TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

NADER DANESHFAR
PERFORMANCE ENHANCEMENT MECHANISM OF IEEE 802.11AH MACHINE COMMUNICATION SYSTEM

Master of Science thesis

Examiner: Prof. Mikko Valkama
Dr. Ali Hazmi
Examiner and topic approved by the
Faculty Council of the Faculty of
Computing and Electrical Engineering
on 5th November 2014

ABSTRACT

NADER DANESHFAR: Performance Enhancement Mechanism of IEEE 802.11AH Machine Communication System
Tampere University of Technology
Master of Science thesis, 78 pages
May 2015
Master's Degree Programme in Information Technology
Major: Communication Systems and Networks
Examiner: Prof. Mikko Valkama
Dr. Ali Hazmi
Keywords: IEEE 802.11AH, IoT, Restricted Access Window, Sectorization, Performance optimization, Dynamic Analysis

As the Internet gets more populated and the number of devices increase dramatically, demanding connectivity anytime, anywhere and for everything, the urge for a novel concept is raised. Consequently, Internet of Things (IoT) is introduced to shed a light on the vision of the future Internet with tremendous amount of "things" interconnected to each other while utilizing various technologies for different applications. As a wide range of wireless technologies are developed and are extensively used worldwide, IEEE 802.11 working group for WLAN standards is developing a new amendment referred as IEEE 802.11AH targeting mainly the IoT based applications. The new amendment has inherited many characteristics from the legacy IEEE 802.11 while benefiting from new enhanced features defined specifically for IoT and Machine to Machine communications (M2M) systems. Ultimately, IEEE 802.11AH which has been defined to operate in sub-1 GHz band, is expected to support high number of simultaneous connections up to 6000 devices for a 1 km coverage range.

This thesis implements some of the enhanced features for IEEE 802.11AH and conducts the corresponding evaluation based on a developed simulator. The aforementioned simulator has been compared to a Markov chain based analytical model, developed in this research. The results have shown that the developed system level simulator is following the results from the modeled network with high accuracy.

The developed system level simulator has been used in performance evaluation of the IEEE 802.11AH main features like the restricted access window (RAW) and sectorization schemes in the case of single and multiple APs deployments scenarios. It is concluded that the implementation of these features, help to improve IEEE 802.11AH overall performance. The performance measures considered in this evaluation are throughput, energy efficiency and average delay in sending successful packets, respectively. Moreover, for resolving the coverage requirements there is a trade-off in using single AP or multi AP configuration. Implementing more APs results in more network capacity while causing additional interference to the network. The RAW and sectorization mechanisms can fortunately reduce this interference by minimizing the hidden node probability and mitigating against the overlapping BSS resulting problems.

PREFACE

This thesis is carried out in completion of the Master of Science (MSc) degree in the department of Electronics and Communications Engineering at Tampere University of Technology during the year 2014-2015. The related research is made in the Internet of Things program of DIGILE (Finnish Strategic Centre for Science, Technology and Innovation in the field of ICT) and is funded by the Finnish Funding Agency for Technology and Innovation (TEKES).

Foremost, I would like to express my sincere appreciation to my supervisor Professor Mikko Valkama for his support and the opportunity he provided me with, to conduct research in a professional atmosphere. I would also like to thank my supervisor Doctor Ali Hazmi for his patience, enthusiasm and motivation. His guidances in all terms of this research, through which I learned many things for increasing my research quality, are invaluable. My thanks are extended to Mr. Felipe Del Caprio, Mr. Parth Amin and Mr. Johan Torsner from Ericsson Research for their dedication. I am thankful to Prof. Yevgeni Koucheryavy, Dr. Sergey Andreev and Aleksandr Ometov for the fruitful cooperation we had on this research work.

I would like to thank all my friends in Tampere specially Saeed Afrasiabi, Mona Aghababaee, Vida Fakour, Sajjad Nouri, Kamiar Radnosrati and Farid Shamani. I am grateful to have such inspiring and gentle circle of friends by my side. My special thanks goes to Orod Raeesi for his attitude towards sharing his experience and invaluable help to me in every possible way he could. I also want to thank my friends in Ankara: Minoo Pourhassan, Mohammad Rafighi and Hadi Sojoudi, for their unconditional kindness. There is not a day passing by without me getting more thankful for their unlimited care and support.

Finally, my heartfelt thanks extends to my father, my mother and my lovely sister for their dedication, devotion and patience. I appreciate their efforts and constant support in every possible aspect of my life. I owe every bit of my achievements to them and I would never be in this stage in my life without their enthusiasm.

Nader Daneshfar
May 15, 2015
Tampere

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS AND SYMBOLS

ACK	Acknowledgement
AID	Association Identifier
AP	Access Point
BSA	Basic Service Area
BSS	Basic Service Set
CA	Channel Access
CCA	Clear Channel Assessment
CS	Carrier Sensing
CSMA/CA	Carrier Sensing Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sensing Multiple Access with Collision Detection
CSMA	Carrier Sensing Multiple Access
CTS	Clear to Send
CW	Contention Window
DCF	Distributed Coordination Function
DS	Distribution System
DSSS	Direct Sequence Spread Spectrum
ESS	Extended Service Set
FC	Fame Control
FCS	Frame Check Sequence
FHSS	Frequency Hopping Spread Spectrum
GI	Guard Interval
HCF	Hybrid Coordination Function
IBSS	Independent Basic Service Set
IEEE	Institute of Electrical and Electronics Engineers
IR	Infrared
ISM	Industrial, Scientific and Medical
LAN	Local Area Network
LLC	Logical Link Control
MAC	Medium Access Control
MCS	Modulation and coding Scheme
MSDU	Maximum Data Unit Size
NAV	Network Allocation Vector
NDP	Null DATA Packet
NED	Network Definition
NIC	Network Interface
OBSS	Overlapping Basic Service Set
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open System Interconnection
PCF	Point Coordination Function
PER	Packet Error Ratio
PHY	Physical Layer
PLCP	PHY Layer Convergence Protocol
PMD	PHY Medium Dependent

QoS	Quality of Services
RAW	Restricted Access Window
RF	Radio Frequency
RID	Response Indication Defferral
RTS	Request to Send
SLRC	STA Long Retry Counter
SSRC	STA Short Retry Counter
STA	Station
TIM	Traffic Indication Map
TXOP	Transmit Opportunity
WLAN	Wireless Local Area Network

1. INTRODUCTION

Wireless communications have been the center of attention as of their evolution over the past three decades, and having wide range of operation distances makes them a premium solution for being utilized in tackling everyday problems. Forming a base for the Internet, networks with just a few hundred connections took a leap towards expanding to interconnecting billions of devices with no geographical limitations. Meanwhile, growth in quantity of various complex technologies was inevitable. As of the day of formation, the Internet has been a living entity, evolving and changing everyday while new technologies are being introduced and more devices are added every other second. In addition to proliferation of more connected devices, they are becoming more powerful with various technologies and sensors on-board [19].

Implying connectivity among diverse type of services and various devices such as computers, sensors, RFID tags, appliances, vehicles and etcetera, opens doors for a new paradigm called the Internet of Things (IoT). This new concept is driven by the expansion of Internet towards the future where an "always connected" scheme is of a high demand anytime, anywhere and for everything. Description entails a vision that any object becomes part of an enormous entity of interconnected things while being individually accessible and uniquely identified. Upon getting access to the huge amount of comprehensive data provided by sets of devices, the impact of utilizing this concept will ultimately emerge in professional, social and personal environments [24]. International Data Corporation (IDC) predicts the growth of IoT to 212 billion "things" connected globally by the end of 2020 including over 30 billion installed autonomously connected smart devices serving various applications for smart systems, enterprises and private consumers [42]. Undoubtedly, developing a new technology for meeting the requirements of IoT is of a high importance.

There are many wireless technologies developed and being extensively used that can act as a infrastructure for developing new technologies like IoT [32]. IEEE 802.11 standard [5] is one of the most popular developed standards aiming for high throughput applications using wireless medium. Already having an infrastructure for connectivity over Wi-Fi using IP which is spread all around the world and is being highly used, makes IEEE 802.11 a top choice for implementing IoT services.

Consequently, IEEE 802.11AH [3] has been defined and is under development for IoT purposes.

Chapter 2 of this thesis discusses about the fundamentals of IEEE 802.11AH pointing out the similarities and differences it possess with IEEE 802.11 standard. Basic elements and architecture of a simple network is described and the use cases for this new amendment is introduced. Furthermore, architecture of the MAC and PHY layer is outlined in more details.

Due to the development of new IEEE 802.11AH amendment, there are several enhancements which are presented and discussed in Chapter 3. It is vital to get a good understanding of the newly developed technologies, which enables the implementation of current enhancements into applications and bringing them to practice. Having in mind the wide range of enhancements, this chapter focuses on the new developments of the MAC layer which are enabling the design of a more performance optimized networks.

In the standardization process, evaluating the performance of the proposed enhancements in an amendment is of a high importance. Hence, a reliable system level simulator has been developed in this research specifically for IEEE 802.11AH amendment. Simulation environment and the corresponding software used as a platform to create it, as well as all the settings for various parts of the simulation has been discussed in Chapter 4.

Chapter 5 evaluates the performance of networks implemented based on IEEE 802.11AH enhancements. In the first part of this chapter a comparison between a developed analytical model based on Markov chain and the system level simulator is conducted to confirm the accuracy of the simulator. Next, a channel accessing mechanism known as Restricted Access Window (RAW) is being evaluated, aiming to tackle the complexities and draw-backs caused by high number of collisions due to the congestion of traffic in the network. A comparison between normal legacy DCF and the new RAW mechanism has also been conducted to make the optimization more tangible. Finally, a simulation with more complex channel access mechanism, called sectorization, is performed to cope with interference in cases with several Access Points (AP) deployed.

The conclusions and discussion about the impact of the implemented enhanced mechanisms are presented in Chapter 6.

2. FUNDAMENTALS OF IEEE 802.11AH

IEEE 802.11^{TM} is another name for Wireless Local Area Network (WLAN) that is being developed by IEEE Standard Association which is a well known organization for developing worldwide technologies under IEEE trademark. Currently operating at 2.4 GHz and 5 GHz bands, IEEE 802.11 provides high data rate along with low cost and ease of deployment which makes it one of the most popular technologies for indoor use nowadays. Various versions and amendments of IEEE 802.11 standards have been developed in order to satisfy specific requirements and different use cases. Following are some of the amendments and their respective descriptions summarized in Table 2.1.

IEEE 802.11AH is an amendment defined under the main IEEE 802.11 protocol to meet the needs for specific use cases in WLAN systems. It mainly targets wireless networks with high number of devices in indoor and outdoor environment with relatively low to moderate traffic and limited power resources. Operating at sub 1 GHz, IEEE 802.11AH can provide relatively extended transmission range compared to the common IEEE 802.11n which operates at 2.4 or 5 GHz.

In this chapter, first the IEEE 802.11 networks basic elements will be discussed. Second, some of the use cases defined for IEEE 802.11AH standard will be intro-

Table 2.1 *The evolution of the IEEE 802.11 standards [51]*

Protocol	**Maximum Data Transfer Speed**	**Frequency**	**Highest Order Modulation**	**Channel Bandwidth**	**Antenna Configuration**
802.11a	54 Mbps	5 GHz	64 QAM	20 MHz	1 × 1 SISO
802.11b	11 Mbps	2.4 GHz	11 CCK	25 MHz	1 × 1 SISO
802.11g	54 Mbps	2.4 GHz	64 QAM	25 MHz	1 × 1 SISO
802.11n	6.5 to 600 Mbps	2.4/5 GHz	64 QAM	20 and 40 MHz	Up to 4 × 4 MIMO
802.11ac	6.5 Mbps to 6.933 Gbps	5 GHz	256 QAM	20, 40, 80 and 160 MHz	Up to 8 × 8 MIMO

duced and shortly elaborated. Finally, in the latter sections, MAC and PHY layer architectures in the new IEEE 802.11AH amendment will be presented which has some common properties with the previously developed standards.

2.1 Motivation

In the recent years, the Internet has started to evolve rapidly from a network of networks containing few hundred users to a massive interconnected devices that use various technologies. This process have introduced several technologies to the network standards to enable utilizing resources for vast amount of diverse applications. IoT is one of the major technologies presented for various applications. It is aimed to provide support for connectivity anytime, anywhere and for anything in the world of information and communication technology.

Considering the very high number of communicating devices, the newly introduced IEEE 802.11AH, will face a major challenge in handling these situations where tremendous number of entities require connection almost simultaneously. Furthermore, devices that participate in these networks are intended to operate with very little power supplies that are non-changeable. This issue adds another degree of limitations to the physical and operational design.

2.1.1 Basic Elements of 802.11 Networks

Wireless networks consist of various elements which enable data transfer. They also form the fundamental characteristics of the network. The basic components are being illustrated in Figure 2.1

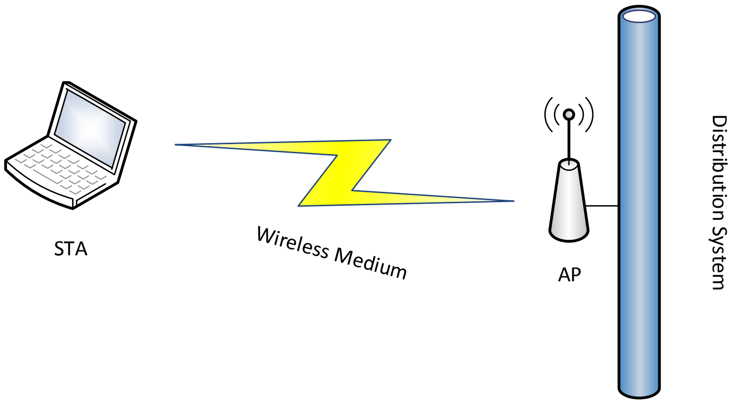


Figure 2.1 Basic components of 802.11 LANs [31]

Station (STA)

Simply, stations in WLANs are addressable battery operated devices with wireless Network Interfaces (NIC) enabling them to connect to network. Portability is not a must though, because in some conditions wireless networking is being used to avoid excessive cabling [16]. Stations, despite of being in the same network, may have different characteristics which distinguishes their unique functionalities. A network must have at least one STA to operate.

Access Point (AP)

A device that enables access of network to distribution system for its associated stations is called an access point. APs (as shown in Figure 2.1) are responsible to perform bridging functionalities between different types of mediums [16] [31]. Having an AP in network, STAs are obliged to associate with and communicate through it. Therefore AP has the ability to control the network performance and data flow. All the messages generated by STAs to various destinations are sent to the AP and it has the responsibility to forward the messages to their corresponding destinations.

Wireless Medium

Messages from different devices need to be transmitted over a medium and this is being met by various physical layers standards that have been developed [16]. They can be categorized into Radio Frequency (RF) and infrared physical layer standards in IEEE 802.11 technologies whereas twisted pairs, coaxial cables and optical fibers are used in wired networks.

Distribution System (DS)

Interchanging data between several STAs connected to an AP and located in different wireless networks requires a type of backbone to enable APs to track and forward packets towards their final destination. This is made possible by implementing distribution system which is basically consists of a bridge and distribution system media.

Relay

Exchanging frames between STAs and an AP can be done through relays. A relay is a device that has a relay-STA and a relay-AP in order to be able to connect to its relay agents. A basic schematic of a functioning network with relay entity is illustrated in Figure 2.2.
Using relays, STAs are able to use higher data rates to transfer data and implement Transmit Opportunity (TXOP) sharing to access the channel. A TXOP is a period of time in which each STA can try to transmit as much packets as it can unless the required time to transmit the whole packet exceeds this period. This improves the energy consumption by decreasing the required time a STA needs to be active. The reason behind limiting relay function to two hops is to avoid further delay and complexity [3].

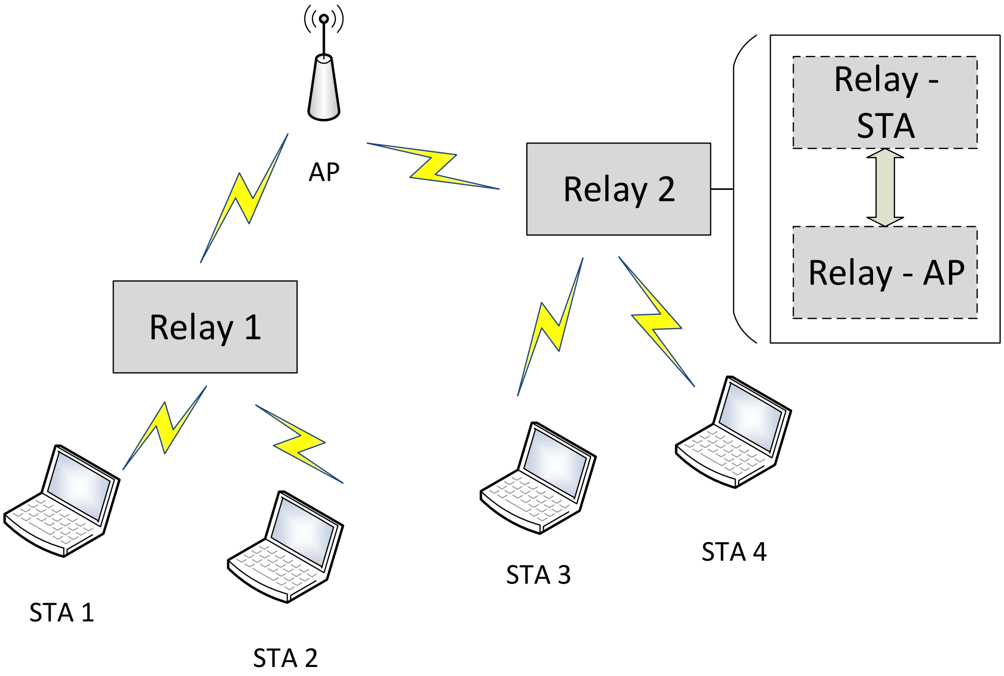


Figure *2.2 Structure of a relay entity in a network*

2.1.2 Network Architectures

A typical IEEE 802.11 network is called Basic Service Set (BSS) which is a block containing a number of STAs that have been successfully synchronized and are able to communicate with each other. The coverage area in which the STAs can remain connected is defined by the propagation characteristics of the wireless medium and is called Basic Service Area (BSA). A BSS does not generally refer to a particular area, due to the uncertainties of electromagnetic propagation. Generally, two types of BSSs exists as shown in Figure 2.3.

Independent BSS (IBSS)

An independent BSS, being the most basic type of IEEE 802.11 network, must contain at least two STAs to function properly. As illustrated in the left side of Figure 2.3, STAs are connected directly to one another and thus must be within their coverage range. This kind of Service area is mainly formed for short time purposes and is dissolved once the computer are out of each other's zones. Therefore they are sometimes called as ad-hoc networks or ad-hoc BSSs.

Infrastructure BSS

A simple instance of infrastructure BSS is shown in the right side of Figure 2.3. This type of network can be distinguished by the use of an AP in the network structure. All STAs must associate to their respective BSS APs. Consequently all communications, even an STA to STA message delivery, must be done through the AP. This means if one STA in the BSS wants to communicate with another STA in the same BSS which is in its own communication range, the transmission is done by two hops.

Although this may add some communication overhead compared to the version where STAs can connect directly to each other but this offers two major advantages as:

- The infrastructure BSS coverage area is determined by the maximum distance its AP can maintain successful data transmission. Thus as long as STAs are in a BSS, there is no limitation on two STAs. It is important to remind that STA need to maintain a neighbor relationship with all other STAs in the same BSS.
- Power-saving can be assisted by APs in infrastructure BSSs. An AP can detect when a STA enters power-saving mode and starts to buffer frames destined to it. Meanwhile, STAs running on battery power can periodically turn off their wireless transceiver to optimize their power efficiency.

These make the infrastructure mode a perfect option for IEEE 802.11AH scenarios and use cases which will be discussed further in section 2.2.

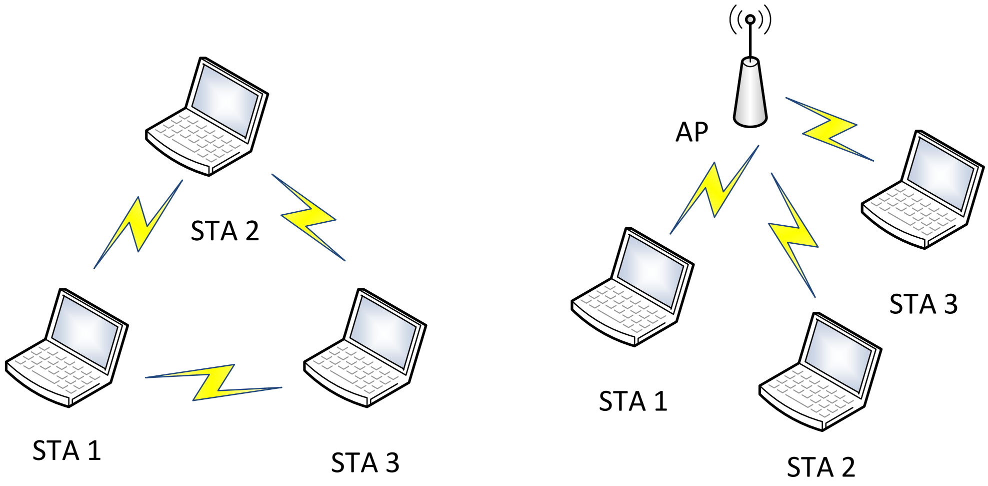


***Figure* 2.3** *Independent and infrastructure basic service sets (BSSs)*

Extended Service Set (ESS)

An Extended Service Set is a number of interconnected infrastructure BSSs via a backbone called Distribution System, where the APs communicate among themselves to forward traffic from one BSS to another and to enable the roaming of mobile stations between the BSSs. Utilizing this structure in IEEE 802.11 networks, as illustrated in Figure 2.4, limitless extension and arbitrary sized networks can be created.

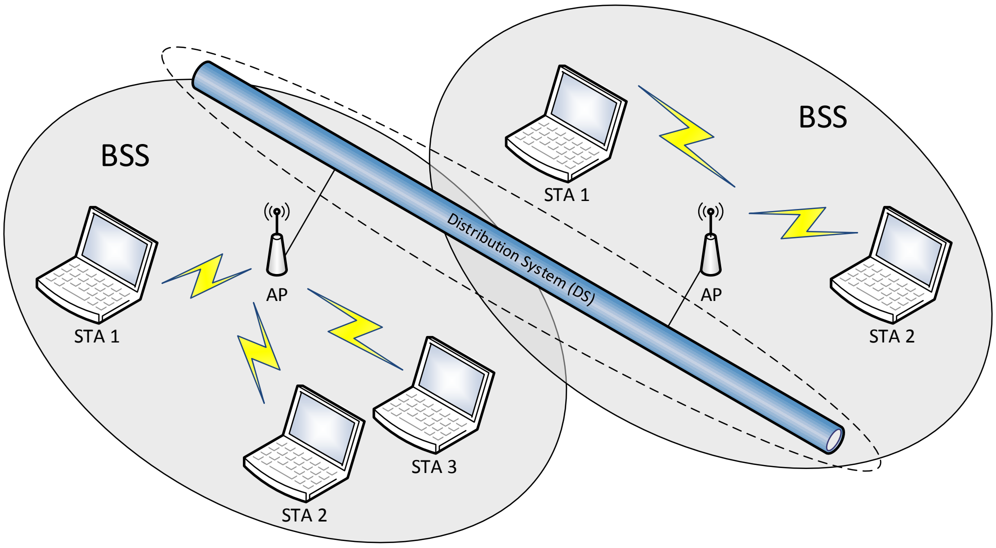


***Figure* 2.4** *Extended service sets (ESS)*

***Table 2.2** IEEE 802.11 network services*

Service	**Type**	**Description**
Distribution	Distribution	Service used by stations to exchange frames when its needed to be transmitted between two BSSs.
Integration	Distribution	Delivering frames to a wired network outside the wireless network.
Association	Distribution	Used to start a logical connection between a STA and an AP in order for the distribution system to deliver the frame properly.
Reassociation	Distribution	Enables STA mobility between BSSs by maintaining the established association with the previous AP.
Disassociation	Distribution	Removes the wireless station from the network.
Authentication	Station	Identification before establishing association.
Deauthentication	Station	Terminating authentication and association of an STA.

Furthermore, connectivity between STAs in different BSS is facilitated by forwarding of data through APs in each basic service set to the other. So by implementing ESSs, there is no boundary for network expansion.

2.1.3 Network Services

A Network technology, such as IEEE 802.11AH, can also be defined by its provided services. There are several services defined for two types of use in IEEE 802.11 for "Station" and "Distribution" purposes as illustrated in Table 2.2. Each of the aforementioned types are used for data delivery or management purposes [43]. The Table 2.2 summarizes a number of the most important services.

2.2 Use Cases

IEEE 802.11AH has already been introduced to many applications requiring the interaction between numerous devices. Supply chain logistics and asset tracking, industrial automation, health care systems, life assisting and etcetera have already been formulated into using this technology. Therefore the task group for IEEE 802.11AH have classified these use cases under 3 main categories as Sensors and meters, Backhaul sensor and meter data, and Extended range Wi-Fi [27]. In the following sections, these use cases will be discussed in detail to help understand the advantages of employing IEEE 802.11AH in various scenarios.

2.2.1 Sensors and Meters

Sensors and meters are simply act as data collecting devices. They are being implemented in different applications and various functions can be done by processing their collected information of the premises. They can monitor their surrounding environmental or physical conditions such as humidity, pressure, movement, sound and etcetera. Considering tons of applicable areas for these kind of sensors and due to the elevated possibility of high density deployment of sensors, IEEE 802.11AH is going to be highly used among these sensor devices for communication purposes.

Smart Grid - Meter to Pole

Smart grid can be seen as a new paradigm for power industry rather than a new technology. It can be conceptualized as an infrastructure of electrical grid merged with IT communication systems to provide better real-time management over electrical services [36].

There are various forms and application areas in which smart grids can be beneficiary such as electronic control, metering, power usage optimization and remote power distribution control. Thus, wireless sensor networks can be implemented and enable smart grids to provide these services in more reliable and secure manner, which is also one of high concerns in deploying smart grids [64]. Figure 2.5 illustrates a simple scenario for smart grid applications.

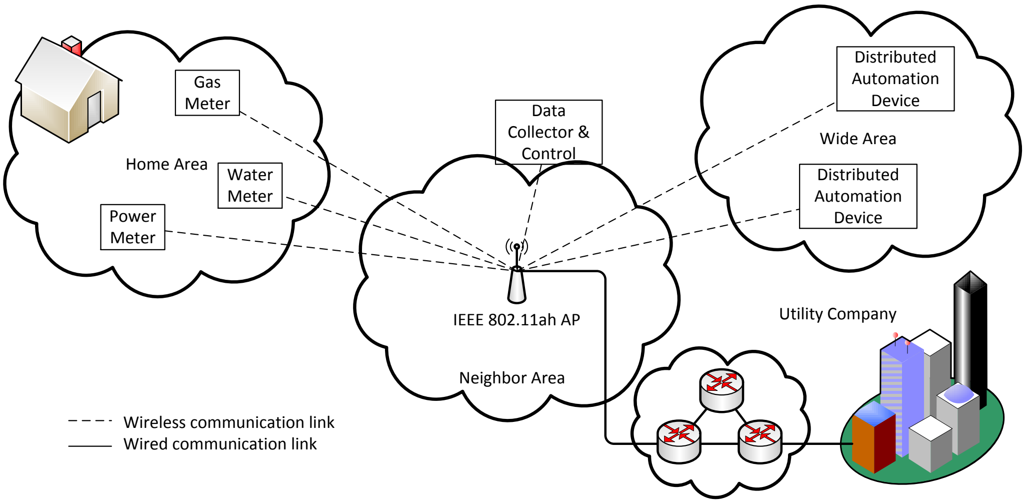


***Figure* 2.5** *A scenario for deploying smart grid infrastructure using IEEE 802.11AH [18]*

Environmental/Agricultural Monitoring

Due to the increase in production and inevitable evolving process for monitoring the suitable conditions for cultivation, sensors play an undeniable role in these application implementation. Moreover, having a real-time data from surroundings and earth-level information is highly useful for predicting and preventing different unwanted occurrences. These can be categorized in natural disasters (e.g. flood, earthquake, forest fire, green house gas emission) and environmental conditions (e.g. pressure, humidity, temperature, water-level) that their data can be collected by sensors and delivered for use in a fast and precise manner. IEEE 802.11AH enables the use of sensors in higher mobility, lower deployment cost and efficient employment of resources [44].

There are several other applications for environmental monitoring which can be employed for pollution detection, energy generation and live stock (e.g. animals) condition monitoring [56].

Industrial Process Sensors

Industrial automation processes such as process customization, production control and quality check can be done using proper employment of sensors. Petroleum refinement, metal industry and pharmacy are the most applicable use cases for this technology. Reliability, real-time communication, energy efficiency, high number of input/output data points and vast area of coverage are the key concerns which can be covered relatively by using IEEE 802.11AH as the underlying connecting protocol [33].

Healthcare

There are two main types of healthcare scenarios, namely Indoor and Outdoor applications. In indoor mode, IEEE 802.11AH can be used to implement the wider wireless network needed for scenarios such as hospital or clinic, elderly care or independent living and personal fitness [48]. On the other hand, in outdoor mode, it is proposed in [54] that this technology would be exploited in emergency conditions where other networks infrastructures are not functional. Here, IEEE 802.11AH can be deployed relatively quickly and support numerous devices requiring interconnection.

Home/Building Automation

As for many suitable existing devices in our living environment, especially at homes, sensors in home automation can be deployed for outdoor/indoor temperature monitoring and control, audio/video visualization, kitchen appliances automation and remote control, security and safety features (e.g. intrusion/presence detection, entrance lock/unlock, smoke/gas detection) and multi-dwelling unit deployment for energy management system [27] [40].

Traffic Information Dissemination

Vehicles, or any means of transportation, in a coverage area of an AP in traffic information network can receive various information broadcasted. These information can help improving navigation by providing local traffic updates and GPS data. These infrastructures may also be used for promotions in local businesses. In addition, STAs can also request customized information from APs such as list of nearby gas stations, restaurants, ATMs and general city services [29].

2.2.2 Backhaul Sensor/Meter Data

Implementing IEEE 802.15.4g for devices and sensors in industrial scenarios due to their ability to operate on battery for a considerable amount of time, is desirable. However, its transmission range and data rates are relatively low. Another proposed use case by task group for IEEE 802.11AH is to cover the gap between the main servers and databases with these low range wireless networks. IEEE 802.11AH APs form a backhaul connection between IEEE 802.15.4g or IEEE 802.15.4 routers and remote servers so the gathered information from leaf sensors can easily be forwarded to farther networks for better network management [68].

Network operation and management can be considered into two categories, namely network optimization and power saving. Former one can be achieved through network diagnostic and troubleshooting, load balancing, efficient channel utilization and location services where the latter is done by optimizing different states of the network's devices by considering the amount of data they want to transfer and the type of message delivery in various number of destinations [62].

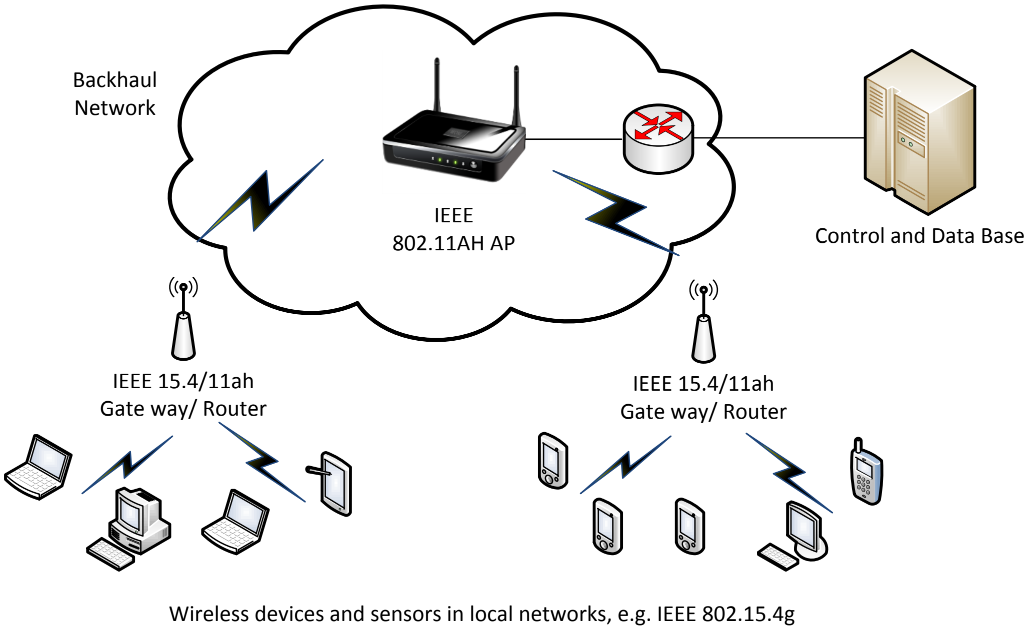


Figure 2.6 *Backhaul networks aggregation use case for meters and sensor networks*

2.2.3 Extended Range Wi-Fi

Different IEEE 802.11x technologies posses advantages discerning them of others. IEEE 802.11AH has a wider range and supports different data rates that enables the extension for other IEEE 802.11x family standards.

Outdoor Extended Range Hotspot

Being able to provide a robust network coverage in an area, increases the interest to use WLANs for outdoor network extension. Considering mobility, traffic type and rate, environmental condition reliability and security is of a high importance. Using lower frequency bands, IEEE 802.11AH can provide higher extended range and throughput while covering a major portion of the aforementioned requirements makes it a demanding choice for various Wi-Fi applications [27]. Nowadays, hotspots are used all around the world for implementing various use cases such as:

- Extended home coverage
- Shopping mall wireless Internet access
- Campus wide coverage
- Stadiums/Sport facilities

Moreover, the use of this technology in establishing instant WLANs in temporarily situations like exhibitions and rural sport events to provide better services are on the horizon.

Outdoor Wi-Fi for Cellular Traffic Offloading

Emerging new technologies force the urge for accessing Internet on demand for users and thus leading to mobile traffic explosion in recent years by increasing number of mobile users and devices on daily basis. Therefore, as illustrated in Figure 2.7, cellular network providers tend to use procedures to offload the traffic to help prevent saturation and consequently network halt.

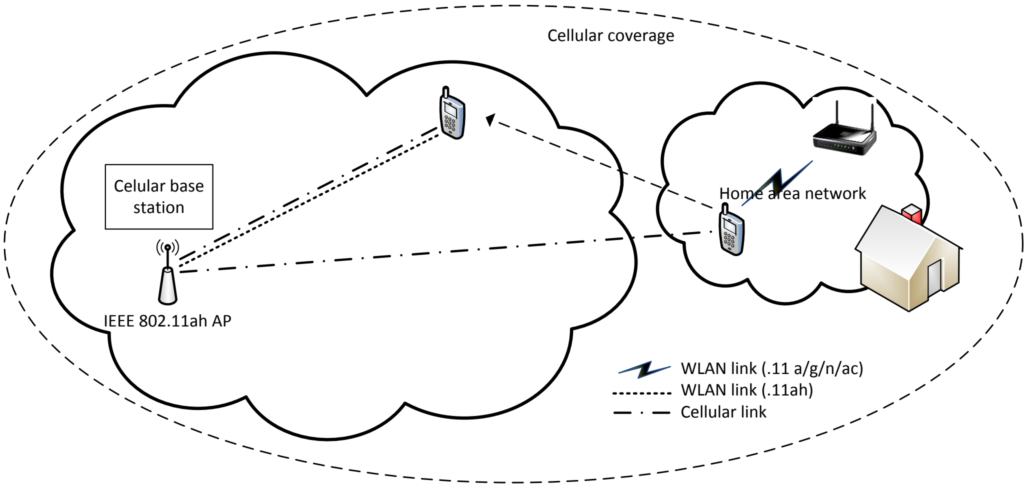


Figure* *2.7 *Outdoor Wi-Fi for cellular traffic offloading*

Current IEEE 802.11 b/g/n/ac technologies serve as a reasonable candidate to approach this problem but also lack to provide desirable coverage with adequate throughput. In the contrary, IEEE 802.11AH aims to meet these requirements by having a relatively large coverage area of approximately 1 km and enough data rate to support mobile traffic offloading which makes it a perfect candidate to overcome this issue [37].

2.3 MAC Layer Architecture

Of all the various services, the Medium Access Control (MAC) layer enables addressing and channel access control that makes it possible for multiple stations to communicate on a network. MAC layer is the lower sub-layer in layer 2 (i.e Data

Link Layer) of the Open System Interconnection (OSI) model. Being a member of IEEE 802 LAN family, IEEE 802.11 benefits from IEEE 802 48-bit global address space which makes it compatible with Ethernet in the link layer. Once the package is sent in unicast, this is the key factor enabling MAC to distinguish and decode the package destined to it [51].

Being a part of one service set and being able to communicate within all associated devices, all the STAs need to follow certain set of rules, called protocols, that makes it possible for MAC layer to control packet transmission in every single STA. In designing a MAC protocol the key issue is using the control mechanism over the transmitting STAs.

Carrier sensing (CS) is another important issue in IEEE 802.11 WLANs. While a STA in not using the channel for transmissions, it requires a mechanism that enables the STA to get information about channel status. For this, CS is used to determine whether the channel is idle or busy. Two types of CS that are introduced and used in WLANs are: Clear Channel Assessment (CCA) that is a physical carrier sensing done in PHY layer and Network Allocation Vector (NAV) which is a virtual kind of carrier sensing and is conducted in MAC layer.

IEEE 802.11 MAC, like Ethernet, uses Carrier Sensing Multiple Access (CSMA) mechanism to control accessing the shared medium. But unlike Ethernet which uses Collision Detection (CSMA/CD), it employs Collision Avoidance (CSMA/CA) to handle collisions. Both techniques sense the media and wait until it is "idle" and then start the transmission with their defined algorithms but if the medium is detected to be "busy", that indicates ongoing transmission from other devices, the device trying to access the channel defers its transmission.

2.3.1 MAC Frame Structure

All IEEE 802 family members use formats with similar characteristics so to make frame delivery between IEEE 802.11 wireless networks and IEEE 802.3 wired networks easier. Having the maximum similarities, they have some differences. One of the differences is frame size. It emerges from their unique capabilities in transporting distinctive frames sizes. This means it may happen that while moving data from wireless to wired network, the AP encounters a data frame that is too large to be handled in wired networks [25]. Since most of the networks use TCP/IP, and the IP has a maximum transmission unit, this may merely be a problem because the IP maximum transmission unit value is less than the Ethernet maximum data frame size.

Frame Types

Unlike IEEE 802.3 Ethernet which has just one type of MAC frame, IEEE 802.11 defined three different MAC frame types:

Management Frames

A high portion of the exchanged frames in IEEE 802.11 are management frames. They are used by STAs to join or leave a network, thus being able to transmit data through DS. All the association, authentication, probe and beaconing are of this type. Management frames do not carry any upper layer information in their bodies.

Control Frames

Control frames are mainly used to assist data frames with their delivery. Therefore, they must be received by all STAs and transmitted in the most robust and reliable data rates possible. They play an important role in reducing collisions while they are being used in channel clearance, providing acknowledgments and channel acquiring process.

Data Frames

Actual data transfer is done by these type of frames. Data frames carry data from higher-layer protocols. There are also Null data frames to facilitate power saving mode and inform the AP of the changes made in power saving mechanism. There are 8 types of data frames, 2 of which is used by Distributed Coordination Function (DCF).

Frame Format

Every IEEE 802.11AH MAC frame format consists of three main parts: MAC Header, Frame body and FCS. The first two are variable in size depending on the frame type and Maximum Data Unit Size (MSDU) but the latter one, Frame Check Sequence (FCS), is fixed in size and is used to provide detecting errors in MAC layer level.

As Figure 2.8 illustrates, the MAC frame in IEEE 802.11AH consists of several components that are combined in a fixed manner once the MAC frame is being generated. All of the fields presented posses special functionalities but not all are

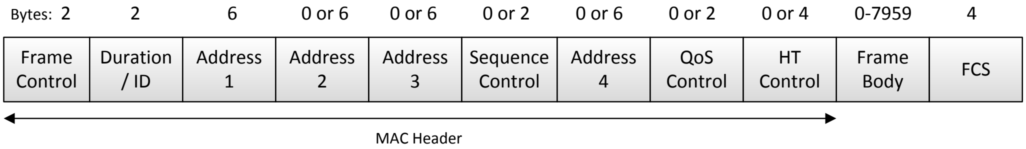


Figure 2.8 *IEEE 802.11AH MAC frame format [14]*

present in every frame. The first three and the last frame (i.e. Frame Control, Duration /ID, Address 1 and FCS) construct the basic MAC frame whereas the other fields are present in different certain frames type. More description on these fields follows:

Frame Control

The first three subfields are constant: Protocol Version, Type, and Subtype. Remaining subfield are dependent on the frame type and subtype subfields. The value of the type subfield determines the presence of other subfields as power management, fragmentation, frame protection and etcetera.

Duration/ID

Same as previous field, the contents to Duration/ID field varies with respect to frame type and subtype. Transmission of the frame is set to be whether in the contention free period and with respect to quality of the sender's services. This field is mainly used to set the NAV, indicating the amount of time needed for successful transmission of the MAC frame in the channel. This value is set based on microseconds.

Address fields

Up to 4 address fields can be present in a MAC frame. When all present, they provide source, destination, receiving station and transmitting station addresses. In scenarios that require STAs to scan the area to discover the existing 802.11 networks by means of probe request and response frames, one of the address fields can contain the BSS identifier.

Sequence Control

This field consists of two subfields: fragment number and sequence number. These two values keep track of transmitted and received fragmented data parts when the original frame size is too large for the destination network.

QoS Control

Delivers the Quality of Service (QoS) requirements of the STAs that has QoS fields set to 1 and demand certain network quality in data transmission.

HT Control

HT Control field is present only if the Control Wrapper frame is used as control frame subtype. This field depicts information about more physical settings like modulation and coding schemes, antenna selection and link adaptation techniques.

Frame Body

This is the field that contain actual data and is specific to every frame type. The variable length of this field allows flexibility in different networks regarding their specific attributes. Thus, the maximum size for Frame Body size is determined by the maximum length for MSDU plus the security overhead.

FCS

The FCS field's only purpose is to provide error detection in receiver's side to erroneous data received by implementing a 32-bit CRC checksum mechanism. This is being calculated over all of the MAC frame's fields containing the MAC Header and Frame Body.

2.3.2 MAC Access Methods

Accessing the shared wireless medium by devices impose different challenges that can be tackled by offering different access functions [43]. Several methods has been offered by IEEE 802.11 to facilitate this application as shown in Figure 2.9. This can be done by implementing a set of functions called coordination functions, a number of which, is being introduced below:

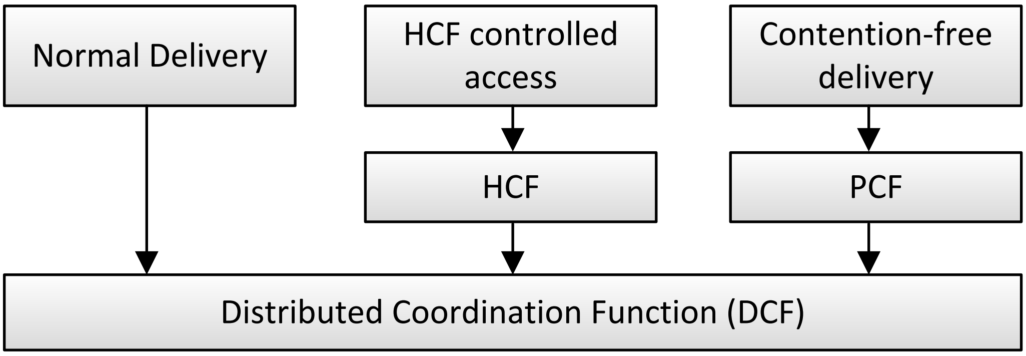


Figure 2.9 *IEEE 802.11AH MAC coordination functions [31]*

Distributed Coordination Function (DCF)

The most fundamental access method of IEEE 802.11 MAC is DCF which can basically use two types of transmission in handling frames: basic access scheme and Request to Sent (RTS)/Clear to Send (CTS) scheme. This implies that DCF must be implemented in every STA that is operating in IEEE 802.11 standard [61]. In addition, it uses binary exponential backoff procedure to cope with the multi-access phenomenon.

DCF is the only coordination function used in this thesis and because of its high importance, more discussions will be elaborated later in Section 2.3.3.

Point Coordination Function (PCF)

Compared to DCF, point coordination function is more simpler. It provides contention free access to network and can only be implemented in infrastructure networks. The center STA or AP, that are referred as Point Coordinator (PC), have the responsibility to grant channel access to each STA. Any STA that is granted by channel access has the right to start data transmission immediately [23]. Because there is no contention among STAs to get the medium in this approach, the duration when PCF is used is called Contention Free Period (CFP).

Hybrid Coordination Function (HCF)

Providing with higher QoS, The hybrid coordination function combines functions from DCF and PCF. Enhanced QoS mechanism and frame subtype to provide better service in both Contention Period (CP) and CFP enables this function to adapt to special channel access request in different situations. While HCF is implemented, Enhanced Distributed Channel Access (ECDA) is used for contention based channel access whereas for contention free access, HCF Controlled Channel Access (HCCA) is applied [22].

2.3.3 Distributed Coordination Function (DCF)

In IEEE 802.11 standard, there are two mechanisms defined to perform data transmission. The two approaches are Basic Access scheme and RTS/CTS Access scheme which are also knowns as two-way handshake and four-way handshake respectively

[39]. This is due to their different methods in transmitting data and handling the collisions that may occur in the system. An illustration of these access schemes can be seen in Figure 2.10 that simply explains the two schemes.

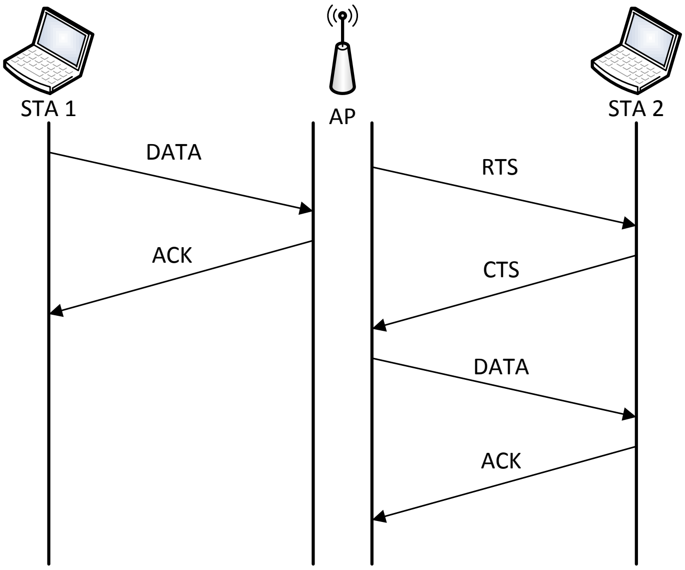


Figure 2.10 *A simple diagram of IEEE 802.11 basic access and RTS/CTS access schems*

DCF is the most important and the only mandatory coordination function that must be implemented in every present STA in the network. Because of the contending nature of DCF, it does not require a central STA to perform as coordinator [66]. Thus, it can also be used in the contention based part of PCF.

All the STAs in DCF use carrier sense multiple access with collision avoidance (CSMA/CA) to contend to access the channel [55]. This is very similar to its other version called carrier sense multiple access with collision detection (CSMA/CD), used in Ethernet to enable the multiple channel access. The only difference is that the first uses avoidance towards collisions whereas the latter one can detect collisions in the network.

Another important feature that is applicable to a scenario with DCF is the ability to recover from errors. This is the STA's responsibility to check and perform this task. Errors may occur due to many circumstances like a lost CTS. Interference in the channel or a collision with another active transmission may be the cause for this. However, retrying to transmit the frame that has not been received correctly or completely, must be done.

Retransmission in the sending STA is conducted but it has some defined limitations. There are two counters defined in each STA, namely STA Short Retry Counter (SSRC) and STA Long Retry Counter (SLRC). They are used for RTS/CTS and

ACK frames respectively. Using RTS/CTS scheme after sending a RTS when a STA detects a erroneous CTS or no CTS after a specified duration called CTSTimeout, it increments SSRC by 1. Similarly while an Acknowledgement (ACK) is expected to be received by a STA but the reception contains errors or there is no ACK is received during ACKTimeout, the STA's SLRC will augmented by 1.

This process will continue until the counters reach their limits or a successful transmission will take place in which case the counters will be reseted to 0. In case the limit is reached the packed will be discarded from transmission queue. The limit for SSRC and SLRC is set by the ShortRetryLimit and LongRetryLimit respectively, each of which is defined by the standards.

2.3.4 Interframe Spacing / Channel Access Timing

The timing used by STAs to access the medium can be categorized into two main parts that includes time for differing transmission and the time for contending to access the channel.

Interframe Spacing (IFS), as its title shows, is the time interval between two frames. They are used to prioritize accessing the channel by STAs. As Figure 2.11 depicts, there are several various IFS durations for different types of channel access. A STA requiring access to the network use carrier sensing to detect that the medium is idle for the whole corresponding IFS before being able to start transmission. Different IFSs will be described in the following:

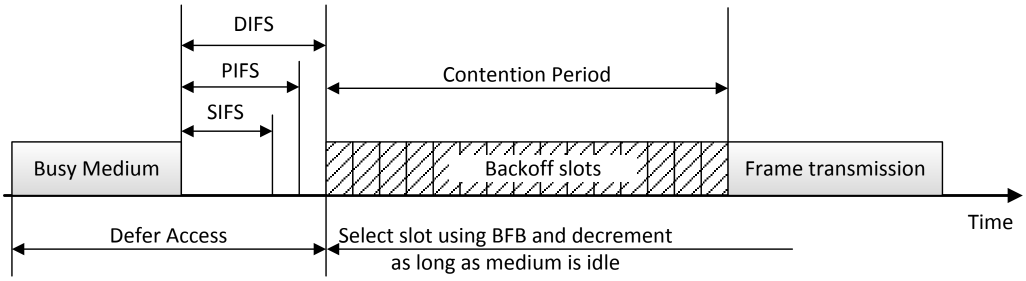


Figure 2.11 *Some of the IEEE 802.11 interframe spacing [43]*

Reduced Interframe Space (RIFS)

Its main objective is to decrease overhead by reducing the time between consecutive frames transmitted by a single transmitter or with the same transmit settings. Therefore, it has less duration from SIFS and increased network efficiency. This interframe spacing is not formulated in IEEE 802.11AH though.

Short Interframe Space (SIFS)

This spacing is used 1. when a sent frame requires response or 2. while one STA is using burst mode to send back-to-back frames. In the first scenario, SIFS separates the two frames, for example a data and its respective ACK, by taking the MAC and PHY latencies and process time into account. On the other hand, considering the second scenario, the STAs accessing the channel by SIFS do not check the medium to be idle and start transmission a SIFS separated from each other.

PCF Interframe Space (PIFS)

Used when a priority access to the medium is required, PIFS provides the next highest possible access after a SIFS. It is defied as:

$$\mathrm{PIFS} = \mathrm{SIFS} + \mathrm{SlotTime}. \tag{2.1}$$

PIFS is used by a STA that needs to send Channel Switch Announcement while APs use this spacing for sending beacon, starting a new contention free period or to access the channel to check a responce for a contention free period.

DCF Interframe Space (DIFS)

When a STA is operating under DCF mode and requires to transmit a data or management frame, it uses this timing defined as below:

$$\mathrm{DIFS} = \mathrm{SIFS} + 2 \times \mathrm{SlotTime}. \tag{2.2}$$

Prior to send a frame, the STA must ensure that the channel is idle for the whole DIFS duration or if it has a pending backoff period the idle time must cover the summation of both durations.

Arbitration Interframe Space (AIFS)

This is also used to prioritize an access category (e.g. audio, video, email and etcetera) over the other. STAs with QoS that access the channel by EDCA may use AIFS to transmit data. It does not have fixed duration and the length is in inverse relation with the importance of frame. As the frame becomes more important, the length of this frame becomes shorter.

The other timings that are highly important in channel access mechanisms will be discussed next. Despite being very general, they are the fundamental elements that determine the duration of the previously mentioned timings.

Slot Time

The most basic timing of all that takes into account the PHY delay, MAC processing delay, air propagation time and send/receive turnaround time. This time is designed to cover slight differences in boundaries that each STA may encounter and allow neighboring STA to detect the transmitting STA.

Random Backoff Time

When a STA wants to transmit data using DCF, it must first invoke the channel sensing mechanism to detect idle medium and start transmission process. Once the channel state changes from busy to idle, there might be several STAs with data in buffer and ready to send. Knowing that all STAs have to wait for DIFS interval after sensing that the channel is idle, they will try to access the channel all at once and collision will happen. To minimize this problem a procedure called random backoff can be implemented.

The random backoff count is a random integer number that is chosen from a uniform distribution over $[0, \mathrm{CW}]$, where CW is the Contention Window value. The STA then defers its Channel Access (CA) process by CW duration. This will assure maximum randomness while keeping the fairness for contending STAs.

Beginning this process, if the backoff counter is 0, then as described earlier, the STA is forced to choose a random integer from $[0, \mathrm{CW}]$ as its initial backoff counter value. The initial CW parameter is also equal to CWmin parameter. In each unsuccessful transmissions, for example each time no ACK is received for a transmitted data frame, the CWmin doubles until it reaches its upper limit on CWmax. Once reached its upmost limit the CW remains at CWmax for the rest of tries until a successful transmission is made or the packet is discarded. It is only that time the CW is rest to the CWmin value.

CWmin and CWmax are two integers defined by the PHY used and specified in each amendment. The CW, along with its two upper and lower limits, may take values that are powers of 2 subtracted by 1. This procedure is also known as Binary Exponential Backoff (BEB). Let n be the number of tries in retransmitting one packet that is equal to 0 for the first attempt. Having all the assumptions, the CW value is calculated as:

$$\mathrm{CW} = \min((2^n \times (\mathrm{CWmin} + 1)) - 1, \mathrm{CWmax}) \tag{2.3}$$

It is very important to note that final random backoff period is obtained when random generated backoff counter is multiplied by the SlotTime. This is the actual time in microseconds that a STA must count down to resume its CA progress.

When a STA wants to start the random backup procedure, it must invoke CS mechanism to detect an idle medium and only after a DIFS/EIFS duration that it can begin decrementing the backoff counter. This counter is decremented by 1 each time an idle SlotTime is detected. The STA must continue to sense the channel constantly to be able to suspend the backoff counter decrementation whenever the channel state switches to busy due to possible transmissions by other STAs. The counter resumes its process once a DIFS/EIFS idle duration is detected.

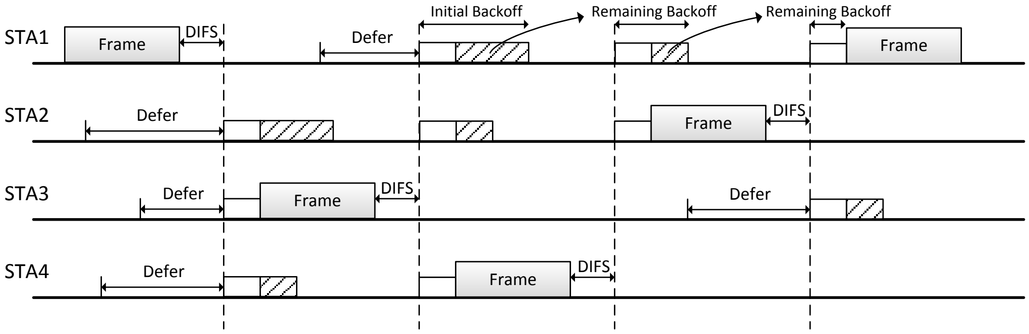


Figure 2.12 *Backoff procedure in IEEE 802.11*

The process of this procedure is illustrated in Figure 2.12. While multiple STA request to access the channel, they defer their CA for the next DIFS idle duration and start their random backoff duration by choosing a random backoff number. Starting the contention for CA, the STA with smallest backoff value (STA3) will get to access the channel and all the other contending STAs pause their backoff decrementation process and continue CS mechanism until the next idle DIFS period. The STA with lowest random backoff value will win next (STA4) and this process is repeated untill there is no STA with deferred access attempt.

2.3.5 Hidden Node Problem

Due to the channel access mechanism in IEEE 802.11 networks which are designed in a distributed manner, it is very crucial to find a carrier sensing mechanism to reduce and avoid collisions to the highest possible amount. This is mainly done by physical CS mechanism which resides in PHY layer [34]. Opposite to wired networks where all STAs can hear each other and hence sense packet transmission, it may not be true in some situations in wireless networks.

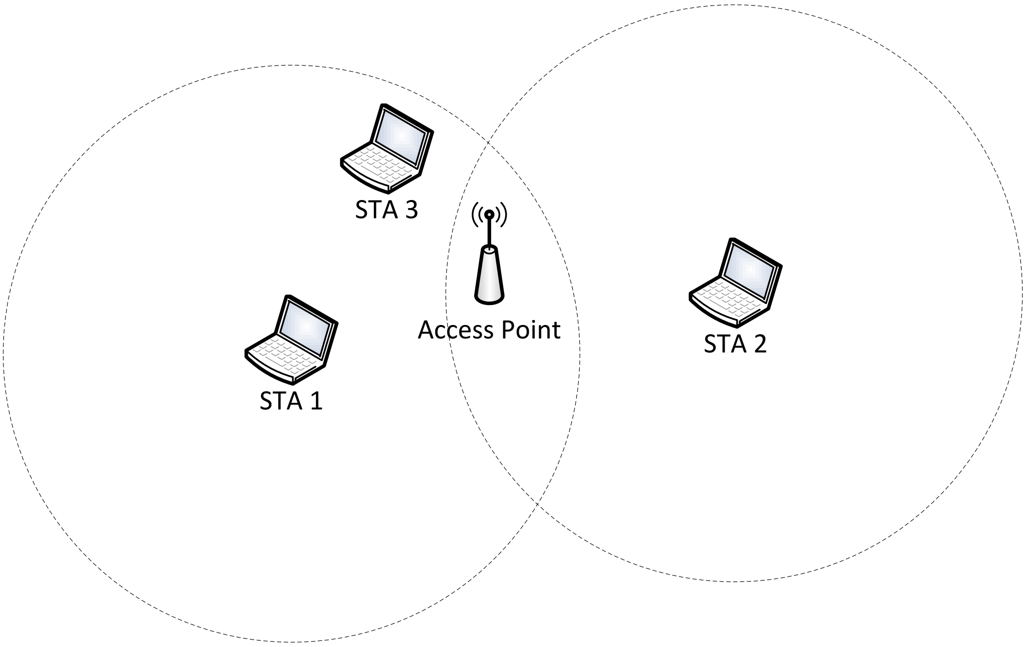


Figure 2.13 *Hidden node problem in IEEE 802.11 WLANs*

Two STAs (or nodes) may be hidden to one another if they are not able to hear each other or not being in each other's transmission range. Each STA's transmission range is determined by several factors such as transmission power, medium properties, channel noise and etcetera. This is known as the hidden node problem.

As can be seen in Figure 2.13, here all nodes are in the transmission range of AP and can communicate with it. If a transmission is happening between STA1 and AP, this busy channel can be sensed by STA3 CS mechanism. But problem arises if STA2 wants to access the medium to transmit data to AP. Since the transmission between STA1 and AP is not detectable by STA3 because of the greater distance than its range, the CS mechanism in STA3 will find the channel idle and starts the data transmission to AP. This causes collision and therefore data lose at AP. Following are several approaches to overcome this problem:

Network Allocation Vector (NAV)

Logically residing in the MAC layer, Network Allocation Vector (NAV) helps to enhance the physical carrier sensing by providing virtual carrier sense. Nearly all of the IEEE 802.11 frames include a field for duration which can be used by NAV to reserve the medium for the desired amount of time. This is done by updating the NAV field in all the STAs that are receiving the frame except the one that the frame is destined to.

Updating the duration field in all the neighboring STAs requires a robust procedure. Using control frames such as RTS/CTS is one effective way to do

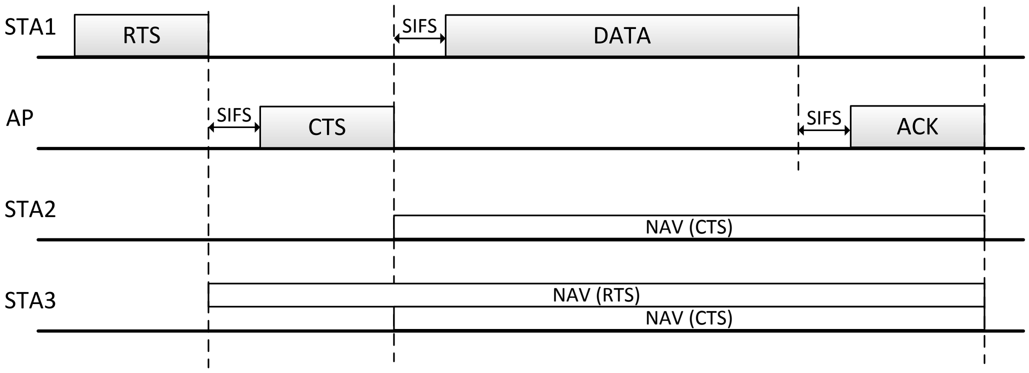


Figure 2.14 *Network Allocation vector and RTS/CTS mechanism in IEEE 802.11*

so. As Figure 2.14 depicts sender, here STA1, initiates a RTS/CTS procedure with RTS packet destined to the receiver which is AP in this scenario. Upon the reply of receiver with CTS all the STAs are able to update their NAV duration field accordingly so to halt their CA until the ongoing transmission is expected to end successfully.

NAV is updated everytime a frame with higher NAV value is received. This value is in microseconds and is always rounded up to ensure full coverage over the current busy channel. An erroneous RTS frame may cause a redundant reservation in STAs since this will update their NAV value and hence the channel will be wasted. Therefore STAs that have updated their NAV regarding RTS are permitted to reset their NAV if they do not receive a CTS in a specific amount of time.

Extended Interframe Space (EIFS)

Another solution for solving the hidden node problem is using EIFS. This spacing is used instead of DIFS if MAC discovers that the FCS for the frame is not correct. This happens if the frame is detected but is not received correctly. EIFS is defined as:

$$\mathrm{EIFS} = \mathrm{SIFS} + \mathrm{ACKTxTime} + \mathrm{DIFS}. \tag{2.4}$$

where ACKTxTime is the required time to send an ACK in the lowest PHY data rate. [14]

The EIFS approaches the hidden node problem by preventing the STA to start transmission during the ACK of a hidden node. This is triggered when an attempt to data frame demodulation is failed. On the other hand, if an ACK is received while EIFS differing process, the STA continues with DIFS. This procedure is illustrated in Figure 2.15.

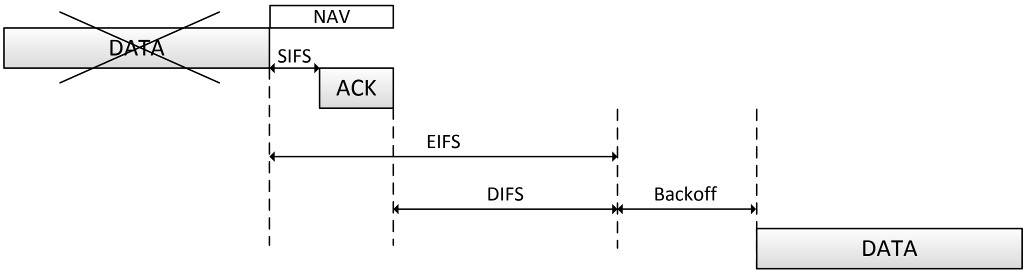


Figure 2.15 *EIFS procedure in handling hidden node problem*

2.3.6 DATA/ACK Frame Exchange

The medium used in IEEE 802.11 WLANs are prone to transmission errors. Being able to repeat the transmission for unsuccessfully demodulated frames in receiver side at link layer is a huge advantage for these networks. To efficiently implement this mechanism, an immediate positive response message, called Acknowledgment (ACK), is sent to the sender from the receiver side indicating the complete reception of the frame. If for any reason the STA sending the data frame does not receive ACK, it will assume that the frame is not successfully received or demodulated at the destined STA and will resend the previous frame [51].

Broadcast and multicast data frames are exempt from being acknowledged upon reception because they are not destined for specific STA. Moreover, there is a limit for the number of retransmission attempts for a data frame. The lowest PHY data rate available is used to send ACK to ensure a robust and reliable way to acknowledge the successful transmission of the data frame. Since the ACK frame is relatively small in size, the overhead caused by sending it in the lowest rate is also negligible.

2.4 PHY Layer Architecture

The PHY layer, as can be seen in Figure 2.16, consists of three sublayers: PHY Layer Convergence Protocol (PLCP), PHY Medium Dependent (PMD) and PHY layer management. The PLCP, which is located between MAC and PMD, is responsible for carrier sensing assessment and making packets suitable for different PHY layers. It is accomplished by mapping the MAC frames into transmittable packets by PMD. On the other hand, PMD sublayer have the main responsibility for modulation, demodulation and coding techniques for transmission and reception of packets in PHY layer. Finally, PHY layer management cares for tuning the channel for various PHY layer options [47].

When IEEE 802.11 standardized for the first time in 1997 by IEEE, it included three wireless data exchange techniques: Infrared (IR), Frequency Hopping Spread

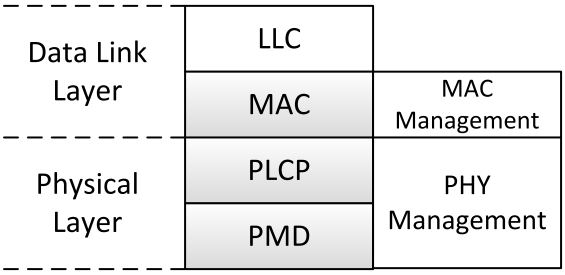


Figure 2.16 *IEEE 802.11 MAC and PHY layers protocol entities*

Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) that the last two operate on 2.4 GHz frequency band [41]. IEEE 802.11a and IEEE 802.11b were two standard amendments that were introduced later and aimed at creating new frequency band and increasing the data rate. Creating a new PHY, IEEE 802.11a succeeded to provide data rate in frequency band at 5 GHz whereas IEEE 802.11b used Complementary Code Keying (CCK) to enhance DSSS. Developing IEEE 802.11a made a revolution in IEEE 802.11 by utilizing Orthogonal Frequency Division Multiplexing (OFDM) and hence increasing the data rate to 54 Mbps while still being bounded to 5GHz. Later OFDM was permitted to be used in 2.4 GHz which led to IEEE 802.11g and combining frequency bands allowed to further developments and higher data rates with IEEE 802.11n and IEEE 802.11ac which could provide 600 Mbps and 6933 Mbps in their highest performance, respectively [16].

This section aims to provide a basic information on different PHY properties of IEEE 802.11AH which benefits from OFDM technology and operates under sub-1GHz frequency band.

2.4.1 Channelization

Due to the availability constraints of sub 1 GHz Industrial, Scientific and Medical (ISM) bands in different countries around the world, IEEE 802.11AH is obligated to define channelization regarding each region's respective available wireless spectra. These countries include United States, South Korea, China, Europe, Japan and Singapore. A summary of the assigned channelization in sub 1 GHz spectra in different countries is illustrated in Figure 2.17.

The available channel bandwidth is divided into 1MHz channels in each region and for getting a higher bandwidth for higher data rate several adjacent narrower channels are bounded together. This is the same method used in IEEE 802.11n and IEEE 802.11ac for getting wider channels. As an example, the channelization for United States will be depicted in Figure 2.18.

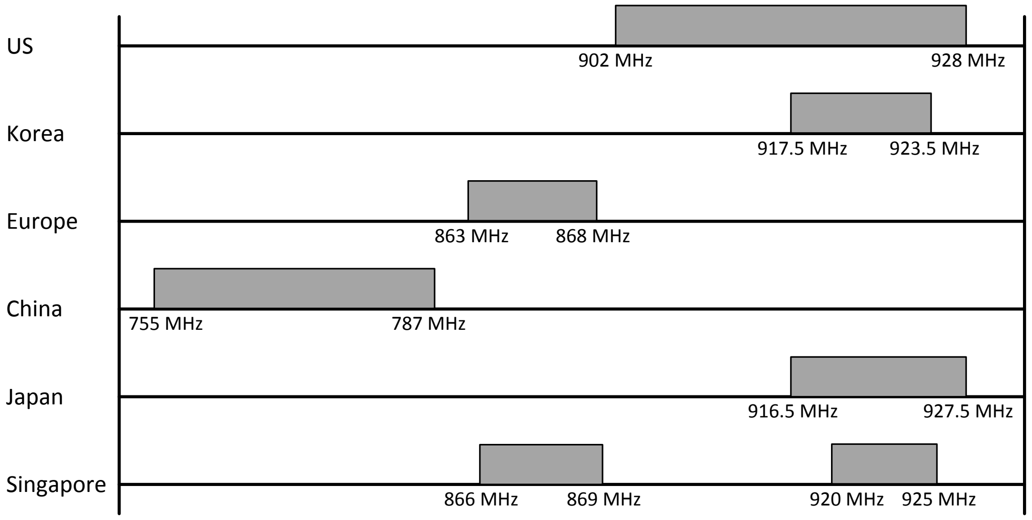


Figure 2.17 *IEEE 802.11AH channelization in sub 1 GHz spectra*

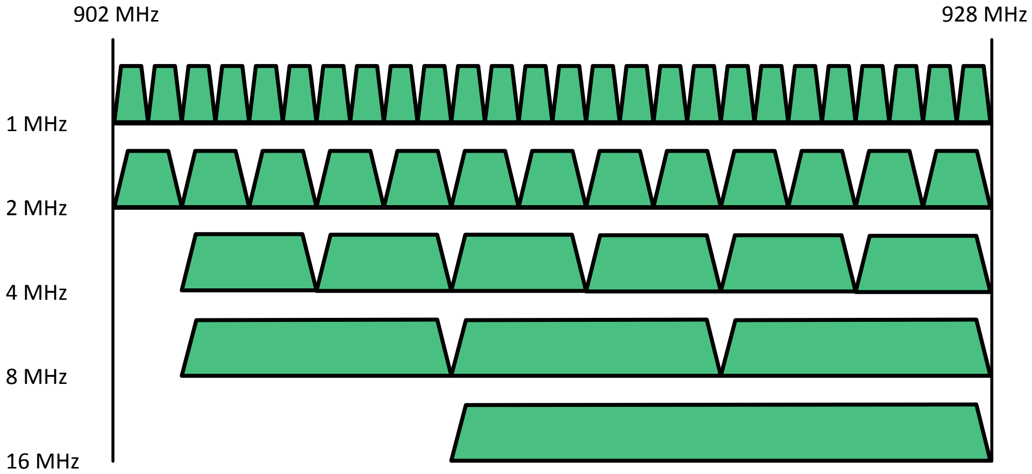


Figure 2.18 *IEEE 802.11AH channelization for US*

As can be seen in Figure 2.18 a total of 26 MHz is available, from 902 MHz to 928 MHz, and hence the available 1 MHz channels are summed to 26. As explained earlier, wider channel bandwidth can be achieved by bonding the available narrower bands. The widest bandwidth is 16 MHz which is also the widest band available in IEEE 802.11AH channelization [49].

2.4.2 Transmission Modes

Being available in all channelizations across countries, 1 MHz and 2 MHz channels are chosen to be the common channel bandwidth for IEEE 802.11AH STAs and they are obliged to support the reception in those channels. Therefore, there are two categories for PHY transmission modes: 1 MHz and greater or equal to 2 MHz.

IEEE 802.11AH PHY layer has exactly been designed based on 10-times down-clocking version of IEEE 802.11n and IEEE 802.11ac where for the first one the channel spacing of 20 MHz, 40 MHz and for the latter one the 80 MHZ and 160 MHz are formulated for higher data rate. Therefore, the channel spacing equal to 2 MHz, 4 MHz, 8 MHz and 16 MHz has been defined for IEEE 802.11AH. The other transmission category of 1 MHz is introduced in IEEE 802.11AH for greater coverage range and reliability [57].

2.4.3 Modulation and Coding Scheme

In IEEE 802.11AH, transmissions can be conducted using various modes. Each of these modes can adaptively be used to assure robustness or range extension for a given use case. It is the Modulation an Coding Scheme (MCS) that determine the transmission modes. This affects the transmission of DATA field in the transmitted packet and the performance of the whole system.

IEEE 802.11AH uses different modulations in OFDM subcarriers such as binary phase shift keying (BPSK), quadrature phase shift keying (QPSK), 16-quadrature amplitude modulation (16-QAM), 64-QAM and 256-QAM. Forward Error Correction (FEC) is performed using low-density parity-check (LDPC) coding or binary constitutional with available coding rates.

Throughout this thesis, the basic mode of 2 MHz for bandwidth is used along with the Nss of 1 (because there is no scenarios with MIMO and hence no spatial stream) where the Guard Interval (GI) is set to be 8us. Defined MCSs for IEEE 802.11AH with the specified assumptions is presented in Table 2.3 [3].

***Table* 2.3** *Modulation and Coding Scheme in IEEE 802.11AH for 2MHz, Nss = 1, GI = 8us*

Index	Modulation	R	N_{BPSCS}	N_{CBPS}	N_{DBPS}	Data rate (Kbps)
0	BPSK	1/2	1	52	26	650
1	QPSK	1/2	2	104	52	1300
2	QPSK	3/4	2	104	78	1950
3	16-QAM	1/2	4	208	104	2600
4	16-QAM	3/4	4	208	156	3900
5	64-QAM	2/3	6	312	208	5200
6	64-QAM	3/4	6	312	234	5850
7	64-QAM	5/6	6	312	260	6500
8	256-QAM	3/4	8	416	312	7800

where R is the coding rate, N_{BPSCS} is number of coded bits per single carrier for each spatial stream, N_{CBPS} is number of coded bits per OFDM and N_{DBPS} is the number of data bits per OFDM symbol. There are two variables that are constant under these assumptions. N_{SD} which is equal to 52 and N_{SP} that has 4 as its value and they represent the number of data subcarriers per OFDM symbol and the number of pilot subcarriers per OFDM symbol respectively.

There is also a specific modulation scheme defined in IEEE 802.11AH for 1MHz band which uses repetition to increase the packet reception reliability. This modulation is named as MCS10 and has half the data rate of its respective MCS0 because, as the name implies, it repeats the data sent towards any destination to cover the possible degradation and loss in packet reception and enhance the coverage limit [50].

2.4.4 Pathloss Models

Different path loss models have been developed for different environments in IEEE 802.11AH [52]. They include two categories named Indoor and Outdoor that will be discussed briefly in the following:

Outdoor

It is based on the Spatial Channel model (SCM). The SCM are 3GPP models that are used for simulating SISO and MIMO links [1] [2]. The path loss models defined as follows:

Macro Deployment

The path loss value in [dB], considering that the antenna is 15 meters above the rooftop is equal to $PL = 8 + 37.6 \times \log_{10}(d)$.

Pico/Hotzone Deployment

When assumed that the antenna is at the rooftop height the path loss model is $PL = 23.3 + 36.7 \times \log_{10}(d)$.

Device to Device

Assuming the antenna to be in 1.5 meters of roof top height, the path loss would be equal to $PL = -6.17 + 58.6 \times \log_{10}(d)$.

Where d is in meters and all aforementioned formulas, that represent the median path loss, are defined in RF carrier assumed to be at 900 MHz and the deviation is taken into consideration. In case STA are communicating with outdoor APs, a penetration loss of 10 dB must be added. Moreover, If other frequencies are used, a correction factor of $21 \times \log_{10}(f/900\text{MHz})$ must be added too.

Indoor

Proposed model for indoor purposes is based on the IEEE 802.11n channel models that have been tuned for Task Group IEEE 802.11ac (TGac) use cases [15] [28]. The developed path loss model is then formulated as:

$$L = L_{FS} = 20 \times \log_{10}\left(\frac{4\pi d f_c}{C}\right) \qquad for\ d \leq d_{BP} \tag{2.5}$$

$$L = L_{FS} + 35 \times \log_{10}\left(\frac{d}{d_{BP}}\right) \qquad for\ d > d_{BP} \tag{2.6}$$

where d, f_c and C are distance in meters, center carrier frequency equal to 900 MHz and speed of light, respectively. d_{BP} is the breakpoint distance at critical distance. It is important to note that this model is developed for single floor scheme. The more comprehensive schemes for multi-floor and STA-to-STA scenarios are available in [52].

3. IEEE 802.11AH MAC FEATURES ENHANCEMENT

IEEE 802.11AH, as a novel standard, is defined to support a tremendous number of devices with power limitations and small packet transmissions. Thus TGah has a difficult task of defining the new standard to meet all the requirements. Being well defined, IEEE 802.11 MAC acts as a reliable base for this amendment and has only a few limitations related to its frame format that prevents it to be utilized in networks with high number of devices. The main effort in developing the new IEEE 802.11AH standard is developing the MAC layer to improve the power efficiency and reduce the overhead caused by short packets and long time characteristics of the new developed PHY layer. All of these issues make the channel highly occupied with frame headers, interframe spaces, control and management headers or to be wasted while channel access processes conducted by high number of devices.

This chapter will introduce some of the many enhancements introduced by TGah to improve the IEEE 802.11 network characteristics to be suitable for IEEE 802.11AH. Section 3.1 introduces the main updates for frame formats in IEEE 802.11 characteristics that are one of the main causes for limitations. New frame formats for shorter frames to decrease the overhead and increase network performance and efficiency is discussed in Section 3.2. Next, Section 3.3 will elaborate on novel channel access methods aiming to handle huge amount of STAs request to access the channel and reduce channel busy time, collisions and power consumption. New power management schemes that have the ability to support high number of nodes are presented in Section 3.4.

3.1 General Improvements

As the IEEE 802.11 standard has been developed for small to medium sized networks there is not a explicit limitation defined for number of associated STAs. Thus the only limit preventing high number of nodes to be associated is the length of some fields in management frames.

A unique number is assigned to a STA once it is associated to an AP, called the Association Identifier (AID), that has a 14 bits length and ranges from 0 to 16383 but all the values other than 1-2007 are reserved. Therefore, an operating AP under IEEE 802.11 network can not provide service for more than 2008 devices. Another limitation is imposed by the Traffic Indication Map (TIM) bitmap. TIM is a map that indicates the maps of STAs that the AP has buffered packets to be sent to and is used by power management schemes. The TIM field length is limited to 2008 bits.

As the IEEE 802.11AH is aimed to support up to 6000 STAs, the TGah has extended the range of AID numbers that can be used by a STA operating in IEEE 802.11AH networks to 0-8191. In addition, the length for TIM bitmap has increased to 8192 bits to be equaly capable of supporting very high number of STAs.

3.2 Frame Shortening

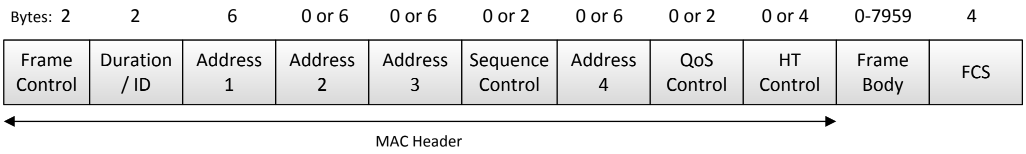
One of the typical main problems in sensor networks is the overhead in transmissions. This is because of transmitting packages that have more header bits. Apart from degrading the network throughput in first sight, this overhead reduces the power efficiency. On the other hand, most of the times the use of aggregation and other IEEE 802.11 solutions are not applicable to many use cases. Therefore this section will discuss the new ways to approach these issues by the work group for IEEE 802.11AH.

3.2.1 Short Headers

Headers, as added bits to the main data, are always a part of sent frames and are highly valuable to induce information for routing, channel utilization and several parameters that are required to be met by the associated devices in a BSS.

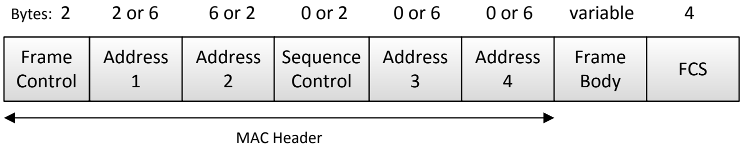
As shown in Figure 3.1, in the legacy IEEE 802.11 networks, the length of the MAC frame when using the full capacity, with 4 address fields, can reach to 36 bytes and the overhead is increased also by a 4 bytes FCS field. Considering some use cases in IEEE 802.11AH which use 256 bytes of data field, it introduces a 13 % overhead which is relatively high.

To solve this problem, TGah has come up with the idea of defining a new short headers for data, management and control frames which is distinguishable from the legacy one by an indication in Frame Control (FC) field of both formats. A significant change, illustrated in Figure 3.2 that is imposed to frames by using short version, is that they do have the Duration/ID field which is necessary for NAV operation in legacy IEEE 802.11 networks. Therefor, the task group for IEEE 802.11AH are obliged to develop a new mechanism for channel access. The novel channel access mechanism is called Response Indication Defferal (RID) and will be discussed further in Section 3.3.



Bytes: 2	2	6	0 or 6	0 or 6	0 or 2	0 or 6	0 or 2	0 or 4	0-7959	4
Frame Control	Duration / ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	QoS Control	HT Control	Frame Body	FCS

***Figure* 3.1** *Frame format for legacy IEEE 802.11 with full MAC header*



Bytes: 2	2 or 6	6 or 2	0 or 2	0 or 6	0 or 6	variable	4
Frame Control	Address 1	Address 2	Sequence Control	Address 3	Address 4	Frame Body	FCS

***Figure* 3.2** *Frame format for IEEE 802.11AH with short MAC header*

Frames using short MAC header can transmit frames between an AP and a STA directly using two address fields, while transmissions originated from a STA to another STA in the same BSS must use three address field because they use an AP to forward frames. Moreover, if the transmission is required to be done using multi-hop network, the use of four address field are necessary for transmitter, receiver, source and destination addresses.

3.2.2 NDP MAC frames

Apart from main data frames in networks there exist several different types of frames for management and control purposes like ACK, CTS and etcetera. Because these frames are mainly used to report frame reception and do not carry a lot of useful information, aside form duration field used for setting NAV, TGah decided to benefit from previously developed frames in IEEE 802.11ac networks called Null DATA Packet (NDP) and extend a new frame type called NDP MAC frames for IEEE 802.11AH networks.

NDP frames has been used in IEEE 802.11ac as short frames for channel calibration required for beamforming. This process is done by inspecting the received sounding symbols in PHY header so the NDP frames does not need to carry any payload. TGah tends to use this type of frames and add just the sufficient amount of data to carry out the functionalities of the control frames.

3.2.3 Short Beacons

Beacons are another source for overhead in networks. Being sent periodically and containing relatively large amount of information, they must be sent in the most robust modulation scheme to ensure the reception by edge members of the operating basic service set. Considering IEEE 802.11AH lowest data rate that is a little bit more than 0.5 Mbps, transmission of even a few bytes in this mode will take significant amount of channel time and power in both receiving and sending sides.

To reduce this effect IEEE 802.11AH task group has developed two type of beacons, namely short and full. Short beacons are sent more frequently and do not contain all the informations but the very essential ones. In contrast, full beacons are sent less frequently but contain all the information which in the case of no change in network are unessential.

Unchanged information are excluded form short beacons to reduce the overhead. When a STA is required to be notified about a change in the network, the AP changes a field in short beacon field to notify the STA about the update. The STA then, knowing the information about the next full beacon transmission, can go to sleep to further enhance its power efficiency.

3.3 Channel Access

IEEE 802.11AH task group has developed several approaches for minimizing the drawback in legacy wireless networks in accessing the channel when very high number of devices are present. In this section the main objective is to decrease the channel's wasted time by avoiding unnecessary collisions, interframe spaces, ACKs and overlapping transmission by STAs transmitting simultaneously.

3.3.1 Virtually Sensing the Carrier (RID)

The legacy IEEE 802.11 standard, from the first version released, has been defined to use virtual carrier sensing mechanism called Network Allocation Vector (NAV) beside the physical carrier sensing to avoid collisions while transmissions. In other words, NAV is responsible for blocking all neighboring STAs in the receiver's area to access the channel during the time interval that the STA is expecting to receive an ACK after sending a data frame. The neighboring STAs can learn about the duration they are forbidden to access the medium by looking at the duration filed of the data frame that has been sent by the transmitting STA.

As described previously, the NAV is disabled when using short frames because of the elimination of duration field. Thus, TGah started to develop a new virtual carrier sensing mechanism to cover NAV operations which is called RID.

Both RID and NAV have several similarities like they both can be assumed as countdown timers to the time indication channel idle time. On the other hand, there are some differences which make these two CS mechanism usable for their respective standard. The main difference is that the NAV can be set after the complete and correct reception of the whole frame while RID can be set just right after the PHY header is received. This enables NAV to have a very high accuracy about the exact timings of the channel state changes, while RID tries estimating the duration of channel events based on the type of response with 2 bits length stored in Response Indication field in PHY header.

RID defines four types of responses named Normal Response, NDP Response, No Response and Long Response to distinguish different channel states. Information about these responses are included in PHY header which impose some advantages and disadvantages. Using No Response, RID does not let a STA to waste channel time by waiting a very long time for an expected ACK when a collision may have occurred and an EIFS must be wasted using legacy DCF. In contrary, If a frame requires the use of Long Response, the channel is reserved for that STA and becomes busy for all others. It may happen that the STA needs less time than reserved for its transmission and it can use Response indication field to inform the other STAs to update their RID and use the excess channel time. Here, the Nodes that are hidden to the receiver can not get the updated information and their channel resource is wasted.

3.3.2 Restricted Access Window

As the IEEE 802.11AH is mainly developed for supporting networks with very high number of nodes, even with very low traffic, the congestion is always is a big concern in all stages when STAs need to access the wireless medium including association or data transmission. Collisions are considered as a source to many issues and IEEE 802.11AH has used several approaches to address this phenomenon, one of which is Restricted Access Window (RAW). This method manages to limit the access of simultaneous STAs trying to get the channel by a small portion in a specified time intervals, trying to minimize the effect of collisions on network efficiency and maximize the wireless channel utilization.

When RAW is enabled in IEEE 802.11AH frames, being a centralized scheme, AP chooses to assign RAW as a medium access interval to STAs in a beacon and use broadcasting to send this controlling frame to all STAs. The STAs that have received beacon frames transmitted by the AP that they have been associated with and are allowed to use RAW, can determine which RAW group they belong according to the information in the RAW group field of the frame and thus learn their respective RAW start time and the duration of it. In addition, RAW can be divided into several smaller slots for imposing more control over STAs contending to access the channel. Once there is an uplink data ready to be sent in STAs, they can try to access medium to start their transmission towards AP. They can only start this procedure following two main rules. First, it must be during the time period that is specified for the RAW group that they belong to and second, they must check the remaining time of their RAW slot to make sure that there is enough time for a complete successful transmission cycle.

This is also called Cross Slot Boundary which is one of the fields in the beacons containing RAW information. If this is allowed in the received beacon from AP, the STAs can skip the second rule mentioned earlier, and send their frames only if their start time is in their RAW duration. This allows transmissions from one RAW slot to be able to continue during the next slot's duration. Otherwise, if not allowed by the AP, both rules must apply to commence a transmission cycle. Moreover, it may happen that a STA would not have any uplink data to send in the beginning of its RAW slot duration. The STAs can start contending to access the wireless channel whenever they receive a data to their transmission queue. Figure 3.3 illustrates the RAW procedure in one beacon interval.

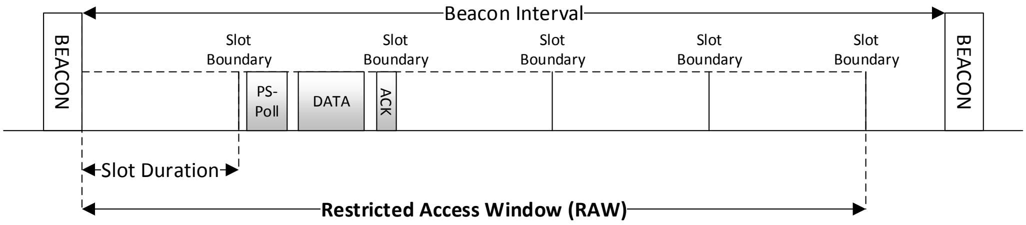


***Figure* 3.3** *Detailed Restricted Access Window (RAW) structure*

The first element in slot assignment procedure in STAs is to know how many time slots a mechanism has. A STA can obtain the number of time slots in one RAW (N_{RAW}) that it is allowed to contend, from the specified subfield in the beacon frame it has received from the AP. Next, it can calculate the duration of each time slot (T_{slot}) based on the duration of the whole RAW (T_{RAW}) which is also can be found in the beacon frame.

As illustrated in Figure 3.4, the time slots in a RAW are indexed from 0 to (N_{RAW} −

1). A STA uses a mapping function to calculate its time slot index (i_{slot}) where it is allowed to start the channel access procedure defined as

$$i_{slot} = (x + N_{offset})\ mod\ N_{RAW} \tag{3.1}$$

where x is the STA's original position index starting from 0, N_{offset} represents the offset value in the mapping function encapsulated in the beacon frame. The aim of this variable in the mapping function is to improve fairness among the STAs competing in a RAW. Using different random values for N_{offset} in beacons, the AP prevents to delay the channel access for a particular group of STA permanently. Finally, the *modX* indicates the modulo X operation.

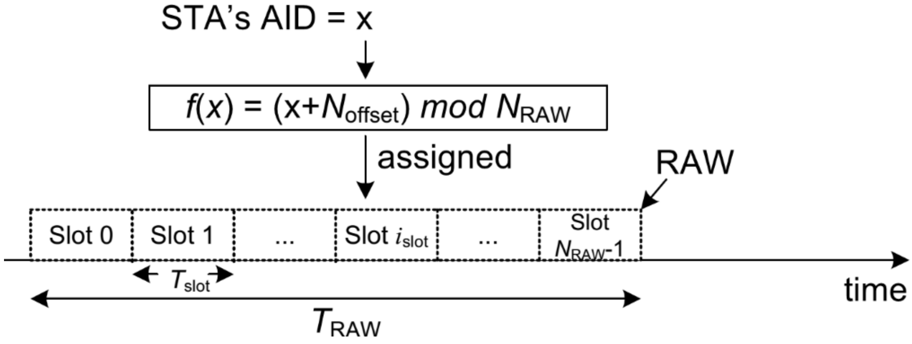


Figure 3.4 *RAW slot assignment*

Backoff procedure in RAW

Once the RAW is enabled in the network, each STA will be able to maintain two separate backoff counters and function states to be able to support the restricted channel access control based on the Enhanced Distributed Channel Access (EDCA). These two backoff functions are completely independent from each other and does not effect or interfere one another. One of them is to be used outside the RAW and the other one is intended to perform the back off procedure needed inside the RAW.

As illustrated in Figure 3.5 STAs have their regular backoff system until they are allowed to use RAW for channel access. At this point, they create their secondary backoff function and a backoff counter to be able to perform it independently. When a STA tries to contend in RAW, it suspends its primary backoff counter and function state and stores them. Then it lunches the secondary backoff procedure to use during the RAW. Once the RAW is finished and no longer is available to use, STAs restore their primary backoff function and state to resume. In case the primary backoff

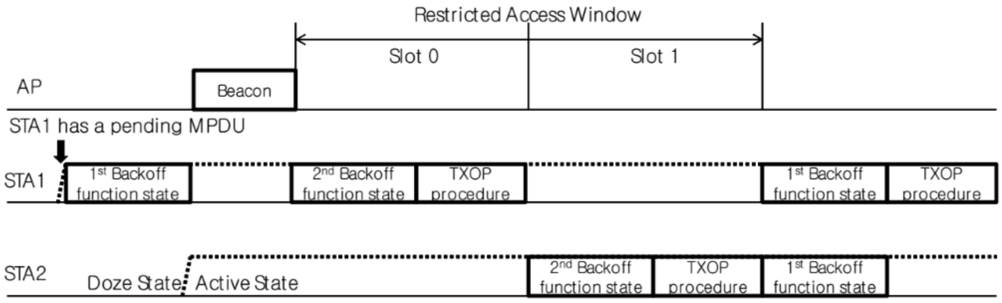


***Figure* 3.5** *Backoff procedure in RAW*

counter is empty or equal to 0, the backoff function will generate a new backoff value.

It is important to note that in backoff procedure during RAW, STAs can count down their backoff only in their respective RAW slot time, where they can operate and get to access the channel. At the end of each RAW slot the backoff counter and state will be saved to be restored and resumed in the next RAW slot time specified for each node.

3.3.3 Fast Association and Authentication

This feature aims to optimize the authentication process for higher number of nodes by deploying two strategies namely Centralized and Distributed control mechanisms. In the first one the AP includes a threshold in each beacon that is determined by some rules in the implementation. Each STA, then generates a random number from [0, 1022] interval and the STAs that have their random values less than that threshold are eligible to authenticate in that beacon interval. The latter one is based on truncated exponential backoff. Each time there is an attempt for authentication, every STA generates two random numbers based on the number of whole slots in beacon interval and transmission interval.

3.3.4 Sectorization

One of the main mechanisms introduced to handle the complications in channel access is referred as sectorization. In simple context, it is the act of partitioning of the AP coverage area into sectors so that each of the sectors contain a subset of associated STAs. This can be done by using a set of omni-directional antennas or synthesized antenna beams in AP to perform the transmission and reception. The entire coverage area of an AP is assumed to be covered and every associated STA must belong to a sector.

IEEE 802.11AH defines two types of sectorization which will be referred as Spatial Sectorization and TXOP-based Sectorization throughout this thesis. Following is a general description of the two aforementioned sectorization schemes.

Spatial Sectorization

High number of nodes associated to a single AP and trying to transmit their data is one of the main challenges that IEEE 802.11AH is encountering. Besides, long coverage requirement can also get complicated in some network deployments. Therefore, TGah has come up with a scheme like time devision multiplexing to address this phenomenon.

Being a beacon based operation, this scheme allows the STAs to be grouped into sectors relative to their location. The AP sends periodic beacons containing the sectorization information added into the frame headers to inform all STAs about their respective sector ID. This way STAs get to adjust their medium access based on the timing in the beacon they receive. Other STAs that do not belong to the active sector and thus are not allowed to compete in data transmission, are set to go to sleeping mode until their timer finishes.

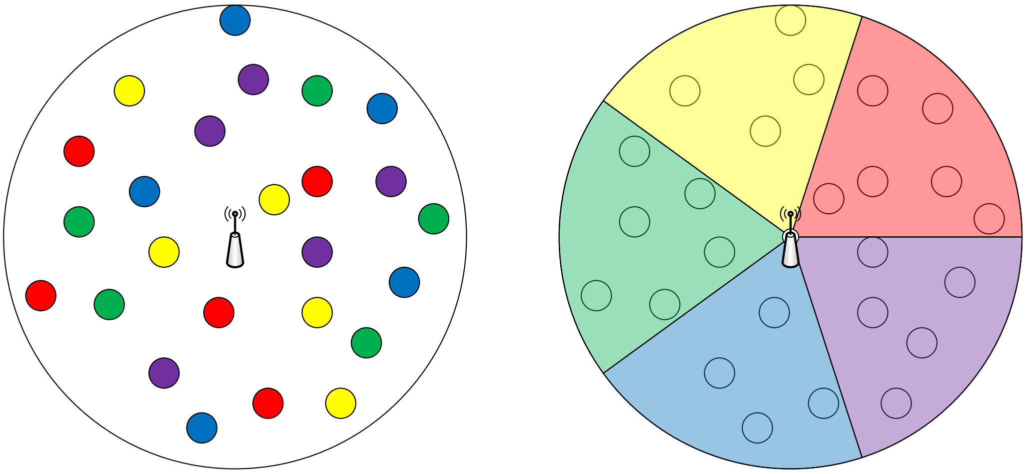


Figure 3.6 *RAW (left) and Sectorization (right) node assignment*

It is straight forward that the spatial sectorization will help mitigate the hidden node problem by allowing nearby STAs to contend in an instance of time. Moreover this scheme aims to improve the energy efficiency by letting the STAs that are not allowed to send data, to go to sleeping mode.

TXOP-based Sectorization

Using several AP to manage the coverage for an area is one of the approaches that can be expected in deploying IEEE 802.11AH technologies. With high number of expected STAs and several BSS, overlapping of these BSSs (OBSSs) will impose a critical interference in transmission that are taking place in the same wireless medium. TGah has introduced TXOP-based sectorization in IEEE 802.11AH specification to solve this problem by letting associated STAs in different OBSS to send their data using the spatially orthogonal technique under certain rules.

As the name implies, this scheme is based on the AP transmitting and receiving through TXOP duration of each established data transfer. Commencing the frame exchange sequence, the AP sends an omni-directional beam that can be received by all its associated STAs - regardless of their support for TXOP-based sectorization - to set up their Network Allocation Vector (NAV) protection and to establish a link with the desired STA prior switching to directional beam transmission.

Next, the AP switches to sectorized beam transmission during interframe spacing. Being aware of the sector that the STA is, AP may start transmission or reception using appropriate sectorized beam during any scheduled transmission. An AP can use different sectorized beams to communicate with STAs in different TXOPs. During this kind of frame exchange, spatial reuse of the same shared wireless medium between OBSS APs or STAs can be done if when a NAV protection is set for a duration within a TXOP and an OBSS member (STA or AP) receives the omni-directional beam but not its corresponding sectorized transmission from the AP. The IEEE 802.11AH specification defines several methods to deploy this scheme that includes the use of long or short PHY headers.

3.4 Power Saving

Power management and consumption has always been an important issue in remote and wireless devices to pay attention to. Using wireless devices, IEEE 802.11 standard has used numerous power management mechanisms that are based on changing states of devices so that they can save power and optimize their energy consumption. There are two main states, namely doze and awake, that are initially developed.

While a STA is awake, it continues to transmit and receive packets and perform channel access. By switching to the doze state the STA turns off its radio module and can not interact with network in anyway. The STA must inform its associated AP prior to switching states. The STA then wakes up periodically to transmit/receive data to/from AP.

IEEE 802.11 has many power management features to enhance IEEE 802.11AH too but their efficiency is not high. Therefore new procedures have been developed based on them to meet the requirements of IEEE 802.11AH network. Some of the newly developed approaches will be discussed in this section.

3.4.1 Optimizing Max Idle Duration

This represents the maximum time a station can be in doze state before being deassociated from AP and since it is sent over a 16-bit field in 1024 ms time units, it is bounded to 18.64 hours as shown in equation 3.2.

$$\frac{2^{16} * 1024}{3600} = 18.64 \qquad Hours. \tag{3.2}$$

But there are some use cases where this is a frequent interval for the station to switch to awake state just to send a keep alive packet to AP (e.g fire alarm sensors). There are two ways imposed by TGah for improving this issue.

First is the usage of two most valued bits of 16-bit field as 1, 10, 100 and 1000 times scaling factor so that the Max idle duration can be scaled by 1000/4 = 2500 times and second is the ability enabled for AP to send different values for individual STAs or for the STAs to request this value from AP.

3.4.2 Station Classification

Wireless network can have several devices in them. It is possible that they differ in requirements regarding QoS, packet size, duty cycle and etcetera. For addressing different STAs with their requirements, TGah has developed two different types of STAs named Sensor and Offloading stations. The idea is to tag stations, in order to be able to implement networks based on each group's requirements.

Sensor stations are designed with limited power supply and may have limited capabilities. The limitations can be in their transmission and reception periodicity and/or packet size. They may require to go to doze mode for recovery after transmitting several packets. The number of associated Sensor STAs can reach up to 6000 per an AP.

Offloading stations, on the other hand, require high traffic transmission such as video streaming. Laptops, wireless gadgets and cameras are classified as this type.

Due to the high throughput required by the STAs of this kind the number of devices associated to an AP can not be as high as the previous type.

That being said, TGah specifies three different modes of BSS operation:

- Sensor only BSS
- Non-sensor only BSS
- Mixed mode, When the BSS contains both of the above

The frequency to wake up is higher in sensor mode compared to non-sensor and mixed mode. Different types of BSSs can be separated spatially or can be assigned different channels to minimize the effect of sensors of two types on each other.

3.4.3 Target Wake Time (TWT)

This feature aims to efficiently put stations in doze mode to improve power management. Here the STAs are given a Target Wake Time for their first interval start, minimum TWT, TWT interval, direction of packet flow for the first transmission, flow ID, channels on which the stations can transmit. The TWT can have two types as implicit or explicit.

Since the protection for TWT separately increases overhead, TGah suggest the grouping of of TWT time meaning that to assign TWT grouped side by side in time. By this mechanism, the AP is allowed to create TWT groups and inform STAs about them. The STAs, then send requests to join to a TWT group and the AP will assign it to the appropriate group.

4. SIMULATION ENVIRONMENT AND SYSTEM SETTINGS

As new technologies emerge rapidly nowadays, the importance of research and development supporting the new technologies rises significantly. Network simulation is a method in computer networks and communication where a software models various behaviors of the formulated networks either by using mathematical equations or by actually performing all the networks operations and capturing the results. This will allow network administrators to monitor and inspect the interaction between network entities, evaluate performance, tune its functionalities and correct potential defects before physically implementing a complex network. Using this approach saves a remarkable amount of budget and time in respect of resources.

A network simulator is a program capable of predicting the behavior of a designed computer network. They allow researchers to implement and test scenarios virtually where emulating the same in real world is highly difficult. Network simulators are useful in enabling researchers to test new protocols by supporting various networks technologies in a controlled environment. Nevertheless, the accuracy of network simulators are still in progress. Their evaluation depends on several factors like testability, visual (graphical) interface, modeling assistance, resource management, computational power, time limitation and how detailed a simulator can be with respect to network entities deployment [45].

There are numerous network simulators available for academic and industrial use. Distinguished examples include OPNET [9], NetSim [4], Ns-2 [10], Ns-3 [11], J-Sim [7], QualNet [12], OMNeT++ [8]and JiST [6]. An extensive comparison between different network simulators has been conducted in [65] and [59] considering the key evaluation criteria. OMNeT++, as one of the best options, has shown a remarkable performance among other simulators regarding the use cases used in this thesis and thus is chosen to perform the simulation scenarios.

4.1 OMNeT++

OMNeT++ is a C++ based object-oriented discrete event simulation framework with modular structure [58]. Being open-source, OMNeT++ can either be used with GNU General Public License or under its own, that makes this software free for non-profit use. In addition, in discrete-event systems changes occur in discrete instances in time and event take zero time to happen so the system state is unchanged in between event [21]. It is important to mention that OMNeT++ is not a network simulator but a generalized framework that provides a base for building generic architecture to be utilized in various problem domains as:

- modeling of wired and wireless communication networks
- protocol modeling
- modeling of queuing networks
- modeling of multiprocessors and other distributed hardware systems
- validating of hardware architectures
- evaluating performance aspects of complex software systems

Feasibility of OMNeT++ to be implemented in different simulation frameworks and the fact that it is an open-source platform, makes OMNeT++ a perfect choice for developers to built frameworks upon it [13]. The simulator that has been developed to carry out the simulations in this thesis is based on INET frame work which is considered as the standard protocol model library of OMNeT++ that enclose models for wired and wireless link layer protocols along with many other models to support different application models.

CMDEBNV and TKENV are two user interfaces that OMNeT++ provides to its users. The first one is a command-line based, small, portable and fast user interface that is primarily designed for executing simulations in batches. The latter one, on the other hand, is a powerful Graphical User Interface (GUI) that provides three major tools namely *automatic animation*, *module output window* and *object inspector* that helps visualizing the formulated scenarios and enhances inspection and modification.

In general, OMNeT++ is capable of modeling and simulating any kind of discrete event system that consists of several entities and use messaging for communication among them. Due to its GUI support and feasibility to be embedded in simulation kernel, it is used in scenarios simulating communications and networks frequently [38]. Following are the main parts that an OMNeT++ model consists of:

- **NED language topology description (*.ned* files)**: that describe the module structure with parameters, gates, etc.
- **Simple module sources**: They basically are C++ files, with *.h* or *.cc* suffix.
- **Message definitions (*.msg* files)**: You can define various message types and add data fields to them. OMNeT++ will translate message definitions into full-fledged C++ classes.

Next, the aforementioned parts will be explained and discussed.

4.1.1 NED Language

A network model can be defined by Network Definition (NED) language in OMNeT++. NED is a descriptive language for defining the network that has been employed in OMNeT++. Constructing a model in NED includes defining the modules and their interconnections [45]. Typical parts of a NED description are simple module declarations, compound module definitions, network definitions and channels.

Simple module declarations describe the interface of the module: gates and parameters. Compound module definitions consist of the declaration of the module's external interface (gates and parameters), and the definition of submodules and their interconnection. Network definitions are compound modules that qualify as self-contained simulation models [59].

4.1.2 Module Structure

As mentioned earlier, OMNeT++ has a component-based modular structure that is also one of its main advantages over other platforms. This enhances reusability of components, called modules, that construct a network by combining in different manners. As Figure 4.1 presents the simplified structure, there are two types of modules in OMNeT++: Simple and Compound modules.

Simple modules are the basic elements in OMNeT++ that perform atomic function and can not be divided into simpler modules. They have several virtual functions

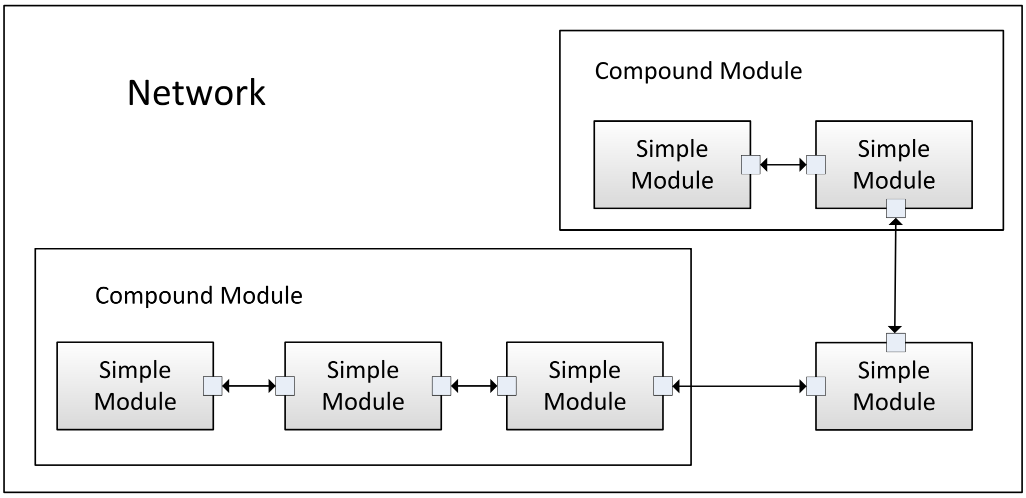


Figure 4.1 *Schematics of modules in OMNeT++*

that can be defined by the user to implement a specific model's behavior. Due to the fact that components interconnect through messages, message handling is one of the most important functions and is called whenever kernel receives a message.

By combining two or more simple modules, a compound modules can be constructed. Compound modules have hierarchal structure but the depth of their hierarchy is unlimited in OMNeT++. The definition of compound modules is same as their simple version. However, their most significant task is to add flexibility to the system so the system can be built in an structured and organized way.

4.1.3 Gates, Connections and Messages

OMNeT++ modules connect via gates that have three types: *input*, *output* and *inout*. The latter one is the combination of first two gates. Because OMNeT++ only use one directional communication, there must be at least an inout or an input plus an output gate defined for each module to perform correctly [60]. Gates facilitate and direct the flow of messages between two specific modules.

Messaging is an essential part of the system architecture as all modules in a system model communicate by exchanging messages. Depending on the model type, OMNeT++ posess a message class that determine the type of messages as events, packets, commands, frames, bits and etcetera. In addition, messages can facilitate intra-layer information delivery and can also be used to implement timers in one module when the source and destination are set to the same module [8].

Connections (or links), which are represented as arrows in 4.1, join gates together to enable message exchange. They can be created within one level of module hierarchy which means that they can not surpass across several layers. One can connect two submodule gates, a submodule gate and the compound gates, or two gates of the parent module.

4.2 General Setting

Using the tools to carry out simulations for the desired network designs, there are plenty of parameters and factors to consider that will affect various parts of the simulation and thus alter the results. These parameters are either dependent on the protocol that is used in the system development or they are put into the system as of the described or designed network topology and scenarios. The characteristics of environment and traffic model will be discussed in the this section.

4.2.1 Environment

IEEE 802.11AH is defined to be applied to wide range of applications and scenarios. This thesis targets the study and simulation of infrastructure BSSs and thus, unlike ad-hoc network topology, there is at least an AP present in all the scenarios and simulations. The environment properties, in this manner, varies in respect of the number of APs involved in that particular study case. Various simulation environments characteristics and issues related to arrangement of APs are discussed in the following.

Single AP & Multi AP

Simulation scenarios in this thesis are divided to two groups based on the number of APs. It is due to several reasons like maintaining the effective throughput, increasing network capacity and enhancing network coverage.

When using a single AP in the network, all STAs need to associate and connect to that AP to be able to communicate whiten that service set. The AP is located in the center of a circle where all STAs are randomly distributed in it to simulate the real world scenario. The maximum distance (i.e. circle radius) where AP can reach STAs depends on the MCS and the corresponding sensitivity used. Connection availability between STA and AP is guaranteed by assigning identical power to both ends of communication.

Considering that the STAs are distributed in a circle, it may happen that two STAs on the opposite sides of coverage area would not be able to hear eachother and therefore the hidden node problem, that has been described earlier in section 2.3.5, will occur in the network.

In the second scheme the area coverage is provided by using multiple APs that are located side by side. This is referred as Multi AP scenarios in the simulations. Again the STAs are distributed in a random manner to mimic the actual performance situation as much as possible. STAs, then, choose to associate with an AP based on the received beacon SNR from multiple APs.

Due to overlapping of the APs coverage area with their neighboring ones, some STAs that are possibly located in that area may suffer from exposed node problem. In exposed node problem, a STA associated to an AP would mistakingly detect the channel as busy because of the ongoing transmission of a STA that is associated to the neighboring AP [63].

Overlapping Basic Service Set (OBSS)

Overlapping basic service set is an inevitable phenomenon in most of technology deployments nowadays. It occurs when two or more APs that are not related to each other but are functioning on the same channel are located in a distance that can interfere in each other's coverage range. Thus, transmissions in each BSS can be influenced by the other one [35]. Figure 4.2 illustrates an OBSS including two APs.

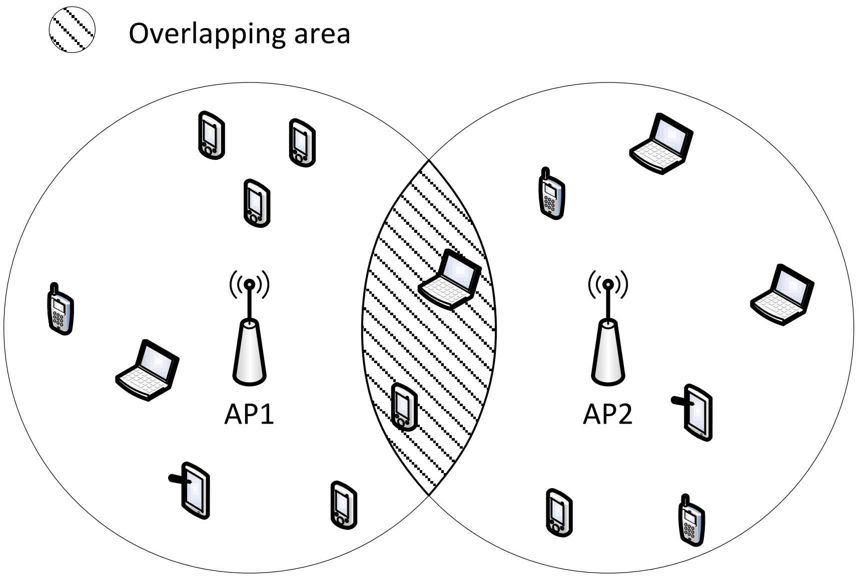


***Figure** 4.2 Overlapping basic service set scheme*

There are several literatures studying the effect of OBSS and also presenting solutions, trying to mitigate its effect on network performance including a novel carrier sensing mechanism [30] and a new admission control scheme [67]. IEEE 802.11AH task group has defined a set of requirements for OBSS case [17]. The OBSS effects on the system throughput have been evaluated in [53], using the defined requirements and different maximum overlapping area between two APs.

4.2.2 Traffic

Traffic in networks are categorized into two main parts: Uplink and Downlink. Uplink mostly refers to the data transferred from devices in lower network hierarchy to the higher ones. Conversely, the traffic destined to devices in higher network hierarchy are known as downlink. Considering the scenarios and simulation in this thesis and in this use case in general, the flow of data from STA to AP will be referred as uplink whereas the flow in the opposite direction will be known as downlink.

The only data flow that will be considered throughout this thesis will be uplink type because there will be no data transfered from AP to STAs. Moreover, STAs can use this to their benefit and go to idle mode for power saving because they know that they are the initiators of transmission. This implies that there is no data to be sent from STAs, therefore no need to perform CS and stay awake.

Other point of view, traffic can be discussed by its periodicity which can be grouped into two class of *saturated* and *non-saturated* traffic. Saturated traffic means that there is always at least a packet in STAs transmission queue to be sent. But in non-saturated mode the traffic pattern can be altered based on the studied scenario. The default non-saturated traffic in this thesis is set to one packet in every beacon interval which is equal to 10 packets per second according to network configurations. The packet generation start time has been distributed in a uniformly random fashion in the starting beacon interval to avoid congestion while commencing the simulation.

4.3 MAC Layer Setting

IEEE 802.11AH MAC layer is designed with number of unique MAC layer properties to fulfill the requirements of the use cases it has been developed for. There are specific values set for sensor networks by the amendments that is necessary to construct service and protocol data units in MAC layer so that it can be mapped to the corresponding PHY layer by using a convergence procedure. Elements that will be discussed in this section have an important effect in formulating scenarios to make it as close to real world condition as possible.

4.3.1 Beaconing

As a management frame, beacons are used to enhance network's overall performance and update the system with new parameter values so the network can adapt effectively to system changes. Beacon frames are sent by APs in each BSS periodically and is destined to the STAs associated to that AP. They are set to be transmitted once in every 100 microseconds and because the management frames are always sent in the most robust modulation, its duration is fixed to 1280 microseconds regardless of the MCS used to transmit DATA frame.

Beacons are not used when DCF is deployed in the network, but as it is the only coordination function used in this thesis, it has been formulated in the simulations to mimic the real case scenarios as much as possible and also to help implement some features in the developed simulator.

4.3.2 DATA Packet Properties

Since the development of IEEE 802.11AH has started, its applicability for sensor networks has been a high priority for the developers. There are many use cases that IEEE 802.11AH is aimed for which consequently resulted in having a Maximum Service Data Unit (MSDU) ranging from 64 to 2400 Bytes and PER ranging from 10% to 0.05% [20]. However these parameters are bounded to the specific use cases chosen for the applications in the network.

As per the growing rate of devices used in the world and the increasing demand for communication, the urge to use IoT networks is inevitable. Thus, IEEE 802.11AH is expected to be used as the main technology for this use case and the chosen maximum size for DATA packet (L_{DATA}) is set to be equal to 256 Bytes as specified by traffic models in [20].

4.3.3 IEEE 802.11AH Constants

There are defined parameters for each technology that is set by the corresponding task group and TGah have specified fixed parameters for IEEE 802.11AH technology in its amendment. Values presented here are based on the latest updates in [3] but they are subject to change as IEEE 802.11AH is still under development. Table 4.1 lists the system simulation parameter values.

Table 4.1 *IEEE802.11AH system simulation parameters*

Parameter	Value
T_{sym}	40 us
SlotTime	52 us
MAC header	14 Bytes
PHY header	$6\times T_{\text{sym}}$
ACK	PHY header
Basic data rate (MCS 0)	650 Kbps
SIFS	160 us
DIFS	SIFS + 2×SlotTime
CWmin	15
CWmax	1023
m_{short}	7
m_{long}	4
Traffic interval	100 ms
Beacon interval	100 ms
DATA packet size	256 Byte

Here, T_{sym} is a symbol duration in OFDM and is fixed which implies that it is not dependent on modulation and coding. MAC and PHY headers refer to the ovehrhaed value that each layer adds to the frame but the latter one is in seconds because PHY header is always transmitted by the most robust MCS and is fixed like the number of required OFDM symbols for its transmission. Therefore, it always takes a specific amount of time to transmit PHY header. CWmin and CWmax represent the minimum and maximum contention value respectively whereas m_{short} and m_{long} specify Short Retry Limit and Long Retry Limit correspondingly.

4.4 PHY Layer Setting

Like previous section, IEEE 802.11AH PHY layer also has several distinctive properties defined for it to meet the requirements in transmission of frames through wireless medium. These requirements are affected by various parameters including the channel condition, modulation and coding schemes and the physical equipments of the device used. The next section will provide more details on the studied parameters focused in this thesis.

4.4.1 Channel Properties

There are many factors that can affect a channel in wireless networks and thus the definition of channel can depend on several parameters. One of the main characteristics is the pathloss model that has been described in 2.4.4. *Pico Pathloss* model has been chosen to be used throughout this thesis based on the IEEE 802.11AH use cases definitions and requirements.

Moreover, thermal noise is taken into consideration in this thesis as another affecting factor of the channel properties and is defined as:

$$P_{watt} = kTB \tag{4.1}$$

where k is Boltzmann's constant measured in joules per kelvin and is equal to 1.38×10^{-23}, T is the temperature in kelvins and is set to 300 and B is equal to 2 MHz which denotes the bandwidth. By calculation, the thermal noise level would be equal to -111 dBm and a receiver noise figure of 7 dB is added to this value as well.

4.4.2 Sensitivity

Performance of a wireless device rests upon several factors like sensitivity, noise figure, baseband algorithm for channel estimation, decoding, demodulation and etcetera. Receiver sensitivity plays an important role of all the aforementioned factors and is one of the key specifications in a radio receiver. As the required performance quality of the receiver gets higher, the minimum required sensitivity becomes higher and that explains the desirability of higher sensitivity level to achieve better quality in radio reception [26].

Generally, the sensitivity of a wireless receiver is measured as the minimum input signal to have a specified output signal. On the other hand, the receiver sensitivity can be measured in dBm which the values in this thesis are used based on the defined use case and relative DATA packet size described in 4.3.2. To meet the requirements, the Packet Error Ratio (PER) must be less than 10% in [3] and the corresponding minimum sensitivity level is summarized in Table 4.2.

4.4.3 Energy Consumption Parameters

Energy consumption is one of the highest concerns in sensor network implementation. Design and resource limitations force developers to use power cautiously, thus

Table 4.2 *Minimum sensitivity level for different MCSs, L_{DATA} = 256 Bytes*

MCS index	Data rate (Kbps)	Minimum Sensitivity (dBm)
0	650	-92
1	1300	-89
2	1950	-87
3	2600	-84
4	3900	-80
5	5200	-76
6	5850	-75
7	6500	-74
8	7800	-69

power management and consumption models are carefully formulated. In addition, based on devices design complication and limitations, the amount of power can not be assumed as a considerably high value and therefore the default value of transmission power for devices is assumed to be 1 mW and is subjected to increase in cases a wider coverage is required. Evaluating the network from energy consumption point of view is generally calculated in mJ/packet representing the energy consumed to successfully send a packet.

There are several states during the whole functioning time of a STAs in the network that has been defined as *Transmit*, *Receive and CS* and *Sleep*. Energy consumption differs in every state that has been wrapped up in Table 4.3. A STA is in transmit mode while sending RTS and DATA, receiving mode while receiving management frame (e.g. beacon, ACK, CTS) and sleep for when the STA does not have any data to send.

Table 4.3 *Energy consumption in IEEE 802.11AH*

Mode	Energy consumption (mW)
Transmission	255
Receiving and CS	135
Sleep	1.5

It is good to note that the energy consumption for receiving and CS are considered as equal due to the negligible amount for energy used in baseband processing in comparison to energy consumption in the whole receiving mode.

5. IEEE 802.11AH MAC FEATURES PERFORMANCE EVALUATION

As described in Chapter 4 there are many new features developed in IEEE 802.11AH amendment for machine to machine communications for different use cases. It is really important to be able to have a comprehensive understanding about the proposed technology with respect to time and costs prior to implementation. To evaluate the performance and get a better real-world overview of the newly introduced technologies, simulations offer a stable and reliable approach.

This chapter aims to address some of the most important features that are beneficial in solving some of the highest concerned issues in IEEE 802.11AH implementations. These mainly target congestion management by spatial channel access control and adaptation.

5.1 IEEE 802.11AH Basic Dynamic Analysis

In this section, system analysis for throughput is presented by an analytical approach introduced in [46]. This model is based on the Markov chain and observing the system at periodic intervals. In the following, the state transition matrix and the relevant stationary distribution vector will be introduced. Then the analytical model will be presented and discussed. Finally, a comparison of the simulation and derived mathematical analysis will be presented for verification.

5.1.1 System Model and Parameters

Here, all the parameters and assumptions that have been applied to the model will be presented. For simplicity and to make mathematical analysis feasible, a BSS with one AP is formulated with an error-free channel where there are no hidden nodes. All STAs are assumed to start at the same time and are synchronized to have a perfectly matched slot times for starting possible packet generation. It is also assumed that the whole system simulation time is divided into small slots of d_{gen} that is equal to slot duration listed in Table 4.1.

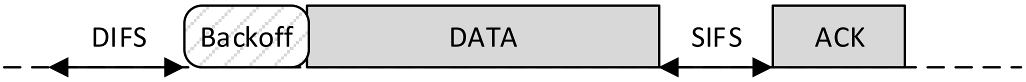


Figure 5.1 *Complete transmission cycle of a successful transmission*

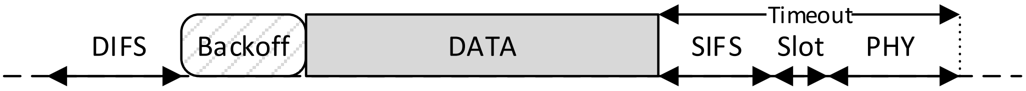


Figure 5.2 *Complete transmission cycle of a collided transmission*

Considering the basic access mechanism in our model, the complete transmission cycles are illustrated in Figure 5.1 and 5.2. Based on the transmission cycles, three different system state events are defined as:

- *Successful*: When there is just one transmission in the system and the STA successfully transmits it's DATA and ensure it's reception by getting an ACK. The duration of this event, d_{succ}, can be calculated by:

$$d_{succ} = \mathrm{DIFS} + \mathrm{DATA} + \mathrm{SIFS} + \mathrm{ACK} \tag{5.1}$$

- *Collision*: If there are, for any possible reasons, more than one simultaneous transmission initiated by different STAs, thus making it impossible in the AP to receive the packets correctly. As shown in Figure 5.2, the duration of this event, noted as d_{col}, can be formulated as:

$$d_{col} = \mathrm{DIFS} + \mathrm{DATA} + \mathrm{Timeout} \tag{5.2}$$

  where the *Timeout* is equal to:

$$\mathrm{Timeout} = \mathrm{SIFS} + \mathrm{SlotTime} + \mathrm{PHY} \tag{5.3}$$

- *Idle*: This is when there are no ongoing transmissions and the channel is free. This event duration is being noted by d_{idle}.

For STAs to have the opportunity to generate packets in every state of the system, we divide the system operation time into smaller slots of d_{gen} duration and therefore the 3 different event durations can be presented as $D_{suc/col/idle} \cdot d_{gen}$ is chosen such that the final values for $D_{suc/col/idle}$ are integers for ease of use. The packets are generated in a Bernoulli fashion and the STAs can try to access the channel with the probability p. The probability of a STA to generate a packet is δ.

Considering the system defined in this section, the transmission can occur in two modes. It may possible that there isn't any ongoing transmission in the system when a new packet arrives and the STA will immediately initiate the channel access process to send the packet, which is called the immediate transmission. On the other hand, a packet may arrive at one STA while the channel is busy and it is when STA uses probabilistic channel access to transmit the packet. Both methods suggest the Markov chain for proceeding in the analysis.

To better help with understanding, we need to establish the transmission probability matrix that summarizes all the states. This matrix is presented in Table 5.1.

Table* *5.1 *System states for immediate transmission*

States (n/m)	**1**	**2**	$\dots$	**m**	$\dots$	**U+1**
1	$s_{1,1}$	$s_{1,2}$	$\dots$	$s_{1,m}$	$\dots$	$s_{1,U+1}$
2	$s_{2,1}$	$s_{2,2}$	$\dots$	$s_{2,m}$	$\dots$	$s_{2,U+1}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
n	$s_{n,1}$	$s_{n,2}$	$\dots$	$s_{n,m}$	$\dots$	$s_{n,U+1}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
U+1	$s_{U+1,1}$	$s_{U+1,2}$	$\dots$	$s_{U+1,m}$	$\dots$	$s_{U+1,U+1}$

Each cell in this table correspond to all available state transitions for $n \longrightarrow m$. For getting a better understanding, Figure 5.3 continues to elaborate on one state transition with more details.

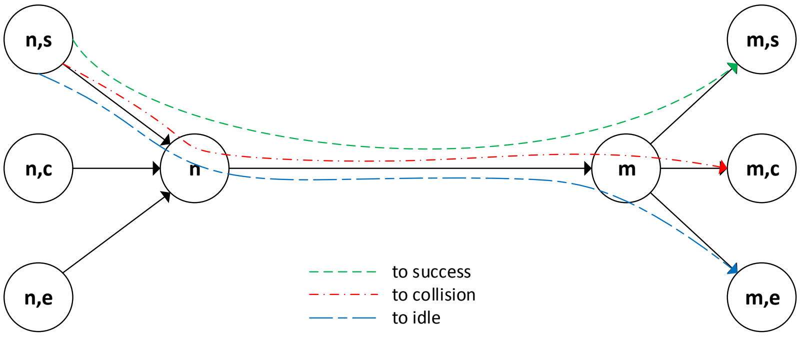


Figure* *5.3 *System state transitions Markov chain in immediate transmission mode*

5.1.2 Analytical Approach

In this section the analytical model will be discussed and the parameters will be introduced. The model is considering all of the states that can be experienced in the network. Thus, all the elements required for calculating throughput are derived in respect with the system state.

The total number of packets transmitted during the x^{th} event with n active STAs can be obtained from

$$N(n,x) = B(0, D_x|U-n)np(1-p)^{(n-1)} + B(1, D_x|U-n)(1-p)^n. \tag{5.4}$$

where D_x is the number of opportunities for a STA to generate new packets during the event x which can be of any *suc/col/idle*. U is the total number of users and $B_{suc/col/idle}(a, x|u)$ is the exact number of having a new arrivals during x number of slots, while there are u possible new STA to generate a packet. Additionally, the STAs can try to access the channel with probability p.

Second, the required time in average for the next system event is calculated by

$$\overline{V}_{(n,x)} = \sum_{m=0}^{U} \sum_{y=suc/col/idle} P_{(n,x)\longrightarrow(m,y)} D_y. \tag{5.5}$$

Here the probability of a state transition is presented as $P_{(n,x)\longrightarrow(m,y)}$ that can be calculated for all the transitions individually. n and m represent the number of existing users in each state while x and y refer to the current system state.

Finally, to compute the system throughput, the total number of packets that can be transmitted in the designated state can be derived from

$$E[N] = \sum_{n=0}^{U} \sum_{x=suc/col/idle} N(n,x)\pi_{(n,x)}^{(0)} \frac{1}{\overline{V}_{(n,x)}}. \tag{5.6}$$

Using the previously introduced formulas, the amount of data sent in packet generation interval in bits, which is another definition for throughput, can be obtained by

$$R = \frac{E[N]L_p}{d_{gen}} \tag{5.7}$$

where L_p is the length of the sent packet and d_{gen} is the duration it takes for a packet to be generated in the system.

5.1.3 Numerical Results

In this section the numerical results obtained from the introduced analytical model and the simulations will be presented to enable a robust understanding and comparison of the system throughput measured by the total number of successfully sent data packets. The presented model in 5.7 establishes a base for networks with all traffic models and different channel access methods like normal DCF and RTS/CTS.

As to align the simulation in this section with the simulations throughout this thesis, the normal DCF channel access mechanism is chosen for this simulation. The data rate generation is fixed to one packet per every 10 seconds with respect to requirements in [20]. The related results for simulations and analytical approach are shown in Figure 5.4.

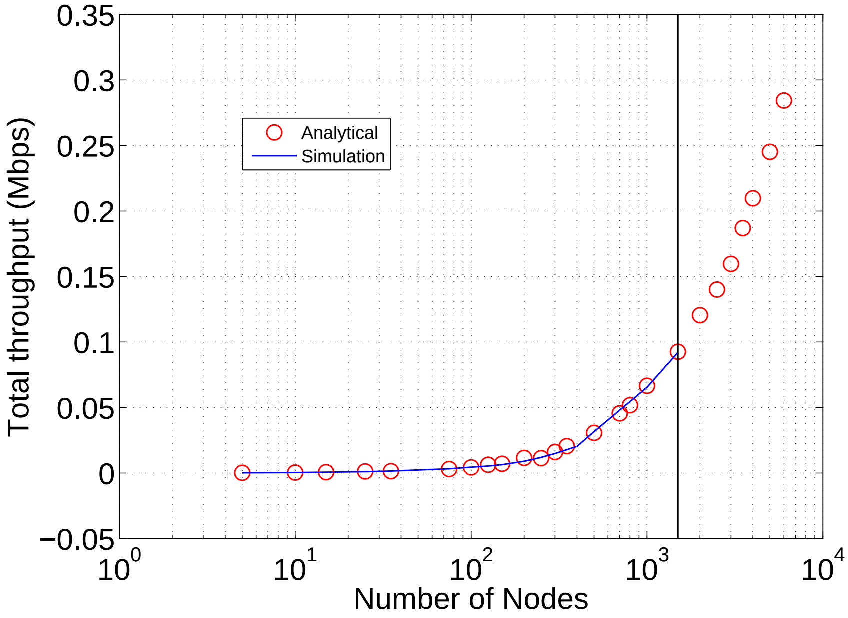


***Figure* 5.4** *Simulation and analysis throughput comparison for very high number of nodes*

It can be concluded that the results from simulations show a perfect convergence to the analytical model despite the fact that the simulation results are not available for very high number of nodes due to the high complexity of the simulations and limitations in the simulator. Nevertheless, the analytical model is able to give an insight for up to 6000 associated STAs.

5.2 RAW

While the main mechanism of RAW is previously described in 3.3.2, there are different parameters that affect the performance of RAW. Considering the importance of this mechanism and the amount of contribution it has towards network's overall performance enhancement we have choose to investigate this mechanism deeply in this thesis. Thus, different scenarios have been implemented to measure the network performance while RAW is enabled.

In the first part of this section, RAW performance is evaluated in respect of various number of RAW slots, i.e. N_{RAW} value, to find the best option to use throughout this thesis. Next, the performance of a network with RAW and legacy DCF is measured to illustrate the contribution of RAW regarding the previous approaches.

5.2.1 Optimum N_{RAW} value

The number of time slots used in a RAW, represented as N_{RAW}, plays an important factor in IEEE 802.11AH network performance. It is important to have in mind that this value can highly be effected by the MCS used in the packet transmission but due to robustness and reliability, MCS0 has been used to conduct the simulations in this part. Choosing very small number of RAW time slots does not impose any improvements over the normal DCF because too many STAs are allowed to contend at the same time. On the other hand, choosing a very high value for N_{RAW} will allocate a very shorter duration for each group of STAs to contend (T_{slot}) to the extend where there will not be enough time for completion of a successful transmission.

Two important factors, throughput and energy consumption, of the network has been compared, along with the average delay for successfully sent packets, for a range of different values for N_{RAW} in order to evaluate and determine the optimum number of time slots in a beacon interval. Figures 5.5, 5.6 and 5.7 illustrate the throughput, energy consumption and average delay of successfully sent packets for the modeled network. All the parameters are set to default.

A similar study conducted in [53] suggests that the optimum value for N_{RAW} is 10, but this research studies the network up to 100 STAs scenarios which is relatively low for use cases in this thesis that aims to support as many as 6000 nodes in the future. Thus, considering the limitations of this simulator, a more congested network has been modeled in this thesis.

As can be seen in the Figures 5.5 and 5.6 it can be concluded that for higher number of STAs the optimum value for N_{RAW} is equal to 17. It is obvious that when very few STAs are present in the system, lower values show a slightly better performance than 17 RAW time slots but for higher number of STAs, which is the objective of

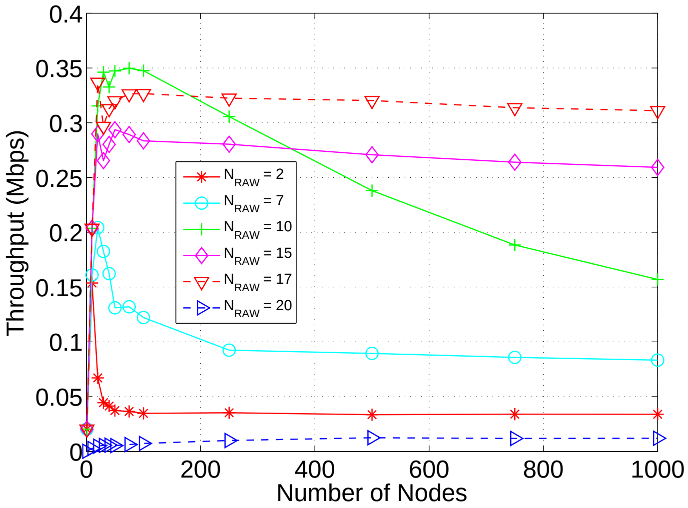


Figure 5.5 *Performance throughput for various* N_{RAW} *values*

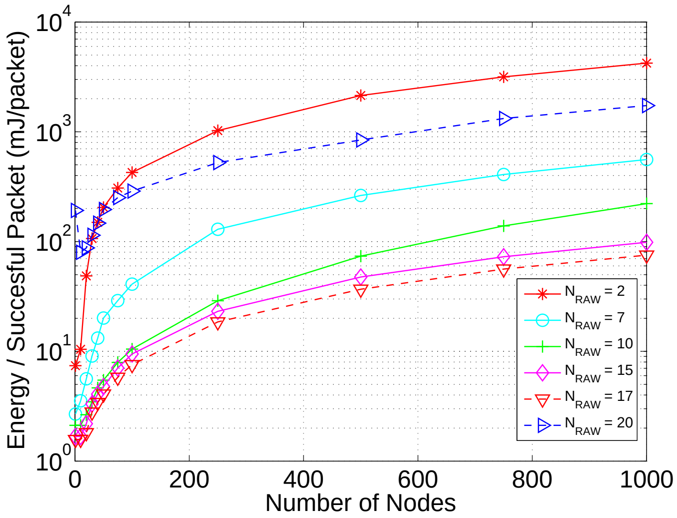


Figure 5.6 *Energy consumption for various* N_{RAW} *values*

this study, N_{RAW} set to 17 outperforms the other scenarios in matter of throughput.

It is inevitable to notice the performance of the system when N_{RAW} is equal to 20. From throughput point of view the performance has been dramatically degraded compared to the previous scenarios. That is because of the extreme conditions that timing in obligating to STAs in this scenarios. By the configuration and settings used in this network, dividing a beacon interval into 20 time slots will leave a very small margin for STAs to resolve collisions and back off counters. Therefore only a very few of them succeed to finish the required process to start data transmission before their allowed time for being active is over. This is also the cause for distinct difference for average delay in Figure 5.7.

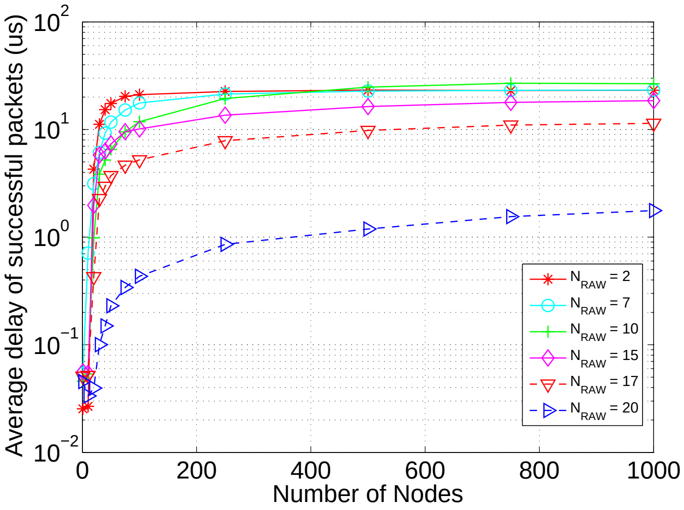


Figure 5.7 *Delay measurements for various N_{RAW} values*

5.2.2 RAW and DCF Comparison

For providing an insight about the RAW performance, a comparison is done between networks operating under the normal legacy DCF and RAW. All the assumptions and parameters that are used in simulating different values of N_{RAW} in RAW scheme is valid for the simulations conducted in this section. Different MCSs are used to enable a solid performance evaluation on throughput, energy consumption, fairness and delay.

As the conclusion of the section 5.2.1, the N_{RAW} value is set to 17. Simulation parameters are same as the previous section and only the MCS is varied for different scenarios. Throughput, energy consumption and average delay of the simulated system is being illustrated in Figures 5.8, 5.9 and 5.10 respectively.

Reviewing Figure 5.8 it is straight forward to get that using higher MCSs increases the system throughput due to the use of higher data rate. Therefore, by using higher data rates, more data can be transfered in certain amount of time. Furthermore, employing RAW mechanism into the network increases the whole throughput with significance in all three scenarios by packet transmission management.

As for the energy efficiency aspect of the system, it can be seen that using higher MCSs and consequently benefiting from higher data rates, transmitting a fixed amount of payload takes less time and relatively will result in lower energy consumption. The amount of optimization in energy consumption for each MCS clearly represents the amount of increase in throughput for its respective case. Again, using Raw will furthermore improve the energy consumption optimization for all scenar-

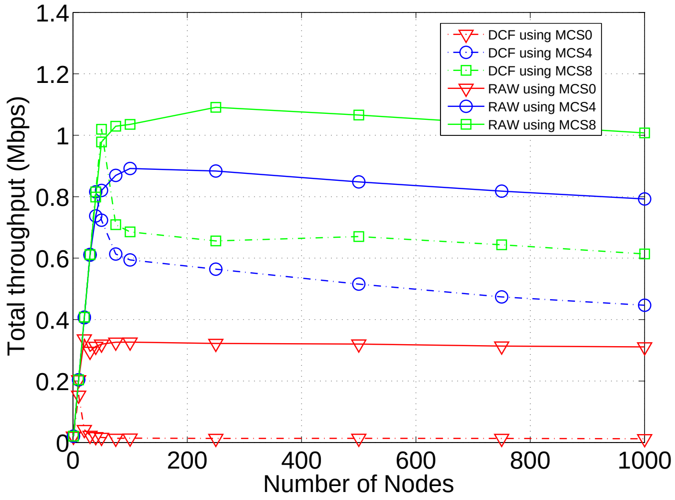


Figure 5.8 *Throughput comparison for different MCSs,* $N_{RAW} = 17$

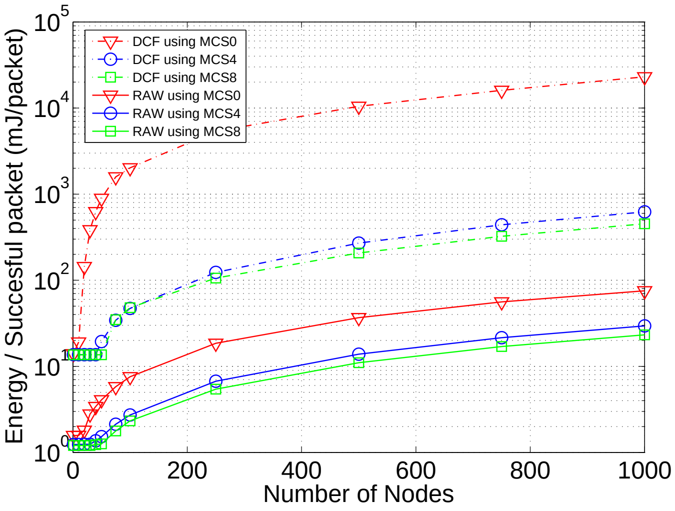


Figure 5.9 *Energy consumption for different MCSs,* $N_{RAW} = 17$

ios. This is achieved by activating a portion of nodes to try to access the channel and minimizing the contention time between them.

Inspecting the system for average delay measurements, it can be noticed that when lower number of STAs are present in the system, higher MCS scenarios experience less average delay because most of the generated packets are sent with very little delay. It can also be seen that for the cases with no congestion, DCF performs better than RAW. This is due to the fact that relatively low number of STAs tend to generate lower traffic in total which can be handled with not much collisions and that RAW mechanism is holding back the STAs to start transmission while the channel is not busy. But as the system gets congested, by increasing number of STAs and more traffic, the average delay is improved by employing RAW mechanism.

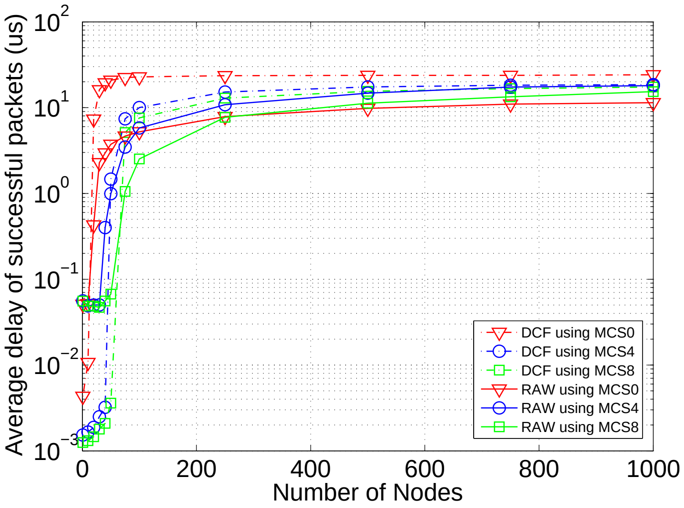


Figure 5.10 *Throughput comparison for different MCSs,* $N_{RAW} = 17$

Considering all the figures it can be concluded that using RAW definitely increases the system performance compared to legacy DCF significantly. Improvements in throughput and energy consumption which are the two main factors in IEEE 802.11AH networks are highly noticeable. Moreover, Average delay is decreased where is very important in the applications requiring strict delay-tolerant networks.

5.3 Sectorization

As described in section 3.3.4 there are two main type of sectorization introduced in IEEE 802.11AH specification. This thesis is mainly targeting the hidden node and OBSS problem by considering the spatial sectorization approach. The main idea behind spatial sectorization is to use the benefits of space division multiplexing along with time division multiplexing. Here the AP divides the coverage area into number of sectors prior to start the association phase. Once the STAs start to associate with an AP, they receive a sector ID of the one that they belong to. Then the AP divides the time between each beacon interval into equal intervals to assign to every sector. Each STA participating in any of the sectors will get the information about when it can start the channel access process from the information in the beacon that is sent periodically.

However, two basic configuration in this scheme for network deployment are investigated through simulations. System setting in this scenario are the default settings described in 4.2. The pathloss model used in these scenarios is the pico deployment introduced in 2.4.4. Moreover, The results from simulations with RAW in the previous sections are included in this section's figures to help better understand the possible and expected improvements of sectorization under different schemes.

In this section, performance evaluation of the aforementioned channel access algorithm in two different network equipment deployments using single AP and multiple AP to conceal the coverage area, will be presented.

5.3.1 Single AP scenario

In this section a simple network deployment has been studied using a single AP to administer the data transmission in BSS. As there is just one AP, no overlapping problem is expected to be observed. Thus network performance degradation will not occur due to this phenomenon. On the other hand, because only one AP is obliged to handle all the traffic in the BSS, after some point when the data traffic flow is increased due to the inclining amount of associated STAs, many collisions and delays in channel access will occur.

Next, various network evaluation criteria for network performance evaluation is used to carry out a comprehensive understanding of this comparison. All the simulation parameters are set to default and the number of RAW slots are set to 17 based on the results from Section 5.2.1. Figures 5.11, 5.12 and 5.13 are illustrating system throughput, energy consumption and average delay respectively.

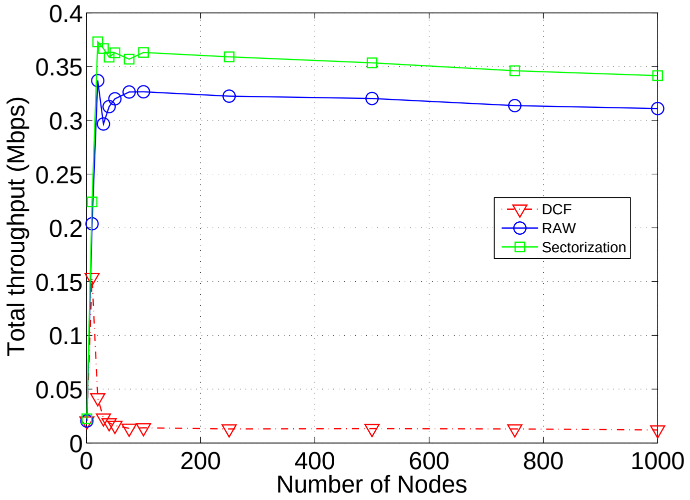


Figure 5.11 *Throughput comparison between generic and new scenarios for single AP*

As sectorization is targeting to handle the congestion problem by adding another dimension to channel access scheme the figures clearly present the effect of such implementation in the network. It is obvious that the use of sectorization improves system throughput with lower energy consumption. This is achieved by adding a

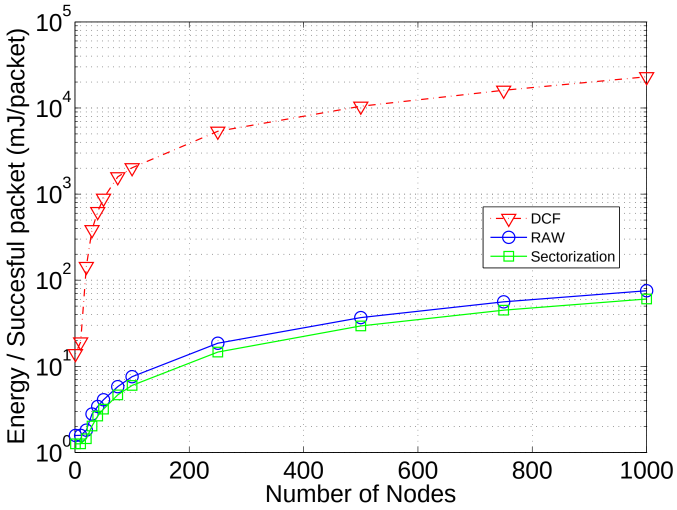


Figure 5.12 *Energy consumption for generic and new scenarios for single AP*

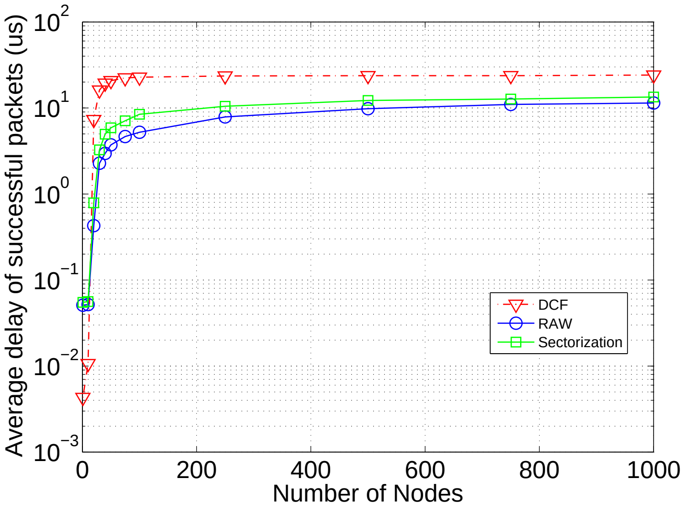


Figure 5.13 *Delay comparison between generic and new scenarios for successfully sent packets in single AP mode*

small amount of delay into packet transmission. However, the increment in delay is negligible in comparison to throughput and energy consumption optimization.

It is concluded that implementing sectorization helps to optimize the overall system performance in two of the highly important aspect and is better to be used in network implementations to benefit existing resources.

5.3.2 Multi AP scenario

As one of the most important aspects of deployments in any wireless network is its efficiency in covering the desired area, here we extend the single AP scenario into Multi AP scenario with 9 APs. Since there is a trade-off between transmission power of devices using wireless communication and their maximum transmission range, APs are located in a uniform pattern to cover a 500 meters square playground as illustrated in Figure 5.14. Here, network's total capacity is increased due to the implementation of multiple APs, where a 30% overlap between APs is imposed based on the arrangement of APs that causes more transmission complications.

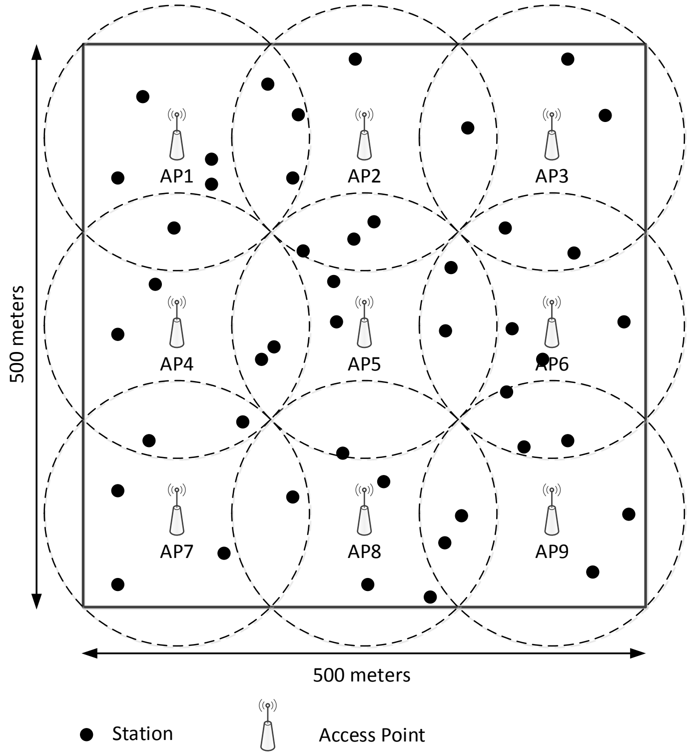


Figure 5.14 *Defined playground and AP positioning for multi access point scenario simulations*

All the previous assumption for parameters are still valid for this case. STAs are randomly distributed in the predefined playground and they certainly are able to associate to one of the existing APs. A STA will try to associate based on the one or multiple beacons that has received from AP(s). Because the STAs are assumed to be stationary throughout this thesis, a STA will not change its association once the association process is completed.

Once again total system throughput is compared for various N_{RAW} values in the new multi AP deployment to check and determine the optimum value to be used in relative scenarios. Simulation results, which are shown in Figure 5.15, depict that although having 17 RAW time slots still have better performance than most of the other MCSs but in this simulation settings, having N_{RAW} equal to 13 outperforms all the other modulation and coding schemes. Hence, for all the simulations with 9 AP, the number of RAW slots in each beacon interval will be set to 13 to get the

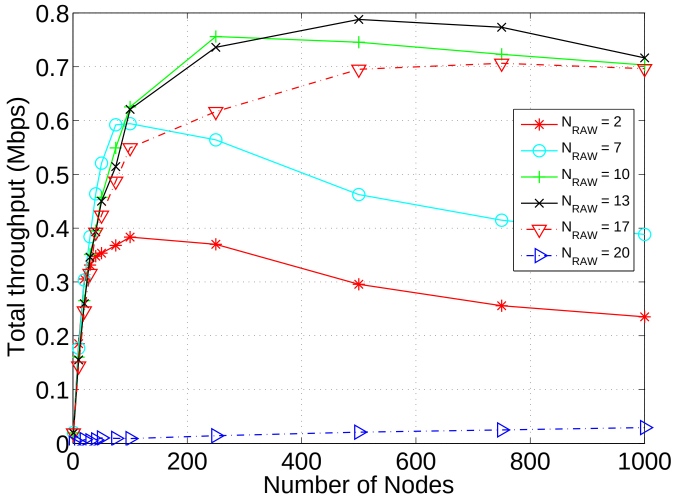


Figure 5.15 *Total system throughput comparison for different MCSs in multi-AP mode for scenario with 9 APs.*

maximum performance of the resources.

Performance evaluation of utilizing sectorization in multi AP scenarios over legacy DCF, RAW and sectorization in MCS0 has been conducted. Their comparison is summarized in Figures 5.16, 5.17 and 5.18 which are representing total throughput, energy consumption and average delay of the successfully sent packets respectively.

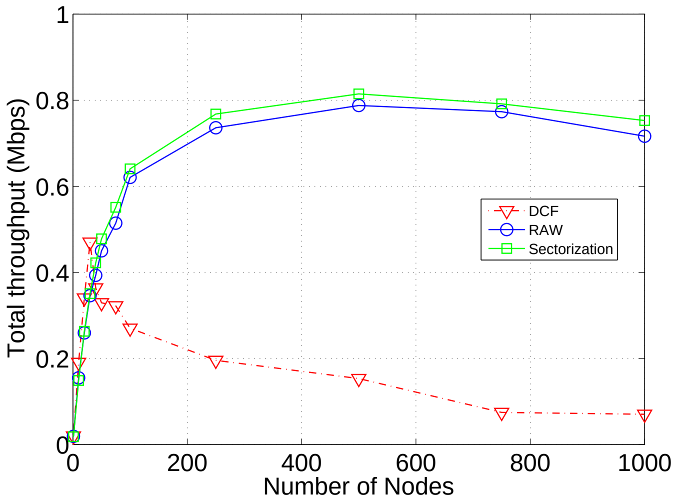


Figure 5.16 *Total throughput comparison between legacy DCF, RAW and Sectorization for 9 APs,* $N_{RAW} = 13$

Optimization in every important aspect of the network is clearly visible by inspecting the provided figures. It can be concluded that implementing RAW in multi AP scenarios also improve total throughput and decrease energy consumption. The superiority of applying RAW and sectorization in multi AP is seen from certain

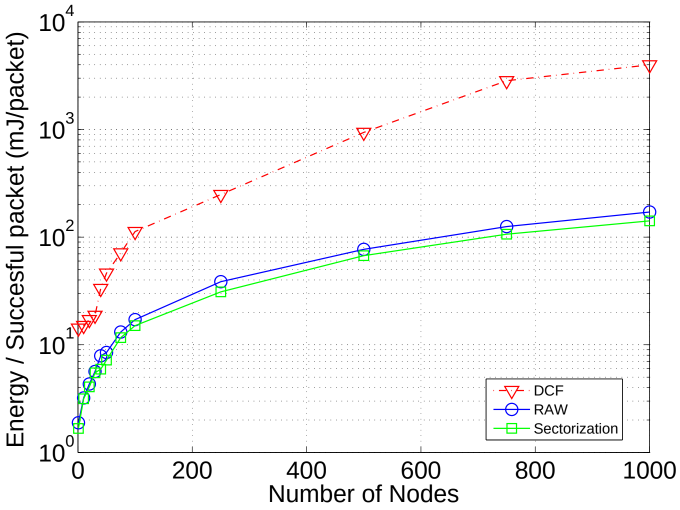


Figure 5.17 *Energy consumption comparison between legacy DCF, RAW and Sectorization for 9 APs,* $N_{RAW} = 13$

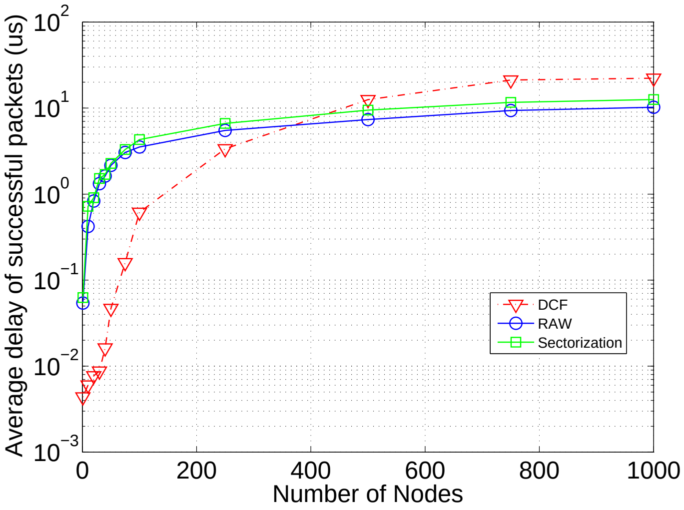


Figure 5.18 *Average delay comparison between legacy DCF, RAW and Sectorization for 9 APs,* $N_{RAW} = 13$

point in the figure where the system gets saturated relative to use of 9 APs in the multi AP implementation. Looking at Figure 5.18 it may seem that the network is not efficient using enhanced channel access mechanisms but studying the trade-off among all aspects in all three figures, the excess delay in the earlier stage of network is acceptable towards better performance regarding total throughput and consumed energy.

6. CONCLUSION

This thesis focused on further optimizing the performance of IEEE 802.11AH standards. This standard is being developed for ultimately handling networks with up to 6000 connected devices having relatively low data rate and limited power for everyday use. The optimization has been conducted in respect of total network throughput, energy consumption per a successfully sent packet and average delay of a successfully transmitted packet. These measurements are carried out in a developed simulator which is used throughout this thesis.

The aforementioned simulator has been developed using OMNeT++ platform and has been tested for accuracy using an analytical model which has been developed and introduced in this thesis. This model is based on Markov chain and considers all the possible states a node in the simulated networks may encounter, which are listed as successful transmission, collision and idle mode. Comparing the results shows that the simulator is genuine and has high accuracy.

Considering networks with high number of associated devices, saturation is one of the major problems to be addressed. It is in direct relation with number of nodes and their data rates. When huge number of STAs are trying to start accessing a shared channel in wireless technologies, a lot of collisions are expected to occur while using legacy DCF mechanism. Moreover, hidden node phenomenon is another common issue to deal with when multiple STAs are not able to hear each other while trying to detect channel status. Enhanced channel access mechanisms are an important approach toward solving these issues.

Restricted Access Window (RAW) has been implemented to cope with increasing number of collisions in networks with high number of associated devices and has shown a significant improvement regarding the legacy DCF channel access in total system throughput, energy consumption and average delay in packet transmission. The optimization has been taken to the next level by implementing sectorization as another channel access mechanism and has shown its superiority over the other mechanisms in optimizing the overall network performance. It is important to mention that sectorization introduces higher average delay in packet transmission which is negligible compared to the improvements in throughput and energy consumption.

In addition, two types of scenarios are conducted using different number of APs. Firstly, a single AP is used to manage the whole traffic in the defined coverage and for the second scenario we have arranged 9 APs to cover the same area. The benefits of using multi AP over single AP are to decrease the required transmitting power for devices to be able to successfully reach the AP and also to increase the overall network capacity. On the other hand, using multi AP scenario increases the amount of interference between neighboring OBSS and degrades system throughput. It is crucial to mention that the optimum number of N_{RAW} used in every scenario is dependent on the specific setting corresponding to it and this value has to be determined by the change of network characteristics and topology.

Finally, it can be concluded that using RAW and sectorization definitely help to overcome the overloading in congested networks and has advantages from throughput, energy consumption and average delay point of view. Network implementation in a multi AP fashion will provide more capacity and decrease required power, which is of high importance in IoT sensor network design, but adds more complexity in handling interferences. It is also recommended to choose N_{RAW} in an adaptive manner. This way, one can assure to get the optimum performance in cases when the network or traffic behavior alters in time.

There are many enhanced features defined in designing IEEE 802.11AH to meet the requirements for IoT use cases which are partly covered in this thesis. Meanwhile, the amendment for this technology is being updated and the urge for evaluating is left for future work.

BIBLIOGRAPHY

[1] "3GPP TR 25.996 - Technical Specification Group Radio Access Network; Spatial channel model for Multiple Input Multiple Output (MIMO) simulations, Section 5."

[2] "3GPP TR 36.814 - Further advancements for E-UTRA physical layer aspects, Annex A.2 - system simulation scenario."

[3] *Draft Standard for Information technology-Telecommunications and information exchange between systems Local and metropolitan area networks-Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 6: Sub 1 GHz License Exempt Operation.* IEEE P802.11ah/D0.2, New York, 2013.

[4] "Boson NetSim Network Simulator," [Accessed on: 18.02.2015], Available: http://www.boson.com/netsim-cisco-network-simulator.

[5] "IEEE 802.11 WLAN," [Accessed on: 18.02.2015], Available: http://standards.ieee.org/getieee802/802.11.html.

[6] "JiST," [Accessed on: 18.02.2015], Available: http://jist.ece.cornell.edu/.

[7] "JSim Java-based Simulation System," [Accessed on: 18.02.2015], Available: http://www.physiome.org/jsim/.

[8] "OMNeT++," [Accessed on: 18.02.2015], Available: http://omnetpp.org/.

[9] "OPNET Modeler Suite," [Accessed on: 18.02.2015], Available: http://www.riverbed.com/products/performance-management-control/network-performance-management/network-simulation.html.

[10] "The Network Simulator - Ns-2," [Accessed on: 18.02.2015], Available: http://www.isi.edu/nsnam/ns/.

[11] "The Network Simulator - Ns-3," [Accessed on: 18.02.2015], Available: http://www.nsnam.org/.

[12] "The QualNet communications simulation platform," [Accessed on: 18.02.2015], Available: http://web.scalable-networks.com/content/qualnet.

[13] "INET Framework," [Accessed on: 19.02.2015], Available: http://inet.omnetpp.org/.

[14] *Draft Standard for Information technology-Telecommunications and information exchange between systems Local and metropolitan area networks-Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 6: Sub 1 GHz License Exempt Operation.* IEEE P802.11REVmc/D1.2, New York, April 2013.

[15] "TGac Channel Model Addendum," IEEE 802.11-09/0308r12, March, 2010.

[16] *IEEE Standard for Information technology-Telecommunications and information exchange between systems Local and metropolitan area networks-Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.* IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007), New York, March 2012.

[17] A. Ashley, B. Hart, and G. Smith, "IEEE P802.11 Wireless LANs - OBSS Requirements," IEEE 802.11-08/0944r5, July, 2008.

[18] S. Aust, "Proposed IEEE 802.11ah use cases," IEEE 802.11-11/0017r5, January, 2011.

[19] N. Bari, G. Mani, and S. Berkovich, "Internet of Things as a Methodological Concept," in *Computing for Geospatial Research and Application (COM.Geo), 2013 Fourth International Conference on*, July 2013, pp. 48–55.

[20] M. Cheong, "TGah Functional Requirements and Evaluation Methodology," IEEE 802.11-11/0905r5, January, 2012.

[21] B. K. Choi and D. Kang, *Modeling and Simulation of Discrete Event Systems.* John Wiley & Sons, Inc, 2013.

[22] N. Choi, S. Han, Y. Seok, Y. Choi, and T. Kwon, "Hybrid distributed coordination function for next-generation high-bandwidth wlans," in *Local Computer Networks, Proceedings 2006 31st IEEE Conference on*, Nov 2006, pp. 308–315.

[23] K.-H. Chou and W. Lin, "Performance analysis of packet aggregation for ieee 802.11 pcf mac-based wireless networks," *Wireless Communications, IEEE Transactions on*, vol. 12, no. 4, pp. 1441–1447, April 2013.

[24] L. Coetzee and J. Eksteen, "The Internet of Things - promise for the future? An introduction," in *IST-Africa Conference Proceedings, 2011*, May 2011, pp. 1–9.

[25] D. D. Coleman and D. A. Westcott, *CWNA: Certified Wireless Network Administrator Study Guide.* Wiley Publishing, Inc., Nov 2006.

[26] S. Das, "Optimizing mobile communication receiver design for sensitivity boosting," in *Emerging Trends in Communication, Control, Signal Processing Computing Applications (C2SPCA), 2013 International Conference on*, Oct 2013, pp. 1–6.

[27] R. de Vegt, "Potential compromise for IEEE 802.11ah use case document," IEEE 802.11-11/0457r0, March, 2011.

[28] V. Erceg, L. Schumacher, and P. Kyritsi, "TGn Channel Model," IEEE 802.11-03/940r4, May, 2004.

[29] P. Fang, "Traffic information dissemination use case," IEEE 802.11-11/0763r0, May, 2011.

[30] Y. Fang, D. Gu, A. McDonald, and J. Zhang, "A two-level carrier sensing mechanism for overlapping bss problem in wlan," in *Local and Metropolitan Area Networks, 2005. LANMAN 2005. The 14th IEEE Workshop on*, Sept 2005, pp. 6 pp.–6.

[31] M. S. Gast, *802.11 Wireless Networks: The Definitive Guide, 2nd Edition.* O'Reilly Media, April 2005.

[32] V. Gazis, K. Sasloglou, N. Frangiadakis, and P. Kikiras, "Wireless sensor networking, automation technologies and machine to machine developments on the path to the internet of things," in *Informatics (PCI), 2012 16th Panhellenic Conference on*, Oct 2012, pp. 276–282.

[33] M. Iwaoka, "IEEE 802.11ah use case - industrial process automation," IEEE 802.11-11/0260r1, February, 2011.

[34] J. Jeong, H. Kim, T. Lee, and J. Shin, "An analysis of hidden node problem in ieee 802.11 multihop networks," in *Networked Computing and Advanced Information Management (NCM), 2010 Sixth International Conference on*, Aug 2010, pp. 282–285.

[35] H. Kang, G. Ko, I. Kim, J. Oh, M.-S. Song, and J. ick Choi, "Overlapping bss interference mitigation among wlan systems," in *ICT Convergence (ICTC), 2013 International Conference on*, Oct 2013, pp. 913–917.

[36] J. Kim, D. Kim, K.-W. Lim, Y.-B. Ko, and S.-Y. Lee, "Improving the reliability of IEEE 802.11s based wireless mesh networks for smart grid systems," *Communications and Networks, Journal of*, vol. 14, no. 6, pp. 629–639, Dec 2012.

[37] S. Kim, "IEEE 802.11ah use case - outdoor Wi-Fi for cellular traffic offloading," IEEE 802.11-11/0244r1, February, 2011.

[38] B. A. Kozlovszky, M. and A. Varga, "Enabling OMNeT++-based simulations on Grid Systems," in *Proceedings of the 2nd International Workshop on OMNeT++ (hosted by SIMUTools 2009).*, 2009.

[39] S. Kuppa and R. Prakash, "Adaptive ieee 802.11 dcf scheme with knowledge-based backoff," in *Wireless Communications and Networking Conference, 2005 IEEE*, vol. 1, March 2005, pp. 63–68 Vol. 1.

[40] N. Langhammer and R. Kays, "Performance evaluation of wireless home automation networks in indoor scenarios," *Smart Grid, IEEE Transactions on*, vol. 3, no. 4, pp. 2252–2261, Dec 2012.

[41] J. Lorincz and D. Begusic, "Physical layer analysis of emerging ieee 802.11n wlan standard," in *Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference*, vol. 1, Feb 2006, pp. 6 pp.–194.

[42] D. Lund, C. MacGillivray, V. Turner, and M. Morales, "Worldwide and Regional Internet of Things (IoT) 2014-2020 Forecast: A Virtuous Circle of Proven Value and Demand," May 2014, pp. 1–27.

[43] I. Marsic, *Wireless Networks. Local and Ad Hoc Networks.* Department of Electrical and Computer Engineering and the CAIP Center, Rutgers University.

[44] G. Mendez, M. Yunus, and S. Mukhopadhyay, "A wifi based smart wireless sensor network for monitoring an agricultural environment," in *Instrumentation and Measurement Technology Conference (I2MTC), 2012 IEEE International*, May 2012, pp. 2640–2645.

[45] S. A. H. N. I. Sarkar, "A review of simulation of telecommunication networks: Simulators, classification, comparison, methodologies, and recommendations," in *Journal of Selected Areas in Telecommunications (JSAT)*, March 2011.

[46] A. Ometov, N. Daneshfar, A. Hazmi, S. Andreev, L. F. D. Carpio, P. Amin, J. T. Y. Koucheryavy, and M. Valkama, "Analyzing Traffic Dynamics of IEEE 802.11ah Technology for Massive MTC Deployments," in *IEEE Internet of Things Journal*, Jan 2015, submitted.

[47] K. Pahlavan and P. Krishnamurthy, *Principles of Wireless Networks: A Unified Approach.* Prentice Hall - Paper, 608 pp, 2002.

[48] M. Park, "Additional indoor use cases for 802.11ah," IEEE 802.11-11/0241r0, February, 2011.

[49] ——, “IEEE 802.11 Wireless LANs - Specification Framework for TGah,” IEEE 802.11-11/1137r15, May, 2013.

[50] ——, “Proposed Specification Framework for TGah,” IEEE 802.11-11/1137r12, November, 2012.

[51] E. Perahia and R. Stacey, *Next Generation Wireless LANs, 802.11n and 802.11ac.* Cambridge University Press, May 2013.

[52] R. Porat, S. Yong, and K. Doppler, “TGah Channel Model,” IEEE 802.11-11/0968r3, November, 2011.

[53] O. Raeesi, J. Pirskanen, A. Hazmi, J. Talvitie, and M. Valkama, “Performance enhancement and evaluation of ieee 802.11ah multi-access point network using restricted access window mechanism,” in *Distributed Computing in Sensor Systems (DCOSS), 2014 IEEE International Conference on*, May 2014, pp. 287–293.

[54] V. Rohokale, N. Prasad, and R. Prasad, “A cooperative internet of things (iot) for rural healthcare monitoring and control,” in *Wireless Communication, Vehicular Technology, Information Theory and Aerospace Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on*, Feb 2011, pp. 1–6.

[55] J. Simo Reigadas, A. Martinez-Fernandez, J. Ramos-Lopez, and J. Seoane-Pascual, “Modeling and optimizing ieee 802.11 dcf for long-distance links,” *Mobile Computing, IEEE Transactions on*, vol. 9, no. 6, pp. 881–896, June 2010.

[56] W. Song, “IEEE 802.11ah use case - outdoor environmental / agricultural monitoring,” IEEE 802.11-11/0253r0, February, 2011.

[57] W. Sun, M. Choi, and S. Choi, “Ieee 802.11ah: A long range 802.11 waln at sub 1 ghz,” in *Journal of ICT Standardization*, vol. 1, May 2013, pp. pp.83–107.

[58] A. Varga, “The OMNeT++ Discrete Event Simulation System,” in *Proceedings of the European Simulation Multiconference (ESM)*, 2001.

[59] A. Varga and R. Hornig, “An overview of the OMNeT++ simulation environment,” in *Proceedings of the 1st international conference on Simulation tools and techniques for communications, networks and systems & workshops (Simutools)*, 2008, pp. 1–10.

[60] A. Varga and Y. A. Sekercioglu, “Parallel Simulation Made Easy With OMNeT++,” in *Research, Development and Application on Information and*

Telecommunication Technology (ICT Journal), vol. E-1, Number 1 (5), 2008, pp. 5–14.

[61] G. Wang, X. Zhong, S. Mei, and J. Wang, "A new constrained-send mechanism to enhance the performance of ieee 802.11 dcf," in *Communications and Networking in China (CHINACOM), 2011 6th International ICST Conference on*, Aug 2011, pp. 448–452.

[62] L. Wang, "Considerations of compatibility with 802.11v and 11k," IEEE 802.11-10/0973r2, July, 2011.

[63] L. Wang, K. Wu, and M. Hamdi, "Combating hidden and exposed terminal problems in wireless networks," *Wireless Communications, IEEE Transactions on*, vol. 11, no. 11, pp. 4204–4213, November 2012.

[64] W. Wang, Y. Xu, and M. Khanna, "A survey on the communication architectures in smart grid," *Computer Networks*, vol. 55, no. 15, pp. 3604 – 3629, 2011. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S138912861100260X

[65] E. Weingartner, H. vom Lehn, and K. Wehrle, "A performance comparison of recent network simulators," in *Communications, 2009. ICC '09. IEEE International Conference on*, June 2009, pp. 1–5.

[66] X. Xu and X. Lin, "Throughput enhancement of the ieee 802.11 dcf in fading channel," in *Wireless and Optical Communications Networks, 2006 IFIP International Conference on*, 2006, pp. 5 pp.–5.

[67] Y. Yin and T. Jiang, "A new admission control scheme for the overlapping bss issues in the 802.11 wlans," in *Communications and Information Technologies (ISCIT), 2014 14th International Symposium on*, Sept 2014, pp. 583–587.

[68] J. Zhang, "IEEE 802.11ah network operation and management consideration for functional requirement," IEEE 802.11-11/0672r0, May, 2011.