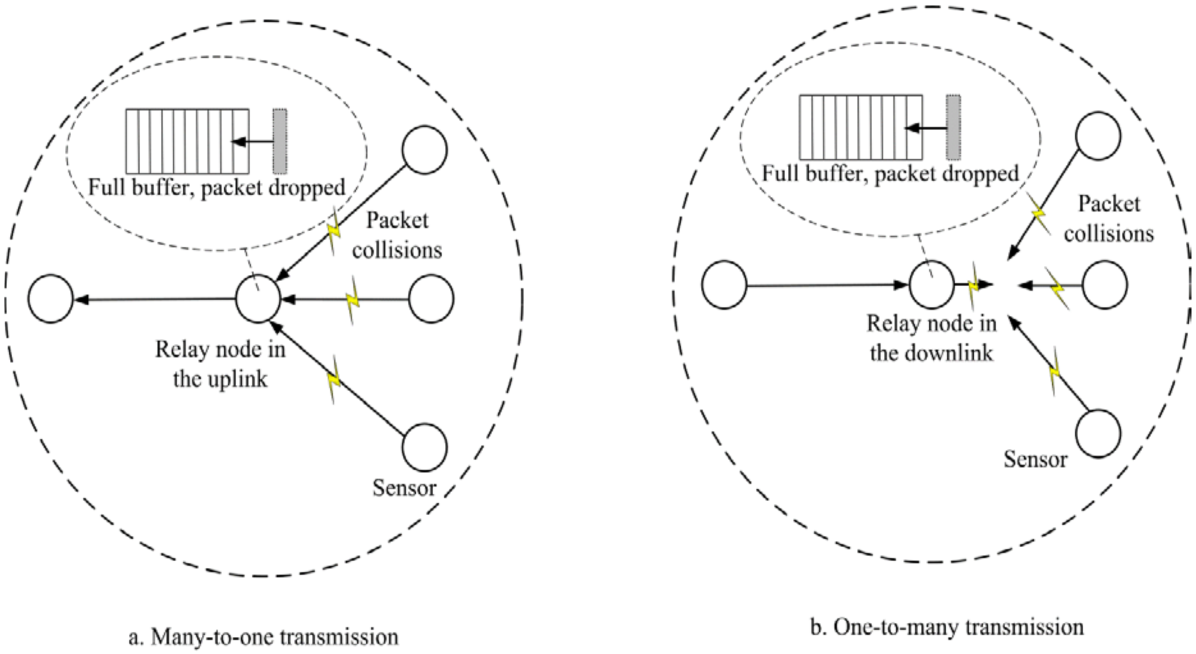

Full buffer, packet dropped
Packet collisions
Relay node in the uplink
Sensor
a. Many-to-one transmission
Full buffer, packet dropped
Packet collisions
Relay node in the downlink
Sensor
b. One-to-many transmission

Fig 6-16 Uplink and downlink transmissions

6.5.2 Congestion Mitigation Algorithm Design

To overcome the downlink congestion, a heuristic congestion mitigation scheme was developed to ensure the QoS of the heterogeneous area network. A downlink congestion mitigation algorithm was proposed to effectively detect and reduce the downlink congestion. This algorithm is a cross-layer optimisation scheme that coordinates the 6LoWPAN MAC layer, the adaptation layer, and the application layer to adjust the packet inter-arrival rate. It is understood that MAC buffer occupancy directly reflects the level of congestion. The buffer occupancy level can be obtained from the queue length statistics. Aside from this, ACK packets can be used as signalling packets to allow the 6LoWPAN nodes to reduce the packet inter-arrival rate, so the congestion level could drop and allow the downlink packets to propagate from the routers to the end devices. The rationale of using ACK packets is that they do not increase overheads into the network and thus can quickly notify sensor nodes to decrease the packet inter-arrival rate.

Figure 6-17 shows that the framework of the proposed downlink congestion control unit. It consists of four parts: a congestion detection unit (CDU), a downlink protection unit (DPU), a congestion notification unit (CNU) and a rate adjustment unit (RAU). The CDU is used to identify any forthcoming congestion in advance. The CDU measures the queue length in the MAC layer to determine the congestion intensity. Specifically, the queue length is divided into several threshold zones according to the level of congestion. Each threshold zone corresponds to a data rate that needs to be altered by the sensor node application layer to reduce the congestion level. The downlink protection unit is used to protect the downlink packets from being lost due to buffer overflow. Once the CDU detects that the queue length reaches a threshold, the adaptation layer stores all of the incoming downlink packets in a protection queue.

Conversely, as the CDU finds the queue length is no longer higher than the threshold, where the intensity of the congestion reduces, the downlink packets are removed from the protection queue and sent to the MAC queue. Meanwhile, the MAC layer of a relay node adds one field in the ACK frame to represent the congestion status. The CNU uses the ACK packets to notify sensor nodes of the router queue length. The reason for adopting ACK packets is that they do not need to wait for the CSMA/CA protocol to access the channel and can inform sensor nodes quickly. Upon receiving the ACK packets, sensor nodes signal the application layer to lower the packet inter-arrival rate, decreasing the number of outgoing packets. The RAU has a mapping table stored in the application layer. Once the CNU informs the application layer, the mapping table is searched to find a corresponding inter-arrival rate, and then this inter-arrival rate is selected as the current data rate. These four units adjust the inter-arrival rate to maximise the throughput and guarantee the QoS of the network. In particular, the CDU and DPU are located in the router nodes, while the CNU and RNU are located in the sensor nodes.

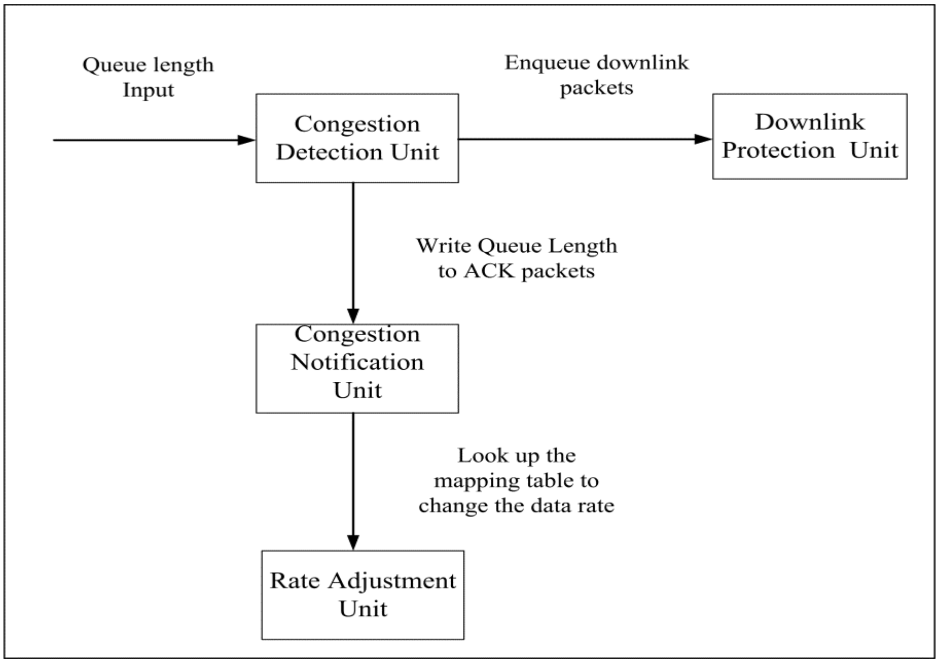


Fig 6-17 Framework of the proposed downlink congestion mitigation

To further demonstrate the proposed congestion mitigation protocol, the four units mentioned in Fig 6-17 are associated with the 6LoWPAN protocol stack. Fig 6-18 shows which layer these four units work at. It can be seen that the CDU works at the MAC layer of the router node, monitoring the queue length for the adaptation layer; the DPU receives the signal from the MAC layer that adopts a protection queue to store the downlink packets. The CNU works in the sensor node’s MAC layer, receiving ACK packets to signal the RAU in the application layer of a sensor node. The RAU is an important component of the proposed protocol, regulating the inter-arrival rate to reduce the queue occupancy duration to protect the downlink packets. On the other hand, if the channel utilization is low and the queue length is below a certain threshold, the queue status is also forwarded by ACK packets to the end device nodes to raise the packet inter-arrival rate. As such, the proposed algorithm uses the inter-arrival rate with incoming traffic loads to optimise QoS metrics such as the throughput, end-to-end delay and packet delivery rate.

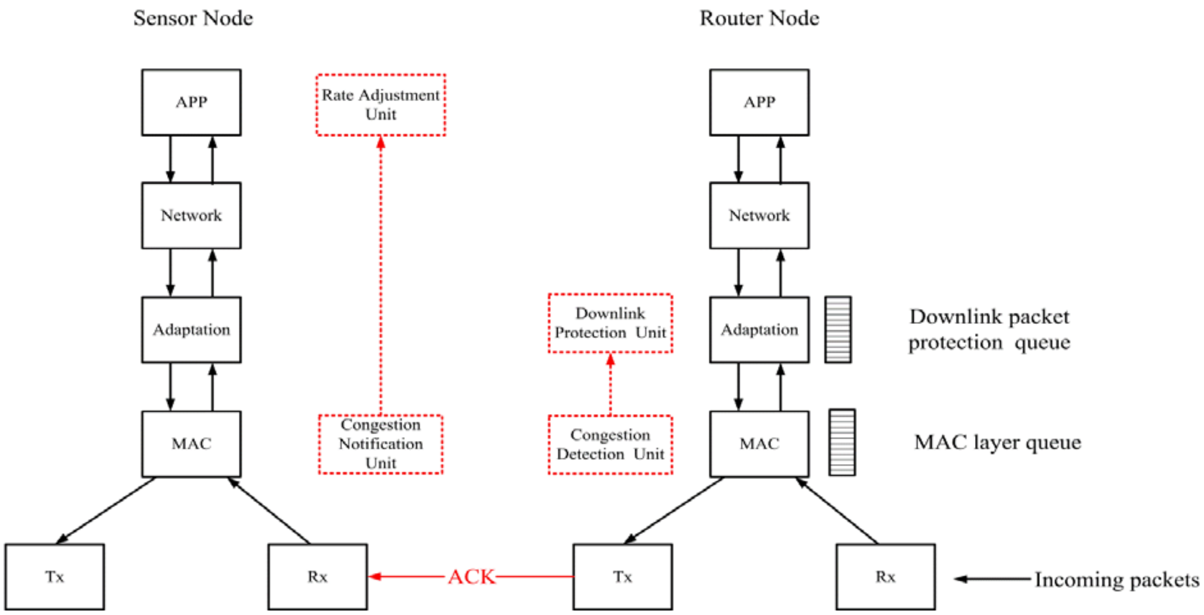


Fig 6-18 Four units illustrated in the protocol stack

To precisely measure the downlink congestion levels at the router node, the queue length is divided into five states: low traffic, medium traffic, high traffic, super-high traffic and congestion. As illustrated in Fig 6-19, five thresholds (Q_{low}, Q_{medium}, Q_{high}, $Q_{superhigh}$ and $Q_{congestion}$) are used to segment the queue. Furthermore, a threshold mapping between the queue length and the inter-arrival rate is introduced to quantify the queue length. This mapping aims to adapt the inter-arrival rate as per the five threshold lengths. The parameter Q is denoted as a random queue length in the system at a given time. The details are below.

1. $0<Q<Q_{low}$, the queue occupancy is low, so sensor nodes need to increase the inter-arrival rate.
2. $Q_{low}<Q<Q_{medium}$, the queue occupancy is still low, thus it is possible to increase the inter-arrival rate of the sensor nodes;
3. $Q_{medium}<Q<Q_{high}$, system can still be allowed to increase throughput.
4. $Q_{high}<Q<Q_{superhigh,}$ traffic is high, but the system is not congested.
5. $Q_{superhigh}<Q<Q_{congestion}$, traffic is super high, but the system is not congested.
6. $Q_{congestion}<Q$, downlink congestion occurs, and it is time to lower the inter-arrival rate.

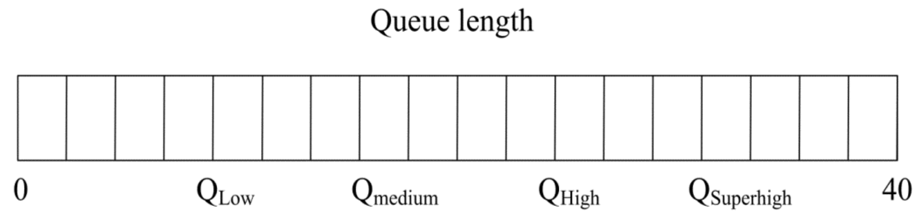


Fig 6-19 Queue length division

The mapping table is shown Table 6-2. It is clear that the inter-arrival rate went up steadily, rising from 0.27 to 2 pkts/sec, whereas the loads were increasing with the inter-arrival rate being slowly adjusted. The rationale is that when loads and channel utilisation are low, it is necessary to increase the packet inter-arrival rate to increase the channel utilisation; when the load is moderate; the increase of the inter-arrival rate is slow. This means that the channel is fully utilised without compromising QoS metrics such as the end-to-end delay and packet success rate. When the system was about to congest, the inter-arrival rate decreased to 0.5 pkt/sec. As congestion occurred, it further dropped to 0.25 pkt/sec. This volatility ensures that the downlink congestion can be effectively controlled with the proposed protocol. The main objective of this protocol is to maintain the QoS requirements for the downlink traffic while maximising the uplink throughput. This is because the M2M communication networks are uplink-oriented and the downlink traffic only occupies a small proportion of the total traffic load, while the uplink traffic accounts for the majority of network loads.

Table 6-2 Inter-arrival rate and queue length mapping table

Queue length (pkt)	**Inter-arrival Rate (pkt/sec)**
$0 < Q < Q_{low}$	0.27 0.5 1 2
$Q_{low} < Q < Q_{medium}$	1.3
$Q_{medium} < Q < Q_{high}$	2
$Q_{high} < Q < Q_{superhigh}$	1
$Q_{superhigh} < Q < Q_{congestion}$	0.5
$Q_{congestion} < Q$	0.25

To accurately measure the downlink congestion level, the router queue length is divided into five states: low traffic Q_{low}, medium traffic Q_{medium}, high traffic Q_{high}, super-high traffic $Q_{superhigh}$, and congestion $Q_{congestion}$. The details are as follows.

1. $0<Q<Q_{low}$, the queue occupancy is low, so sensor nodes need to increase the inter-arrival rate four times recorded by a counter.

   At the first time, the packet inter-arrival rate starts from 0.27 pkt/sec.

   At the second time, after receiving five packets, the router MAC layer evaluates the queue length if $0<Q<Q_{low}$ the packet inter-arrival rate rises to 0.5 pkt/sec

   At the third time, after receiving five packets, the router MAC layer evaluates the queue length if $0<Q<Q_{low.}$ the packet inter-arrival rate rises to 1 pkt/sec.

   At the fouth time, after receiving five packets, the router MAC layer evaluates the queue length if $0<Q<Q_{low,}$ the packet inter-arrival rate rises to 2 pkt/sec.
2. After receiving five packets, the router MAC layer evaluates the queue length, and if $Q_{low}<Q<Q_{medium}$, the queue occupancy is still low, thus it is possible to increase the inter-arrival rate to 1.3 pkt/sec.
3. After receiving five packets, the router MAC layer evaluates the queue length, and If $Q_{medium}<Q<Q_{high}$, the packet inter-arrival rate rises to 2 pkt/sec.
4. After receiving five packets, the router MAC layer evaluates the queue length, and If $Q_{high}<Q<Q_{superhigh,}$ the packet inter-arrival rate starts to decrease to 1 pkt/sec to lower the contention level.
5. After receiving five packets, the router MAC layer evaluates the queue length, and if $Q_{superhigh}<Q<Q_{congestion}$, the packet inter-arrival rate starts to decrease to 0.5 pkt/sec to lower the contention level.
6. After receiving five packets, the router MAC layer evaluates the queue length, and if $Q_{congestion}<Q$, downlink congestion occurs. It is time to lower the inter-arrival rate to 0.25 pkt/sec.

6.5.3 Downlink Congestion Mitigation Algorithm

The proposed downlink congestion mitigation algorithm is described below. The algorithm consists of four algorithms, and algorithm 1, 2, 3 and 4 correspond to the CDU, DPU, CAU and RAU, respectively. The four units collaborate to mitigate the downlink congestion. Firstly, the CDU in algorithm 1 detects the current router queue length, compares it to the threshold zones and then writes the queue length information into the field of an ACK packet, which will be transmitted to the end devices. When the current queue length is lower than Q_{low} , the counter and queue length are written into an ACK packet, meaning that the inter-arrival rate will be increased four times. The DPU in algorithm 2 stores the downlink packet in the protection queue when the adaptation layer is notified by the MAC layer that the congestion is about to happen. In the meantime, the uplink packet is still allowed to be passed to the MAC layer. The CNU in algorithm 3 simply passes the queue length and the counter to the application layer. The RAU in algorithm 4 receives the queue length and counter to map these two values to the mapping table in Table 6-2. It can be seen from algorithm 4 that the inter-arrival rate is gradually increased four times with a low queue length threshold, which is in line with the algorithm 1 in the CDU. The other adjustments are performed by using the mapping table.

Algorithm 1: Congestion Detection Unit

```
Input: Queue length ($R_{current}$), $Q_{low}$, $Q_{medium}$, $Q_{high,}$ $Q_{superhigh}$, $Q_{congestion}$, counter
$Q_{low}$:= 5; $Q_{medium}$: = 10; $Q_{high}$:= 15; $Q_{superhigh}$: =20; $Q_{congestion}$: =25; counter: =0
If 0<$Q_{current}$<$Q_{low}$, Then
        If counter==0 Then
        counter++;    // Increase the packet inter-arrival time for the first time
        Write queue length $Q_{current}$ and counter=0 into an ACK packet;
        End
        If counter == 1, Then
        counter++;    // Increase the packet inter-arrival time for the second time
        Write queue length $Q_{current}$ and counter=1 into an ACK packet;
        End
        If counter==2, Then
         counter++;     //Increase the packet inter-arrival time for the third time
        Write queue length $Q_{current}$ and counter=2 into an ACK packet;
        End
        If counter ==3, Then
        Write queue length $Q_{current}$ and counter=3 into an ACK packet;
        counter: = 0; // Increase the packet inter-arrival time for the fourth time and count return to zero
        End
End
If $Q_{curren}$ >$Q_{medium}$ , Then
        Maintain the current packet inter-arrival rate
        Write queue length $Q_{current}$ into an ACK packet
If $Q_{curren}$ >$Q_{superhigh}$ , Then
       Start to lower the inter-arrival rate
       Notify the adapation layer to enqueue downlink packets in the protection queue;
       Write queue length $Q_{current}$ into an ACK packet;
If  $Q_{curren}$ > $Q_{congestion}$, Then
       Notify the adapation layer to enqueue downlink packets in the protection queue;
       Write queue length $Q_{current}$ into an ACK packet;
End
```

Algorithm 2: Congestion Protection Unit

```
If Receive congestion signaling from the MAC layer Then
  A downlink packet enters the protection queue;
  Send an uplink packet to the MAC layer;
Else
    If The protection queue is not empty&& receive notification the $Q_{curren}$ <$Q_{superhigh}$
    Obtain a downlink packet from the queue and send it to the MAC layer;
  Else
      Send a uplink packet to the MAC layer
End
```

Algorithm 3: Congestion Notification Unit

```
If receive an ACK packet from the router Then
  Obtain queue length $Q_{current}$ and the counter value;
  If $Q_{current}$ !=0 Then
   Send $Q_{current}$ and the counter value to the application layer;
  Else
      Do nothing;
  End
End
```

Algorithm 4: Rate Adjust Unit

```
Input: Queue length ($Q_{current}$), $R_{low}$, $R_{medium}$, $R_{high,}$ $R_{superhigh}$, $R_{congestion}$, counter, $R_{current}$
$Q_{low}$:= 5; $Q_{medium}$: = 10; $Q_{high}$:= 15; $Q_{superhigh}$: =20; $Q_{congestion}$: =25; counter: =0
Obtain $Q_{current}$ from an ACK packet and search the mapping table in Table 6-2
If 0< $Q_{current}$ < $Q_{low}$, Then
        If counter==0 Then
           $R_{current}$:= 0.27 pkt/sec; // start to increase the inter-arrival rate for the first time
        End
        If counter == 1, Then
           $R_{current}$ := 0.5 pkt/sec;// increase the inter-arrival rate for the second time
        End
        If counter==2, Then
            $R_{current}$ := 1 pkt/sec; // increase the inter-arrival time for the third time
         End
         If counter ==3, Then
            $R_{current}$ := 2 pkt/sec;  // increase the inter-arrival time for the fourth time
        End
End
If $Q_{low}$<$Q_{current}$<$Q_{edium}$  Then
         $R_{current}$ := 1.3 pkt/sec; //continue to increase the inter-arrival rate
End
If $Q_{edium}$<$Q_{current}$<$Q_{high,}$ Then
         $R_{current}$ := 2 pkt/sec;  // continue to increase the inter-arrival rate
End
If  $Q_{high}$<$Q_{current}$<$Q_{superhigh}$ Then
         $R_{current}$ := 1 pkt/sec; // start to decrease the inter-arrival rate
End
If  $Q_{superhigh}$<$Q_{current}$<$Q_{congestion}$ Then
         $R_{current}$ := 0.5 pkt/sec; // continue to decrease the inter-arrival rate
End
If  $Q_{current}$ >$Q_{congestion}$ Then
         $R_{current}$ := 0.25 pkt/sec;  // continue to decrease the inter-arrival rate
End
```

6.6 Performance Analysis of the Congestion Mitigation Algorithm

The performance of the proposed congestion mitigation algorithm is discussed in this section. A typical M2M networking is created, where two types of M2M traffic were used: smart metering and DSM. The simulation model uses 24 DSM nodes, while the remainders are meter nodes, as shown in Fig 6-20. It can be seen that there are eight clusters of end devices, each of which has eight nodes. In each cluster, three are the DSM nodes, while the other five nodes are the meter nodes. The smart meter traffic is unidirectional from a meter to the data sink, whereas the DSM traffic is bidirectional from the DSM nodes to the data sink and a reverse packet transmitted to the DSM for every received packet. To simulate this two-way communication, a static routing table was created in the router nodes. Each router records its child node IPv6 address and uses these addresses to dispatch the downlink traffic. Meter reading has a relatively low end-to-end delay requirement of 15 minutes, while the DSM delay is within 1s to 2s. To show the effectiveness of the proposed algorithm, two scenarios are compared. Scenario 1 did not use the congestion control algorithm, while scenario 2 used the congestion mitigation algorithm. The simulation ran for 600 seconds with multiple seed values, and the results are plotted with a 95% confidence interval. The key parameters of the simulation are presented in Table 6-3.

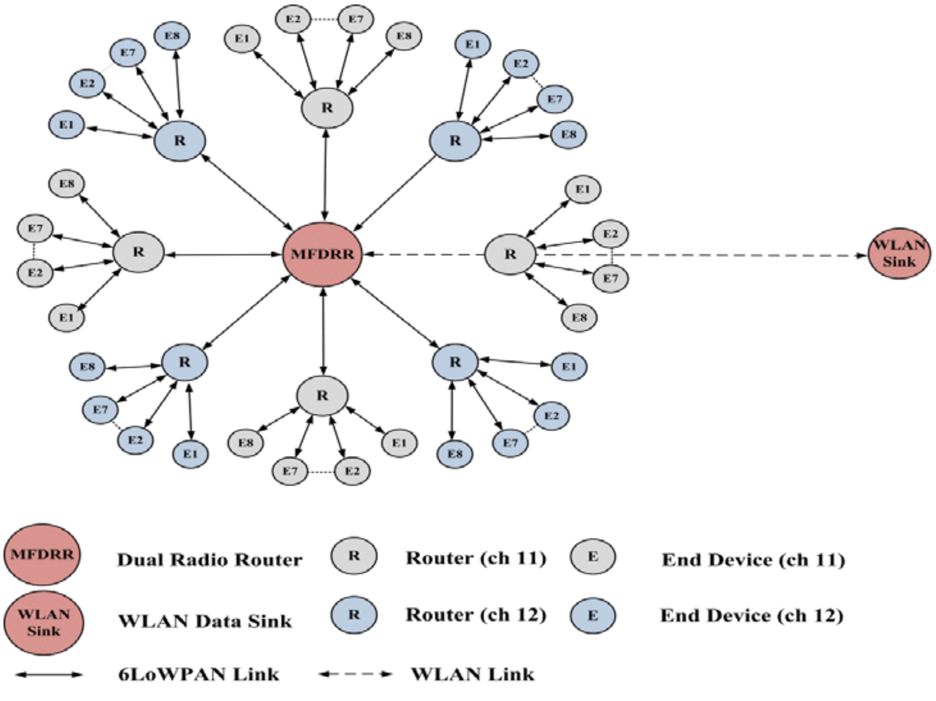


Fig 6-20 Two-way communications in the proposed heterogeneous network

Table 6-3 Key parameters for the proposed congestion mitigation algorithm

Group Name	Parameter		Value
Network	Hop		3
	Number of nodes		64
	Standard		6LoWPAN/IEEE 802.11g
	Operating Frequency		2.4 GHz
	6LoWPAN channel		12
	IEEE 802.11g channel		1
Propagation model	Free space path loss		
Dual Radio Router (Gateway)	6LoWPAN	BO	4
		SO	3
		Transmission Power	1.8 mW
	WLAN	Transmission Power	100 mW
		Packet Size	1200 bytes
		Aggregation Factor	15
		Safety margin	0.2 s
Router Queue Length(packet)	Q_{low}		5
	Q_{medium}		10
	$Q_{high,}$		15
	$Q_{superhigh}$		20
	$Q_{congestion}$		25
End device	Packet size		64 bytes
	Packet generation		Exponentially distributed
	Transmit Power		1 mw
	Packet inter-arrival rate		1, 1.2, 1.3, 1.5 and 2pkts/sec
Target Applications	DSM end-to-end delay		2s
	Meter Reading end-to-end delay		900s

The packet delivery rate reflects the network's performance. Fig 6-21 shows that the proposed congestion mitigation algorithm increased the packet success rate compared to the scenario with no congestion control. More precisely, the proposed algorithm improved the packet delivery rate by 6% from 78% (without the algorithm) to 84% (with the algorithm). In contrast, the meter reading traffic with the proposed algorithm showed a minor 3% improvement when the congestion control technique is used. The rationale behind these results is that the meter nodes had a relatively low generation interval time of 900s, so the total amount of meter reading data does not contribute much to the mixed traffic. As a result, the congestion mitigation algorithm had little impact on the meter reading traffic, but can effectively adjust the DSM traffic to reduce congestion in the routers. The DSM traffic was transmitted from the 6LoWPAN end devices to the data sink. On the reverse link, the data sink sends traffic to the sensor nodes. The downlink traffic adds to the uplink traffic so that most of the congestion was caused by the DSM traffic.

As the lifetime-based BB algorithm was used in the two-way communication, the packets were dropped due to lifetime expiration in the MFDRR to guarantee the QoS of the DSM and meter reading traffic. It can be observed in Fig 6-22 that the congestion mitigation algorithm reduced the number of packet losses by 46%, with the congestion control taking up 949 packets and the non-congestion control accounting for 1386 packets. Given that the DSM packet lifetime is 1s, packet lifetime is checked by the enhanced blank burst algorithm. Once the remaining lifetime exceeds the guard time (the remaining time is not long enough to reach the destination), the packet is dropped. In contrast to the DSM traffic, the meter reading traffic had no packet losses due to longer packet lifetime.

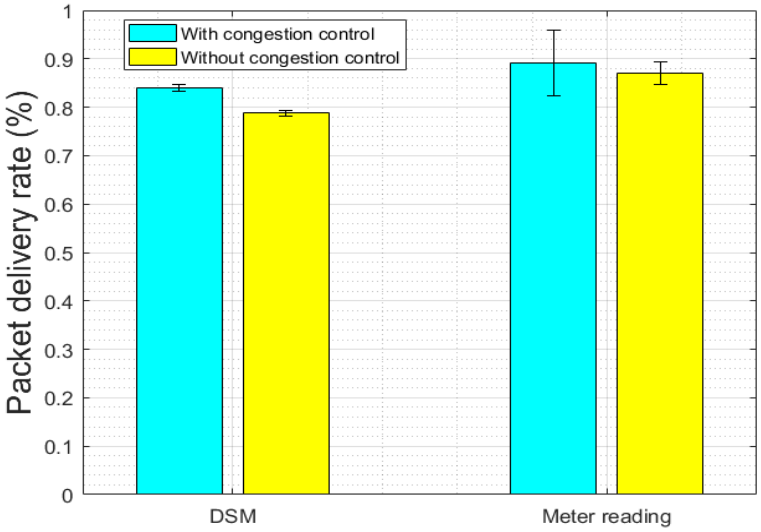


Fig 6-21 DSM and meter reading packet delivery rates with and without the congestion mitigation algorithm

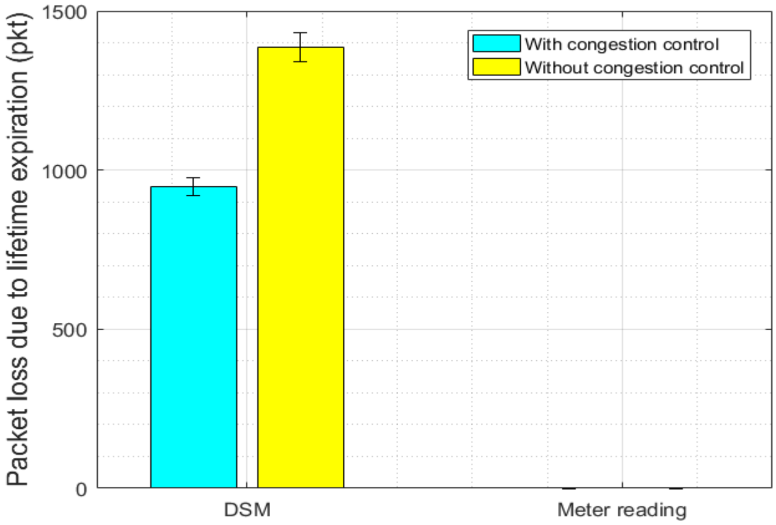


Fig 6-22 DSM and meter reading packet loss due to lifetime expiration

The impacts of the proposed algorithm on the uplink and downlink delays are presented in Fig 6-23. It can be seen that all packet delays do not exceed 1s as required by the QoS of the DSM and meter reading applications. Specifically, the uplink delays of the DSM traffic with and without the proposed algorithm did not have any differences, all being around 0.8s. In contrast, the downlink delay of the DSM traffic with the algorithm is reduced by 11% to 0.63s. It is evident that the downlink delay is lower than the uplink delay because the downlink delay did not include the aggregation delay. The congestion mitigation algorithm helps to decrease the number of packets building up in a router’s queue. With the uplink and downlink delays, it was easy to calculate the total delay of the DSM traffic, which is 1.42s, much lower than the 2s delay requirement. In addition to the DSM traffic, the meter reading traffic has the same trend in which the uplink delay of the high priority DSM traffic is 0.8s. When the improved BB algorithm is triggered by the DSM traffic, the meter reading traffic is also aggregated into the WLAN payload and transmitted to the data sink, if the BB period is long enough after the DSM transmission. It is clear that the new BB algorithm and the congestion mitigation algorithm jointly guaranteed the QoS of various types of M2M traffic. However, the proposed two algorithms are limited by their aggregation delays, which are the longest delay component of the end-to-end delay. If the aggregation delay could be reduced, the total end-to-end delay would be decreased as well.

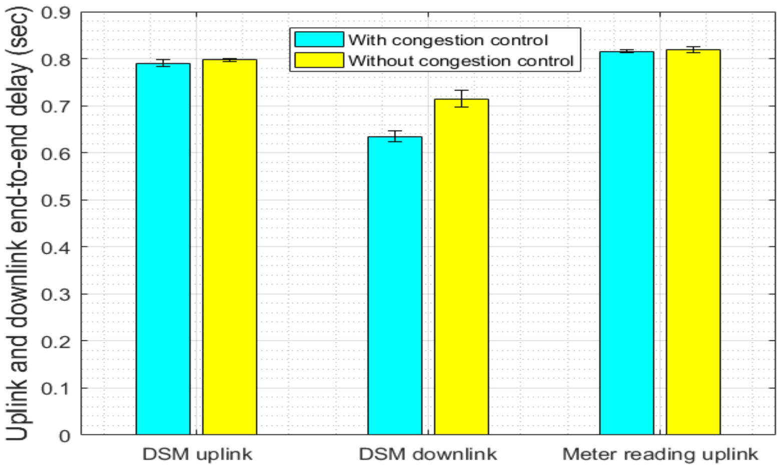


Fig 6-23 Uplink and downlink end-to-end delay for DSM and meter reading traffic

To examine the how the different packet inter-arrival rates are distributed, the CDF of the different inter-arrival rates are presented in Fig 6-24. It can be seen that 2 pkts/sec accounted for 86% of the total rates, meaning that the network runs at 2 pkts/sec for 86% of the time. In comparison with the network which had the traffic load of 2 pkts/sec, the proposed algorithm has shown improvements in the packet delivery rate and the end-to-end delay.

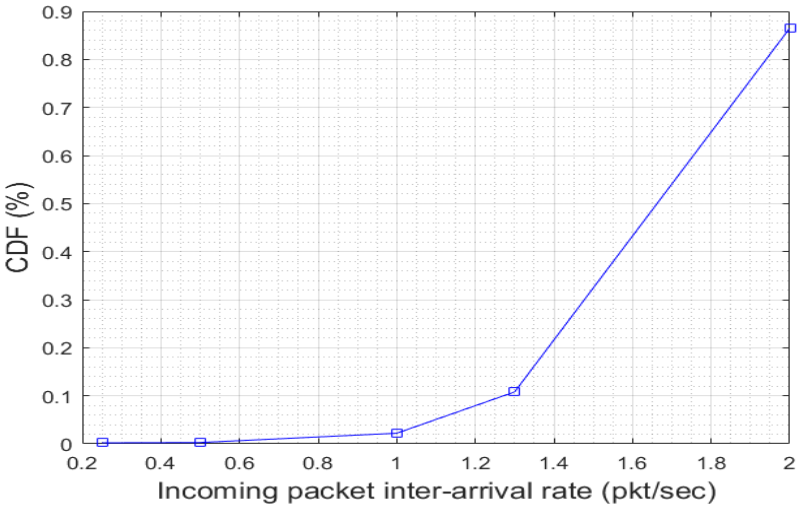


Fig 6-24 The DSM traffic inter-arrival rate CDF

6.7 Conclusion

In this chapter, the lifetime-based BB and congestion mitigation algorithms were proposed. By using the lifetime-based BB algorithm, the QoS of various M2M applications can be guaranteed. This is because any packet that has an expired lifetime is dropped in the MFDRR. A priority-based scheme was introduced to ensure that traffic with a higher priority could be transmitted first. The aggregation factor was used so that the number of aggregated packets in the WLAN payload was regulated. The remainder of the chapter discussed the two-way communications of two types of M2M applications: DSM and meter reading. The underlying problem is that the two-way communications can cause router traffic congestion that in turn could affect the DSM downlink end-to-end delay. To solve this problem, a congestion mitigation algorithm was proposed. The router queue length was employed as a metric to measure the level of congestion. The algorithm implemented in the router detects congestion as the queue length increases and then protects the downlink packet in the adaptation layer queue. In the meantime, the router sends a signal using ACK packets to inform the end devices to adjust their inter-arrival rates. The simulation results show the effectiveness of the two proposed algorithms.

Chapter 7
Modelling and Analysis of a Multi-MFDRR Scenario

7.1 Introduction

Chapter 6 has proposed a lifetime-based BB algorithm to mitigate the effects of the inter-network collisions and ensure the QoS of two types of M2M traffic. The algorithm significantly improved the QoS of the proposed heterogeneous area network in terms of the end-to-end delay and packet delivery rate. The algorithm attempts to mitigate the inter-network collisions between the 6LoWPAN network and the MFDRR interfaces, in which the WLAN packets collide with the 6LoWPAN packets. Chapter 6 proposed another algorithm to alleviate the downlink congestion in a two-way communication scenario for the DSM and meter reading traffic. These two algorithms tackled the uplink and downlink traffic problems. The M2M area networks presented in the previous chapters focused on a dense network scenario but with a medium transmission range. To support a large-scale M2M area network, a multi-MFDRR scenario is proposed to extend the coverage of the heterogeneous 6LoWPAN/WLAN area network, as shown in Fig 7-1. In this large-scale network, changing the operational channel from a busy to idle one may not be a feasible solution to mitigate inter-network collisions. The reasons are twofold. The first is that informing all of the devices in the network to switch the channel can incur huge communication overheads for those devices; the second issue is that sometimes it is difficult to locate a free channel due to the density of interfering devices. For example, a sports stadium deploys a ZigBee-based lighting control system, which can be easily affected by the audience using cell phones or laptops based on the IEEE 802.11 standard.

Without the loss of generality, the proposed scenario can be further replicated and formed into an even larger scenario (up to 1000 nodes) covering several km^2 and serving different types of M2M applications by spatially using the 6LoWPAN and WLAN channels. Given that the simulation results of Chapter 6 has shown that the MFDRR can adversely impact the 6LoWPAN network transmissions within the same area network, the proposed multi-MFDRR scenario is even more complicated than the single MFDRR scenario for several reasons. Firstly, an MFDRR easily create inter-network collisions for the 6LoWPAN nodes in a neighbourhood area network, as shown in the four collision zones in Fig 7-1. Therefore, the nodes in the collision zones tend to be impacted by inter-network collisions. Secondly, since four MFDRRs are involved in the scenarios, they need to contend the channel using the CSMA/CA protocol, thus resulting in longer end-to-end delays. These two assumptions will be tested and analysed using the staggered link design, the lifetime-based BB algorithm and downlink congestion mitigation algorithm. The main objective of this chapter is to evaluate the performances of these scheduling algorithms in a large-scale heterogeneous M2M area network. M2M communication networks should include heterogeneous types of low-power nodes, so the simulation results of this chapter pave the way for the deployment of the large-scale M2M communication networks in the future.

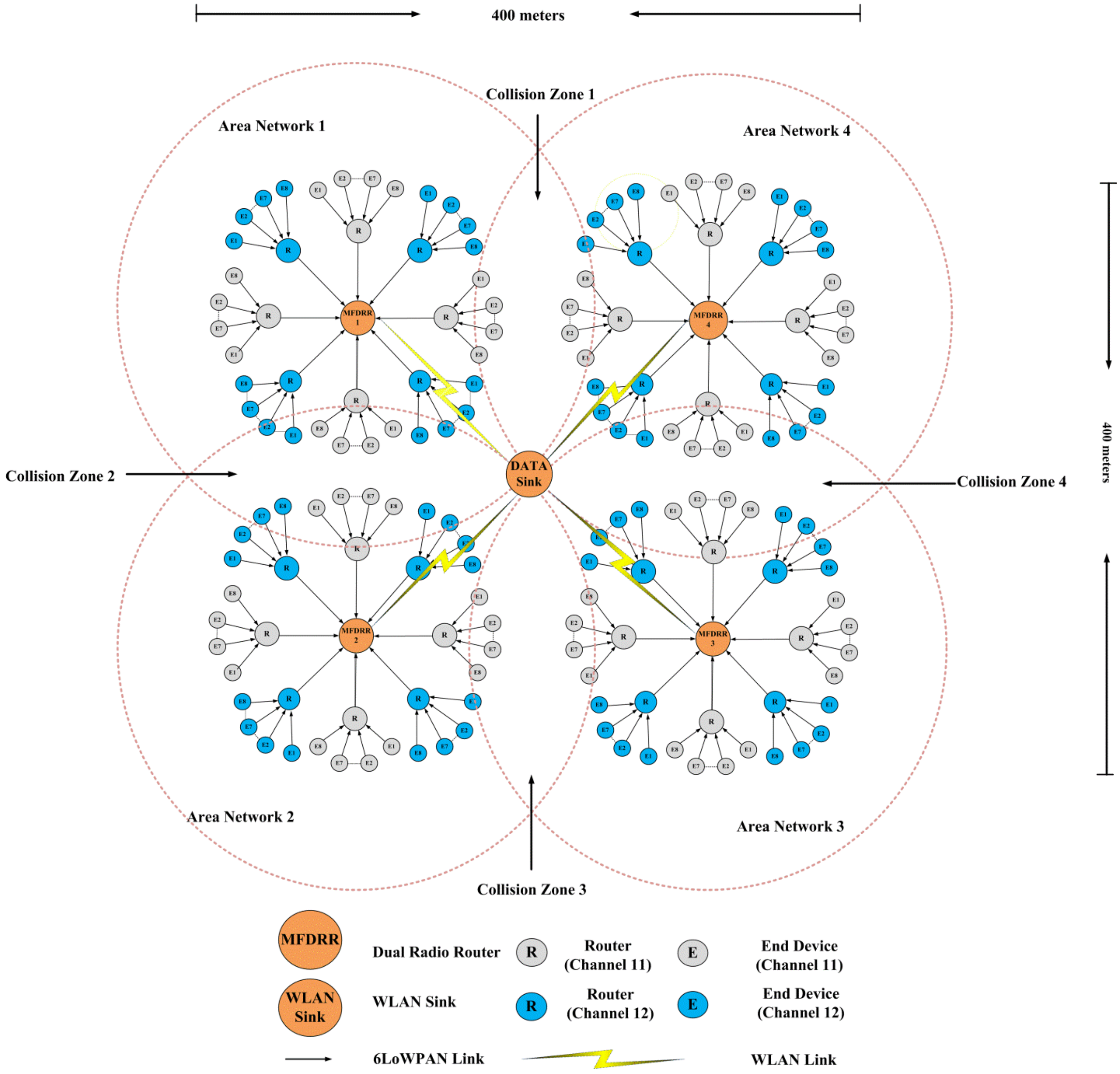


Fig 7-1 Large-scale heterogeneous M2M area network with four MFDRRs

7.2 Multi-MFDRR Simulation Model

Figure 7-1 presents a scenario comprised of four area networks, and each of the networks contains 64 6LoWPAN nodes, eight routers and an MFDRR, so there are totally 293 nodes (including the DATA sink) covering a 400×400 m^2 area. However, this large-scale area network can be extended to several km^2 by using the spatial reuse technique, so thousands of 6LoWPAN devices running various M2M applications can be incorporated in a large-scale geographical

M2M area network. The uplink data flow of the proposed network goes from the 6LoWPAN end devices to the DATA sink via the 6LoWPAN routers and the MFDRRs. The downlink data flow begins from the WLAN sink via the MFDRRs and the 6LoWPAN routers to the 6LoWPAN end devices. It is noted that the four MFDRRs creates four inter-network collision zones, as depicted in Fig 7-1. This implies one MFDRR not only affect its own area network, but affect its two neighbouring area networks. As the MFDRRs start to transmit, the level of the inter-network collision increases, so the performance of the network will be degraded. The algorithms proposed in the previous chapters successfully tackled the intra-and inter-network collisions in the single MFDRR scenario and the performances of these algorithms are evaluated in a large-scale M2M area network with four MFDRRs using the simulation model.

7.3 Performance Analysis of the Multi-MFDRR M2M Area Network

To evaluate the performance of the proposed network and test the feasibility of the proposed algorithms in a large-scale M2M area network, an OPNET simulation model was developed and used to gather simulation results in three stages. In the first stage, no scheduling algorithms were used to mitigate the inter-network collisions; that is, the WLAN transmissions adversely impact on 6LoWPAN devices. This stage is used to show the severity of the inter-network collisions, in which the network performance is degraded in terms of the packet delivery ratio, end-to-end delay and throughput, etc. Specifically, the number of the MFDRR is increased from one to four to show how the level of inter-network collisions varied. In the second stage, the number of the MFDRR is fixed to four, and the previously proposed algorithms were used and compared with the first stage results. In the third stage, the meter reading traffic and the DSM traffic are employed to evaluate the performances of the two-way communication links with the congestion mitigation algorithm. This stage shows the advantage of this heterogeneous network that can alleviation the downlink congestion. The simulation ran with multiple seed values for 200s, and all the results were plotted with a 95% confidence interval. The key simulation parameters are listed in Table 7-1

Table 7-1 Key simulation parameters

Group Name	Parameter		Value
Network	Hop count		3
	Number of nodes		293
	Standard		6LoWPAN and IEEE 802.11g
	Operating Frequency		2.4 GHz
	6LoWPAN channel		12
	IEEE 802.11g channels		1 and 6
Propagation model	Free space path loss		
Dual Radio Router (Gateway)	6LoWPAN	BO	4
		SO	3
		Transmit Power	1.8 mW
	WLAN	Transmit Power	100 mW
		Packet Size	1200 bytes
		Aggregation Factor	25
		Blank Burst algorithm safety margin (s)	0.2 s
Router	BO		4
	SO		2
	Transmit Power		1.8 mW
End device	Packet size		64 bytes
	Packet generation		Exponentially distributed
	Transmit Power		1 mW
	Packet inter-arrival rate		0.5, 1, 1.3, 1.5,1.7, 2 pkts/s
Target Applications QoS Requirements	Sensor end-to-end delay		0.6 s
	Meter Reading end-to-end delay		900 s
	DSM end-to-end delay		2 s

7.3.1 First Stage Simulation

In the first stage, the sensor traffic was employed to evaluate the uplink performance of the proposed heterogeneous M2M network. To evaluate the adverse effects of the inter-network collisions, 6LoWPAN channel 12 and WLAN channel 1 were used. As shown in Fig 5-1, WLAN channel 1, 6 and 13 almost overlap with the whole 2.4 GHz ZigBee transmission band, so it is almost impossible to use the channel-switching technique to avoid inter-network collisions, especially in such a large-scale M2M network. As such, 6LoWPAN channel 12 and WLAN channel 1 were used to evaluate the proposed algorithms. The simulated scenario could tackle inter-network collisions in such a worst case scenario as 6LoWPAN channel 12 overlaps with the central frequency of WLAN channel 1.

To show the severity of the inter-network collisions, extensive simulations were conducted to compare the packet delivery ratio four MFDRRs. It can be seen Fig 7-2 that as the number of MFDRRs increased, the packet delivery ratio dropped from 67% to 28% at the light load of 0.5 pkt/sec. Similarly, as the traffic loads increased, the packet delivery ratio of four MFDRRs steadily went down from 30% to 8%. It is clear from the simulation results that the adverse impacts of the inter-network collisions are detrimental to a large-scale M2M area network with many low-power sensor nodes.

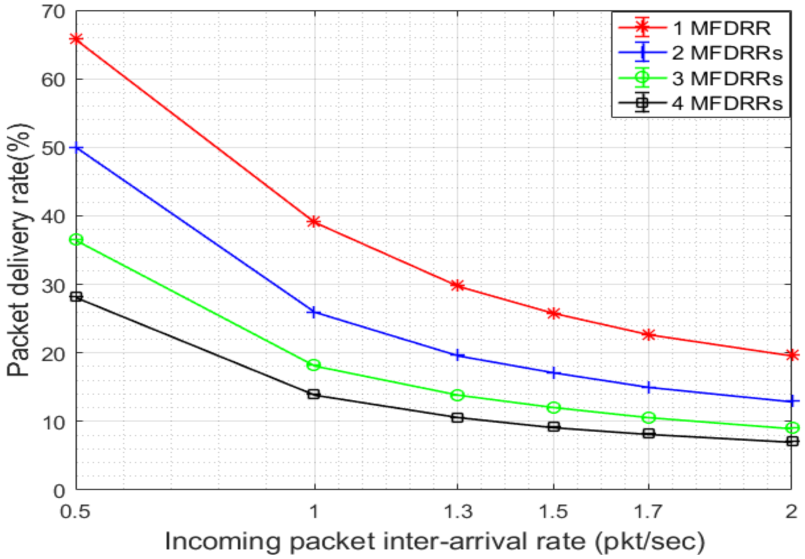


Fig 7-2 The packet delivery rate with different numbers of MFDRRs

Figure 7-3 presents the end-to-end delay of the simulated network. Similar to the packet delivery ratio, the end-to-end delay is susceptible to the inter-network collisions. It is observed that the delays for different numbers of the MFDRRs initially slowly rose to a range from 2s to 7s, then quickly jumped to 32s, 37s, 39s and 39s for 1, 2, 3 and 4 MFDRRs, respectively, as the traffic loads increased. The turning point is at the traffic load of 1 pkt/sec, from which the end-to-end delay values started to rise sharply. It is noted that the end-to-end delays is maintained at below 8s with low traffic loads between 0.5 pkt/sec and 1 pkt/sec. This is because the level of the inter-network collisions was not as high as the case where the load was over 1 pkt/sec. The fundamental reason for the large delay increase is because packets were held up in MAC queue due to the failed transmission attempts caused by the inter-network collisions. The more packets were built up in the queue, the longer the end-to-end delay. Similar to the packet delivery ratio, it is easy to understand that multiple MFDRRs with WLAN transmissions can be detrimental to the low power devices deployed in a large-scale M2M network. In this case, both the packet delivery rate and end-to-end delay are most important QoS metrics of the M2M traffic. The simulation results show that the increasing number of area networks with MFDRRs decreased the QoS values, so it is necessary to develop effective scheduling algorithms to minimize the effects of the inter-network collisions.

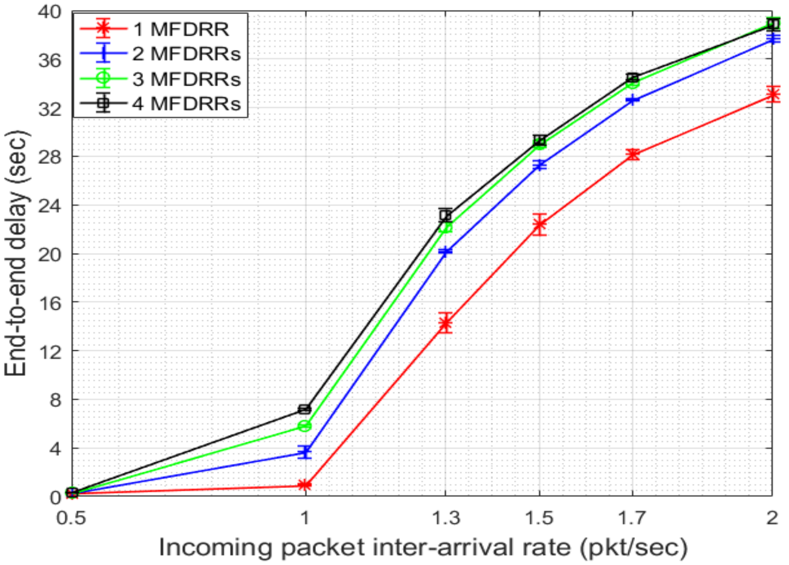


Fig 7-3 The end-to-end delay with different the number of MFDRRs

Figure 7-4 shows the combined network throughput of the MFDRRs in the presence of the inter-network collisions. It can be seen that the total throughput of the four MFDRRs stayed at 36 pkts/sec even with at the traffic loads of 2 pkts/sec (i.e., the total offered load 512 pkts/sec). In contrast, one MFDRR throughput remained at 24.5 pkts/sec at the offered load of 2 pkts/sec. Since the throughput was over 40 pkts/sec of one area network in Chapter 5 by using the proposed algorithm, both cases show a relatively low throughput due to inter-network collisions. It is noted that as the loads increased, the throughput would not increase but remained stable. This was because the increased load led to a higher level of packet collisions, which in turn reduced the throughput. Fig 7-5 depicts the number of packet losses due to the inter-network collisions. It can be seen that the number of packet losses quickly increased from 0 to 8200 packets as the loads increased from 0.5 to 1 pkt/sec, and then steadily increased to 12000 packets with four MFDRRs operating at the same time. It is clear from the results that as the number of MFDRRs was increased, the packet losses increased. It is noted that the WLAN transmissions adversely affected the packet delivery ratio of the 6LoWPAN devices, which sharply dropped from 68% to 20%. If more MFDRRs are used in such M2M area networks, it will be difficult to support a large number of M2M applications

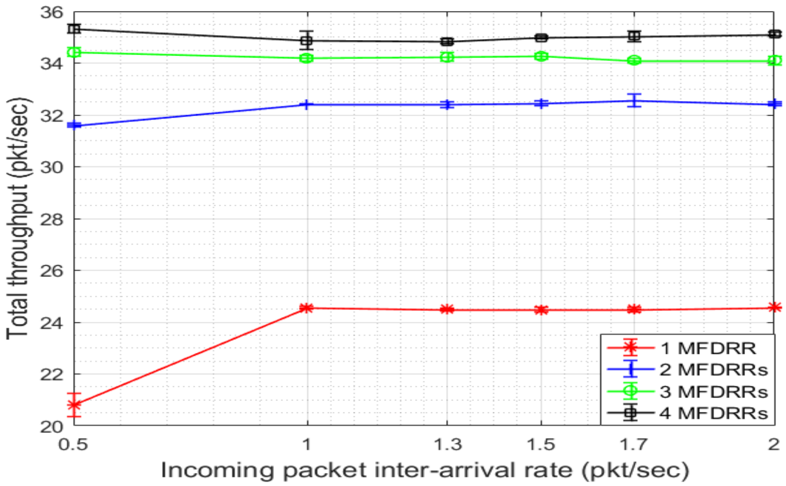


Fig 7-4 Total throughput with different number of MFDRRs

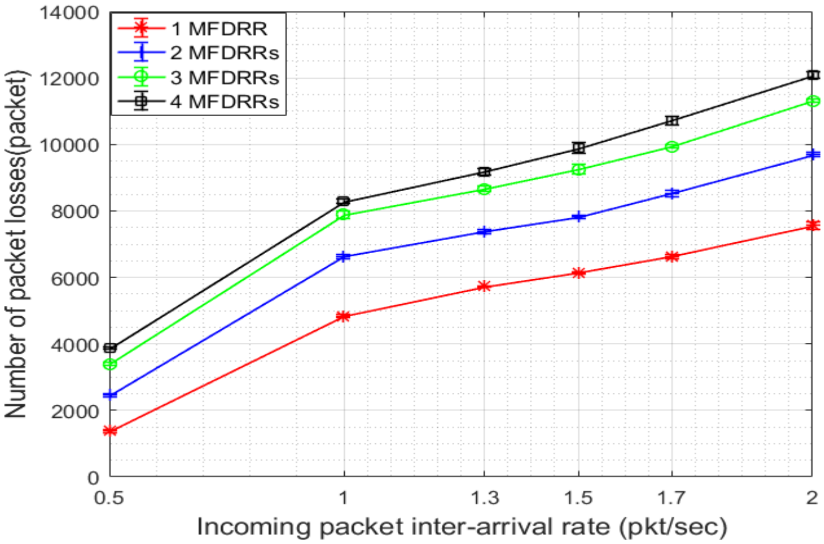


Fig 7-5 Packet loss with different MFDRRs

Figure 7-6 presents the number of collisions for different number of MFDRRs. It follows the same pattern as the previous figures, meaning that the inter-network collisions are detrimental to the M2M data devices. The number of packet collisions almost linearly increased with the increased traffic loads, so it is necessary to use the traffic scheduling algorithms to deal with the interference. Similarly, Fig 7-7 shows that WLAN retransmissions in the presence of the inter-network collisions. This figure followed the same pattern as Fig 7-4. When the throughput reached to the plateau, the number of WLAN packets sent by MFDRRs also remained the same. It can be seen that the more MFDRRs are involved, the more WLAN packets are retransmitted. To reduce the level of the inter-network collisions, the number of the WLAN packet transmission needs to be decreased. The aggregation factor-based BB algorithm was designed based on this principle.

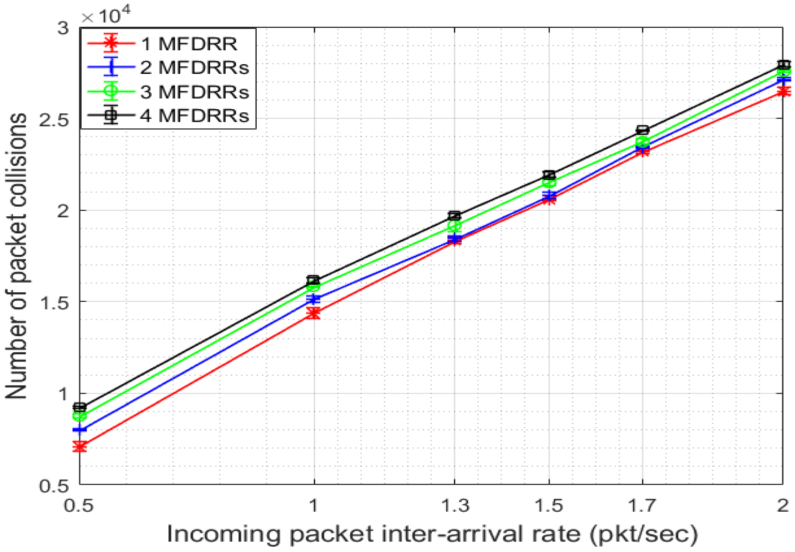


Fig 7-6 Total number of collisions for different number of MFDRRs

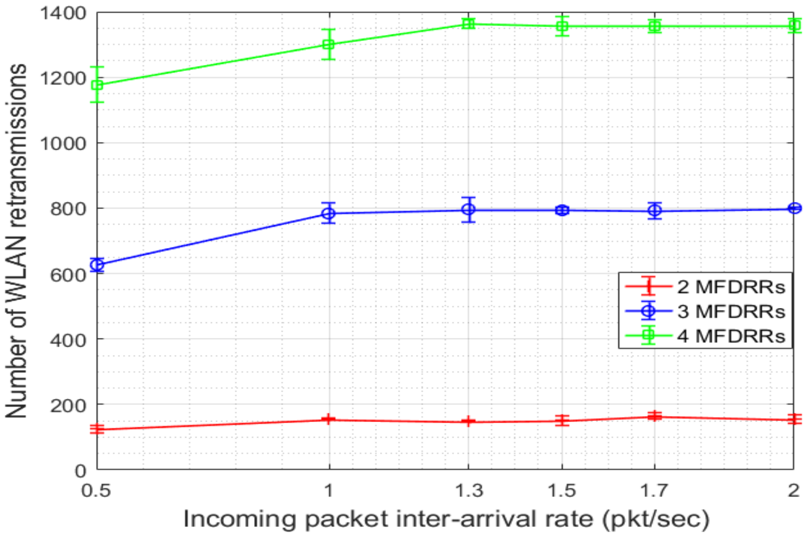


Fig 7-7 The retransmissions of the WLAN transceivers

7.3.2 Second Stage Simulation

Previous simulation results showed that multiple WLAN transmissions can degrade the QoS of a large-scale M2M network. In this section, the effectiveness of the scheduling algorithms will be measured. In this four-MFDRR scenario, four scenarios are considered. This first scenario does not adopt the proposed algorithms, so all the 6LoWPAN devices are subject to the inter-network collisions. The second scenario uses the algorithm proposed in [9], which is an adaptive packet aggregation algorithm (referred as the adaptive aggregation algorithm). This adaptive algorithm aggregates 6LoWPAN packets into a WLAN packet to reduce the number of the transmitted packets, thus alleviating the impacts of the inter-network collision. The third scenario uses the aggregation factor-based algorithm proposed in Chapter 5, and the fourth scenario employs the lifetime-based BB algorithm proposed in Chapter 6.

Fig 7-8 shows packet delivery ratios for the above three algorithms used in the four-MFDRR network. It can be seen that the scheduling algorithms significantly improved the performances of the area network compared to the scenario one where no scheduling algorithm was used. Specifically, it can be seen that the packet delivery ratio in the first scenario declined from 28% to 8%. In contrast, when the BB algorithms were used, the packet delivery ratio decreased from 97% from to 68% as the traffic loads increasing. In particular, the algorithm proposed in [9] had a slightly 20% lower packet delivery ratio than those of the aggregation-factor and lifetime-based BB algorithms. The reason is that the adaptive aggregation algorithm simply aggregated several 6LoWPAN packets without providing any guard time like the two BB algorithms. As a result, as the loads increased, the WLAN packets more severely affected the 6LoWPAN network, thus resulting in a higher number of packet losses. In contrast, the aggregation-factor and lifetime-based algorithms not only used the aggregation technique to reduce the number of packets, but also used a short BB period to protect the 6LoWPAN nodes from being adversely affected by the WLAN transmissions. It is noted that the lifetime-based algorithm had a slightly higher packet delivery ratio than the aggregation-factor based BB algorithm at the high traffic loads higher than 1.3 pkts/sec. This simulation results confirms the effectiveness of the proposed BB algorithms in terms of mitigating the inter-network collisions and maintaining the QoS requirements of the M2M applications.

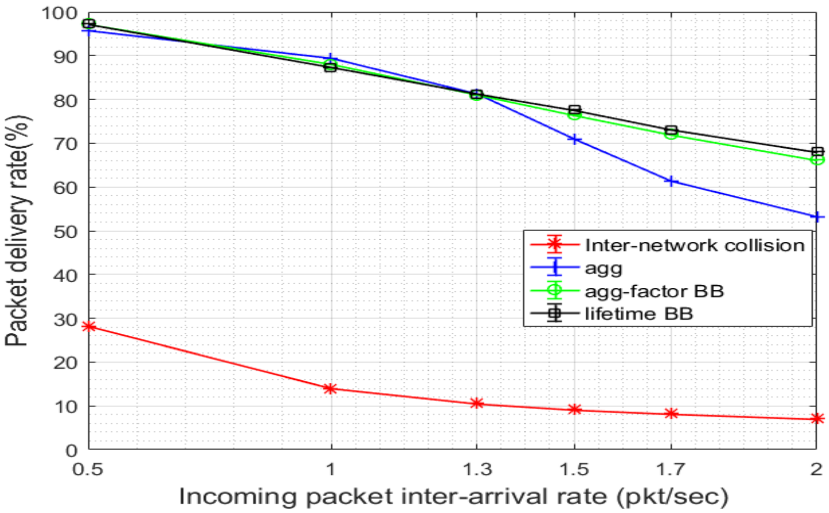


Fig 7-8 The packet delivery rates of four MFDRRs with the proposed algorithms

Figure 7-9 shows the end-to-end delay of four MFDRRs using the proposed algorithms. To show more detailed performance of for the adaptive algorithm, the aggregation factor-based BB algorithm and the lifetime-based BB algorithm are presented in a magnified form in Fig 7-10. It can be seen in Fig 7-9 that the end-to-end delay of the case without any proposed algorithms slowly rose to 7s and then climbed to 36s. By contrast, the other three algorithms maintained relatively low delays, with only the adaptive aggregation algorithm rising to 7.8s at high traffic loads of 1.5 pkts/sec. The reason behind this was the same with the rising end-to-end delay as discussed in Chapter 5. Due to the inter-network collisions, the router's MAC queuing delay increased as shown in Fig 7-12, which was the major delay component for the end-to-end delay. Fig 7-10 presents the end-to-end delays for the adaptive aggregation algorithm, aggregation-factor-based BB and lifetime-based BB algorithms. It is observed that the adaptive aggregation algorithm delay increased as the loads increased beyond 1.5 pkts/sec. The reason is that this algorithm does not have the guard time to protect the 6LoWPAN transmissions, and thus the WLAN interfaces can cause a longer router queuing delay, as shown in Fig 7-12. In contrast, the end-to-end delays of the aggregation factor-based and lifetime-based algorithms maintained at 0.8s, which proved the effectiveness of the proposed algorithms.

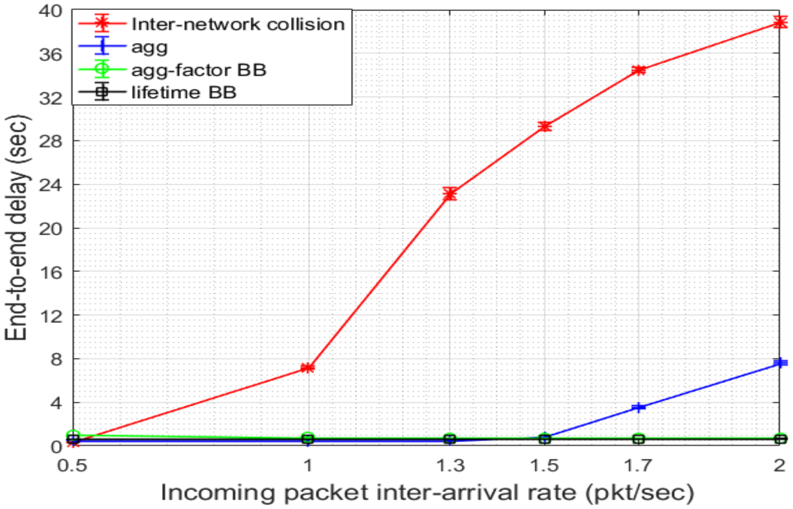


Fig 7-9 End-to-end delay with four MFDRRs

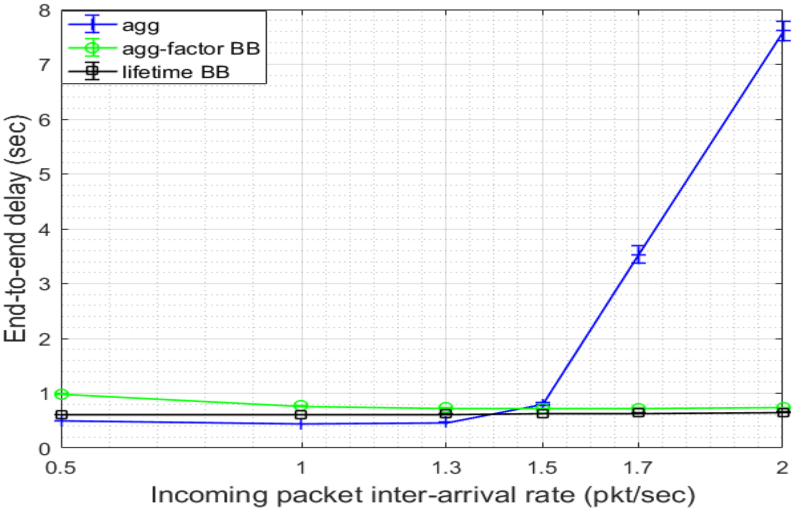


Fig 7-10 Magnified end-to-end delay

Figure 7-11 and Figure 7-12 show the end device queuing delay and router queuing delay. It can be seen from Fig 7-11 that the inter-network collisions negatively impacted on the end devices. This is because the staggered link design schedules the WLAN transmissions within a superframe in which the end devices and routers can communicate. Despite using the BB algorithm, end devices were still subject to the inter-network collisions, so the figure showed the slightly higher delays than those of the scenario with no algorithms involved and the adaptive aggregation scenario. As discussed before, only routers were affected in these two scenarios, as shown in Fig 7-12. It is noted that the adaptive aggregation algorithm had no blank burst period to protect the 6LoWPAN devices, so the routers experienced rising delays. On the other hand, the proposed BB algorithms showed a clear advantage of the end-to-end delay and maintained low delay values regardless of the increased traffic loads. Another reason for such low delays is that the Blank Burst period protected the 6LoWPAN transmissions, so the packets were not subject to the inter-network collisions. Therefore, the proposed two algorithms had lower queuing delays.

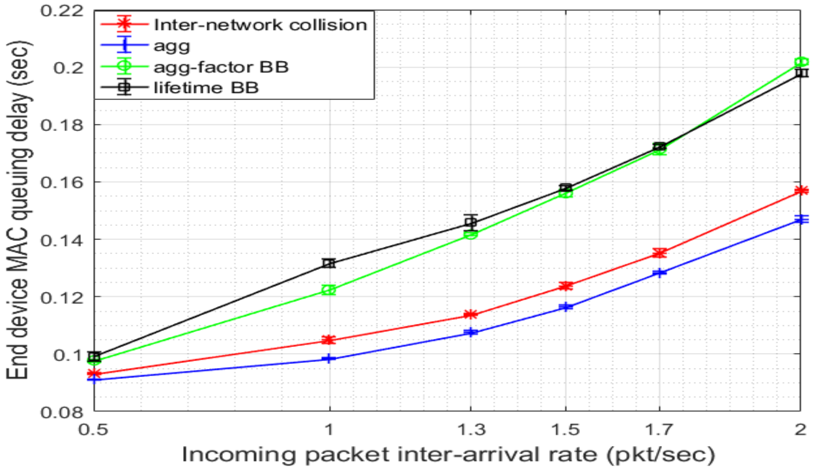


Fig 7-11 End device MAC queuing delay

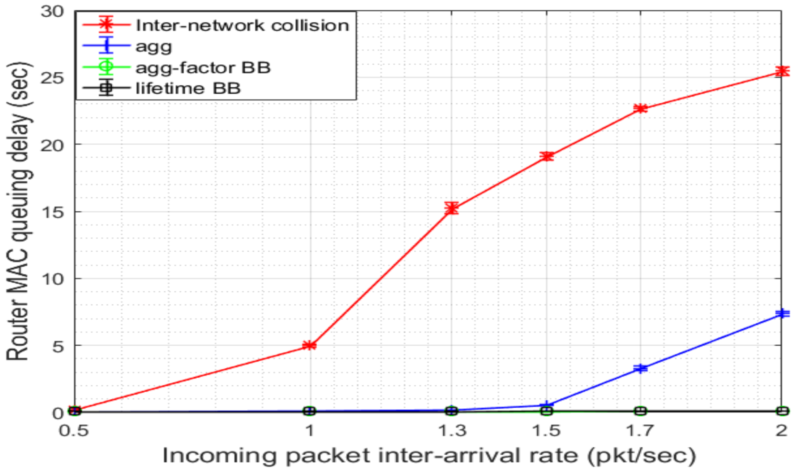


Fig 7-12 Router MAC queuing delay

Figure 7-13 shows the total throughput of the four MFDRRs. It is obvious that the throughput of scenario one without the proposed algorithms stays as low as 35 pkts/sec due to the adverse impact of the inter-network collisions. In contrast, the other three cases the network witnessed a increased throughput up to 350 pkts/sec. The reason was because the packet aggregation technique significantly reduced the number of the WLAN packets transmitted from the MFDRRs, thus minimizing the negative impacts of the inter-network collisions. In addition to the packet aggregation technique, the aggregation factor-based and lifetime-based algorithms used the BB techniques to avoid direct collisions with the WLAN packets. However, the adaptive aggregation algorithm does not use this BB period, resulting in the degradation of the QoS due to the inter-network collisions. This can be reflected in Fig 7-14, where the adaptive aggregation algorithm shows more packet losses than the aggregation factor-based and lifetime-based BB algorithms.

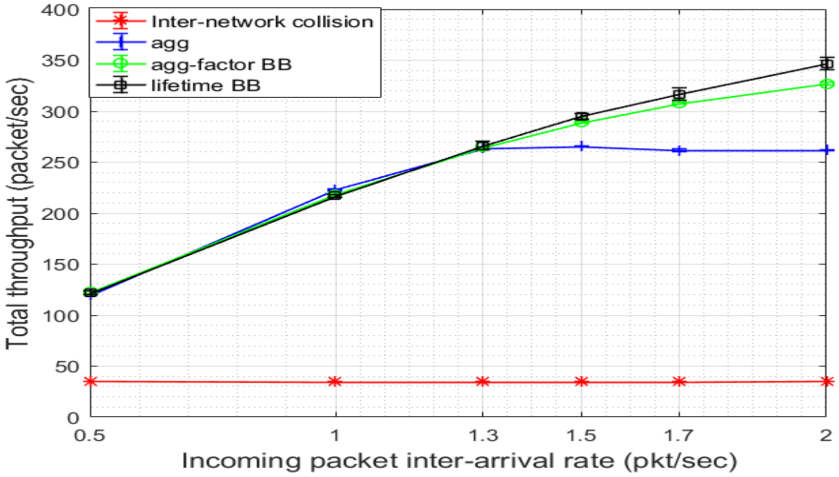


Fig 7-13 Total MFDRRs' throughput

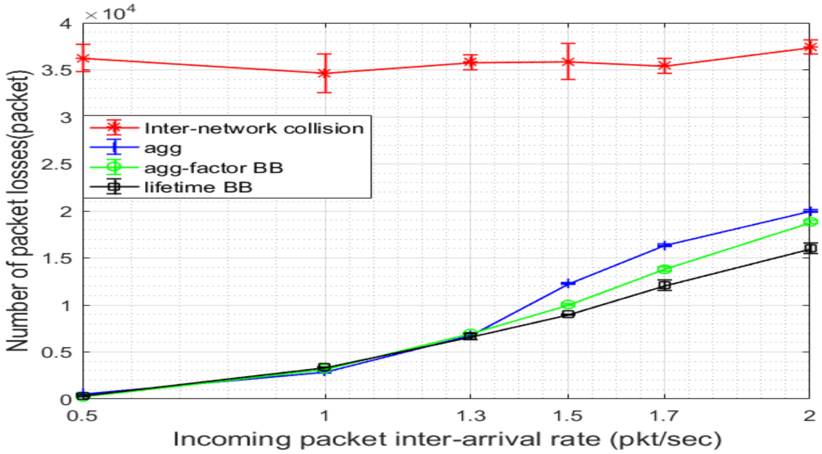


Fig 7-14 Total packet losses

7.3.3 Third Stage Simulation

Given that the lifetime-based blank burst algorithm has proved to be an effective algorithm, the third stage simulation mainly focuses on applying the lifetime-based blank burst algorithm and the congestion mitigation algorithm to a bidirectional large-scale heterogeneous area network. The DSM traffic and meter reading traffic were used in this simulation. In particular, three out of eight nodes were denoted as the DSM nodes, and the rest of the five nodes were used as meter reading nodes. The simulation included two scenarios: scenario 1 without the congestion mitigation algorithm and scenario 2 with the congestion mitigation BB algorithm. The DSM traffic used a traffic load of 2 pkts/sec and the meter reading traffic used a traffic load of 0.001 pkt/s (Inter-arrival time 900s). The proposed lifetime-based BB algorithm was used for both the scenarios to mitigate inter-network collisions. The simulation ran for 200s with multiple seed values, and the results were plotted with a 95% confidence interval. It was assumed there was no hidden node problem in the system.

Figure 7-15 shows that the packet delivery ratio of scenario 2 was higher than that of scenario 1 for uplink and downlink DSM traffic, and meter reading data. Specifically, the downlink DSM packet delivery ratio was increased by 10%; the uplink DSM packet delivery ratio was increased by 8%; and the meter reading packet delivery ratio was increased by 2%. More precisely, as for the DSM downlink delivery rate, the congestion control algorithm increased by 10%. As for the DSM uplink delivery rate, the packet delivery rate was increased by 8%; as for the meter reading traffic, the packet delivery rate only increased 2%. It is also noted that the DSM downlink packet delivery rate was slightly lower (77%) than the DSM uplink one (80%). Note that the uplink packet delivery rates for both the scenarios are slightly higher than those of the downlink for both the scenarios. This is because the downlink traffic experienced more packet losses than the uplink due to the intra-network collisions. It is also noted that the packet delivery rate of the meter reading traffic did not change much as the meter reading traffic inter-arrival time was low.

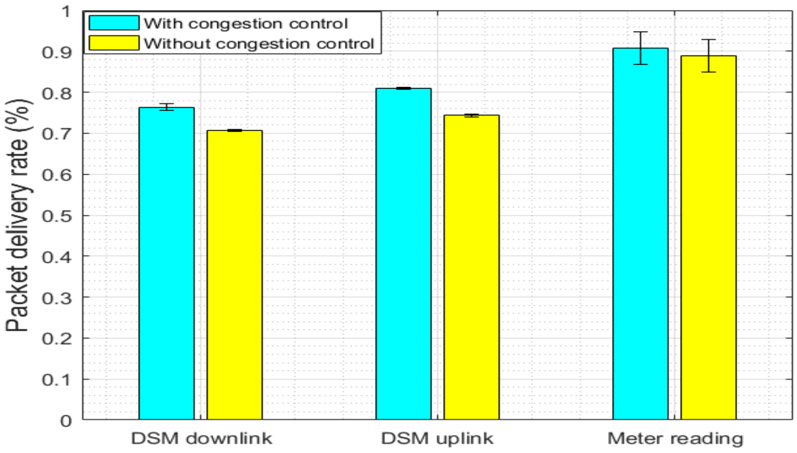


Fig 7-15 DSM and meter reading uplink and downlink packet delivery rate.

Accordingly, Fig 7-16 illustrates the DSM uplink and downlink end-to-end delays and the meter reading end-to-end delay. It is evident that the congestion mitigation algorithm did not improve the DSM uplink delay, and both the delays levelled at 0.78s. The reasons are twofold. Firstly, the congestion mitigation algorithm only enters the downlink DSM traffic into the protection queue, and still allows the uplink DSM traffic to be forwarded. Secondly, the uplink traffic end-to-end delay is strictly controlled by the lifetime-based BB algorithm. If the remainder lifetime of a packet in the MFDRR is less than the guard time (0.2s); the BB algorithm is triggered to ensure the end-to-end delay requirement, regardless of whether congestion occurs or not. In contrast, it can be seen that the downlink DSM end-to-end delay was reduced by 20% from 0.68s to 0.54s, which proved the effectiveness of the congestion mitigation algorithm. It is also noted that the DSM downlink end-to-end delays are lower than those of the DSM uplink for both scenarios. This is because the downlink DSM end-to-end delay did not have the aggregation delay. As for the meter reading traffic, the uplink end-to-end delay was slightly reduced from 0.9 s to 0.86s. This could be attributed to the fact that the congestion mitigation traffic reduced the queuing delay for the meter reading traffic.

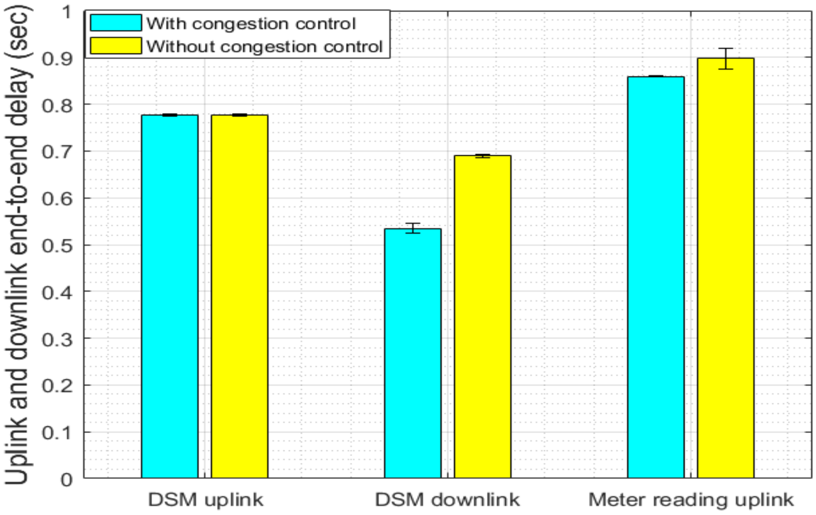


Fig 7-16 DSM and meter reading uplink and downlink end-to-end delay

Figure 7-17 shows the number of packet losses for the DSM and meter reading data in both scenarios. It can be seen that the number of packet losses was reduced by 30% from 900 to 600 packets. This is because the congestion mitigation algorithm effectively reduced the level of contention in the router, thus resulting lower queuing delays and fewer dropped packets in the MFDRRs. In contrast, the meter reading traffic had zero packet losses compared to the DSM traffic. The rational is that the meter reading traffic loads were low, resulting in lower queuing delays in the router.

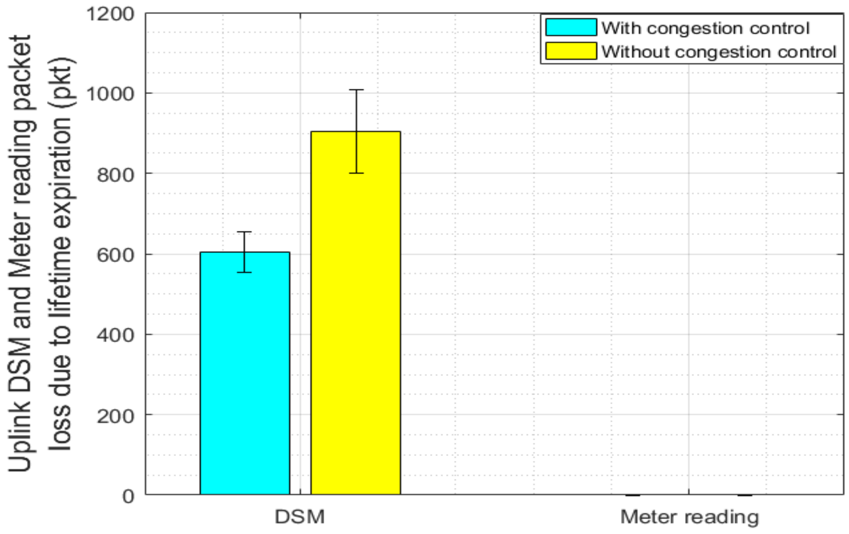


Fig 7-17 DSM and Meter reading uplink packet loss

The CDF of the DSM inter-arrival rate is presented in Fig 7-18. It can be seen that the network performed at 2 pkts/sec for 74% of the simulation time. The congestion mitigation algorithm adapted a lower inter-arrival rate to achieve better QoS performances, and only 26 % of the simulation time was used to perform at a higher packet inter-arrival rate. This also validates the effectiveness of the proposed downlink congestion mitigation algorithm.

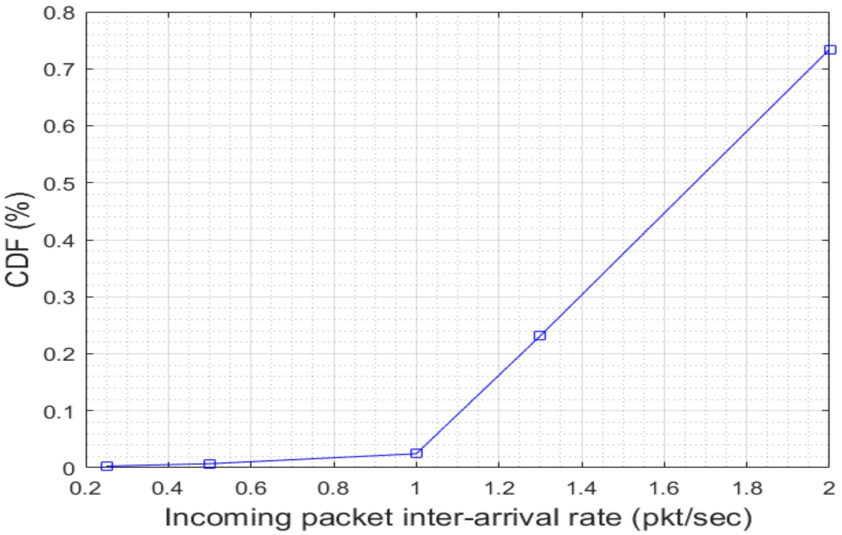


Fig 7-18 Packet Inter-arrival rate CDF

7.4 Conclusion

In this chapter, a large-scale M2M network was presented for three M2M applications such as the sensor traffic, meter reading traffic and DSM traffic. Firstly, the severity of the inter-network collision in a large-scale area network was presented. Then the proposed scheduling algorithms were used to show the significant gains in terms of the packet delivery rate, end-to-end delay and number of packet collisions. In particular, the lifetime-based BB algorithm greatly reduced the number of inter-network collisions and prevented the network from being adversely affected by the inter-network collisions generated not only by its own MFDRR but also its neighboring MFDRRs. The algorithm also guaranteed the QoS of the sensor and DSM traffic by dropping the packets with expired lifetimes. Finally, the congestion mitigation algorithm was adopted to evaluate the performances of the two-way communications in the large-scale area network. The simulation results showed that the algorithm greatly reduced downlink congestion and ensured the QoS of the DSM traffic. It also proved that the scheduling algorithms can be effective in a even larger geographical area network with the spatial reuse technique.

Chapter 8
Conclusions

8.1 Summary

M2M communications is the basis and cornerstone of the IoT system. One of the significant blocks of an IoT communication network is the short-range wireless networks responsible for collecting and relaying information to the data sinks. However, many challenges need to be investigated and solved before the large-scale deployment of these short-range wireless networks. Many M2M applications are supported by short-range wireless networks. For example, sensors periodically monitor actuators and transmit information to data centers for applications such as home security and load balancing. Smart meters use two-way communications between the consumers and the utilities to monitor power consumption and inform the consumers of the electricity usage. DSM traffic is sent from a utility server to control and balance the total energy consumption during peak hours. The success of these M2M applications depends on the reliable and timely data delivery, so thorny problems, such as IP connectivity, scalability, interference management and meeting QoS requirements for M2M applications need to be carefully designed. In this study, several scheduling algorithms were proposed to improve the performances of short-range wireless area networks to satisfy different QoS requirements in a reliable and timely manner.

To enable end-to-end IP connectivity from area networks to an IoT data sink, a 6LoWPAN network was considered and developed in Chapter 3. As the IPv6 protocol supports has a large number of address spaces to support end-to-end connectivity, the 6LoWPAN standard was adopted to develop a 6LoWPAN model including stateless address auto-configuration and the IPv6 header compression algorithm using the built-in OPNET library. Each device is equipped with an IPv6 address to communicate to the data sink to achieve IP end-to-end connectivity. The massive IPv6 deployment of M2M devices will be a norm in near future, so exploring its feasibility using the simulation platform appear to be a cost-effective way to study the underlying problems, which could be solved by newly developed protocols and algorithms.

To mitigate intra-network collisions, a staggered link design and a packet aggregation technique were proposed in Chapter 4. All the incoming and outgoing superframes are carefully scheduled so that unnecessary packet collisions such as beacon-to-beacon and beacon-to-data collisions can be avoided. The total number of the transmitted packets is reduced by aggregating 6LoWPAN payloads, so data-to-data collisions can be alleviated. To increase the packet delivery ratio and reduce the end-to-end delay in a multi-hop area network covering a large-scale area, a heterogeneous area network comprised of the 6LoWPAN and WLAN standards was proposed. The WLAN standard uses a much higher data rate to deal with high volume of accumulated traffic and a longer transmit range to reduce the number of multi-hop links. The standard also supports a longer transmission range links and allows greater flexibilities in the area network design compared to the 6LoWPAN. The results showed that the packet delivery ratio was improved over 60%, and the end-to-end delay was decreased by 39% with the proposed design and technique. The proposed design and algorithms can also be applied to other heterogeneous networks design using such as Bluetooth and WLANs, or WLANs and WiMAX standards.

A new dual-radio node named MFDRR was introduced in chapter 5 to support a collision free dense heterogeneous area network. However, due to the share of the ISM band by both the 6LoWPAN and WLAN interfaces in the heterogeneous network, inter-network collisions can occur. To solve this problem, the BB algorithm was proposed to suspend the 6LoWPAN transmissions while the WLAN link is active. The BB signal is piggybacked by a beacon and relayed to the end devices without incurring extra overhead. An aggregation technique is employed to adjust the number of the 6LoWPAN packets wrapped into a WLAN payload. The results show that the throughput was increased by 100% and the packet delivery ratio was improved by 95%. Unlike many studies that mitigate inter-network collisions from the physical layer, the BB algorithm’s significance is that it reduces the number of inter-network collisions from the MAC layer and application layer, which is a cross-layer approach and can easily be reproduced in other M2M networks without hardware modification.

To improve the QoS of different M2M applications, a lifetime-based BB algorithm was presented in Chapter 6. The main improvement compared to the previous algorithm is that the end-to-end delay for two M2M applications (sensor and meter reading) can be guaranteed. The shortest lifetime value in the system is employed to trigger the BB algorithm, rather than the aggregation factor. Different priorities are also assigned to each traffic type to ensure the QoS. The DSM traffic was used to evaluate the performance of two-way communications. It was revealed that the bidirectional traffic can cause downlink congestion in the proposed area network, so a congestion mitigation algorithm was proposed. The algorithm detects congestion by using the router's queue length. If the congestion occurs, the downlink packets are protected in the router's adaptation layer. The ACK packets are used to notify the end devices to adjust the packet inter-arrival rate. The results show that the packets with expired lifetimes were dropped to guarantee the QoS requirements of the sensor traffic while mitigating inter-network collisions; the congestion mitigation algorithm increased the packet delivery ratio by 7%, reduced the downlink end-to-end delay of the DSM traffic by 11% and decreased the number of packet losses by 46%.

To evaluate performances of the proposed scheduling algorithms in a large-scale area network and to bring the effectiveness of these algorithms to a broader large-scale M2M area network with four MFDRRs was proposed in Chapter 7. The 6LoWPAN end devices are not only subject to the inter-network collisions from the MFDRR in the local network, but are also affected by the inter-network collisions from the other MFDRRs in the vicinity. Three-stage simulations were conducted to firstly present the severity of the inter-network collisions in a large-scale dense area network, then proved the effectiveness of the proposed scheduling algorithms to mitigate the inter-network collisions while maintaining the QoS, and lastly reduced the downlink congestion in bidirectional traffic. The simulation results validated our hypothesis that all these scheduling algorithms can enhance the performance of a large-scale heterogeneous area network.

8.2 Potential Future Research

The deployment of heterogeneous wireless networks for IoT and M2M applications is expected to grow and serve the diverse QoS needs of different services. This study has researched such needs and proposed several new algorithms to improve the performances of the heterogeneous area network comprised of a 6LoWPAN network and an IEEE 802.11g network. Both the unlicensed and licensed heterogeneous networks will be deployed in different forms under the 5G network umbrella. To extend the current study, new algorithms need to be proposed to support diverse ranges of traffic, especially the time-constrained high priority traffic such as the sensor or actuator traffic. The proposed algorithms in this study to support bi-directional traffic need to be extended to guarantee the QoS of the time-sensitive applications on the downlink. Specifically, an alternative to avoid the downlink traffic congestion is to use a multipath routing technique to bypass the congested links, thus ensuring the timely downlink traffic delivery. The proposed BB algorithms can be modified to be adaptive to improve the QoS by using the traffic variability and diversity of IoT applications.

Another potential research area is to investigate the deployment of the cognitive wireless sensor network architecture in order to avoid the inter-network collisions. The current and emerging short-range wireless networks can support multiple channels, which can be spatially distributed either by sensing network conditions or by scheduling channels to mitigate the inter-network collisions in a dense network environment. As shown in Chapter 7, the number of packet losses significantly increased due to the inter-network collisions caused by the multi-MFDRR dense area network. Therefore, two-tiered scheduling algorithms can be developed and deployed, so the higher-power transmitters in the heterogeneous network do not frequently interfere with the low-power networks. This is also an important area to investigate, particularly when researchers are focusing on the development of LPWANs.

Finally, this study would suggest another new potential research area: developing the pseudo-heterogeneous network architecture with the IEEE 802.11ah standard. Recently emerged IEEE 802.11ah standard has many attractive features. Specifically, the standard can operate as a low data rate network or a high data rate network, in which the data rate can vary from 300 kbits/sec to 78 Mbits/sec; the standard can support the transmission range up to 1 km. Future research should focus on developing area and access IoT networks with the single standard operating in different modes in different segments of a LPWAN. The adaptive features of the new 802.11ah standard can be examined to develop the LPWAN architecture, thus offering similar advantages as presented by the proposed heterogeneous area network. Future research should also focus on the development of the energy-efficient packet scheduling algorithms for LPWAN applications, so the batteries of the field-deployed sensors would not require frequent replacement.

Appendix A

Interfacing with the Higher and Lower Layer of the IP Layer in OPNET

This section presents the basic approaches to connecting the adaptation layer to the IP layer from below and connecting a custom application layer to the IP layer from above. In the two processes, interfacing a custom lower layer to the IP layer is far more difficult than interfacing a custom higher layer to the IP layer. In this study, an adaptation layer sits in the middle of the IP layer and open-zb MAC layer, and an application layer is on top of the IP layer as shown in Appendix Fig A-1. This section gives more details on how to develop the OPNET 6LoWPAN simulation model.

Interfacing the Adaption Layer to the IP Layer and the Open-Zb MAC Layer

OPNET allows custom models to interface with the IP layer module in four steps.

Step 1 Assign a MAC address to the model

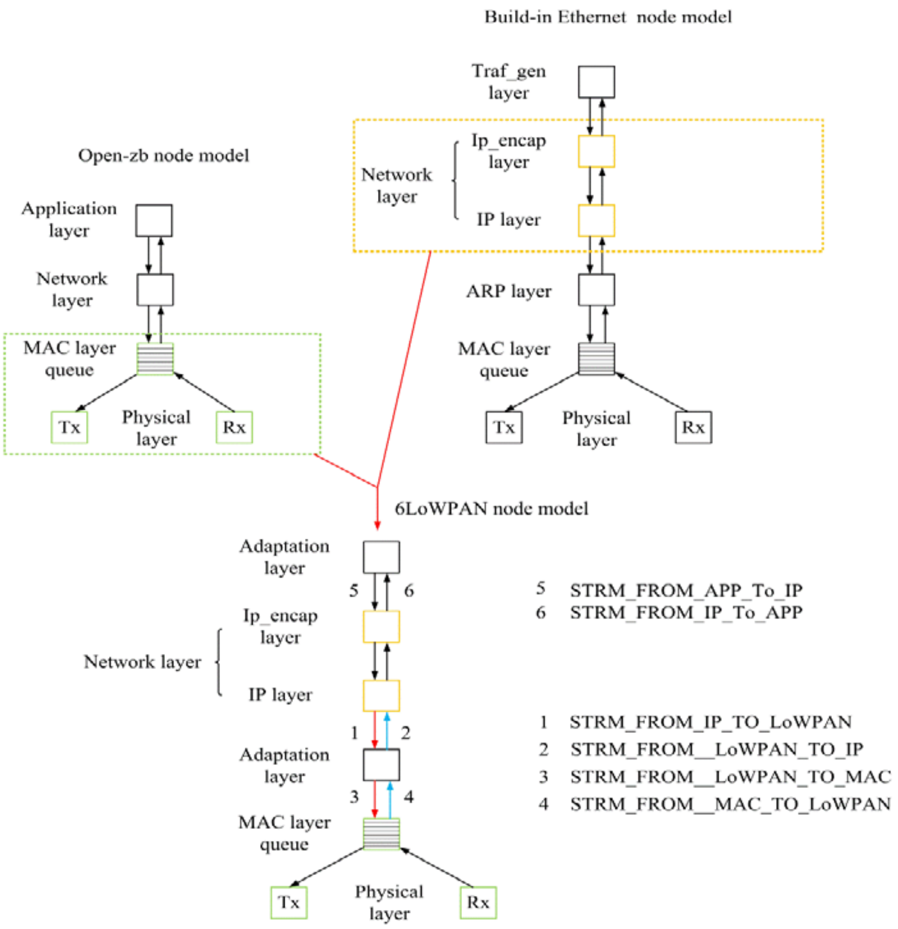
Step 2 Register the process to the IP model

Step 3 Process the packet from the IP layer and send to the MAC layer

Step 4 Process the packet from the MAC layer and send to the IP layer

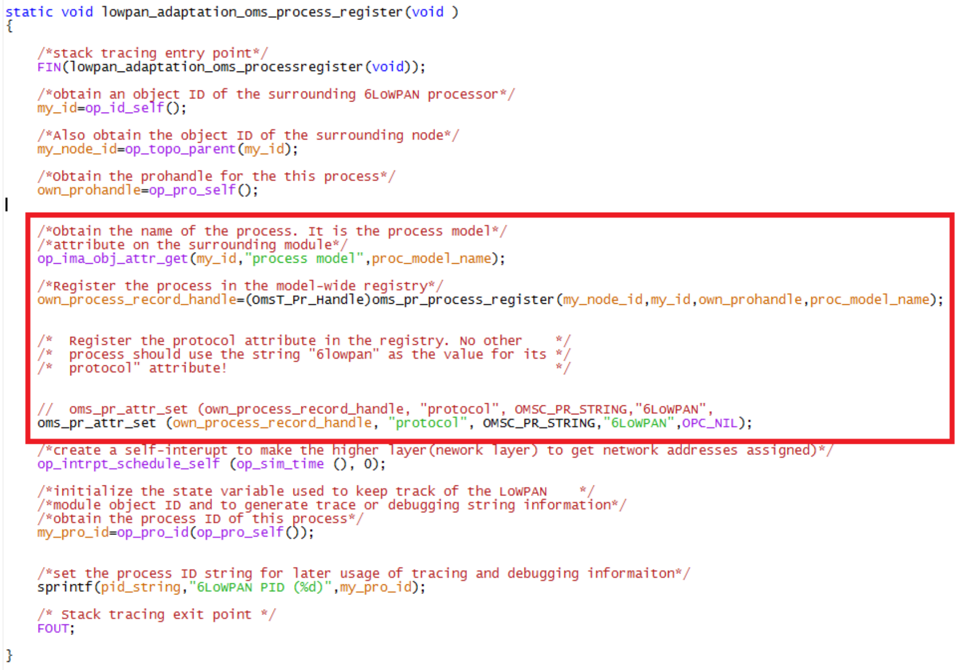
In Step 1, Appendix Fig A-1 shows the how the 6LoWPAN model was developed from the open-zb and the OPNET model library. Each MAC layer in OPNET requires a unique MAC address. A built-in MAC layer uses an OPNET auto-addressing package named oms_aa to assign addresses. For example, the WLAN model in OPNET employs this package to assign an integer to each WLAN node at the beginning of the simulation. However, the open-zb MAC layer does not support the auto-addressing package, so the MAC addresses need to be manually assigned from the model attributes. The MAC addresses were used to support two-way communications in

Chapter 6 and Chapter 7, so manually assigning the MAC address is necessary and it is the only approach to meeting the OPNET requirement.



Appendix Fig A-1 6LoWPAN node model and stream flows

In step 2, Appendix Fig A-1 shows that the adaptation layer replaces the position the ARP layer previously held. For this reason, the adaptation layer must publish its module information in the model-wide process registry as the ARP does. This is because the OPNET IP layer needs to obtain all the information of the modules attached to it. In the adaptation layer, the implemented function used to register the module information is lowpan_adaptation_oms_process_register ( ) as shown in Appendix Fig A-2, where the adaptation model is registered with the function oms_pr_attr_set( ).



```
static void lowpan_adaptation_oms_process_register(void )
{

    /*stack tracing entry point*/
    FIN(lowpan_adaptation_oms_processregister(void));

    /*obtain an object ID of the surrounding 6LOWPAN processor*/
    my_id=op_id_self();

    /*Also obtain the object ID of the surrounding node*/
    my_node_id=op_topo_parent(my_id);

    /*Obtain the prohandle for the this process*/
    own_prohandle=op_pro_self();

    /*Obtain the name of the process. It is the process model*/
    /*attribute on the surrounding module*/
    op_ima_obj_attr_get(my_id,"process model",proc_model_name);

    /*Register the process in the model-wide registry*/
    own_process_record_handle=(OmsT_Pr_Handle)oms_pr_process_register(my_node_id,my_id,own_prohandle,proc_model_name);


    /*  Register the protocol attribute in the registry. No other    */
    /*  process should use the string "6lowpan" as the value for its */
    /*  protocol" attribute!                                          */


    //  oms_pr_attr_set (own_process_record_handle, "protocol", OMSC_PR_STRING,"6LOWPAN",
    oms_pr_attr_set (own_process_record_handle, "protocol", OMSC_PR_STRING,"6LOWPAN",OPC_NIL);
    /*create a self-interupt to make the higher layer(nework layer) to get network addresses assigned)*/
    op_intrpt_schedule_self (op_sim_time (), 0);

    /*initialize the state variable used to keep track of the LOWPAN    */
    /*module object ID and to generate trace or debugging string information*/
    /*obtain the process ID of this process*/
    my_pro_id=op_pro_id(op_pro_self());


    /*set the process ID string for later usage of tracing and debugging informaiton*/
    sprintf(pid_string,"6LOWPAN PID (%d)",my_pro_id);

    /* Stack tracing exit point */
    FOUT;

}
```

Appendix Fig A-2 The adaptation module registration process

In step 3, the adaptation module needs to receive packets from the IP layer. To do this, the adaptation layer first determines if the incoming packet is an IPv6 packet or not and then passes the packet together with the MAC address obtained from the application layer to the MAC layer. This process was implemented in the function lowpan_receive_pk_from_ip ( ). In addition, the open-zb MAC layer requests for three parameters: next hop address, ACK and traffic_type, which are referred to as the next hop MAC address, disable or enable ACK, and real-time traffic or best-effort traffic, respectively. The adaptation layer supports two types of Interface Control Information (ICI): the first type is shared by the adaptation layer and the MAC layer, passing the three parameters to the MAC layer, and the second type is shared by the adaptation layer and the IP layer. The second type is created in the IP layer and is passed down to the adaptation and must not be destroyed. Otherwise, the debugging process will be extremely difficult.

In step 4, the adaptation layer needs to send packets to the IP layer. This process was implemented in the function lowpan_receive_pk_from_mac ( ), which receives a packet from the open-zb MAC layer and sends to the IP layer. Because of the same reason in step 3, a new ARP second type ICI ip_arp_ind_v4 must be created and sent to the IP layer together with the packet.

Above all, another function in the OPNET IP module must be commented out. This function is named ip_rte_outgoing_intf_checks_passed () located in the external file named ip_rte_support.h, which is in child process ip_rte_central_cpu. This function checks all the interfaces and filters attached to the IP layer before send a packet on a physical interface. As the original ARP module has been replaced by the adaptation layer, this function cannot find the ARP module and causes many errors in the debugging process. Once taken out, the function cannot stop packets, and the IPv6 packet can pass through the IP module successfully.

Interfacing the Application Layer to the IP Layer

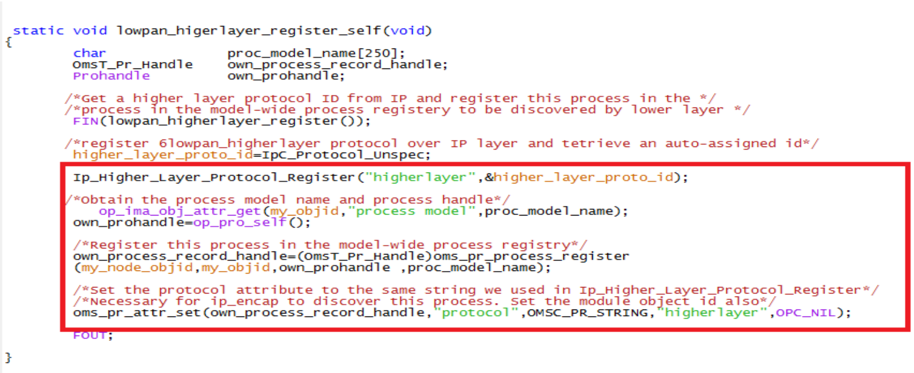
This section discusses how to interface the application layer to the IP layer. Similar to the previous section, interfacing the application layer to the IP layer also involves three steps.

Step 1 Register the application layer to the IP layer

Step 2 Prepare the packet and send it to the IP layer

Step 3 Process the packet received from the IP layer

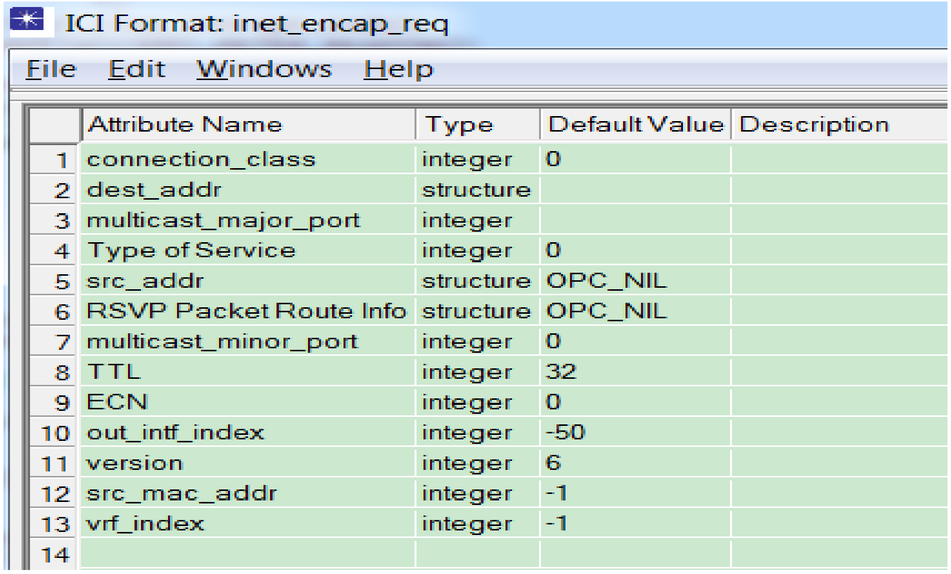
In step 1, the IP layer not only needs to know the module registered below it, but to know the module registered above it. The registration informs the IP layer of the new higher-layer module. As shown in Appendix Fig A-1, the IP layer consists of the ip_encap layer and the ip layer. The ip_encap layer is responsible for discovering the higher layer process. The registration process just generates a unique integer protocol number and passes it to the IP layer. The whole process was implemented in the function lowpan_highlayer_register_self () as shown in Appendix Fig A-3.



```
static void lowpan_higerlayer_register_self(void)
{
        char                proc_model_name[250];
        OmsT_Pr_Handle      own_process_record_handle;
        Prohandle           own_prohandle;

       /*Get a higher layer protocol ID from IP and register this process in the */
       /*process in the model-wide process registery to be discovered by lower layer */
        FIN(lowpan_higherlayer_register());

       /*register 6lowpan_higherlayer protocol over IP layer and tetrieve an auto-assigned id*/
        higher_layer_proto_id=IpC_Protocol_Unspec;

        Ip_Higher_Layer_Protocol_Register("higherlayer",&higher_layer_proto_id);

       /*Obtain the process model name and process handle*/
           op_ima_obj_attr_get(my_objid,"process model",proc_model_name);
        own_prohandle=op_pro_self();

        /*Register this process in the model-wide process registry*/
        own_process_record_handle=(OmsT_Pr_Handle)oms_pr_process_register
        (my_node_objid,my_objid,own_prohandle ,proc_model_name);

        /*Set the protocol attribute to the same string we used in Ip_Higher_Layer_Protocol_Register*/
        /*Necessary for ip_encap to discover this process. Set the module object id also*/
        oms_pr_attr_set(own_process_record_handle,"protocol",OMSC_PR_STRING,"higherlayer",OPC_NIL);

        FOUT;
}
```

Appendix Fig A-3 The application layer registration

In step 2, preparing an IPv6 packet and sending to the IP layer need a different ICI inet_encap_req, rather than IPv4 ICI ip_encap_req_v4. In particular, as for the IPv6 ICI, the dest_addr and src_addr field in ICI must be set to a pointer, as shown in Appendix Fig A-4. In addition, to create an IPv6 address, the function inet_address_create( ) is used to generate an IPv6 address from a string such as 2000::1. After the destination and source IPv6 addresses are generated, they are set in IPv6 ICI and sent out together with the IPv6 packet.

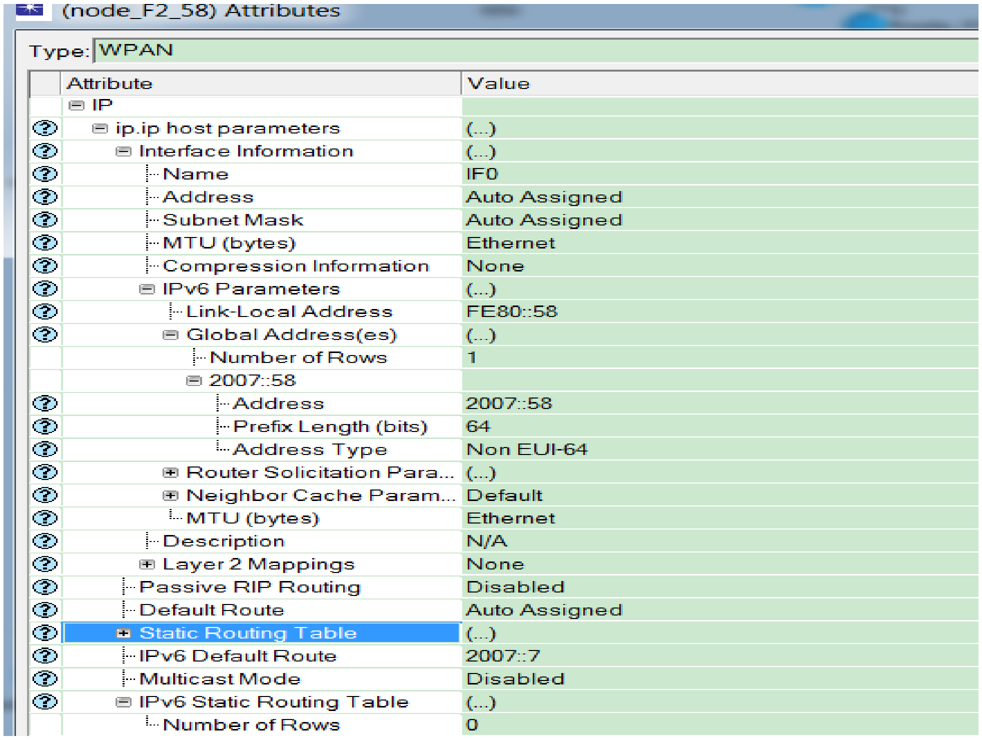


	Attribute Name	Type	Default Value	Description
1	connection_class	integer	0	
2	dest_addr	structure		
3	multicast_major_port	integer		
4	Type of Service	integer	0	
5	src_addr	structure	OPC_NIL	
6	RSVP Packet Route Info	structure	OPC_NIL	
7	multicast_minor_port	integer	0	
8	TTL	integer	32	
9	ECN	integer	0	
10	out_intf_index	integer	-50	
11	version	integer	6	
12	src_mac_addr	integer	-1	
13	vrf_index	integer	-1	
14				

Appendix Fig A-4 OPNET IPv6 ICI structure

In step 3, this step involves processing the packet received from the IP layer. Upon receiving the packet, the destination and source addresses are obtained the ICI, and the number of packets is counted by using custom statistics. After that, the packet and the ICI are destroyed in this layer.

Above all, IP module configuration plays a key part in transmitting IPv6 packets. Without the correct configuration, the IP layer would not forward the IPv6 packet. It can be seen from Appendix Fig A-5 that three IPv6 attributes must be configured: the link-local address, the global address and IPv6 default route. Specifically, the link-local address and the global address are consisted of prefix and the MAC address. For example, if the MAC address is 58, then the link-local address and the global address are FE80::58 and 2007::58. The IPv6 default route is 2007::7, which 7 is the next hop MAC address.



(node_F2_58) Attributes

Type: WPAN

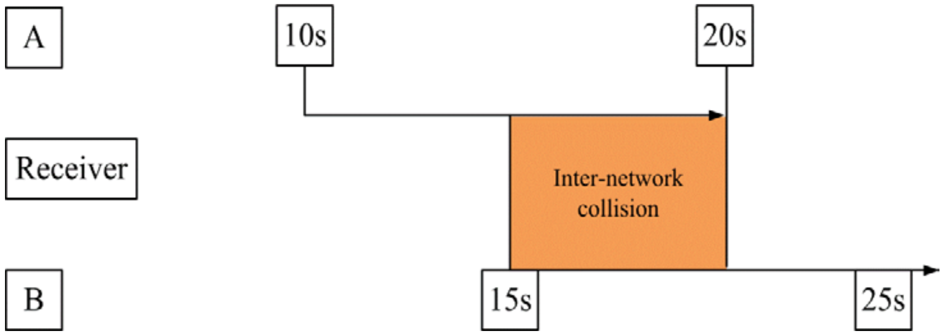
Attribute	Value
⊟ IP	
⊟ ip.ip host parameters	(...)
⊟ Interface Information	(...)
Name	IF0
Address	Auto Assigned
Subnet Mask	Auto Assigned
MTU (bytes)	Ethernet
Compression Information	None
⊟ IPv6 Parameters	(...)
Link-Local Address	FE80::58
⊟ Global Address(es)	(...)
Number of Rows	1
⊟ 2007::58	
Address	2007::58
Prefix Length (bits)	64
Address Type	Non EUI-64
⊞ Router Solicitation Para...	(...)
⊞ Neighbor Cache Param...	Default
MTU (bytes)	Ethernet
Description	N/A
⊞ Layer 2 Mappings	None
Passive RIP Routing	Disabled
Default Route	Auto Assigned
⊞ Static Routing Table	(...)
IPv6 Default Route	2007::7
Multicast Mode	Disabled
⊟ IPv6 Static Routing Table	(...)
Number of Rows	0

Appendix Fig A-5 IPv6 attribute configuration

Appendix B

Inter-Network Collisions Modelling

This section presents how the OPNET pipeline stages calculate the inter-network collisions. Appendix Fig B-1 shows how the inter-network collisions of a packet are calculated over another packet. To do this, three pipeline stages, inoise, snr_ber and error, deal with the computation of the inter-network collisions. For example, packet A that not intended for the receiver arrives at the receiver at time t=10s. This packet lasts about 10s, meaning that it will affect the receiver for 10s and stop at 20s. Packet B also 10s long is intended for the receiver and reaches the receiver at time t=15s.



Appendix Fig B-1 Inter-network collisions modelling in OPNET

Time=10s

Channel match (A marked as noise)

Calculated received power of A

Time=15s

Channel match (B marked as valid)

Calculate received power of B

Add received power of A to the interference power of B in inoise pipeline stage

Calculate SNR of B

Time=20s

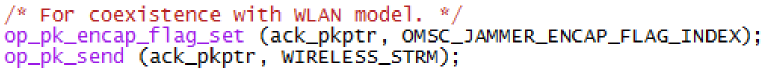
Calculate the BER and resultant errors for the constant SNR from 15-20s, typically use SNR stored from the previous calculation.

Simulation kernel automatically subtracts the received power of A from interference noise of B

Calculate SNR for the new constant SNR segment from 20-25s

Time=25s

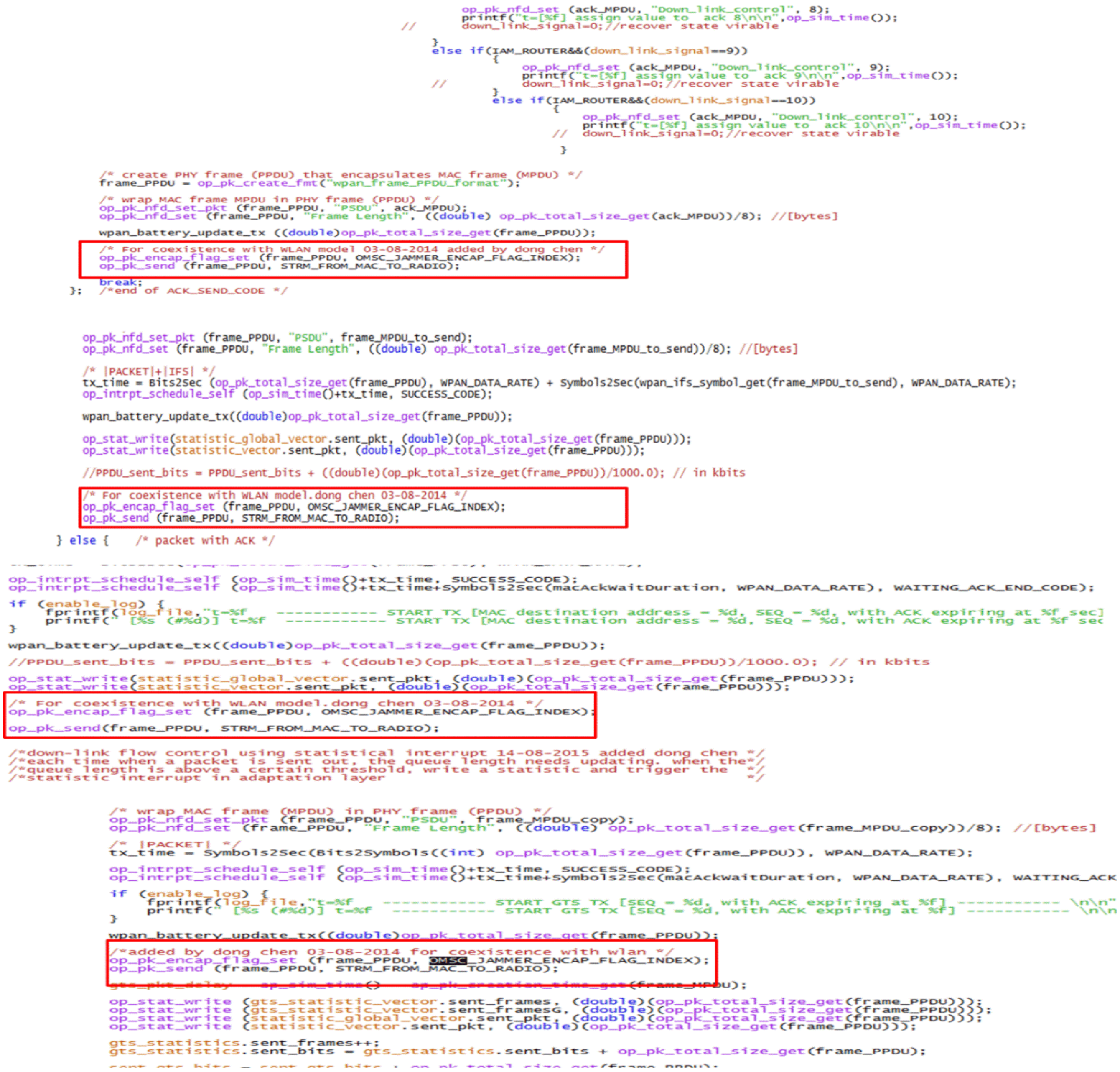
Calculate BER and resultant errors for constant SNR from 20s to 25s (fewer errors since offending packet is gone). It decides whether the errors accumulated during the course of the reception can be corrected or not and allows the packet to be accepted or dropped at the receiver. Besides, OPNET provides a built-in wireless coexistence scenario where the levels of the inter-network collisions are evaluated. However, the network work layer code of the OPNET built-in ZigBee model is hidden from userS due to the protection of intellectual property. For this reason, the open-zb MAC layer model was adopted in the study. As the built-in coexistence scenario uses a flag to tag on every packet the ZigBee sends out, this tag can be also used in the proposed model to make the two types of pipeline stage (the open-zb pipeline stage and the WLAN pipeline stage) compatible. As shown in Appendix Fig B-2, it is the built-in ZigBee-WLAN coexistence model code, the function op_pk_encap_flag_set () sets the tag before a packet can be transmitted. The rationale behind this is because the OPNET modeler tags the 6LoWPAN so that the other packets such as WLAN packets can be treated as noises when calculating the SNR. When the SNR is low, the packet is discarded and the inter-network collisions are simulated.



```
/* For coexistence with WLAN model. */
op_pk_encap_flag_set (ack_pkptr, OMSC_JAMMER_ENCAP_FLAG_INDEX);
op_pk_send (ack_pkptr, WIRELESS_STRM);
```

Appendix Fig B-2 Pipeline stage tag in the built-in ZigBee-WLAN coexistence model

To make the two pipeline stages compatible, code lines such as op_pk_encap_flag_set (ack_pkptr, OMSC_JAMMER_ENCAP_FLAG_INDEX) must be added before any op_pk_send () function callback in the developed 6LoWPAN and MFDRR modules. As there are three types of packets in the 6LoWPAN model such as data packets, ACK packets and beacon packets, the op_pk_encap_flag_set( ) needs to be used several times, as shown in Appendix Fig B-3.



```
                op_pk_nfd_set (ack_MPDU, "Down_link_control", 8);
                printf("t=[%f] assign value to  ack 8\n\n",op_sim_time());
    //          down_link_signal=0;//recover state virable

            }
            else if(IAM_ROUTER&&(down_link_signal==9))
                    {
                        op_pk_nfd_set (ack_MPDU, "Down_link_control", 9);
                        printf("t=[%f] assign value to  ack 9\n\n",op_sim_time());
            //          down_link_signal=0;//recover state virable
                    }
                    else if(IAM_ROUTER&&(down_link_signal==10))
                            {
                                op_pk_nfd_set (ack_MPDU, "Down_link_control", 10);
                                printf("t=[%f] assign value to  ack 10\n\n",op_sim_time());
                            //  down_link_signal=0;//recover state virable

                             }
```

```
    /* create PHY frame (PPDU) that encapsulates MAC frame (MPDU) */
    frame_PPDU = op_pk_create_fmt("wpan_frame_PPDU_format");

    /* wrap MAC frame MPDU in PHY frame (PPDU) */
    op_pk_nfd_set_pkt (frame_PPDU, "PSDU", ack_MPDU);
    op_pk_nfd_set (frame_PPDU, "Frame Length", ((double) op_pk_total_size_get(ack_MPDU))/8); //[bytes]

    wpan_battery_update_tx ((double)op_pk_total_size_get(frame_PPDU));

    /* For coexistence with WLAN model 03-08-2014 added by dong chen */
    op_pk_encap_flag_set (frame_PPDU, OMSC_JAMMER_ENCAP_FLAG_INDEX);
    op_pk_send (frame_PPDU, STRM_FROM_MAC_TO_RADIO);

    break;
};  /*end of ACK_SEND_CODE */
```

```
    op_pk_nfd_set_pkt (frame_PPDU, "PSDU", frame_MPDU_to_send);
    op_pk_nfd_set (frame_PPDU, "Frame Length", ((double) op_pk_total_size_get(frame_MPDU_to_send))/8); //[bytes]

    /* |PACKET|+|IFS| */
    tx_time = Bits2Sec (op_pk_total_size_get(frame_PPDU), WPAN_DATA_RATE) + Symbols2Sec(wpan_ifs_symbol_get(frame_MPDU_to_send), WPAN_DATA_RATE);
    op_intrpt_schedule_self (op_sim_time()+tx_time, SUCCESS_CODE);

    wpan_battery_update_tx((double)op_pk_total_size_get(frame_PPDU));

    op_stat_write(statistic_global_vector.sent_pkt, (double)(op_pk_total_size_get(frame_PPDU)));
    op_stat_write(statistic_vector.sent_pkt, (double)(op_pk_total_size_get(frame_PPDU)));

    //PPDU_sent_bits = PPDU_sent_bits + ((double)(op_pk_total_size_get(frame_PPDU))/1000.0); // in kbits

    /* For coexistence with WLAN model.dong chen 03-08-2014 */
    op_pk_encap_flag_set (frame_PPDU, OMSC_JAMMER_ENCAP_FLAG_INDEX);
    op_pk_send (frame_PPDU, STRM_FROM_MAC_TO_RADIO);

} else {     /* packet with ACK */
```

```
op_intrpt_schedule_self (op_sim_time()+tx_time, SUCCESS_CODE);
op_intrpt_schedule_self (op_sim_time()+tx_time+Symbols2Sec(macAckWaitDuration, WPAN_DATA_RATE), WAITING_ACK_END_CODE);

if (enable_log) {
    fprintf(log_file,"t=%f    ----------- START TX [MAC destination address = %d, SEQ = %d, with ACK expiring at %f sec]
    printf(" [%s (#%d)] t=%f   ------------ START TX [MAC destination address = %d, SEQ = %d, with ACK expiring at %f sec
}

wpan_battery_update_tx((double)op_pk_total_size_get(frame_PPDU));

//PPDU_sent_bits = PPDU_sent_bits + ((double)(op_pk_total_size_get(frame_PPDU))/1000.0); // in kbits

op_stat_write(statistic_global_vector.sent_pkt, (double)(op_pk_total_size_get(frame_PPDU)));
op_stat_write(statistic_vector.sent_pkt, (double)(op_pk_total_size_get(frame_PPDU)));
/* For coexistence with WLAN model.dong chen 03-08-2014 */
op_pk_encap_flag_set (frame_PPDU, OMSC_JAMMER_ENCAP_FLAG_INDEX);

op_pk_send(frame_PPDU, STRM_FROM_MAC_TO_RADIO);

/*down-link flow control using statistical interrupt 14-08-2015 added dong chen */
/*each time when a packet is sent out, the queue length needs updating. when the*/
/*queue length is above a certain threshold, write a statistic and trigger the  */
/*statistic interrupt in adaptation layer                                       */
```

```
    /* wrap MAC frame (MPDU) in PHY frame (PPDU) */
    op_pk_nfd_set_pkt (frame_PPDU, "PSDU", frame_MPDU_copy);
    op_pk_nfd_set (frame_PPDU, "Frame Length", ((double) op_pk_total_size_get(frame_MPDU_copy))/8); //[bytes]
    /* |PACKET| */
    tx_time = Symbols2Sec(Bits2Symbols((int) op_pk_total_size_get(frame_PPDU)), WPAN_DATA_RATE);
    op_intrpt_schedule_self (op_sim_time()+tx_time, SUCCESS_CODE);
    op_intrpt_schedule_self (op_sim_time()+tx_time+Symbols2Sec(macAckWaitDuration, WPAN_DATA_RATE), WAITING_ACK
    if (enable_log) {
        fprintf(log_file,"t=%f    ----------- START GTS TX [SEQ = %d, with ACK expiring at %f] ----------- \n\n"
        printf(" [%s (#%d)] t=%f   ----------- START GTS TX [SEQ = %d, with ACK expiring at %f] ----------- \n\n
    }
    wpan_battery_update_tx((double)op_pk_total_size_get(frame_PPDU));
    /*added by dong chen 03-08-2014 for coexistence with wlan */
    op_pk_encap_flag_set (frame_PPDU, OMSC_JAMMER_ENCAP_FLAG_INDEX);
    op_pk_send (frame_PPDU, STRM_FROM_MAC_TO_RADIO);
    gts_pkt_delay = op_sim_time() - op_pk_creation_time_get(frame_MPDU);
    op_stat_write (gts_statistic_vector.sent_frames, (double)(op_pk_total_size_get(frame_PPDU)));
    op_stat_write (gts_statistic_vector.sent_framesG, (double)(op_pk_total_size_get(frame_PPDU)));
    op_stat_write (statistic_global_vector.sent_pkt, (double)(op_pk_total_size_get(frame_PPDU)));
    op_stat_write (statistic_vector.sent_pkt, (double)(op_pk_total_size_get(frame_PPDU)));
    gts_statistics.sent_frames++;
    gts_statistics.sent_bits = gts_statistics.sent_bits + op_pk_total_size_get(frame_PPDU);
    sent_gts_bits = sent_gts_bits + op_pk_total_size_get(frame_PPDU);
```

Appendix Fig B-3 Code modification in 6LoWPAN model

Appendix C
Link Margin Modelling with the Received Power Attribute

The propagation model used in the proposed area network scenario in this thesis is the free space path loss model. The model refers to a status that the signal strength attenuates as the wave propagates between the transmitter and receiver without any obstruction. The model is calculated with Friss Ttransmission formula as follows.

$$\mathrm{FSPL} = \left(\frac{4\pi \mathrm{d}}{\lambda}\right)^2 , \qquad \text{C-1}$$

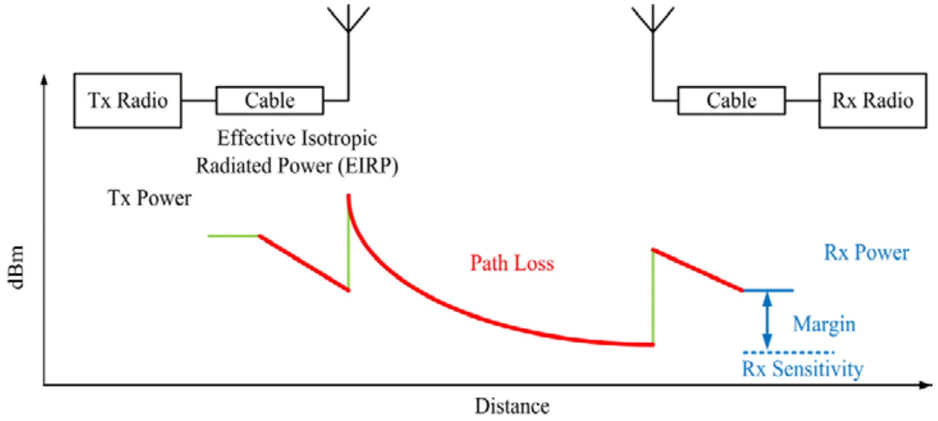
where λ denotes the signal wave length, d represents the distance between the transmitter and receiver. Based on this free space path loss model, the average received power is expressed as

$$\mathrm{P_r} = \frac{\mathrm{P_t G_t G_r} \lambda^2}{(4\pi)^2 \mathrm{d}^2 \mathrm{L}^2} \;\; , \qquad \text{C-2}$$

where $\mathrm{P_r}$ and $\mathrm{P_t}$ are the received and transmit power; $\mathrm{G_t}$ and $\mathrm{G_r}$are the transmitting antenna gain and receiving antenna gain; L is the system loss factor [129]; and the remainder are the same with the parameters in C-1. In a wireless communication system, the received power has to be greater than the minimum received signal level of a receiver as shown in C-3, and then a packet can be received. The minimum received signal level is called receive sensitivity.

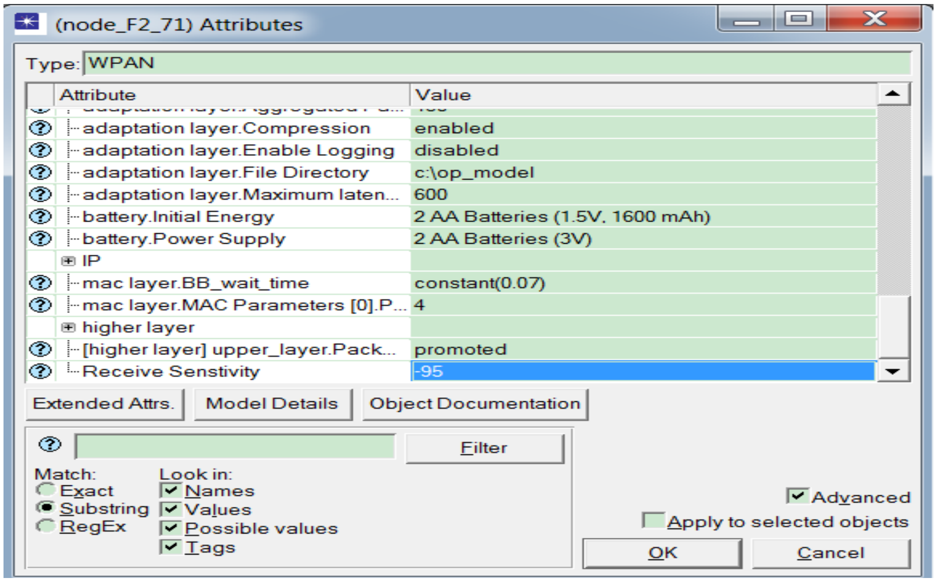
$$\mathrm{P_r} - \mathrm{FSPL} \geq P_{threshold} \;\; , \qquad \text{C-4}$$

Where $P_{threshold}$ is the receive sensitivity. The difference between the received power and the receive sensitivity is called the link margin, as shown in Appendix Fig C-1.



Appendix Fig C-1 Link margin in a wireless system

Unfortunately, the open-zb model, contributing its MAC layer to the customized 6LoWPAN model, adopts the built-in pipeline stage dra_power in the receiver of the model, and the dra_power pipeline stage lacks the receive sensitivity attribute in the model. This leads to a phenomenon that although the transmit power of the transmitter is low to less than 1 mW and distance is up to 1000 m, the receiver still can receive the packet. To solve this problem, the code of the pipeline stage dra_power needed to be modified, and the receive sensitivity attribute was added to the model. As shown in Appendix Fig C-2 and Appendix Fig C-3, the receive sensitivity attribute as well as its code is presented. The value of the attribute -95db is obtained by the pipeline stage and assigned to the variable rx_power_threshold as indicated in a red rectangle. The code means if the received power is less than the receive sensitivity, the packet is locked and will be dropped in the later pipeline stage. This code modification ensures the packet receiving process is in accordance with the free space path loss and link budget.

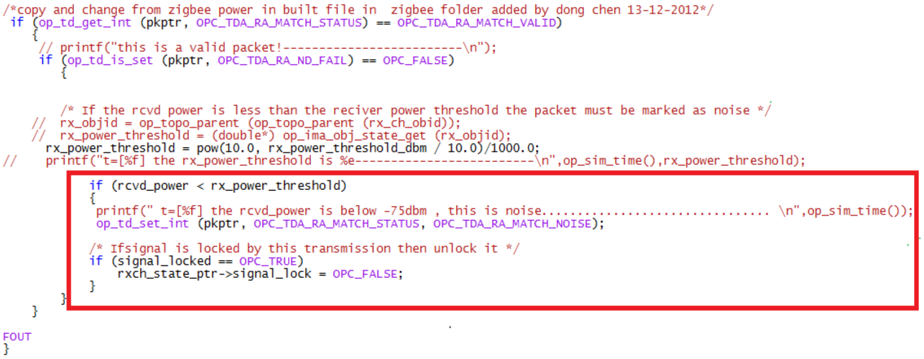


(node_F2_71) Attributes

Type: WPAN

Attribute	Value
adaptation layer.Compression	enabled
adaptation layer.Enable Logging	disabled
adaptation layer.File Directory	c:\op_model
adaptation layer.Maximum laten...	600
battery.Initial Energy	2 AA Batteries (1.5V, 1600 mAh)
battery.Power Supply	2 AA Batteries (3V)
⊞ IP	
mac layer.BB_wait_time	constant(0.07)
mac layer.MAC Parameters [0].P...	4
⊞ higher layer	
[higher layer] upper_layer.Pack...	promoted
Receive Senstivity	-95

Appendix Fig C-2 Receive sensitivity attribute



```
/*copy and change from zigbee power in built file in  zigbee folder added by dong chen 13-12-2012*/
 if (op_td_get_int (pkptr, OPC_TDA_RA_MATCH_STATUS) == OPC_TDA_RA_MATCH_VALID)
    {
     // printf("this is a valid packet!------------------------\n");
     if (op_td_is_set (pkptr, OPC_TDA_RA_ND_FAIL) == OPC_FALSE)
        {


        /* If the rcvd power is less than the reciver power threshold the packet must be marked as noise */
    //  rx_objid = op_topo_parent (op_topo_parent (rx_ch_obid));
    //  rx_power_threshold = (double*) op_ima_obj_state_get (rx_objid);
      rx_power_threshold = pow(10.0, rx_power_threshold_dbm / 10.0)/1000.0;
//    printf("t=[%f] the rx_power_threshold is %e------------------------\n",op_sim_time(),rx_power_threshold);

          if (rcvd_power < rx_power_threshold)
          {
           printf(" t=[%f] the rcvd_power is below -75dbm , this is noise................................ \n",op_sim_time());
           op_td_set_int (pkptr, OPC_TDA_RA_MATCH_STATUS, OPC_TDA_RA_MATCH_NOISE);

          /* Ifsignal is locked by this transmission then unlock it */
          if (signal_locked == OPC_TRUE)
              rxch_state_ptr->signal_lock = OPC_FALSE;
          }
        }
    }

FOUT
}
```

Appendix Fig C-3 Receive sensitivity code

Appendix D

Process Model Code Examples

Four process model code examples are presented in this section. The first is the application layer process model dealing with the packet generation for three types of traffic, and the second is the adaptation layer dealing with the IPv6 header compression and restoration. The meter reading, sensor and DSM traffic were developed in the model. Each traffic generation function firstly obtains the MAC address from the model attributes and then generates the source and destination IPv6 addresses based on the MAC address. The code is on these two links below

https://www.dropbox.com/s/to9x11izpoe4ha2/app_layer_traffic_generation.c?dl=0

https://www.dropbox.com/s/pvi2a5x92rv8l95/adaptation_layer.c?dl=0

The third is the aggregation factor-based BB algorithm, which has been discussed in Chapter 5. This algorithm uses the BB period to avoid the inter-network collisions and uses the aggregation factor to adjust the number of WLAN packets in the network. The algorithm uses the aggregation factor to count the number of the 6LoWPAN packets in the queue. Once the number of the 6LoWPAN packets equals the aggregation factor, the algorithm is triggered. The code is on the link below.

https://www.dropbox.com/s/kf9j5c40wst3781/aggregation_factor_BB_algorithm.c?dl=0

The last is the lifetime-based algorithm, which has been introduced in Chapter 6. Due to the use of the aggregation factor, some packets might stay in the aggregation queue for quite a long time and might not be valide when arriving the data sink. To solve this problem, the lifetime-based algorithm uses the lifetime value of the packet to trigger the WLAN transmissions. Once the remaining lifetime value of a packet is less than the guard time value in the MFDRR, the packet is dropped to ensure the QoS for that traffic. The code is on the link below.

https://www.dropbox.com/s/3pigrvvzpimgk87/lifetime_BB_algorithm.c?dl=0

Bibliography

[1] L. Tan and N. Wang, "Future internet: The internet of things," in *Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on*, 2010, pp. V5-376-V5-380.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems,* vol. 29, pp. 1645-1660, 9// 2013.

[3] A. Zaballos, A. Vallejo, and J. M. Selga, "Heterogeneous communication architecture for the smart grid," *IEEE Network*, vol. 25, 2011.

[4] W. Yuan, X. Wang, and J.-P. M. Linnartz, "A Coexistence Model of IEEE 802.15. 4 and IEEE 802.11 b/g," in *Communications and Vehicular Technology in the Benelux, 2007 14th IEEE Symposium on*, 2007, pp. 1-5.

[5] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks*, vol. 54, pp. 2787-2805, 2010.

[6] M. Chen, J. Wan, S. González, X. Liao, and V. Leung, "A survey of recent developments in home M2M networks," *Communications Surveys & Tutorials, IEEE,* vol. 16, pp. 98-114, 2014.

[7] J. Kim, J. Lee, J. Kim, and J. Yun, "M2M service platforms: survey, issues, and enabling technologies," *Communications Surveys & Tutorials, IEEE,* vol. 16, pp. 61-76, 2014.

[8] Y. Tang, Z. Wang, D. Makrakis, and H. T. Mouftah, "Interference Aware Adaptive Clear Channel Assessment for improving ZigBee packet transmission under Wi-Fi interference," in *Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2013 10th Annual IEEE Communications Society Conference on*, 2013, pp. 336-343.

[9] Y. Jeong, J. Kim, and S.-J. Han, "Interference mitigation in wireless sensor networks using dual heterogeneous radios," *Wireless Networks,* vol. 17, p. 1699, 2011.

[10] "D.LBrock The electronic Product Code (EPC)- A Naming Scheme for Physcial Objects. White Paper. January 2001. ."

[11] "A Sangiovanni-vincentelli, Let's Get Physcial: Marrying Physics with Computer Science. keynote Speech at Horizon 2020 DIITET Conference, Rome, May 2014.."

[12] M. Z. Shafiq, L. Ji, A. X. Liu, J. Pang, and J. Wang, "A first look at cellular machine-to-machine traffic: large scale measurement and characterization," in *ACM SIGMETRICS Performance Evaluation Review*, 2012, pp. 65-76.

[13] Z. Yang, Y. Peng, Y. Yue, X. Wang, Y. Yang, and W. Liu, "Study and application on the architecture and key technologies for IOT," in *Multimedia Technology (ICMT), 2011 International Conference on*, 2011, pp. 747-751.

[14] M. Weiser, R. Gold, and J. S. Brown, "The origins of ubiquitous computing research at PARC in the late 1980s," *IBM systems journal,* vol. 38, pp. 693-696, 1999.

[15] Y. Rogers, "Moving on from weiser’s vision of calm computing: Engaging ubicomp experiences," in *UbiComp 2006: Ubiquitous Computing*, ed: Springer, 2006, pp. 404-421.

[16] R. Caceres and A. Friday, "Ubicomp systems at 20: Progress, opportunities, and challenges," *IEEE Pervasive Computing,* pp. 14-21, 2011.

[17] M. Presser and A. Gluhak, "The internet of things: Connecting the real world with the digital world," *EURESCOM mess@ ge–The Magazine for Telecom Insiders,* vol. 2, 2009.

[18] "B. Sterling, Shaping Things-Mediawork PAMPHLET, The MIT Press."

[19] "A. Dunkels,J.P. Vasseur,IP for Smart Objects, Internet Protocol for Smart Objects (IPSO) Alliance, White Paper, #3, January 2009."

[20] I. Toma, E. Simperl, and G. Hench, "A joint roadmap for semantic technologies and the internet of things," in *Proceedings of the Third STI Roadmapping Workshop, Crete, Greece*, 2009.

[21] I. Strategy and P. Unit, "ITU Internet Reports 2005: The internet of things," *Geneva: International Telecommunication Union (ITU),* 2005.

[22] E. Borgia, "The Internet of Things vision: Key features, applications and open issues," *Computer Communications,* vol. 54, pp. 1-31, 2014.

[23] R. Want, "An introduction to RFID technology," *Pervasive Computing, IEEE,* vol. 5, pp. 25-33, 2006.

[24] P. V. Nikitin, K. Rao, and S. Lazar, "An overview of near field UHF RFID," in *IEEE international Conference on RFID*, 2007.

[25] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer networks*, vol. 38, pp. 393-422, 2002.

[26] C. Wang, K. Sohraby, B. Li, M. Daneshmand, and Y. Hu, "A survey of transport protocols for wireless sensor networks," *Ieee Network,* vol. 20, pp. 34-40, 2006.

[27] R. Bruno, M. Conti, and E. Gregori, "Bluetooth: Architecture, protocols and scheduling algorithms," *Cluster Computing,* vol. 5, pp. 117-131, 2002.

[28] F. M. Al-Turjman, A. E. Al-Fagih, W. M. Alsalih, and H. S. Hassanein, "A delay-tolerant framework for integrated RSNs in IoT," *Computer Communications,* vol. 36, pp. 998-1010, 2013.

[29] P. Du and G. Roussos, "Adaptive communication techniques for the internet of things," *Journal of Sensor and Actuator Networks,* vol. 2, pp. 122-155, 2013.

[30] B. Bellalta, A. Vinel, P. Chatzimisios, R. Bruno, and C. Wang, "Research advances and standardization activities in WLANs," *Computer Communications,* pp. 1-2, 2014.

[31] P. Baronti, P. Pillai, V. W. Chook, S. Chessa, A. Gotta, and Y. F. Hu, "Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and ZigBee standards," *Computer communications*, vol. 30, pp. 1655-1695, 2007.

[32] V. C. Güngör, D. Sahin, T. Kocak, S. Ergüt, C. Buccella, C. Cecati, *et al.*, "Smart grid technologies: communication technologies and standards," *Industrial informatics, IEEE transactions on,* vol. 7, pp. 529-539, 2011.

[33] J. Yu, N. Wang, G. Wang, and D. Yu, "Connected dominating sets in wireless ad hoc and sensor networks–A comprehensive survey," *Computer Communications,* vol. 36, pp. 121-134, 2013.

[34] J. Mitola III, "Cognitive radio architecture," in *Cognitive Radio, Software Defined Radio, and Adaptive Wireless Systems,* ed: Springer, 2007, pp. 43-107.

[35] L. Pelusi, A. Passarella, and M. Conti, "Opportunistic networking: data forwarding in disconnected mobile ad hoc networks," *Communications Magazine, IEEE,* vol. 44, pp. 134-141, 2006.

[36] W. Zhiliang, Y. Yi, W. Lu, and W. Wei, "A SOA based IOT communication middleware," in *Mechatronic Science, Electric Engineering and Computer (MEC), 2011 International Conference on,* 2011, pp. 2555-2558.

[37] K. Hwang, J. Dongarra, and G. C. Fox, *Distributed and cloud computing: from parallel processing to the internet of things*: Morgan Kaufmann, 2013.

[38] "Etsi, TC M2M, ETSI TS 102 921 v1.1.1 (2012-02) - Machine-to-Machine Communication (M2M); mal,dal and mld Interfaces, February 2012.."

[39] "Etsi, TC M2M, ETSI TS 102 690 v1.1.1 (2011-10) Machine-to-Machine Communications (M2M): Functional Architecture, October 2012. ."

[40] "3GPP, 3GPP TS 22.368 v1 1.0.0- Service Requirements for Machine-Type Communications, March 2013.."

[41] A. Rico-Alvarino, M. Vajapeyam, H. Xu, X. Wang, Y. Blankenship, J. Bergman, *et al.*, "An overview of 3GPP enhancements on machine to machine communications," *IEEE Communications Magazine,* vol. 54, pp. 14-21, 2016.

[42] R. Srinivasan, J. Zhuang, L. Jalloul, R. Novak, and J. Park, "IEEE 802.16 m evaluation methodology document (EMD)," *IEEE 802.16 Broadband Wireless Access Working Group,* 2008.

[43] K. Chang, A. Soong, M. Tseng, and Z. Xiang, "Global wireless machine-to-machine standardization," *IEEE Internet Computing,* pp. 64-69, 2011.

[44] J. Luo and J.-P. Hubaux, "A survey of inter-vehicle communication," 2004.

[45] Z. Pala and N. Inanc, "Smart parking applications using RFID technology," in *RFID Eurasia, 2007 1st Annual,* 2007, pp. 1-3.

[46] F. J. Villanueva, D. Villa, F. Moya, M. J. Santofimia, and J. C. López, "Internet of things architecture for an RFID-based product tracking business model," in *Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012 Sixth International Conference on*, 2012, pp. 811-816.

[47] H. Cai, L. Da Xu, B. Xu, C. Xie, S. Qin, and L. Jiang, "IoT-based configurable information service platform for product lifecycle management," *Industrial Informatics, IEEE Transactions on,* vol. 10, pp. 1558-1567, 2014.

[48] P. Hank, S. Müller, O. Vermesan, and J. Van Den Keybus, "Automotive ethernet: in-vehicle networking and smart mobility," in *Proceedings of the Conference on Design, Automation and Test in Europe*, 2013, pp. 1735-1739.

[49] N. Bui and M. Zorzi, "Health care applications: a solution based on the internet of things," in *Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies,* 2011, p. 131.

[50] A. Dohr, R. Modre-Opsrian, M. Drobics, D. Hayn, and G. Schreier, "The internet of things for ambient assisted living," in *Information Technology: New Generations (ITNG), 2010 Seventh International Conference on,* 2010, pp. 804-809.

[51] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: An overview," *IEEE Communications Surveys & Tutorials,* vol. 19, pp. 855-873, 2017.

[52] A. Augustin, J. Yi, T. Clausen, and W. M. Townsley, "A study of LoRa: Long range & low power networks for the internet of things," *Sensors,* vol. 16, p. 1466, 2016.

[53] "SigFox, "SigFox",[online], Availability http://www.sigfox.com."

[54] "RPMA,"RPMA Technology for the Internet of Things," Ingenu,Tech, Rep，2016."

[55] P. J. Burns, S. Kirtay, and P. Marks, "Future use of licence exempt radio spectrum," *Plum Consult., London, UK, Tech. Rep,* 2015.

[56] "“Weightless”[Online], Availabilty:http://www.neul.com."

[57] Z. M. Fadlullah, M. M. Fouda, N. Kato, A. Takeuchi, N. Iwasaki, and Y. Nozaki, "Toward intelligent machine-to-machine communications in smart grid," *IEEE Communications Magazine,* vol. 49, 2011.

[58] F. Leccese, "An overwiev on IEEE Std 2030," in *Environment and Electrical Engineering (EEEIC), 2012 11th International Conference on*, 2012, pp. 340-345.

[59] G. Locke and P. D. Gallagher, "NIST framework and roadmap for smart grid interoperability standards, release 1.0," *National Institute of Standards and Technology,* vol. 33, 2010.

[60] "ETSI TS 102689,"Machine-to-machine communication (M2M); M2M service requirements," July, 2013."

[61] M. Chen, "Towards smart city: M2M communications with software agent intelligence," *Multimedia Tools and Applications,* vol. 67, pp. 167-178, 2013.

[62] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, *et al.*, "Smart grid technologies: communication technologies and standards," *IEEE transactions on Industrial informatics,* vol. 7, pp. 529-539, 2011.

[63] C.-M. Wong, "A novel beacon frame scheduling algorithm based on cluster-tree IEEE 802.15. 4 wireless sensor networks," in *Communication Systems (ICCS), 2012 IEEE International Conference on*, 2012, pp. 285-289.

[64] G. Anastasi, M. Conti, and M. Di Francesco, "A comprehensive analysis of the MAC unreliability problem in IEEE 802.15. 4 wireless sensor networks," *Industrial Informatics, IEEE Transactions on,* vol. 7, pp. 52-65, 2011.

[65] L.-H. Yen, Y. W. Law, and M. Palaniswami, "Risk-aware distributed beacon scheduling for tree-based ZigBee wireless networks," *Mobile Computing, IEEE Transactions on,* vol. 11, pp. 692-703, 2012.

[66] "IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (WPANs)," *IEEE Std 802.15.4-2006 (Revision of IEEE Std 802.15.4-2003),* pp. 1-320, 2006.

[67] E. Toscano and L. L. Bello, "Multichannel superframe scheduling for IEEE 802.15. 4 industrial wireless sensor networks," *Industrial Informatics, IEEE Transactions on,* vol. 8, pp. 337-350, 2012.

[68] E. Toscano and L. L. Bello, "A multichannel approach to avoid beacon collisions in IEEE 802.15. 4 cluster-tree industrial networks," in *Emerging Technologies & Factory Automation, 2009. ETFA 2009. IEEE Conference on*, 2009, pp. 1-9.

[69] J.-W. Kim, J. Kim, and D.-S. Eom, "Multi-dimensional channel management scheme to avoid beacon collision in LR-WPAN," *Consumer Electronics, IEEE Transactions on,* vol. 54, pp. 396-404, 2008.

[70] F. Chen, X. Tong, E. Ngai, and F. Dressler, "Mode switch—Adaptive use of delay-sensitive or energy-aware communication in IEEE 802.15. 4-based networks," in *Mobile Adhoc and Sensor Systems (MASS), 2010 IEEE 7th International Conference on*, 2010, pp. 302-311.

[71] A. Koubâa, A. Van Nieuwenhuyse, M. Attia, and M. Alves, "Collision-free beacon scheduling mechanisms for IEEE 802.15. 4/Zigbee cluster-tree wireless sensor networks," in *7th International Workshop on Applications and services in Wireless Networks*, 2007.

[72] L. Angrisani, M. Bertocco, D. Fortin, and A. Sona, "Experimental study of coexistence issues between IEEE 802.11 b and IEEE 802.15. 4 wireless networks," *Instrumentation and Measurement, IEEE Transactions on*, vol. 57, pp. 1514-1523, 2008.

[73] A. Sikora and V. F. Groza, "Coexistence of IEEE802. 15.4 with other Systems in the 2.4 GHz-ISM-Band," in *Instrumentation and Measurement Technology Conference, 2005. IMTC 2005. Proceedings of the IEEE*, 2005, pp. 1786-1791.

[74] M. Rihan, M. El-Khamy, and M. El-Sharkawy, "On ZigBee coexistence in the ISM band: Measurements and simulations," in *Wireless Communications in Unusual and Confined Areas (ICWCUCA), 2012 International Conference on*, 2012, pp. 1-6.

[75] J. W. Chong, H. Y. Hwang, C. Y. Jung, and D. K. Sung, "Analysis of throughput in a ZigBee network under the presence of WLAN interference," in *Communications and Information Technologies, 2007. ISCIT'07. International Symposium on*, 2007, pp. 1166-1170.

[76] B. H. Jung, J. W. Chong, C. Y. Jung, S. M. Kim, and D. K. Sung, "Interference mediation for coexistence of WLAN and ZigBee networks," in *Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008. IEEE 19th International Symposium on*, 2008, pp. 1-5.

[77] B. H. Jung, J. W. Chong, S. H. Jeong, H. Y. Hwang, S. M. Kim, M. S. Kang, *et al.*, "Ubiquitous wearable computer (UWC)-aided coexistence algorithm in an overlaid network environment of wlan and ZigBee networks," in *Wireless Pervasive Computing, 2007. ISWPC'07. 2nd International Symposium on*, 2007.

[78] Z. Wang, T. Du, Y. Tang, D. Makrakis, and H. T. Mouftah, "ACK with Interference Detection Technique for ZigBee Network under Wi-Fi Interference," in *Broadband and Wireless Computing, Communication and Applications (BWCCA), 2013 Eighth International Conference on*, 2013, pp. 128-135.

[79] N. Torabi, K. Rostamzadeh, and V. Leung, "Ieee 802.15. 4 beaconing strategy and the coexistence problem in ism band," *Smart Grid, IEEE Transactions on*, vol. 6, pp. 1463-1472, 2015.

[80] X. Zhang and K. G. Shin, "Enabling coexistence of heterogeneous wireless systems: case for ZigBee and WiFi," in *Proceedings of the Twelfth ACM International Symposium on Mobile Ad Hoc Networking and Computing*, 2011, p. 6.

[81] K. Hong, S. Lee, and K. Lee, "Performance improvement in ZigBee-based home networks with coexisting WLANs," *Pervasive and Mobile Computing*, vol. 19, pp. 156-166, 2015.

[82] D. G. Yoon, S. Y. Shin, W. H. Kwon, and H. S. Park, "Packet error rate analysis of IEEE 802.11 b under IEEE 802.15. 4 interference," in *Vehicular Technology Conference, 2006. VTC 2006-Spring. IEEE 63rd*, 2006, pp. 1186-1190.

[83] P. Yi, A. Iwayemi, and C. Zhou, "Developing ZigBee deployment guideline under WiFi interference for smart grid applications," *Smart Grid, IEEE Transactions on*, vol. 2, pp. 110-120, 2011.

[84] A. Koubaa, M. Alves, and E. Tovar, "A two-tiered architecture for real-time communications in large-scale wireless sensor networks: research challenges," in *WIP Proceeding of the 17th Euromicro Conference on Real-Time Systems (ECRTS'05), Palma de Mallorca, Spain*, 2005.

[85] J. Leal, A. Cunha, M. Alves, and A. Koubaa, "On a IEEE 802.15. 4/ZigBee to IEEE 802.11 gateway for the ART-WiSe architecture," in *Emerging Technologies and Factory Automation, 2007. ETFA. IEEE Conference on*, 2007, pp. 1388-1391.

[86] Q. Li, D. Han, O. Gnawali, P. Sommer, and B. Kusy, "Twonet: large-scale wireless sensor network testbed with dual-radio nodes," in *Proceedings of the 11th ACM Conference on Embedded Networked Sensor Systems*, 2013, p. 89.

[87] M. Ha, S. H. Kim, H. Kim, K. Kwon, N. Giang, and D. Kim, "SNAIL gateway: Dual-mode wireless access points for WiFi and IP-based wireless sensor networks in the internet of things," in *Consumer Communications and Networking Conference (CCNC), 2012 IEEE*, 2012, pp. 169-173.

[88] H. Y. Tung, K. F. Tsang, H. C. Tung, V. Rakocevic, K. T. Chui, and Y. W. Leung, "A WiFi-ZigBee building area network design of high traffics AMI for smart grid," *Smart Grid and Renewable Energy*, vol. 3, p. 324, 2012.

[89] J. Wang and V. C. Leung, "Comparisons of home area network connection alternatives for multifamily dwelling units," in *New Technologies, Mobility and Security (NTMS), 2011 4th IFIP International Conference on*, 2011, pp. 1-5.

[90] P. L. Shrestha, M. Hempel, Y. Qian, H. Sharif, J. Punwani, and M. Stewart, "Performance modeling of a multi-tier multi-hop hybrid sensor network protocol," in *Wireless Communications and Networking Conference (WCNC), 2013 IEEE*, 2013, pp. 2345-2350.

[91] N. Afrin, J. Brown, and J. Y. Khan, "Design of a buffer and channel adaptive LTE semi-persistent scheduler for M2M communications," in *Communications (ICC), 2015 IEEE International Conference on*, 2015, pp. 5821-5826.

[92] A. Laya, L. Alonso, and J. Alonso-Zarate, "Is the random access channel of LTE and LTE-A suitable for M2M communications? A survey of alternatives," *Communications Surveys & Tutorials, IEEE*, vol. 16, pp. 4-16, 2014.

[93] A. Yarali, "Wireless mesh networking technology for commercial and industrial customers," in *Electrical and Computer Engineering, 2008. CCECE 2008. Canadian Conference on*, 2008, pp. 000047-000052.

[94] A. Biral, M. Centenaro, A. Zanella, L. Vangelista, and M. Zorzi, "The challenges of M2M massive access in wireless cellular networks," *Digital Communications and Networks*, vol. 1, pp. 1-19, 2015.

[95] "Institute of Electrical and Electronics Engineers, Inc, IEEE Std. 802.15.4-2003 "Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks(LR-WPANs), New York, IEEE Press. October 1, 2003."."

[96] A. F. Molisch, K. Balakrishnan, D. Cassioli, C.-C. Chong, S. Emami, A. Fort, *et al.*, "IEEE 802.15. 4a channel model-final report," *IEEE P802*, vol. 15, p. 0662, 2004.

[97] J. Dias, F. Ribeiro, R. Campos, M. Ricardo, L. Martins, F. Gomes, *et al.*, "Evaluation of an RPL/6LoWPAN/IEEE 802.15. 4g Solution for Smart Metering in an Industrial Environment."

[98] A. Milenković, C. Otto, and E. Jovanov, "Wireless sensor networks for personal health monitoring: Issues and an implementation," *Computer communications,* vol. 29, pp. 2521-2533, 2006.

[99] N. F. Timmons and W. G. Scanlon, "Analysis of the performance of IEEE 802.15.4 for medical sensor body area networking," in *Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004. 2004 First Annual IEEE Communications Society Conference on*, 2004, pp. 16-24.

[100] P. Kulkarni, S. Gormus, F. Zhong, and B. Motz, "A self-organising mesh networking solution based on enhanced RPL for smart metering communications," in *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2011 IEEE International Symposium on a*, 2011, pp. 1-6.

[101] C. Anton-Haro and M. Dohler, *Machine-to-machine (M2M) Communications: Architecture, Performance and Applications*: Elsevier, 2014.

[102] F. Österlind and A. Dunkels, "Approaching the maximum 802.15. 4 multi-hop throughput," 2008.

[103] F. Shurui, L. Jingbo, S. Hexu, and W. Rui, "Throughput analysis of GTS allocation in beacon enabled IEEE 802.15.4," in *Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on,* 2010, pp. 561-565.

[104] P. Park, C. Fischione, and K. H. Johansson, "Performance analysis of GTS allocation in beacon enabled IEEE 802.15. 4," in *Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON'09. 6th Annual IEEE Communications Society Conference on,* 2009, pp. 1-9.

[105] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, "Transmission of IPv6 packets over IEEE 802.15. 4 networks," *Internet proposed standard RFC,* vol. 4944, 2007.

[106] J. Hui and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15. 4-Based Networks, IETF RFC 6282," ed: September, 2011.

[107] "IEEE, "Guidelines for 64-bit Global Identifier (EUI-64) Registration Authority", http://standards.ieee.org/regauth/out/tutorials/EUI64.html."

[108] H. Balakrishnan, V. N. Padmanabhan, S. Seshan, and R. H. Katz, "A comparison of mechanisms for improving TCP performance over wireless links," *Networking, IEEE/ACM Transactions on,* vol. 5, pp. 756-769, 1997.

[109] J. W. Hui and D. E. Culler, "IPv6 in low-power wireless networks," *Proceedings of the IEEE,* vol. 98, pp. 1865-1878, 2010.

[110] Z. Shelby and C. Bormann, *6LoWPAN: The wireless embedded Internet* vol. 43: John Wiley & Sons, 2011.

[111] O. Modeler, "OPNET Technologies Inc http://www.riverbed.com/products/steelcentral/opnet.html," ed, 2009.

[112] "open-zb--OpenSource Toolset for IEEE 802.15.4 and Zigbee,http://www.open.-zb.net."

[113] "OPNETWORK 2010 1508 Undertanding TCP/IP Model Internals and Interfaces https://enterprise14.opnet.com/4dcgi/CL_SessionDetail?ViewCL_SessionID=4211."

[114] "OPNETWORK 2007 1510 Understanding IP Model Internals and Interfaces. https://enterprise14.opnet.com/4dcgi/CL_SessionDetail?ViewCL_SessionID=3186."

[115] D. Zhao and X. Shen, "Design of a large scale multi-cluster wireless sensor network," in *Communications and Networking in China, 2009. ChinaCOM 2009. Fourth International Conference on*, 2009, pp. 1-5.

[116] J. Misic and R. Udayshankar, "Slave-Slave Bridging in 802.15.4 Beacon Enabled Networks," in *2007 IEEE Wireless Communications and Networking Conference,* 2007, pp. 3890-3895.

[117] B. Latré, P. D. Mil, I. Moerman, B. Dhoedt, P. Demeester, and N. V. Dierdonck, "Throughput and delay analysis of unslotted IEEE 802.15. 4," *Journal of networks,* vol. 1, pp. 20-28, 2006.

[118] M. Vodel and W. Hardt, "Data aggregation in resource-limited wireless communication environments—Differences between theory and praxis," in *Control, Automation and Information Sciences (ICCAIS), 2012 International Conference on*, 2012, pp. 208-213.

[119] X. Cao, J. Chen, Y. Sun, and X. Shen, "Maximum Throughput of IEEE 802.15.4 Enabled Wireless Sensor Networks," in *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE,* 2010, pp. 1-5.

[120] *J. Geier, Wireless LANs Implementing High Performace IEEE 802.11 Networks., Second ed. United States of America: Sams Publishing, 2002.*

[121] M. Petrova, J. Riihijärvi, P. Mähönen, and S. Labella, "Performance study of IEEE 802.15. 4 using measurements and simulations," in *Wireless communications and networking conference, 2006. WCNC 2006. IEEE,* 2006, pp. 487-492.

[122] D. Chen and P. K. Varshney, "QoS Support in Wireless Sensor Networks: A Survey," in *International Conference on Wireless Networks*, 2004, pp. 1-7.

[123] Z. M. Fadlullah, M. M. Fouda, N. Kato, A. Takeuchi, N. Iwasaki, and Y. Nozaki, "Toward intelligent machine-to-machine communications in smart grid," *Communications Magazine, IEEE,* vol. 49, pp. 60-65, 2011.

[124] J. Rezgui, S. Cherkaoui, and D. Said, "A two-way communication scheme for vehicles charging control in the smart grid," in *Wireless Communications and Mobile Computing Conference (IWCMC), 2012 8th International*, 2012, pp. 883-888.

[125] Y. Zhang, R. Yu, M. Nekovee, Y. Liu, S. Xie, and S. Gjessing, "Cognitive machine-to-machine communications: visions and potentials for the smart grid," *IEEE Network,* vol. 26, pp. 6-13, 2012.

[126] S. Pandey, M. J. Choi, M. S. Kim, and J. W. Hong, "Towards management of machine to machine networks," in *Network Operations and Management Symposium (APNOMS), 2011 13th Asia-Pacific*, 2011, pp. 1-7.

[127] C. Wang, B. Li, K. Sohraby, M. Daneshmand, and Y. Hu, "Upstream congestion control in wireless sensor networks through cross-layer optimization," *Selected Areas in Communications, IEEE Journal on,* vol. 25, pp. 786-795, 2007.

[128] G.-S. Ahn, S. G. Hong, E. Miluzzo, A. T. Campbell, and F. Cuomo, "Funneling-MAC: a localized, sink-oriented MAC for boosting fidelity in sensor networks," in *Proceedings of the 4th international conference on Embedded networked sensor systems*, 2006, pp. 293-306.

[129] "T.S.Rappaport, Wireless Communication Principles and Practice. New Jersey, 1996. ."