TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

MUHAMMAD QUTAB-UD-DIN
ENHANCEMENTS AND CHALLENGES IN IEEE 802.11AH - A SUB-GIGAHERTZ WI-FI FOR IOT APPLICATIONS

Master of Science Thesis

Examiners: Prof. Mikko Valkama
Dr. Ali Hazmi
Examiner and topic approved by the
Faculty Council of the Faculty of
Computing and Electrical Engineering
on 4th November 2015

ABSTRACT

MUHAMMAD QUTAB-UD-DIN: Enhancements and Challenges in IEEE 802.11ah - A Sub-Gigahertz Wi-Fi for IoT Applications
Tampere University of Technology
Master of Science Thesis, 62 pages
November 2015
Master's Degree Programme in Electrical Engineering
Major: Wireless Communications Circuits and Systems
Examiners: Prof. Mikko Valkama
Dr. Ali Hazmi
Keywords: M2M, IoT, Wi-Fi, IEEE 802.11ah, Restricted Access Window, Sectorization, Duty Cycle, Energy Efficiency, Long Range

Internet of Things is a concept which brings ubiquitous connectivity to objects that we interact with in the course of our daily activities. With the projected estimates of the number of wireless connected devices reaching massive numbers, it is expected to revolutionize our daily lives significantly. This sort of augmented connectivity will enable new applications in a myriad of domains including smart cities, smart houses, healthcare monitoring, industrial automation and smart metering. These applications entail efficient operation of wireless networks with a large number of energy constrained devices. However, the existing infrastructure for wireless connectivity is not designed to handle such volume of projected growth.

Addressing this requirement, the IEEE 802.11ah task group is working on a new amendment of the IEEE 802.11 standard, suitable for high density WLAN networks in the sub 1 GHz band. It is expected to be the prevalent standard in many Internet of Things (IoT) and Machine to Machine (M2M) applications where it will support long-range and energy-efficient communication in dense network environments. Therefore, significant changes in the legacy 802.11 standards have been proposed to improve the network performance in high contention scenarios. In this thesis we evaluate the performance of many of the new features that have been introduced in the new standard including the Restricted Access Window, Sectorization and Subchannel Selective Transmission mechanisms by means of analytical and simulated models. We propose novel Medium Access Control (MAC) layer algorithms which are shown to have improved the throughput and energy efficiency performance in IEEE 802.11ah networks. We consider practical deployment scenarios in our simulations and evaluate the effects of challenges such as dense networks, interference from neighboring cells and duty cycle limitations on the performance metrics. Overall, we find that the advanced new features make 802.11ah standard a true IoT-enabling technology towards seamless integration of massive amount of connected devices in the future. Our research effort supports the notion that IEEE 802.11ah will be a key technology for future IoT and M2M applications especially in long-range and energy efficient deployments.

PREFACE

This thesis is written in partial fulfillment of the requirements for a Masters of Science degree in Electrical Engineering at Tampere University of Technology, Tampere, Finland. This work was done under the Internet of Things program of DIGILE (Finnish Strategic Centre for Science, Technology and Innovation in the field of ICT) which is owned by 40 companies in the Finnish industry and academia. The project was funded by the Finnish Funding Agency for Technology and Innovation (TEKES).

I would like to show my most sincere gratitude to Dr. Ali Hazmi who has been working with me tirelessly on this research effort. This work is the result of his ever present guidance, mentoring, ideas and most of all his patience throughout the course of this research. I would also like to thank Prof. Mikko Valkama who gave me the opportunity to work in his excellent research group and provided me with all the necessary support. His valuable suggestions and deep insight were the catalyst for this work's success. I would also like to thank my fellow researchers Orod Raeesi, Nader Daneshfar and Adnan Kiyani who were always eager to help me whenever I needed it.

I would also like to thank people from Ericsson Research, Finland including Behnam Badihi, Phelipe del Carpio and Parth Amin as they provided valuable comments and suggestions in this work. My special thanks goes to Atif Sajjad for reviewing this work. I would like to extend my deepest gratitude for my wonderful friends including Adnan, Zohaib, Angiras and Usama for helping me out on various occasions with this thesis.

I would like to thank my parents, Ameen and Kausar and my siblings, Abdullah and Abdulrehman whose constant support and affection have always been a motivating and inspiring factor for me. Without a doubt, I owe my achievements to them. Last but not the least, I would like to thank my dear wife, Marriam Irfan, whose love, patience and unconditional support has been the cornerstone of my success. It would not have been possible without her.

Tampere, 29.7.2015

Muhammad Qutab-ud-din

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS AND SYMBOLS

IoT	Internet of Things
RAW	Restricted Access Window
BSS	Basic Service Set
MAC	Medium Access Control
M2M	Machine to Machine
WLAN	Wireless Local Area Network
S1G	Sub-1 Gigahertz
PHY	Physical Layer
TXOP	Transmit Opportunity
ETSI	European Telecommunications Standards Institute
OFDM	Orthogonal Frequency Division Multiplexing
STA	Station
AP	Access Point
DS	Distribution System
ESS	Extended Service Set
ACK	Acknowledgment Frame
NDP	Null Data Packet
UL	Uplink
DL	Downlink
SST	Subchannel Selective Transmission
ISM	Industrial, Scientific and Medical
EDCA	Enhanced Distributed Channel Access
QoS	Quality of Service
DCF	Distributed Coordination Function

1. INTRODUCTION

Recent years have seen a tremendous growth in the volume of wireless connected devices. It is expected that by 2020 the number of such devices will reach above 40 billion [1]. This increase can be attributed to various trends converging towards increased use of electronic devices for sensing, monitoring and reporting of real-time data. Such applications include smart cities, smart metering, medical monitoring, agricultural monitoring and industrial automation, just to name a few [2, 3]. The term “Internet of Things” was coined to describe such networks in which devices are able to share and report data without human intervention [4]. In a broad sense it refers to the interconnection of heterogeneous smart embedded devices within the internet infrastructure.

The IoT is a rapidly evolving concept and it is expected to transform our daily lives noticeably in the near future. In principle, the IoT will offer advanced connectivity of devices, systems and services. Several implementations of the IoT ideas are already being deployed or investigated, especially in areas like healthcare, industrial automation and smart cities, leading smoothly to the next stage of the IoT evolution.

The future expansion of IoT and M2M communication particularly for sensor networking is predicted to be enormous [5, 6, 7]. It is therefore of paramount importance to develop an infrastructure that can efficiently support such numbers. In general, the IoT and M2M industries have different use cases and requirements, however their common denominators include low cost of devices and infrastructure, reliability, security, connectivity to the internet and long battery operating times of end terminals.

Currently, several radio technologies exist that may be used for the M2M and IoT applications. These include technologies such as ZigBee [8], 6LoWPAN [9] or Bluetooth [10]. In some cases, Wi-Fi or cellular networks have also been used for M2M applications. However, no explicit variant of these technologies exist which is optimized for IoT and M2M use cases or for sensor network purposes.

The 802.11 line of standards are known to be the de-facto standards for ubiquitous

Wireless Local Area Network (WLAN) communications and are among the most widely deployed solutions for the enterprise architecture. Although the major focus of many 802.11-related standardization efforts has been on delivering higher user throughput to a WLAN environment, there are multiple M2M-based scenarios that can benefit from low-power device connectivity and relatively wider communication ranges when compared to the existing technology. Therefore, in order to overcome the above challenges and to provide an effective solution for IoT and M2M applications, the Task Group ah (TGah) of the IEEE 802.11 standardization committee is working on the development of a new sub-1 GHz (S1G) amendment [11, 12, 13], namely the IEEE 802.11ah.

Studies regarding the deployment of the IEEE 802.11ah technology in IoT and M2M applications have substantiated its adequacy for the targeted use cases and the ability to operate well at the unlicensed Sub-1 GHz bands [14]. Studies done in [5, 15, 16] also establish IEEE 802.11ah as an efficient radio technology for M2M and IoT applications.

Compared to other IEEE 802.11 technologies and proprietary solutions like Bluetooth and ZigBee, the IEEE 802.11ah can achieve higher ranges owing to its OFDM based PHY operating in the sub-1 GHz bands and lower data rates. Additionally, with the help of the newly introduced power saving mechanisms, IEEE 802.11ah can also noticeably reduce the energy consumption when compared to other existing technologies and can support an increased number of devices per Basic Service Set (BSS) [15]. As the enhanced MAC features of the new standard make it suitable for high density and energy efficient WLANs, it holds great potential to be a catalyst for further market growth in the IoT and M2M communication spheres, including smart-homes, building automation, healthcare and other such applications [2, 3].

In this thesis, we present a comprehensive overview of the IEEE 802.11ah technology by describing the motivations behind its development, its main requirements and its general MAC and PHY characteristics. A key feature proposed in the IEEE 802.11ah standard is its Restricted Access Window (RAW) mechanism which enables the efficient operation of a large number of devices in a network. RAW mechanism reduces the collisions by allowing only a subset of stations in the network to contend for channel access periodically in their allocated time slots. We present an analytical framework to evaluate the saturation throughput performance of RAW mechanism. In this thesis we also extend the work of [17] by doing performance evaluation and enhancement of the RAW mechanism using different holding schemes that a station may adapt to prevent its transmission from crossing the boundary of its allocated RAW slot. Novel holding schemes as well as a grouping scheme for RAW are proposed and formulated and their performance is also evaluated.

Our other contributions in this thesis include primarily the performance evaluation and enhancement study of the most important newly proposed mechanisms in the IEEE 802.11ah MAC specification for throughput enhancement and interference mitigation, namely frame shortening, TXOP-based and Group Sectorization and subchannel selective transmission mechanisms. We have evaluated these features under practical deployment scenarios considering also the effect of nearby interfering BSSs by means of extensive system level simulations.

Additionally we have also investigated the effects of the maximum duty cycle limitation imposed by ETSI in Europe to prevent excessive emissions in the sub-gigahertz ISM frequency bands. If any chip maker is to sell its equipment for IEEE 802.11ah operation in Europe then they must comply with these regulations. Taking this into account, our work provides relevant and useful insight into the practical deployment considerations of this new standard.

2. OVERVIEW OF IEEE 802.11AH

The major design goal for IEEE 802.11ah is to fulfill the requirement of many IoT and M2M applications. It implies that the standard has to be designed so that it supports the operation of a huge number of devices in contention based media under strict energy-constrained conditions. The IEEE 802.11ah promises to solve these problems by introducing several features and mechanisms which make it suitable for high density extended range wireless networks for battery powered end terminals [11].

Before we go on to explain the details of IEEE 802.11ah it is important to focus on the problems that it tries to solve and its possible and intended use cases. In the following section we briefly describe these problems and hence the motivation behind the development of this new standard.

2.1 Use cases and Requirements

M2M and IoT systems are expected to enable a wide range of important services and applications including smart metering, healthcare monitoring, fleet management and tracking, remote sensing, industrial automation, agricultural monitoring and on-demand business-charging transactions among many others [14, 18]. A massive number of devices are likely to be connected to enable these services and applications which is the primary challenge for the existing technologies. Additionally, in many scenarios of the IoT use cases, end terminals have to operate without battery replacement or recharge for up to many years. Energy efficiency is thus becoming of paramount concern when designing an M2M network [18, 19]. Furthermore, it is also deemed essential for the network operators to be able to offer M2M services and devices at lower cost levels while serving relatively larger areas.

Due to the increasing interest in IoT, M2M and sensor applications, the WLAN industry has also taken important steps to address this business segment by introducing the new IEEE 802.11ah amendment [11, 20] to the IEEE 802.11 baseline standard mainly considering the above mentioned applications.

***Table 2.1** IEEE 802.11ah use cases and related parameters*

Use Case	STAs	Data Rate	Traffic Type
Meter to Pole	6000	100 kbps	C/P/B
Environmental Monitoring	300	100 kbps	P/EB
Industrial Automation	500	1 Mbps	P(0.1s-100s)/B
Healthcare Systems	50	100 kbps	P/EB
Extended Range WiFi	50	10 kbps	B/Pmt
Cellular Offloading	50	20 kbps	B

C = Continuous, P = Periodic, B = Burst, EB = Event Based, Pmt = Permanent

Use cases for the new amendment are divided into three broad categories namely [12]:

- Sensors and meters
- Backhaul sensor and meter data
- Extended range Wi-Fi

Each of these use cases have different requirements for capacity, data-rates and traffic intensity. The standard however contains provisions that can be adapted to satisfy the requirements for any of these use cases. Table 2.1 shows some of the intended use cases and their associated requirements for capacity, data rates and traffic type.

The new amendment mandates a minimum data rate of 100 kbps with a coverage radius of 1 km [13]. It is also a requisite to support at least one mode of operation capable of achieving a maximum aggregate Multi-Station data rate of 20 Mbps. Another requirement for IEEE 802.11ah is that it should support up to six thousands stations for outdoor applications and provide enhanced power saving mechanisms to support battery-powered operation with long replacement cycles [12, 21].

2.2 Challenges and Motivations for IEEE 802.11ah

The major challenge for the IEEE 802.11ah standard is the strict capacity and energy efficiency requirements of many of the use cases. In the following we discuss these challenges and the proposed features in the standard to counter them.

2.2.1 Dense Network Operation

As described in section 2.1, IEEE 802.11ah may require very dense operation of the network. For instance up to 6000 stations can be associated to a single Access Point (AP) in one of the use cases. It is not possible to provide acceptable data-rates in such high contention scenarios using the legacy MAC techniques. IEEE 802.11ah, therefore, describes many mechanisms to cope with this problem. Restricted Access Window (RAW) is one of the mechanisms which enables the operation of a large number of devices in a single BSS without degrading the throughput performance to inadequate levels. It does so by limiting the channel access in the BSS to a subgroup of stations in its assigned interval of time. Another mitigation mechanism described in the standard is the sectorization mechanism which counters issues such as interference and hidden node problem in high density networks. These mechanisms are discussed later in detail.

2.2.2 OBSS Problem

The OBSS problem refers to the case when two or more BSSs, that are unsynchronized and operating at the same channel, are close enough to hear each other. In such a scenario, transmissions by some STAs in one BSS will be heard by the STAs in the other one, and eventually degrade the overall performance. Such a study was done in [5] where the authors concluded that the OBSS problem degrades the performance substantially as the overlap between the two access points is increased.

To get a handle on this, the IEEE 802.11ah specifications provide the sectorization mechanism. The sectorization mechanism not only helps reduce the interference from adjacent BSSs but also gets rid of the hidden node problem which is also a profound source of impairment in wireless networks using basic access mechanism. There are two kinds of sectorization mechanisms described in the new standard which we will cover later in detail. Subchannel selective transmission is another technique that can be used to reduce the impact of interference from neighboring BSS. In this thesis we thoroughly evaluate the performance of these novel mechanisms through extensive simulations which give a realistic estimate of the performance improvements achievable by using these features.

Now that we have described the motivations behind this new standard and the applicable usecases we can proceed with providing an overview of the standard itself.

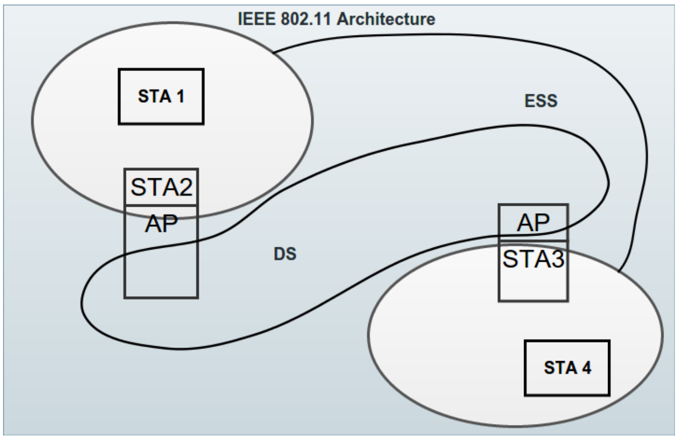

Figure 2.1 *Network Architecture of IEEE 802.11 WLAN*

2.3 Architecture of IEEE 802.11ah

In an 802.11 network, a station (STA) is a single addressable unit which is the source or destination of a message. A STA can be fixed, portable or mobile. The basic architectural unit of an IEEE 802.11 network is a Basic Service Set (BSS) which can be thought of as the coverage area in which the STAs remain connected to each other. The area covered by the BSS is termed as Basic Service Area (BSA). A STA outside the BSS can not directly communicate with the ones inside the BSS.

An independent basic service set (IBSS) is formed when two or more STAs capable of communicating directly with each other operate in a BSS thus forming a so called ad-hoc network. In contrast to that, in an infrastructure BSS the STAs associate to a fixed STA called the Access Point (AP) which broadcasts special management frames such as beacon frames to keep the network synchronized. Two or more BSS can be connected by means of a Distribution System (DS) to form an Extended Service Set (ESS). An AP acts as a gateway for connecting multiple BSS to form an arbitrarily large Wireless Local Area Network (WLAN). An ESS formed in this manner allows the associated STAs to communicate with each other via the APs and DS even if they don't belong to the same BSS. Fig. 2.1 shows the basic architecture of an IEEE 802.11 network. In addition to that the IEEE 802.11 networks also provide the possibility of forming mesh networks in a Mesh Basic Service Set (MBSS). In an MBSS each STA is connected to its neighbor STAs and multi-hop routing is used for delivery of packets while there is no central entity [22].

An IEEE 802.11ah network maintains the network architecture of the legacy IEEE 802.11 systems therefore the above mention network architectures are also incorporated in the new standard. It supports fixed, outdoor and point-to-multi-point applications while being compatible to the IEEE 802.11 management plane [13]. In

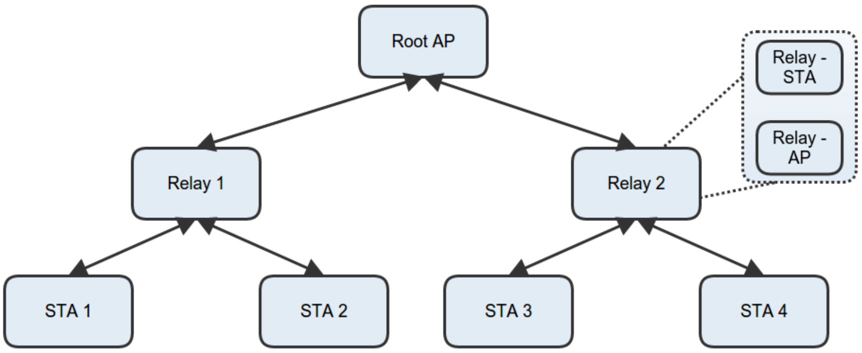

***Figure* 2.2** *Relay Architecture in IEEE 802.11ah*

addition to that it also supports a relay architecture in which the coverage area of an AP is increased by use of a two-hop relay mechanism. A high level abstraction of the relay operation is shown in Fig. 2.2. It can be seen in the figure that the relay consists of a relay-STA and a relay-AP. The relay-STA is connected to the Root AP and the relay-AP is connected to the end STAs. Frames can be transmitted between the Root AP and the end STAs using the Relays in both directions. Relays not only increase the coverage area of the BSS but can also decrease the transmission time (usually) and energy consumption for successful packet delivery.

In IEEE 802.11ah, different BSSs can be set up around the same or different carrier frequencies which are determined by the regulations in the region of action. Additionally these BSSs will operate on channel bandwidths that range from 1 MHz to 16 MHz depending on the channelization policy of the respective country. The channelization for IEEE 802.11ah in Europe and the US is shown in Fig. 2.3 [23].

Throughout this thesis we will consider only the infrastructure BSS in our analysis since it is the most commonly deployed network architecture for WLANs. In an IBSS the APs primarily broadcast management frames (e.g. beacon frames) which help the STAs to operate and remain synchronized within the BSS. APs are also in charge of setting up associations with the STAs entering the BSS. Additionally they serve data traffic to STAs on the downlink and respond with ACKs for incoming uplink traffic. Consequently, because of their key role in the BSS, the APs generally need to transmit more frequently than an individual STA.

In the following we describe the physical and medium access control layers of IEEE 802.11ah and some of the new features that the standard has introduced.

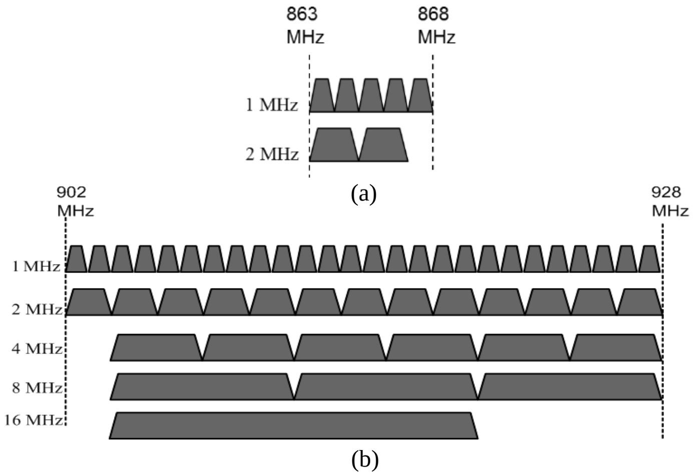

Figure 2.3 *Channelization for IEEE 802.11ah in (a) Europe and (b) US*

2.4 Physical Layer

The draft standard IEEE 802.11ah proposes operation in the sub 1 GHz (S1G) license-exempt bands excluding the TV whitespace bands. The proposed bands for deployment in the current draft are 863-868 MHz in Europe, 916.5-927.5 MHz in Japan, 755-787 MHz in China, 917.5-923.5 MHz in South Korea, 866-869 MHz, 920-925 MHz in Singapore and 902-928 MHz in the U.S. The TV whitespace bands are instead targeted by the IEEE 802.11af standard. The standard includes several MAC enhancements and also provides mechanisms to allow coexistence with other systems operating in the same bands, namely IEEE 802.15.4 and IEEE P802.15.4g [24]. It specifies a communication range of up to 1 km and a minimum data rate of 100 kbps [11].

The IEEE 802.11ah PHY supports multiple space-time streams and multi-user transmissions. It uses a downclocked version of the IEEE 802.11ac PHY and its primary design goals include multiple interoperable operation bandwidth modes and support for a wide range of data rates [19]. Consequently, 2MHz, 4MHz, 8MHz and 16 MHz channels are specified with an additional 1 MHz channel in order to achieve longer transmission ranges. The OFDM tone spacing across the different bandwidth modes is a constant 31.25 kHz.

It is mandatory for a station to support MCS 0 - MCS 2 for 1 MHz and 2 MHz channel bandwidths with a single spatial stream. For an access point (AP) it is mandatory to support MCS 0 to MCS 7 for all supported channel widths for a single spatial stream [11]. The MCS supported by the S1G PHY specified in IEEE 802.11ah for 1 MHz and 2 MHz channel widths are shown in Table 2.2. The corresponding coding rate (CR), data bits per OFDM symbol (DBPS) and data

***Table 2.2** Supported MCS and related parameters by IEEE 802.11ah for single spatial stream and normal guard interval*

MCS	Mod.	CR	1 MHz		2 MHz	
			DBPS	DR (Mbps)	DBPS	DR (Mbps)
MCS 0	BPSK	1/2	12	0.30	26	0.65
MCS 1	QPSK	1/2	24	0.60	52	1.30
MCS 2	QPSK	3/4	36	0.90	78	1.95
MCS 3	16-QAM	1/2	48	1.20	104	2.60
MCS 4	16-QAM	3/4	72	1.80	156	3.90
MCS 5	64-QAM	2/3	96	2.40	208	5.20
MCS 6	64-QAM	3/4	108	2.70	234	5.85
MCS 7	64-QAM	5/6	120	3.00	260	6.50
MCS 8	256-QAM	3/4	144	3.60	312	7.80
MCS 9	256-QAM	5/6	160	4.00	-	-
MCS 10	BPSK	1/4	6	0.15	-	-

rate (DR) are also shown in the table.

In IEEE 802.11ah, transmissions are frame based with each frame consisting of multiple OFDM symbols. However during the design, the system was specifically optimized in the lower bandwidth modes to support lower data rates and longer ranges that would be useful for power limited (e.g. battery operated sensors) devices operating in S1G bands.

The IEEE 802.11ah draft standard lists a few channel models including an outdoor and an indoor path loss model. In this thesis, we consider only the outdoor path loss model with macro deployment scenario where antenna height is assumed to be 15m above rooftop, as described as one essential 802.11ah deployment scenario in [25]. The path loss in dB is given by (2.1) where d is the distance in meters and carrier frequency is 900 MHz.

$$PL = 8 + 37.6 \times log_{10}(d) \tag{2.1}$$

The minimum receiver sensitivity for each MCS according to the standard is listed in Table 2.3.

Table 2.3 *IEEE 802.11ah Minimum Receiver Sensitivity for 2MHz PPDU*

MCS	Sensitivity (dBm)
0	-92
1	-89
2	-87
3	-84
4	-80
5	-76
6	-75
7	-74
8	-69
9	-67

2.5 Medium Access Control Layer

In order to address the IoT and M2M requirements the core changes and enhancements in IEEE 802.11ah are related to the MAC layer. The introduced MAC features aim mainly at enabling the IEEE 802.11ah technology to support the expected high number of stations with power limited characteristics while transmitting short packets. In the following, we first briefly describe the essential MAC features and then focus on investigating the features addressing capacity requirements and interference mitigation.

2.5.1 Channel Access

The IEEE 802.11ah MAC provides Enhanced Distributed Channel Access services for an S1G STA using the services of the Distributed Coordination Function [11]. EDCA services mean that the STA in an IEEE 802.11ah network is a QoS station, supporting different priorities for different types of traffic.

DCF is a type of Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) technique for channel access in a shared medium. In the DCF procedure, a station first senses the channel to be idle for an interval equal to Distributed Interframe Space (DIFS). It then chooses a random number of backoff slots from the range $[0-CW]$ to wait before it can start its transmission. CW is the size of the contention window, which is initially CW_{min}. The receiving station first checks if the packet is destined for itself. If this is the case, then it sends an acknowledgment frame (ACK) back to the sending station after waiting for a period called Short Interframe Space (SIFS). SIFS is smaller than DIFS so ACKs have always higher priority than normal packets. A full transmission cycle therefore is the sum of

DIFS, backoff, duration of data frame, SIFS, ACK and the associated propagation delays. The sum of data frame duration, SIFS and ACK is also known as a transmit opportunity (TXOP).

If an ACK is not received by the sending station within the timeout interval, the packet is considered to be lost and is re-transmitted with the size of contention window doubled on each attempt until it reaches its maximum size CW_{max}. For this reason, DCF is also termed as a binary exponential backoff scheme. A packet is dropped after m_{long} number of unsuccessful transmission attempts. The contention window is reset to CW_{min} if a packet is transmitted successfully which is indicated by successful receipt of an ACK frame. A collision is said to have occurred when one or more stations transmit at the same time [22]. In legacy 802.11 networks, when a collision occurs, the station waits for Extended Interframe Space (EIFS) time before attempting another transmission, which is larger than DIFS to avoid possible collision again. However, in IEEE 802.11ah, EIFS is not used [26].

There are other coordination functions also available in IEEE 802.11ah such as Point Coordination Function (PCF) or Hybrid Coordination Function (HCF). We will, however, not discuss these as they are not mandatory to be supported and we only consider DCF in our work.

2.5.2 Frame Shortening

In the legacy IEEE 802.11 networks, MAC header overhead can even exceed 30% for a 100-byte payload, therefore, rendering the use of legacy frame formats impractical in sensor applications as it is typical to have frequent short payload transmissions and long transmission delays [12, 20]. Therefore, to reduce the control overhead, Task Group ah (TGah) has introduced short headers, short beacons and Null Data Packet (NDP) frames in the new standard.

The newly introduced short header excludes few uncritical fields like the Duration/ID, the Quality of Service (QoS) and High Throughput (HT) fields. As a result, size of the MAC header can be reduced to as low as 14 Bytes in the new standard including the FCS field. Additionally, to reduce channel occupancy time and subsequently power consumption, the IEEE 802.11ah introduces short beacon frames that are sent more frequently than normal ones and do not carry any redundant or uncritical information that can be alternatively obtained from the legacy beacons [26]. IEEE 802.11ah also proposes the use of Null Data Packets (NDP), a concept first introduced in IEEE 802.11ac, in which packets have no payload from the MAC layer and contain all essential information in the PHY header. IEEE

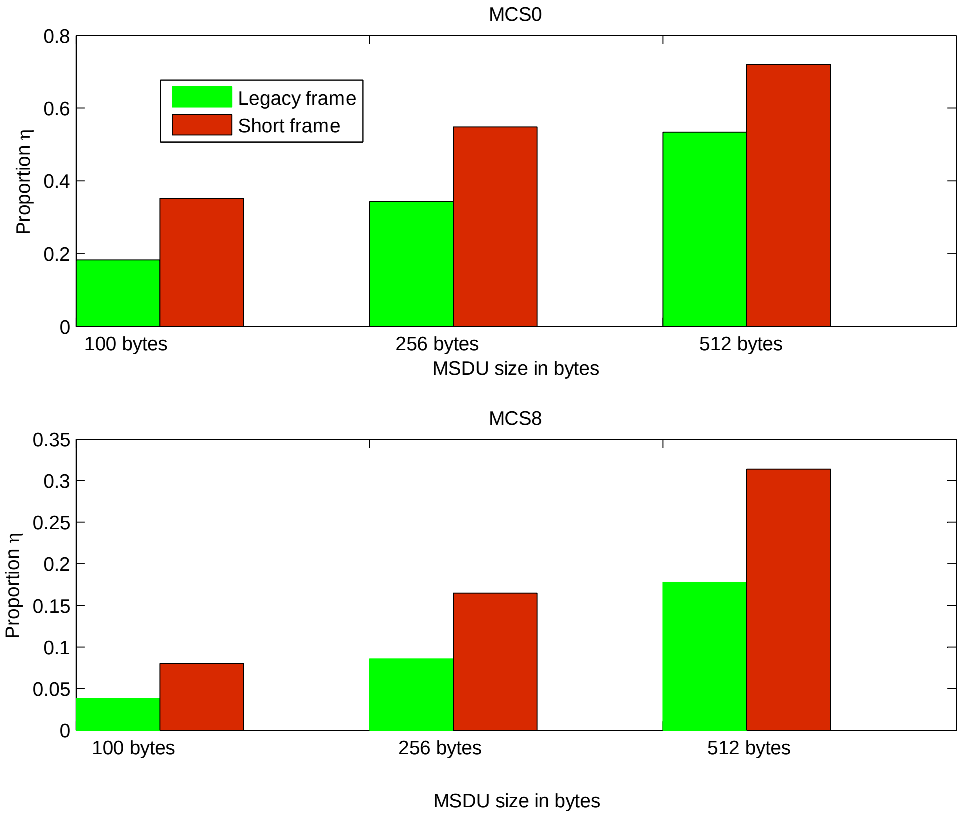

***Figure** 2.4 The proportion of the useful throughput for different MSDU sizes when MCS 0 and MCS 8 are used.*

802.11ah proposes the use of NDP frames for control frames such as ACK, CTS, BlockAck etc.

In order to assess the upper performance of the IEEE 802.11ah system, and to measure the throughput enhancement when short frames are considered, we assume that a single STA in an IEEE 802.11ah network successfully transmits a single data frame. The total transmission time can be divided in two parts, T_{tr} needed for the MPDU transmission plus a constant overhead $T_{Overhead}$ [27] given in (2.2). Here we have neglected the delay due to the propagation time.

$$T = T_{Overhead} + T_{tr} \tag{2.2}$$

where the constant overhead $T_{Overhead}$ is expressed as follows:

$$T_{Overhead} = T_{DIFS} + T_{PHY} + T_{SIFS} + T_{PHY} + T_{ACK} \tag{2.3}$$

Table 2.4 *IEEE 802.11ah Timing and Simulation Parameters (2 MHz mode)*

Parameter	Description	Value
T_{sym}	OFDM Symbol Duration	40 µs
PHY HDR	Physical Layer Header Length	240 µs
MAC HDR	MAC Layer Header Length	14 B
ACK	Acknowledgment	14 B
SlotTime	The slot time	52 µs
SIFS	Short interframe space	160 µs
DIFS	DCF interframe space	264 µs
CW_{min}	Min. back-off window size in SlotTime	15
CW_{max}	Max. back-off window size in SlotTime	1023
L	Payload Size	256 B
m_{long}	Maximum number of Tx attempts	4
δ_{max}	Propagation delay	6 µs
T_g	Guard Time ($2 \times \delta_{max}$)	12 µs
T_{RAW}	Duration of RAW	1s
P_{TX}	Transmit Power	1mW

The frame transmission time T_{tr} varies according to the bit rate used by the STA. If MCS 0 is used and if the frame size is of 256 bytes of payload (MPDU of total 290 bytes in normal frame case and of total 270 bytes in the shortened frame case), the proportion of the useful throughput η measured above the MAC layer in both cases [27] is given as follows:

$$\eta = \frac{T_{tr}}{T} \bullet \frac{\text{Payload Size}}{\text{Frame Size}} \tag{2.4}$$

Given Table 2.4, proportion of the useful throughput is 0.35 and 0.55 in normal frame and short frame cases respectively. We can easily notice the considerable improvement of the achieved throughput when the shortened frames are considered. In Fig. 2.4 we show a comparison of the useful throughput for different MCSs and payloads sizes when legacy and short frames are considered. Here we also neglected the back-off time, as we assumed that only one STA is in the cell.

2.5.3 Virtual Carrier Sense

The legacy virtual carrier sense mechanism in 802.11 WLANs is called the Network Allocation Vector (NAV). It is used on top of physical carrier sensing to save power. Every station who is listening on the wireless medium can receive frames from other stations. When such a frame is detected which is not destined for the receiving station, that station reads the duration field of the frame which indicates the amount of time this transmission will continue. It subsequently updates its Network Allocation Vector (NAV) which is effectively a timer that indicates the time during which the network will be busy. The stations which set their NAV in this manner do not attempt to transmit until the NAV timer is zero which indicates that the channel is idle [28].

Since the duration field is omitted when short MAC header is used in IEEE 802.11ah, NAV can not be used as the only virtual carrier sense mechanism. TGah has developed a new carrier sense mechanism called response indication deferral (RID). By using RID it is possible to specify the type of response required by the transmitting station in the response indication field of the PHY header. Based on this value the listening stations can defer channel access for an appropriate interval of time [26].

2.5.4 Hierarchical Addressing and Page Slicing

IEEE 802.11ah describes a hierarchical addressing scheme for the association identifiers (AID) of the stations in the infrastructure BSS. The hierarchy consists of 4 pages of 32 blocks each. Every block then consists of 8 sub-blocks, each having 8 stations. Therefore, a 13-bit AID is sufficient to uniquely identify a station. In legacy 802.11 networks it was only possible to have a little over 2000 devices associated to an AP as the rest of the values in the 14-bit association identifier (AID) were kept reserved. Also, the length of the Traffic Indication Map (TIM) bitmap is increased from 2008 bits to 8192 bits [26] and hence up to 8192 stations can be addressed using this scheme within a single BSS.

This hierarchical addressing can facilitate the use of many other enhancement mechanisms by allocating AIDs to stations with similar characteristics such that they fall into logical hierarchical groups. This type of addressing scheme may also help in reducing the size of the Traffic Indication Map (TIM). Although the standard does not describe in detail how the TIM can be compressed, it does however provide a framework to do so using creative and efficient means and is an open research topic.

An extension of this hierarchical structure is the page slicing mechanism. The page slice information element (PSIE) present in the DTIM beacon contains the information that whether there is buffered data for at least one station in the page. The stations see that and calculate the approximate time at which they should wake up to receive the appropriate full beacon to retrieve buffered data. This helps in conserving the energy for sensor stations.

2.5.5 Target Wake Time

In an IEEE 802.11ah network a station can be either in Awake state where it is active or in the Doze state in which the station conserves battery by not listening to the channel transmissions. When a station goes to Doze state, it must notify the AP it is associated to, so that it can buffer any frames for the dozing station. These buffered frames can be sent to the dozing station by the AP upon receipt of a PS-Poll frame by the station. The Traffic Indication Map (TIM) which is broadcasted as part of the beacon frame contains the information about presence of buffered data for the stations. A station upon noticing that the AP has buffered data for it, can send a PS-Poll frame and retrieve the data. For this purpose the dozing stations repeatedly need to wake up to listen to the beacon frames, at least in the legacy standard.

IEEE 802.11ah defines a new power saving mechanism called the Target Wake Time (TWT) specifically for the stations which do not want to wake up to listen to each beacon frame. These stations can negotiate a wake up time with the AP at which they wake up for an interval called Service Period (SP) during which they can exchange frames. Stations can remain in doze state for extended periods of time using this mechanism thus increasing the battery life cycle of sensor nodes to months or even years.

2.5.6 Restricted Access Window

Restricted Access Window (RAW) is one of the most promising and well studied feature of IEEE 802.11ah. A major portion of this thesis is also therefore dedicated to the performance analysis and enhancement of this feature. The importance of RAW mechanism is well established in [5] and [15] while [17] also describes the RAW operation considering the cross slot boundary condition. RAW uses enhanced distributed channel access (EDCA) which uses DCF as the underlying access mechanism [11].

To support a large number of devices associated with a single AP, TGah has developed a novel mechanism to reduce contention in the channel access. In this mechanism, during a particular time window called the restricted access window (RAW), a group of stations is allocated time slots during which they can contend for channel access. Stations are not allowed to contend for the channel outside their designated slots. To conserve power the remaining stations can sleep outside their RAW slots. Additionally, within a beacon interval there can be multiple RAWs as well as open access intervals during which any station is allowed to contend for the

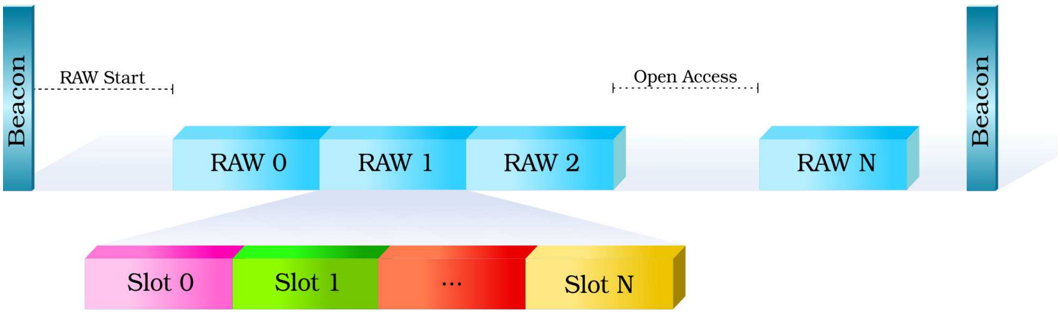

Figure 2.5 *Restricted Access Window Structure*

channel [11, 3]. Inside a RAW slot, stations in a group contend for the channel access using the DCF procedure, which is the same as used in legacy 802.11 networks and described in Section 2.5.1.

When a STA gets uplink data from the upper layers it can contend for the channel access at the beginning of its allocated RAW slot. It is however necessary that the STA is allowed channel access in that particular RAW slot. It stops attempting packet transmission as soon as the time assigned for that slot ends. It is also possible that a STA may not be allowed to use any of the RAW slots. In that case it may only attempt channel access in an open interval. Fig. 2.5 shows the structure of the time assignment in RAW during a beacon interval.

The grouping of stations may be done by the AP which assigns the group to a station by means of the RAW Parameter Set (RPS) element broadcasted in the beacon frame. Besides group assignment information, the RPS element contains essential control information about the RAW operation including duration of a slot and the number of RAW slots (N_{RAW}). This information is used by the station to calculate the total duration of the RAW (T_{RAW}). A simple slot assignment criteria is described in the standard in which stations are allocated RAW slots according to the mapping function defined as

$$i = (x + N_{offset}) \bmod N_{RAW} \tag{2.5}$$

Here, i is the index of the assigned RAW slot and ranges from 0 to $N_{RAW} - 1$ and x is the Association Identity (AID) of the station. N_{offset} is a parameter that improves fairness among the stations and is equal to the two least significant bytes of the beacon FCS. If a total of N stations are present in the network then each RAW group has $N_g = N/N_{RAW}$ number of stations contending in a RAW slot.

The standard also allows the AP to configure multiple RAWs with different param-

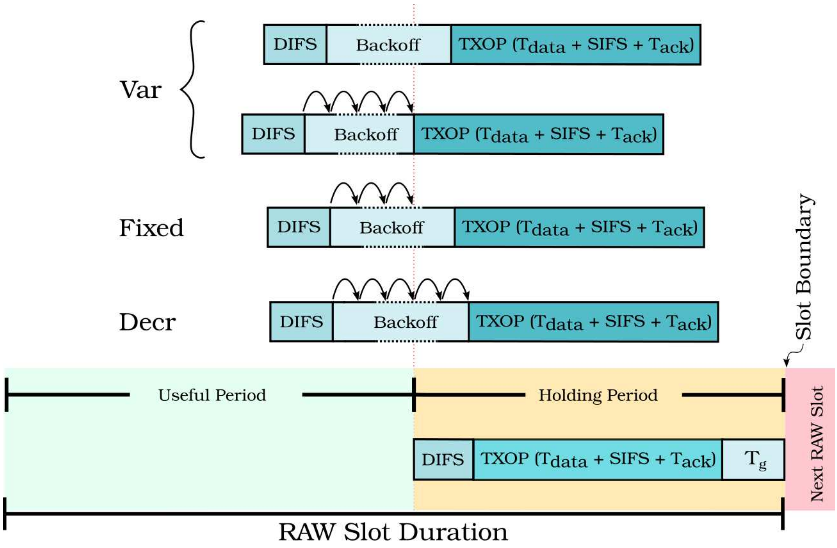

Figure 2.6 *Holding period description for different holding schemes*

eters during beacon interval so that either different STAs will use different RAWs or channel access parameters between RAWs are different. Additionally, the AP can configure periodic RAW so that channel access is possible for certain STA periodically.

The RPS element also contains a field called the cross slot boundary (CSB) condition. If CSB condition is false i.e. the CSB field is set to 0, then a station must not start a transmission if the remaining time in the current RAW slot, albeit non-zero, is not enough to complete the transmission before the end of the slot. Otherwise, if the CSB condition is true, it is allowed for a station to transmit even if the transmission will not be completed before the end of the current RAW slot [11].

In this thesis we consider only the non-cross slot boundary case and propose and analyze the performance of new schemes for backoff counting within the holding period. We also propose a novel grouping scheme of stations for RAW based on the apriori information obtained from the backoff states of the previous RAW. These schemes are discussed in Section 2.5.7.

2.5.7 Holding Schemes for Non-Cross Slot Boundary RAW

To prevent a transmission from crossing the RAW slot boundary, a station shall hold its transmission a certain amount of time before the end of the RAW slot, termed as the ‘holding period’ [29]. No station is allowed to start a transmission within the holding period. Thus, it should at least be equal to the sum of DIFS and the time taken by one TXOP ($T_{data} + SIFS + T_{ack}$). It may also include a guard period to

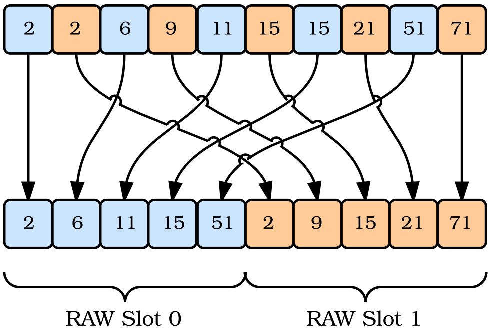

Figure 2.7 *BIN scheme for deterministic grouping in RAW slots with* $N = 10, N_{RAW} = 2$ *and* $N_g = 5$.

allow for propagation delays.

There can be several options for how the station counts its backoff within the holding period which we call here as a holding scheme. The different holding schemes analyzed in this thesis are described in this section. While 'FIXED' and 'DECREMENTING' schemes are mentioned in [17], it contains the analysis of only the 'FIXED' holding scheme. In our work, we also evaluate the 'DECREMENTING' holding scheme and propose and evaluate two new holding schemes which we term as 'VARIABLE' and 'HYBRID' schemes. We provide their detailed description in the following.

1. FIXED: In the fixed holding period, the backoff counter is frozen when the holding period starts. The station goes to idle and stores its backoff state. The station restores its backoff state in the following RAW.
2. DECREMENTING: In this scheme the station keeps decrementing its backoff counter inside the holding period. If the counter reaches zero inside the holding period, it is renewed with the same contention window. Otherwise, the backoff state is stored at the end of the slot boundary and restored in the next RAW.
3. VARIABLE: In this holding scheme, the station freezes its backoff as soon as it generates the backoff number and anticipates that the generated backoff will cause the slot boundary to be crossed. This effectively decreases the useful slot duration but can be useful in some scenarios where using a larger backoff or synonymously a larger holding period is beneficial, as we will later see.
4. HYBRID: In this scheme the stations choose the holding scheme based on their distance from the AP. The stations which are far from the access point choose the 'VARIABLE' holding scheme and the ones which are near use the 'FIXED' holding scheme.

Fig. 2.6 shows the basic holding schemes described above. In addition to these holding schemes we also propose and evaluate the performance of a new novel grouping scheme. After the end of the first RAW within a beacon interval, all stations have their backoff states stored. These states contain some information about the contention scenario present in the network and can thus be used to assign groups to stations in the next RAW so that channel utilization is increased. With the assumption that it is possible for the AP to know the backoff states of all the stations, it can regroup them in each subsequent RAW in order to improve the network performance.

Assuming that the AP has the backoff states of all the nodes in the network, the new grouping scheme, which we term as the 'BIN' scheme, works on the following algorithm. It first sorts the list of backoff counter numbers of all the stations in the network in ascending order, from which the index of the kth station in the ith RAW group is found using mapping function in (2.6)

$$I_{i,k} = i + N_{RAW} \times k \tag{2.6}$$

where $i \in [0 - N_{RAW})$ and $k \in [0 - N_g)$. The procedure is illustrated in Fig. 2.7 for $N = 10$, $N_{RAW} = 2$ and $N_g = 5$. The procedure can be repeated after the end of each RAW, whereas in the first RAW the mapping function in (2.5) can be used. There can be a difference of one between the number of stations in different RAW groups when group size N_g is not an integer.

The 'BIN' scheme reduces the collisions by increasing the channel utilization as it places stations in a group with their backoffs in ascending order. It also reduces collisions by placing stations with equal backoff counters in different groups and hence allows more packets to be transmitted in a RAW slot. In the following sections we evaluate the performance of the above mentioned schemes through analytical considerations as well as comprehensive network simulations.

2.5.8 Subchannel Selective Transmission

STAs in a BSS can benefit from the fact that they may not require the whole available channel bandwidth for their transmissions. For instance, sensor stations may only support 1 MHz and 2 MHz channel bandwidths and can therefore select the best subchannel among the available channel bandwidth. IEEE 802.11ah defines the Subchannel Selective Transmission clause to enable this mechanism. An AP may indicate the support for SST by including an SST Operation Element in a management frame which contains the set of channels enabled for SST operation.

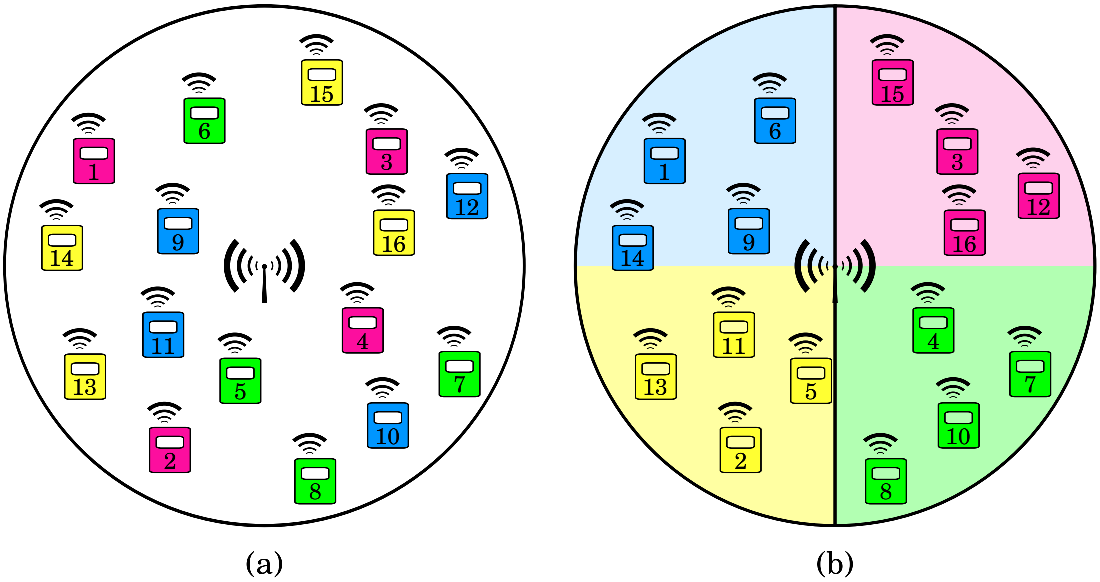

Figure 2.8 *(a) RAW with grouping based on the AIDs (b) Group sectorization based on Spatial Distribution of STAs. Each color corresponds to a different slot/sector.*

The AP may then include an SST Element in a beacon frame containing a subset of enabled SST channels on which SST operation is allowed in the following beacon interval.

The SST Element also contains a channel activity schedule containing information about expected DL and UL activity on the allowed subchannels and the duration for which the activity is allowed. In the downlink the AP may send sounding frames to the STAs on the allowed subchannels which in turn can be used by the STAs to estimate channel parameters in order to determine which subchannel is the best. Once a STA determines the best subchannel it can then use it in UL transmissions during the time indicated in the channel activity schedule. The AP may also use RAW for transmission of the sounding frames or it can send these frames periodically. The SST mechanism can help in mitigating selective fading and interference due to OBSS.

2.5.9 Sectorization

The new amendment proposes the use of Sectorization mechanism which addresses issues like channel contention, hidden node problem and interference from OBSS by partitioning the BSS into several spatial sectors. This partitioning is achieved by means of beamforming antennas to cover different sectors of the BSS. Depending on the considered deployment scenario (one AP or multi-APs), the IEEE 802.11ah specifications define two types of sectorization mechanism namely Group sectorization and TXOP-based sectorization.

Group Sectorization

The group sectorization mechanism is developed with an intent to address the hidden node problem which is especially more pronounced in dense long-range networks. During the association procedure, the AP assigns each associated STA an ID of the sector which it belongs to. The AP divides the time into sector intervals and at the start of each sector interval it transmits a beamformed beacon to the sector which is allowed to access the channel during that interval. This alleviates the hidden node problem as all the stations belonging to the same sector can hear each others transmissions. The mechanism is very similar to RAW as illustrated in Fig. 2.8. In RAW mechanism, STAs in a given RAW slot are grouped based on their AIDs whereas in group sectorization the STAs in each others spatial vicinity are grouped into sectors.

TXOP-based Sectorization

TXOP based sectorization aims at minimizing the interference caused by OBSS while allowing the associated stations to transmit their data simultaneously. In TXOP-based sectorization, the AP starts a transmission with an omni beam which sets up the NAV of all listening stations. After the receipt of ACK from the destination node, the AP transmits the second frame such that part of it is omni and part is sectorized. If the OBSS STAs listen the omni beam but cannot listen the ACK nor the sectorized beam transmission, they can start their own transmission until the end of sectorized TXOP transmission. The standard also describes few other ways to implement the TXOP-based Sectorization. A comparative study of these schemes and their specific applications form an important research issue.

Having described the main features of the IEEE 802.11ah standard, in the following we first describe our simulation platform and then develop an analytical model for saturation throughput performance of RAW. Since RAW and sectorization are fundamentally similar, the same model can be applied to calculate the saturation throughput of the sectorization mechanism. We then proceed with the detailed performance analysis of IEEE 802.11ah MAC features and our proposed enhancements under practical deployment scenarios by means of realistic system level simulations.

3. SIMULATION SETTINGS AND PLATFORM

It is important to verify the result of network modeling by means of an analytical as well as simulated model. In this thesis we have used the Omnet++ tool for the network simulations for our analysis purposes. The accuracy of these simulations is then verified by means of two analytical models. In this section we will describe Omnet++ tool used for the system level simulations of our network model.

Omnet++ is an object-oriented discrete event network simulator based on the C++ language. It provides a rich set of tools and libraries to develop and simulate network components and protocols. It is an open source tool and therefore highly customizable according to specific requirements. It takes a modular approach on system design, allowing reusable, independent and highly efficient modules. The main components of the Omnet++ framework are described here.

3.1 Architecture of Omnet++ Platform

Fig. 3.1 presents the high level architecture and constituent blocks of the Omnet++ simulation platform. The arrows show the interaction between the high level modules. SIM is the library linked to the simulations program and contains the classes which perform the tasks of a kernel for the simulations. It handles the I/O from the user, schedules the events and manages the execution of parallel simulations. It is also responsible for managing CPU resources.

There are two type of user interfaces available in Omnet++ namely CMDENV and TKENV. As the name suggests, CMDENV is a command line user interface which basically provides minimal information about the simulation events, the simulation progress and its configuration. This is a light user interface and does not require much computing resources. It is ideal to use when long and stable simulations are being run. The other user interface is TKENV which is a graphical user interface (GUI) and provides a rich set of tools to monitor, inspect and analyze the simulations in real time. It is a computing intensive interface and requires extra dependencies to be installed in order to run. However, this UI is well integrated to suit the needs of most Omnet++ users as it has advanced options for monitoring and debugging

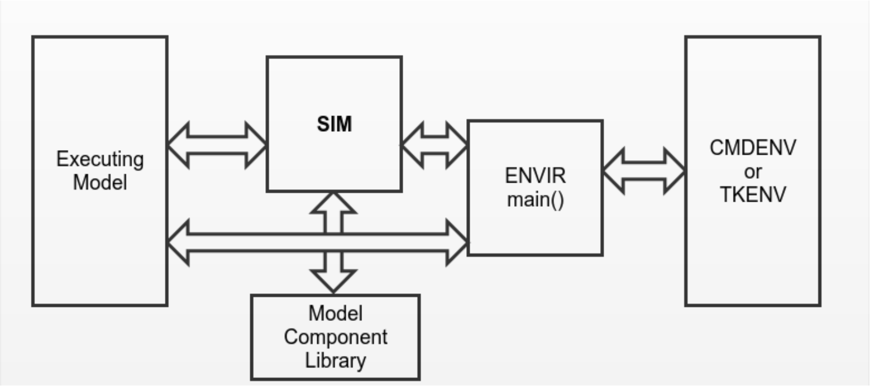

Figure 3.1 *High level architecture of Omnet++ simulation platform*

simulations. Its use is recommended when it is necessary to perform validation of a certain function in the simulations or when debugging is required in order to ensure correct behavior of the program. ENVIR is the library which contains the code common to both these interfaces.

In Object Oriented terminology, ENVIR is the interface while TKENV and CMDENV are concrete implementations of this interface. The most important part of the ENVIR module is the 'ev' facade object, which it presents to the Executing Model as well as the simulation kernel (SIM). The call to 'ev' resolves at run-time to either CMDENV's or TKENV's implementation and it provides methods such as writing to the standard output/standard error and watching the value of a simulation statistic in run-time. In addition to that ENVIR also contains the main() method which is the starting point of the simulation. This module is in fact in full control of the simulation and instructs the simulation kernel about which modules should be set up. It contains the main event loop as it invokes the simulation kernel for the required functionality. It also catches and handles any errors or exceptions that occur during the simulation.

Model Component Library (MCL) contains definitions for a wide range of frequently used modules in network simulations such as channels, networks, messages and compound modules etc. While MCL provides blueprints or classes for the functional blocks of simulation elements, the exact instances are held by the Executing Model. The information about these instances is also made available to the simulation kernel by the Executing Model.

3.2 Module Hierarchy

Omnet++ follows a simple module level hierarchy where 'simple modules' make up the 'compound modules'. In implementation terms, each simple module is a C++

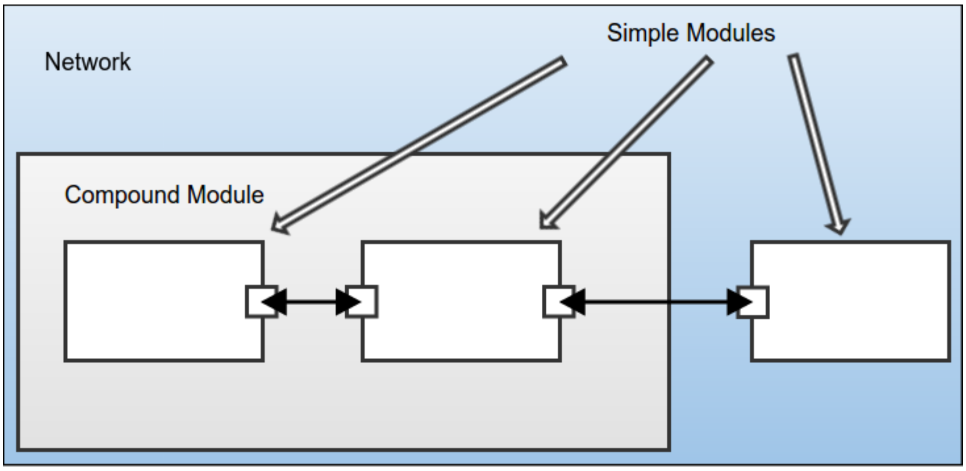

***Figure* 3.2** *Module hierarchy and network elements in Omnet++*

class which has a declaration and a definition, like in any other C++ implementation. There is no limit on the levels of hierarchy or the number of simple modules that make up the compound modules. Modules interact with each other by passing 'Messages'. Every module can have multiple 'Gates' which act as the entry or exit point for receiving or sending messages to other modules. A gate is a directional entity and it can be used for incoming or outgoing messages or both. A simple diagram showing a network composed of simple and compound modules in Omnet++ and related entities is shown in Fig. 3.2.

This hierarchical approach to modules in Omnet++ allows the simulated networks to be modular and makes it trivial to implement any kind of protocol stack. The design goal of Omnet++'s simple modular hierarchy was to make the modules cohesive and decoupled. Cohesiveness implies that a module performs a well defined task by itself whereas decoupling means that it has no dependency on other modules. By following these best practices of object oriented design, Omnet++ makes it possible to simulate complex network scenarios while keeping the code base clean, reusable and easily maintainable with minimum effort. Usually the algorithms are implemented in simple modules while compound modules act as a container for a number of simple modules. Modules in Omnet++ can have several parameters which are used to configure it. The parameters can be specified in either the INI files or NED files which are described shortly after.

3.3 Inter-module Communication

Modules communicate with each other by means of exchanging 'messages'. Usually these messages are sent through a module's 'gates' which travel through a link or a predetermined path, but they can also be sent directly to another module. The

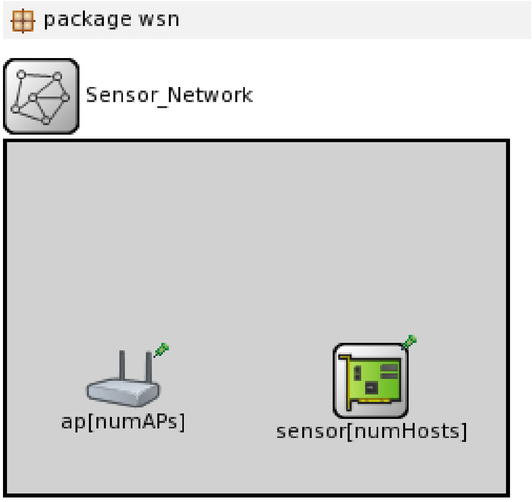

Figure *3.3 NED Topology for a simple wireless network model*

messages are defined in .msg files which follow a simple C-like syntax. Omnet++ comes with compiler support (MSGC) to generate C++ code from message definition files. This compiler generates appropriate getters and setters for the data structure fields used in messages which then can be used in module implementations.

The links or connections through which these messages travel can for instance represent a channel with a path loss, delay, data rate and other related parameters. Otherwise, a link can simply be an interconnection of two modules within a single level of module hierarchy. The messages can be arbitrarily complex data structures and may represent frames, packets, customers or jobs in a queue depending on the context. Omnet++ provides several built-in types for channels that can be customized by providing them appropriate parameters.

3.4 Network Topology and Configuration

In Omnet++, the structure of the network model is described in the NED (Network Description) language. The language as its name implies 'describes' the composition of the network as well as each individual component. The user can assemble simple and compound modules and connect their gates through links using the NED language. Basically it acts as a glue for different components in the network. The NED language supports object oriented features such as inheritance and interfaces which makes the components to be readily extensible and easily reusable.

To sum it up until this point the network topology is described using the NED language (.ned files), specific algorithms for active modules are written in C++

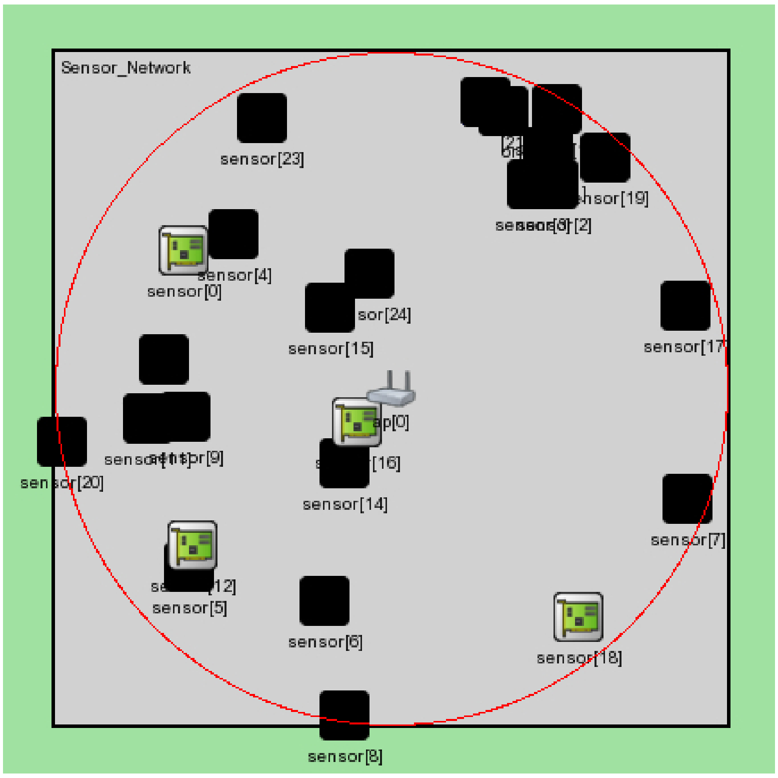

***Figure** 3.4 TKENV view for network simulation*

(.h/.cpp files) and message definitions are written in (.msg) files. Omnet++ requires every simple and compound module to have a NED declaration while its behavioral and algorithmic implementation is written in a C++ class registered with that NED declaration. Omnet++ provides us with a visual NED file editor for easy manipulation of network topologies. One such topology is shown in Fig. 3.3 which is the top level NED architecture of our basic simulation scenario. It contains an array of Access Points (APs) and Sensor Stations (STAs) which are configured so that stations are uniformly distributed around the APs in a radial region. This is shown in Fig. 3.4 which is the TKENV view when the simulation is run.

Such configurations can be provided by specifying the parameters of the modules either in NED files or in INI(initialization) files. INI files override the parameters already provided in the NED files and are usually used to provide common configurations for several modules. The source code of the simple NED topology shown above is given in Prog. 3.1 which has two parameters numHosts and numAPs. It also contains two compound modules named Wireless_STA and Wireless_AP which will be defined in their respective NED definitions. The parameters should be provided in the INI file in this example before executing the network model because NED files contains no default values for them.

Program 3.1 *NED Topology for a simple wireless network model*

```
package wsn;

import inet.nodes.wireless.WirelessAP;
import inet.linklayer.ieee80211.Ieee80211NicSTA;

network Sensor_Network
{
    parameters:
        int numHosts;
        int numAPs;

    submodules:
        sensor[numHosts]: Wireless_STA {
            @display("r=,,#707070");
        }

        ap[numAPs]: Wireless_AP {
            @display("p=61,124;r=,,#ff0000");
        }
}
```

A sample INI file for this network would look like Prog. 3.2 if we only consider the top level parameters. This would initialize the simulation with 10 wireless stations and 1 access point. The first two lines here represent the name of the configuration and the name of the network.

Program 3.2 *INI file for simple network model*

```
[General]
network = Sensor_Network
**.numHosts = 10
**.numAPs = 1
```

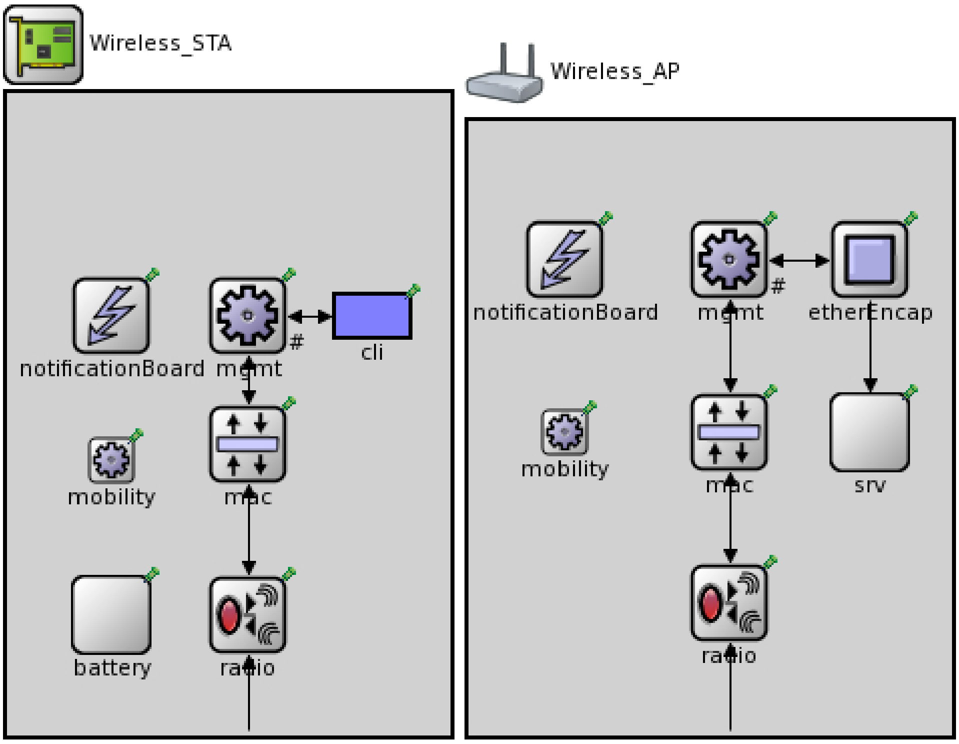

***Figure** 3.5 Internal stack for a Wireless AP and Wireless STA*

3.5 Protocol Stack Implementation

Until now we have described how basic networks are formed in Omnet++ using the NED language. However, the submodules that we have used in our previous example can be made arbitrarily complex to implement any kind of protocol stack. We have used the same blocks in this thesis to implement the physical and MAC layers of IEEE 802.11ah in Omnet++. On top of that there is a management module whose purpose is to manage the overall activity of a station including doze and awake times, beacon handling and packet handling from upper layers. Above the management layer, a traffic generator module generates packets with specified size and inter arrival time (time between generation of consecutive packets). Moreover, every station has a mobility module which keeps track of the movement of the station and whether it can move or not. In this thesis we have only considered stationary nodes as mobility is not the prime focus of IEEE 802.11ah. There is also a battery module with every station which keeps track of the amount of energy consumed by it during the course of the simulation and other similar statistics. A diagram showing the internal structure of both a wireless station and wireless AP is shown in Fig. 3.5.

At the AP side, the energy consumption is not so critical so we do not keep track of the energy consumption statistics there. Therefore, no battery module is used with AP implementation. The AP receives the messages from all the stations in the network in uplink and after successfully decoding them, transmits an acknowledgment. It also needs to generate beacon frame periodically which are broadcasted to the whole network.

4. ANALYTICAL CONSIDERATIONS

It is important to verify the results of the simulations by analytical means as they cannot be declared accurate with a good degree of confidence without such verification. In this thesis we have verified our work with two analytical models. More specifically the analytical models presented in this chapter verify the saturation throughput of RAW and Group Sectorization mechanisms. The first model is presented in [17] and gives an accurate model for saturation throughput of RAW mechanism. The second model present by us is a simple analytical model based on [30] which offers a good estimate of saturation throughput of RAW and verifies our simulation results.

4.1 Accurate Analytical Model for Saturation Throughput of RAW

The analytical model presented in [17] provides the saturation throughput for RAW under the basic 'FIXED' holding scheme and ideal channel conditions. We use this model to prove that our simulations are accurate and henceforth analyze our newly proposed holding and grouping schemes described in section 2.5.7. The saturation throughput S is given as

$$S = \frac{LN_{RAW}}{T_{RAW}} \times E_{tr} \times P_s, \tag{4.1}$$

where L denotes the payload bits, N_{RAW} is the number of RAW groups (slots), T_{RAW} is the duration of the RAW, E_{tr} is the expected value of the number of full transmission cycles and P_s is the probability of a station transmitting a packet successfully. A full transmission cycle is the sum of DIFS, Backoff and TXOP (DATA + SIFS + ACK).

In the foregoing analytical model, the probability of successful packet transmission is the same as mentioned by Bianchi in [30] and is given by (4.2). Here, N_g is the number of stations in a RAW group which are contending for channel access in a

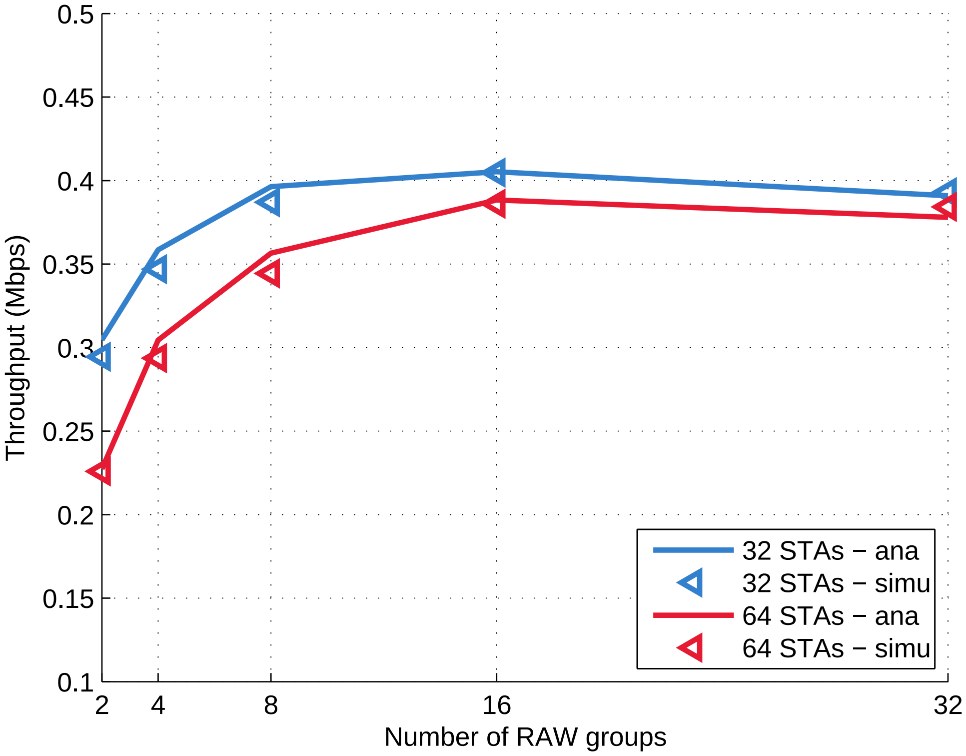

Figure 4.1 *Analytical model vs simulated results*

RAW slot and τ is the probability that a station transmits in a randomly chosen slot time. The model assumes that the number of backoff slots follows a geometric distribution between consecutive TXOPs in a RAW slot. Calculation of τ and E_{tr} along with rest of the analytical treatment can be found in [17].

$$P_s = \frac{N_g \tau (1-\tau)^{N_g - 1}}{1-(1-\tau)^{N_g}}. \tag{4.2}$$

We use the Omnet++ tool for our simulations as described in Chapter 3. Fig. 4.1 presents a comparison of the aforementioned analytical model with our simulations using the 'FIXED' holding scheme. The results are shown with 32 and 64 STAs associated to a single AP in the Infrastructure Basic Service Set (IBSS) with varying number of RAW groups. Saturated traffic is considered which means that a station always has a packet to transmit. The effects of path loss and propagation delays are also ignored in this case and ideal conditions are assumed. Other system parameters are shown in Table 2.4. It can be seen that the analytical and simulated results match nearly perfectly with an error of about 3% or less.

4.2 Simple analytical model for Saturation Throughput of RAW

In this section we propose a simple analytical model for the RAW performance under saturated traffic. Previously, the analysis work on IEEE 802.11 DCF performance either includes the Markov-chain-based analysis [30, 31, 32] or the mean value methodology [17, 33, 34, 35]. In both schemes it is assumed that the probability for transmitting a packet in an arbitrary slot is the same. We use the same assumption in our analysis.

To derive the analytical RAW performance, we consider a fully-connected IEEE 802.11ah network with N STAs accessing the wireless channel within a RAW period, i.e., there are no hidden terminals in the network. We also assume an ideal channel condition where no communication errors or capture effects occur. Furthermore, all transmitted packets are assumed to have the same length.

We start our analysis by noticing that within each RAW slot the stations are basically contending for channel access using the standard DCF procedure. The main differences are that the allocated time duration is smaller and the number of contending stations is fewer. Additionally in each RAW slot, there is a holding time period where the stations are not allowed to transmit due to the non-cross slot boundary feature imposed by the IEEE 802.11ah standard. In the following analysis we will first assume that the whole raw slot is used, i.e. the holding time period is set to zero. Therefore the total throughput in RAW period is basically the aggregate throughput over all N_{RAW} slots. In [17], a similar analytical study of the saturation throughput in RAW has been considered where the mean value methodology has been used.

In our analysis we will extend the well referenced work by Bianchi [30], where he derived the saturation throughput performance of the IEEE 802.11 DCF using Markov-chain based analysis, to the RAW scenario. Let $S_{DCF,N}$ be the normalized throughput as derived in [30] for DCF scheme with N STAs contending for channel access. We refer to this as the normalized Bianchi throughput and it is defined as the portion of the time utilized for successfully transmitting payload bits in a slot time. The expression for the normalized throughput is given as

$$S_{DCF,N} = \frac{P_s P_{tr} E[P]}{(1 - P_{tr})\sigma + P_{tr} P_s T_s + P_{tr}(1 - P_s) T_c}, \tag{4.3}$$

where P_{tr} and P_s denote the probability of transmission and successful transmission

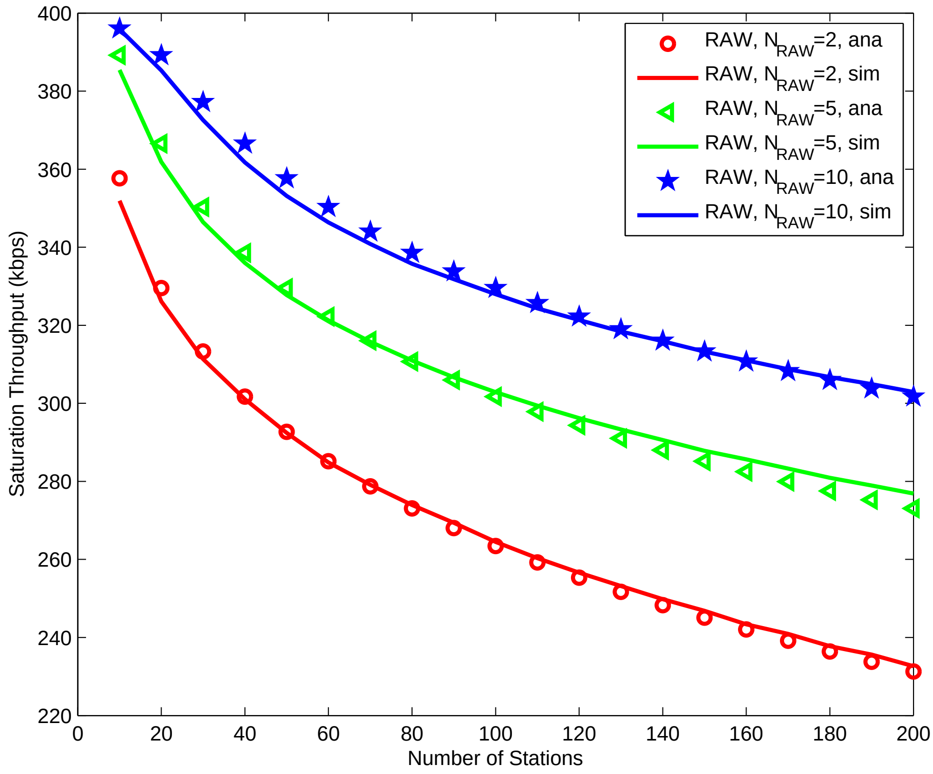

Figure 4.2 *Simulated vs Analytical Saturated Throughput of RAW with Holding Period.* μ *= 10%*

respectively. $E[P]$ is the average payload size and σ is the duration of an empty time slot. Finally, T_s and T_c represent the time taken by a successful and failed (due to collision) transmission respectively. More details on how to obtain each individual parameter can be found in [30].

If the total RAW duration is T seconds, then the Bianchi saturated $S^T_{DCF,N}$ throughput in T seconds can be simply expressed as

$$S^T_{DCF,N} = S_{DCF,N} \times T. \tag{4.4}$$

In a given raw slot, only $N_s = \frac{N}{N_{RAW}}$ stations will contend using the same DCF mechanism. Therefore in a given RAW slot $T_{RAW_{slot}}$ the total RAW slot throughput becomes

$$S_{RAW_{slot}} = S_{DCF,N_s} \times T_{RAW_{slot}}. \tag{4.5}$$

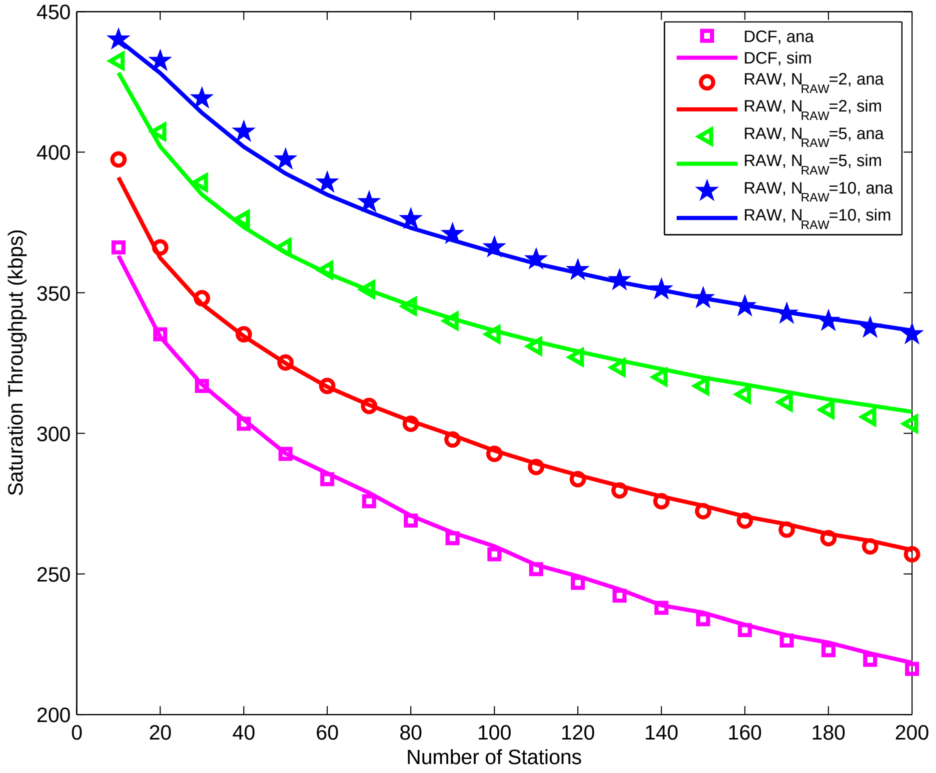

Figure 4.3 *Simulated vs Analytical Saturated Throughput of RAW without Holding Period.*

The total RAW throughput in a duration T of RAW period interval is given as

$$S_{RAW,T} = N_{RAW} \times S_{RAW_{slot}} \tag{4.6}$$

$$= \underbrace{N_{RAW} \times T_{RAW_{slots}}}_{T} \times S_{DCF,N_s}. \tag{4.7}$$

Finally the normalized total RAW throughput of a network with N STAs given that N_s STAs are contending in one RAW slot can be expressed as

$$S_{RAW,N} = \frac{S_{RAW,T}}{T} = S_{DCF,N_s}. \tag{4.8}$$

Therefore the saturated RAW throughput for N STAs is basically equal to the Bianchi throughput in DCF case with only N_s STAs contending in the network. It is worth mentioning here that in the above analysis we are assuming a zero holding time period. Otherwise, if we assume a fixed holding time in each raw slot then less time will be allocated in average for the stations to contend in a given RAW slot. Consequently the saturated RAW throughput will be less. If μ is the fraction of the total RAW slot duration represented as a percentage, then the saturated RAW throughput with fixed holding time can be expressed analytically as

$$S_{RAW,N}^{fixed-holding-time} = S_{RAW,N} - \mu S_{RAW,N}. \tag{4.9}$$

The analytical saturated RAW throughput expressions in (4.8) and (4.9) are now validated through simulations. For this purpose, we assume an ideal channel for the stations with no propagation delay or path loss with saturated traffic. The system simulation parameters are given in Table 2.4. Fig. 4.3 shows the analytical (markers) and simulated (lines) saturation throughput of DCF and RAW with varying number of RAW slots (N_{RAW}). It can be seen that the analytical and simulated results match perfectly. Similarly, Fig. 4.2 shows the analytical and simulated saturation throughput of RAW considering a fixed holding time of 10% and shows a near perfect match between them.

5. PERFORMANCE EVALUATIONS

In this chapter we present the results of our proposed enhancements as well as the performance evaluation results of the new features of IEEE 802.11ah MAC layer. We have studied different deployment scenarios which will be described in their corresponding sections. In our assessment, only short headers and compact frames are considered, as it was demonstrated in chapter 2 that they are better suited for sensor applications characterized by short data packets exchange. The performance is assessed for 2 MHz mode with a single spatial stream, using three main metrics i.e. the network aggregate throughput, energy efficiency and fairness. Other simulation parameters are listed in Table 2.4.

5.1 RAW Performance with Cross-Slot Boundary Condition

In this part of our performance analysis we consider the Infrastructure BSS with a single Access Point (AP) having a maximum coverage area of R at MCS 0. At this distance the received signal level due to path loss is at the minimum sensitivity level. The corresponding values of sensitivities for different MCSs can be found in Table 2.3. Stations are uniformly distributed around the AP as shown in Fig. 5.1. The figure shows two regions where some of the stations lie at a distance less than half of the maximum coverage radius from the AP while others lie beyond it. We use this scenario to show that depending on the distance from the AP it is beneficial for stations to prefer one holding scheme over the other.

Similar to our analytical analysis in chapter 4, here also we assume a saturated traffic scenario. We evaluate the performance of all holding and grouping schemes described in section 2.5.7 for 1000 stations uniformly distributed around a single AP. The duration of RAW is 1 second which is enough to allow for the transmission of at least one packet with 100 RAW groups. The payload size is chosen to be 256 Bytes and NDP ACK is used. We consider only the basic access mechanism since it is shown to be more efficient in case of smaller payload sizes [15].

Since, in the 'FIXED' scheme all the stations are using the same holding period

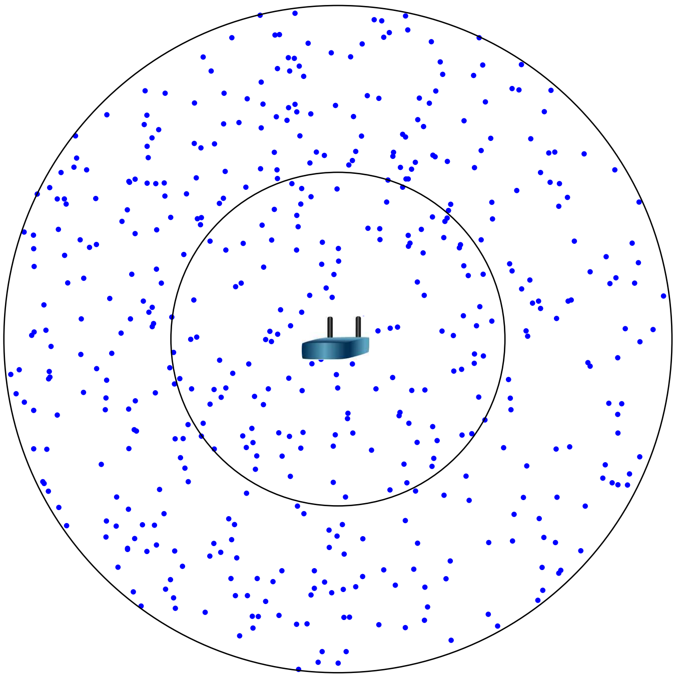

Figure 5.1 *Distribution of stations around the AP*

regardless of their distance from the AP, it can be regarded as a benchmark for performance comparison to our proposed schemes in the RAW non-cross slot boundary case. A benefit of using the 'FIXED' scheme is that the resource allocation is fair, as all the stations in a RAW slot are allocated the same time in which they contend for channel access.

Fig. 5.2 shows the throughput of the network with 1000 stations associated with the AP. It can be seen that 'DECREMENTING' scheme performs almost similar to the 'FIXED' scheme with a little improvement when the number of stations in a RAW group is small. The 'VARIABLE' scheme performs better than the 'FIXED' scheme and this effect is more pronounced when the number of RAW groups is large. This is due to the fact that when the size of the RAW slot is small, it is advantageous for the stations to retain a higher backoff value to reduce the number of collisions in their next RAW slot. The throughput fluctuation with different number of RAW groups, most notably between RAW groups 60 and 80, can be attributed towards non-monotonic dependence of throughput on RAW slot size in the non-cross slot boundary case [17].

In the 'HYBRID' scheme the stations which are located in the outer ring of the AP cell use the 'VARIABLE' scheme while those located close to AP use the 'FIXED' scheme. This improves the throughput performance even more, because the stations which are far from AP are more likely to have collisions due to the hidden node

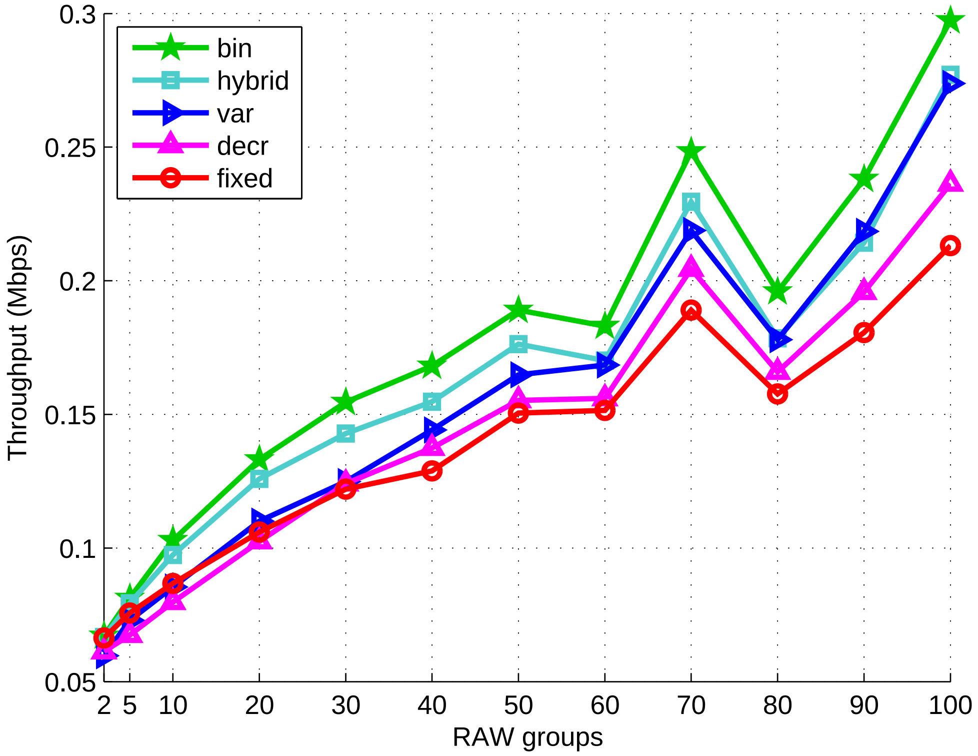

***Figure* 5.2** *Throughput for different number of RAW groups (N=1000)*

problem and using a larger backoff or effectively a larger holding period prevents that from happening.

Finally, the proposed 'BIN' scheme provides the best throughput performance and there is a significant performance improvement compared to the 'FIXED' scheme which generally performs the worst. The proposed 'BIN' scheme should not be regarded as a holding scheme as it is rather a grouping scheme and uses the 'HYBRID' scheme as its holding scheme. The gain in performance over the 'HYBRID' scheme is due to the fact that 'BIN' scheme uses a deterministic criteria for the grouping of stations which is based on their backoff state (backoff counter) in the previous RAW. It allocates the stations to groups so that channel utilization is increased by making the group of stations with their backoff counters sorted in ascending order contend for channel in a RAW slot. Moreover, stations with equal backoffs are placed in different groups, thus reducing the overall number of collisions.

Fig. 5.3 shows the energy consumption per successful packet of different holding schemes under a network size of 1000 stations. To calculate the energy consumption we multiply the values from Table 5.1 for different states of the transceiver by the amount of time the transceiver spends in that state. The obtained results

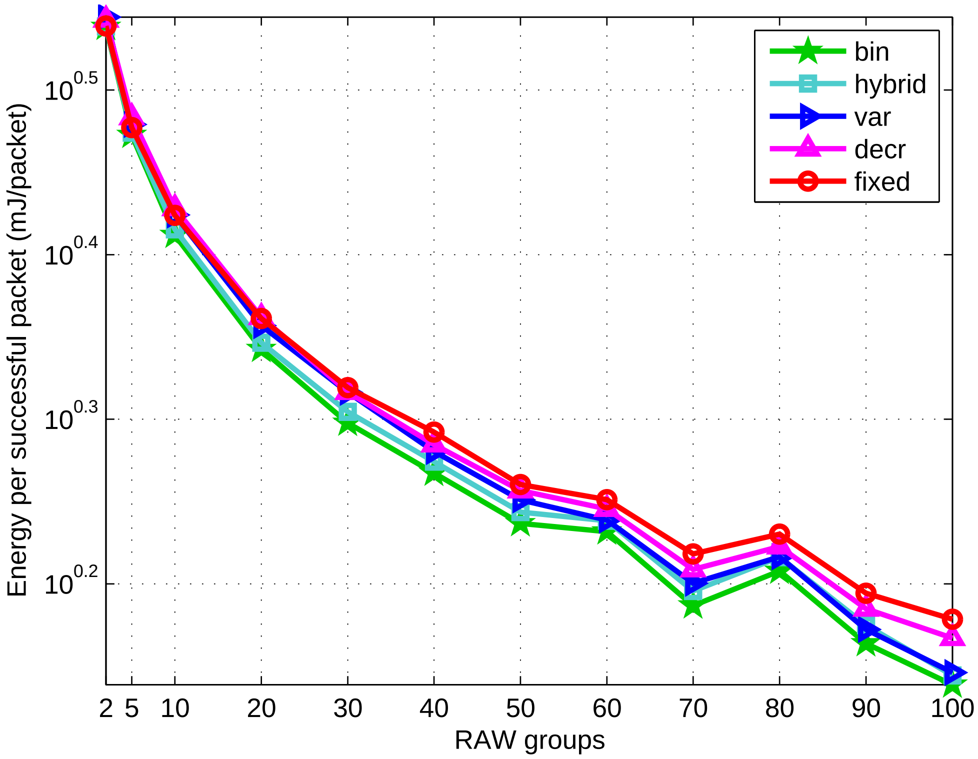

***Figure* 5.3** *Energy Consumption for different number of RAW groups (N=1000)*

are in consistency with the throughput performance i.e. the schemes which give a better throughput also consume less energy in the successful delivery of a packet, as increased throughput is a result of decrease in collisions. We can see that the proposed 'BIN' scheme consumes the least amount of energy.

***Table* 5.1** *Energy consumption for different transceiver modes*

STA Mode	Energy (mW)
Transmit	255
Receive/Channel Sense	135
Sleep	1.5

Fairness in the network is also an important performance metric that we consider in the analysis of our proposed holding schemes, using the well-known Jain's fairness index [36]. Fig. 5.4 shows that the throughput improvements do not come at the expense of fairness in the network and (with negligible differences) it remains the same for all holding schemes. While the figure shows the fairness values for selected values of number of RAW groups, similar results hold for other values as well which are not shown here.

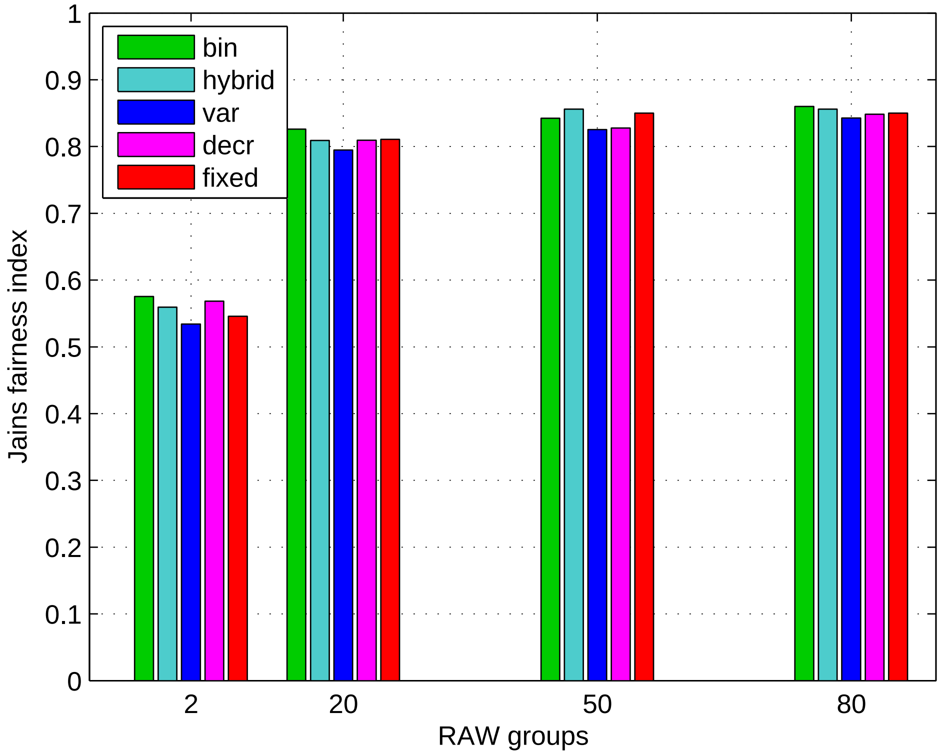

Figure 5.4 *Fairness for different number of RAW groups (N=1000)*

5.2 Multi-Access Point Scenario

In this section, we evaluate the performance of earlier discussed IEEE 802.11ah MAC features while the network operates in an overlapping BSS scenario. Here also we, consider uniform random distribution of stations in a BSS but with a coverage radius of $\frac{R}{2}$. With this setting we assume that there are no hidden nodes within a single BSS. There may be however hidden nodes in the OBSS. We consider a packet size of 256 Bytes like in the previous section and only consider uplink saturated traffic which means that a station always has a packet to transmit. For the OBSS scenario we consider a maximum 30% overlap between the coverage radii of two BSS as shown in Fig. 5.5. The access points are assumed to be unsynchronized and no coordination strategies are used between them.

5.2.1 TXOP Based Sectorization

The performance of the TXOP based sectorization feature of the new IEEE 802.11ah amendment is evaluated here in the presence of OBSS with a 30% overlap in coverage area. In practical deployment scenarios the STAs in the overlapping BSS can use

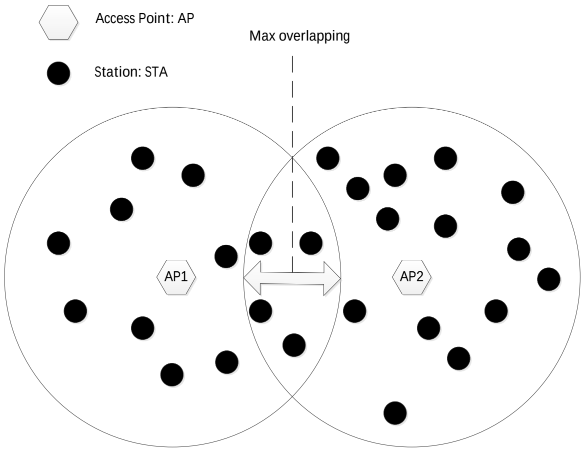

Figure 5.5 *OBSS problem settings.*

the same channel for their transmissions for the duration of the TXOP when they satisfy the condition of spatial orthogonality with the ongoing transmission. It is however difficult to predict the portion of the time the STAs will be participating in the TXOP based sectorized transmissions.

In this experiment we evaluate the performance of TXOP based sectorization for varying portions of the total network operation duration. For instance, 10% operation duration means that out of the total network operation time, the AP is using 10% of the time for sectorized transmissions and 90% time for the normal omni transmission. Fig. 5.6 shows the saturated throughput performance of the TXOP based sectorization mechanism. We can see that as the portion of time used for sectorized transmissions increase, there is a proportional increase in the throughput. This is due to the fact that during the sectorized beam operation a high number of packets are successfully transmitted due to lower collisions and reduction in channel contention.

5.2.2 Subchannel Selective Transmission

In this section, we evaluate the performance of the subchannel selective transmission (SST) and identify the parameters that can be tuned to achieve optimal performance using SST. In our simulations we consider that the SST Element is sent with every beacon containing the UL activity schedule since we only consider UL traffic. A fixed percentage of stations among all present in the network are randomly selected by the AP and allocated a portion of the beacon interval during which they can transmit UL traffic on a secondary subchannel. As the algorithm for selecting the best subchannel is beyond the scope of our study we assume that there is only one available secondary subchannel.

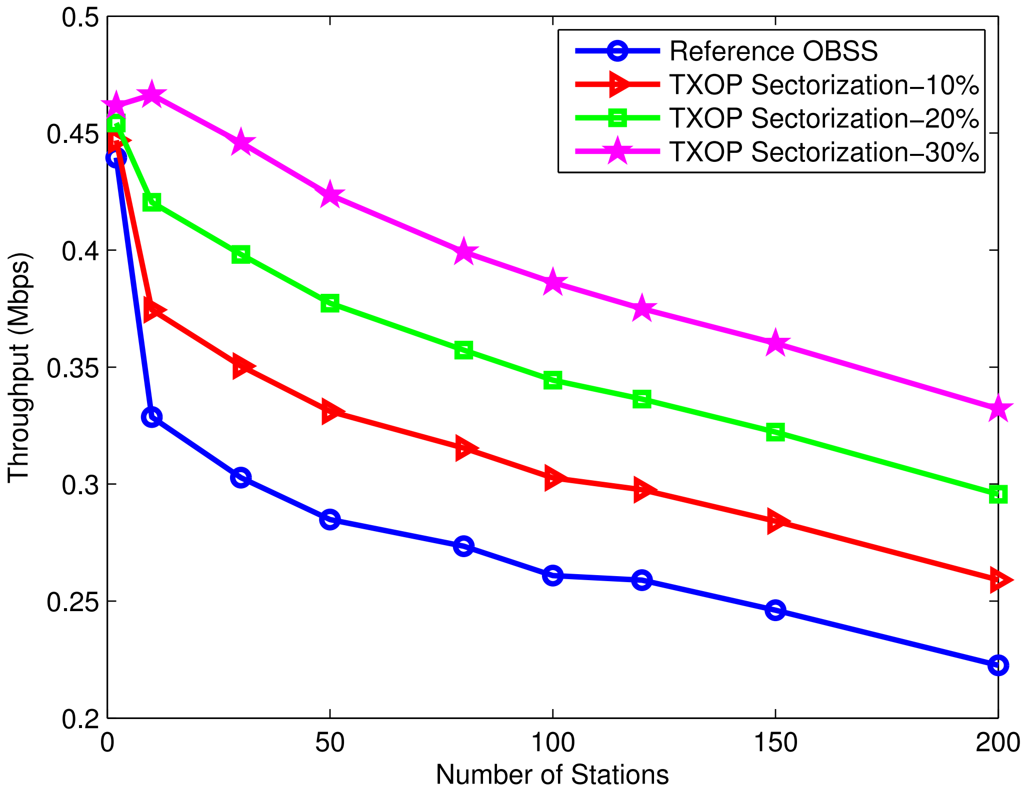

Figure 5.6 *TXOP Based Sectorization*

Fig. 5.7 shows the saturation throughput of the SST mechanism with varying SST duration and percentage of stations taking part in SST. In can be seen that highest throughput is achieved when all of the beacon interval is reserved for SST. It is however impractical to do so and is shown to estimate the upper limit of throughput gain using SST. It is more practical that the SST duration is chosen to be a fraction of the beacon interval and the SST is not used with each beacon interval to keep fairness among stations. The throughput performance of 10% STAs is greater than 30% STAs which is intuitively because of the reduction in channel contention with lesser number of STAs.

5.2.3 RAW and Group Sectorization

In this section, we evaluate the performance of group sectorization with varying number of sectors in the OBSS scenario with two overlapping BSS and compare it to the performance of RAW mechanism as well as the basic DCF. In the sectorization mechanism, we consider two cases. In the first case we assume that the number of sectors is equal to the number of RAW slots N_{RAW}, i.e. 10 sectors. In the second

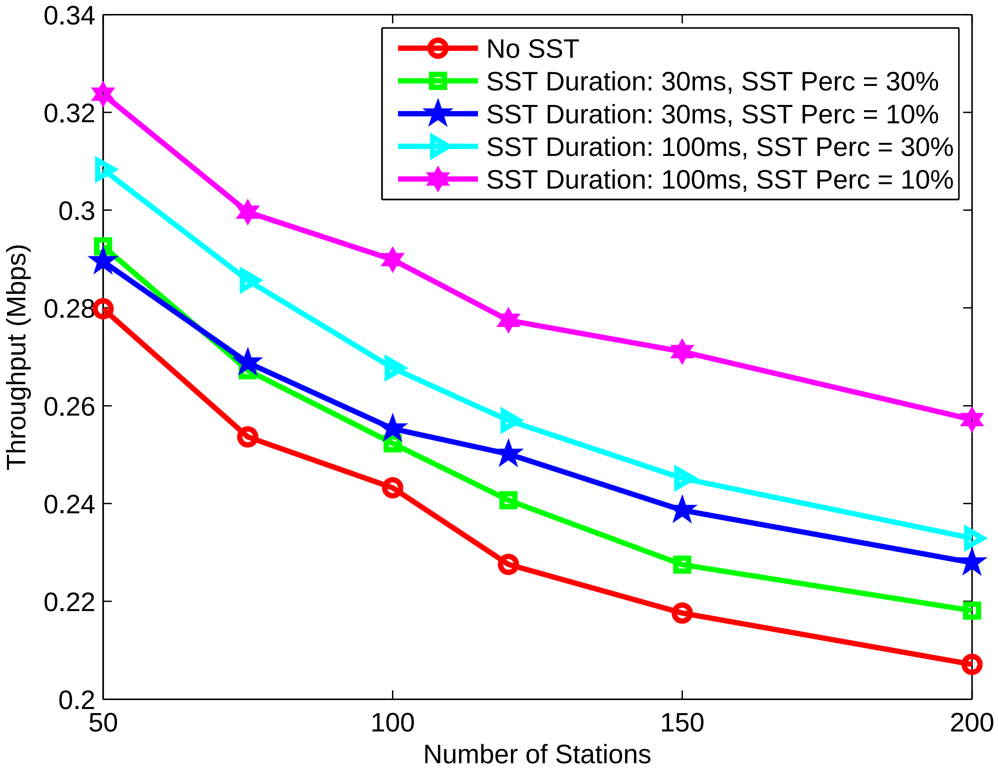

Figure 5.7 *Subchannel Selective Transmission*

case, we assume however that the number of sectors is 5, meaning that every STA in a given sector will use two consecutive RAW slots.

To evaluate the energy consumption performance (mJ/packet), a similar approach is taken as described in the previous section. A power consumption value is associated with each state of the transceiver and then the total energy consumption is calculated based on how much time the transceiver spends in each particular state. Table 5.1 summarizes the energy consumption in different STA modes.

Regarding the RAW mechanism settings, the value of parameter N_{RAW} needs to be tuned depending on the considered configuration to maximize the throughput performance. Such an optimization study was conducted in [15] in a single AP case. The authors of [15] concluded that N_{RAW} equal to 10 is the best option for similar sets of parameters.

The aggregate throughput performances for the OBSS case is shown in Fig. 5.8. It can be also seen that the RAW scheme highly improves the system performance as compared to the basic scheme (DCF). A further improvement can be achieved when sectorization is also used, particularly when the number of RAW slots is equal to the

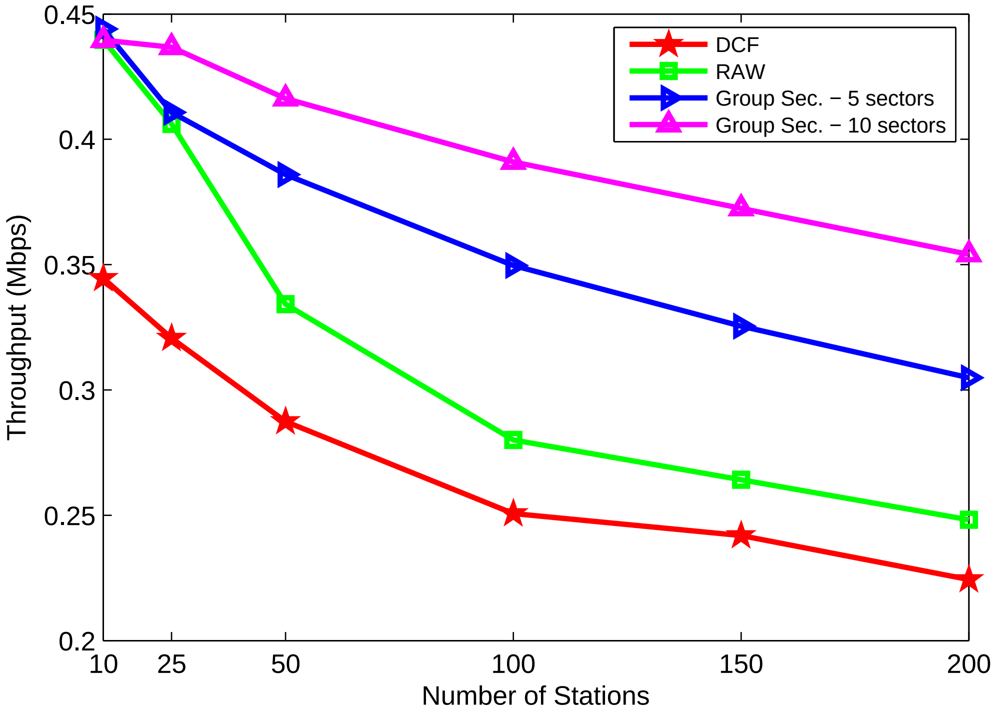

Figure 5.8 *Aggregate network throughput for two APs case.*

number of sectors. The energy efficiency performance follows the same trend. As shown in Fig. 5.9, the basic DCF scheme consumes the most amount of energy while group sectorization with 10 sectors provides the best energy efficiency performance. Hence these findings clearly demonstrate the importance of RAW and sectorization mechanisms in practical IEEE 802.11ah deployment scenarios especially in the OBSS case where high interference due to overlapping BSS is common.

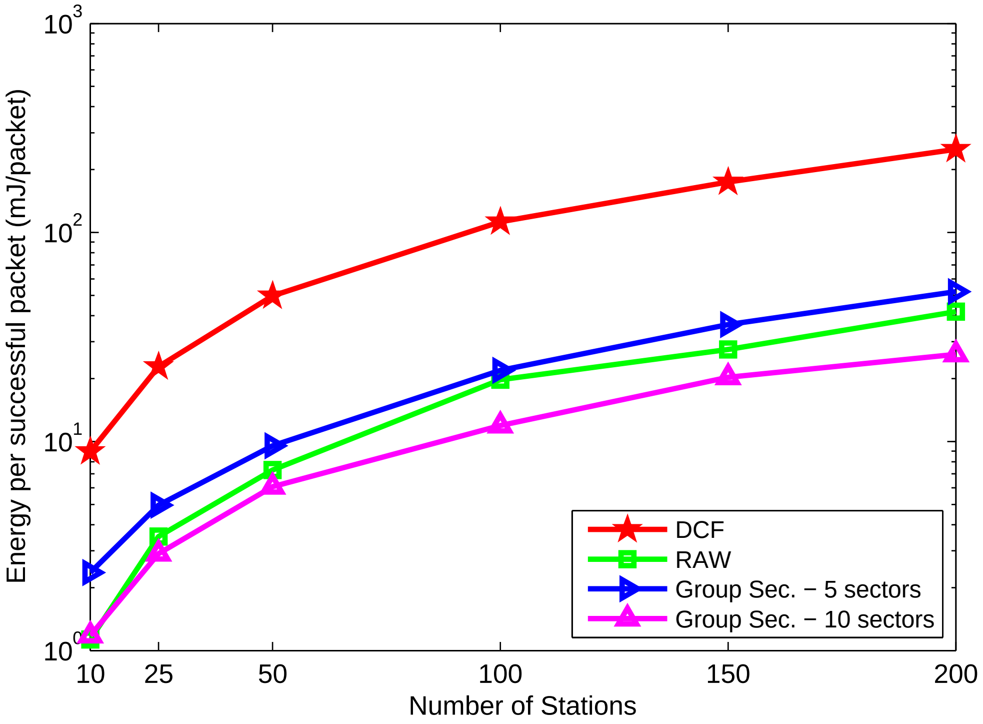

Figure 5.9 *Energy efficiency for two APs case.*

6. DUTY CYCLE CHALLENGES

The IEEE 802.11ah standard is designed to operate in the license free sub-1 GHz ISM bands. These bands although unlicensed are subject to various regulations regarding the transmission characteristics and spectrum requirements set by different regulatory authorities such as ERC and ETSI in Europe and FCC in the US. These organizations set guidelines for example on the maximum allowed transmit power, channel spacing and radio duty cycle for radio technologies deployed in these bands.

In this context and observing the regulations in Europe, Sub-1 GHz ISM bands are subject to a maximum duty cycle limit per device that prevents a given transmitter from occupying a channel for an extensive period of time. As IEEE 802.11ah operates in this band, it needs to adhere to this maximum duty cycle limitation per device. This affects the performance claimed by the IEEE 802.11ah specifications and has an effect on the target use cases.

The limits on the maximum duty cycle are in the order of 1% - 2.8% for devices complying with (Listen Before Talk) LBT and Adaptive Frequency Agility (AFA) mechanisms [37]. LBT is the mechanism in which a device listens to the channel to detect whether the shared medium is idle before it attempts transmission itself. Adaptive frequency agility means that a device is capable of adaptively switching to a subchannel of the wider operation bandwidth. The duty cycle limitations for stations which do not comply to LBT+AFA are more strict as such devices cause excessive emissions in the unlicensed bands and pose interference problems to other devices operating in the same frequency region. The maximum duty cycle requirement for the devices not supporting LBT and AFA ranges from 0.1% to 1%.

In this chapter we investigate the challenges of the maximum duty cycle limit and its effect on the IEEE 802.11ah performance. This chapter is self contained as the results of our evaluations are also presented in it. We first derive the theoretical maximum achievable duty cycle in an IEEE 802.11 network under saturated traffic scenario. We then proceed on to analyzing the throughput performance of the network with the duty cycle limit imposed on the stations by means of system level simulations using our Omnet++ simulator under both saturated and unsaturated traffic assumptions. Our focus in this work remains on the analysis of the uplink duty cycle whereas only beacons and acknowledgment frames are transmitted in the downlink.

As described in section 2.5.8, one of the new MAC features introduced by TGah is the Subchannel Selective Transmission (SST) mechanism, allowing devices to rapidly select and then switch to the most favorable channel amongst a larger set of channels on which they can operate. For instance, a single AP operating in an 8 MHz bandwidth can serve multiple sensor type stations which use 1 MHz channel bandwidth. In this case, the standard allows the stations to select the most suitable 1 MHz sub-channel within the wider 8 MHz bandwidth to transmit and receive.

6.1 Theoretical Upper Limit of IEEE 802.11ah Duty Cycle

As the IEEE 802.11ah system was defined to work globally across regions with different restrictions, APs and STAs need to adhere to the regulatory requirements within the region of its operation. While there is no limitation on the duty cycle for the sub GHz ISM band in the US, in Europe the duty cycle for a device can not exceed 2.8% provided that it complies with the LBT and AFA channel access requirements.

We start our analysis with investigating whether IEEE 802.11ah in fact complies to the LBT+AFA requirements. In principle, the IEEE 802.11ah system was designed with well-defined rules for channel access. For instance, the IEEE 802.11ah employs Carrier Sense Multiple Access protocol with collision avoidance (CSMA-CA) where all devices are required to listen to the channel before transmission. Therefore, the CSMA-CA can be considered as a refined LBT procedure. Furthermore, the Subchannel Selective Transmissions (SST) feature introduced by the IEEE 802.11ah which allows the STAs within the BSS to rapidly select and then switch to the most favorable channel, can also be seen as an example of the AFA procedure. Therefore it is safe to assume that the IEEE 802.11ah based devices are LBT and AFA compliant. However, the IEEE 802.11ah does not have specific limitations on the maximum transmit duty cycles for individual devices.

The ERC Recommendation [37] defines the duty cycle as the percentage of the maximum transmitter "on" time (active duration t_{active}(s)) on one carrier frequency, relative to a one hour period. We can formulate the duty cycle percentage D as

$$D = 100 \times \frac{t_{active}}{3600}. \tag{6.1}$$

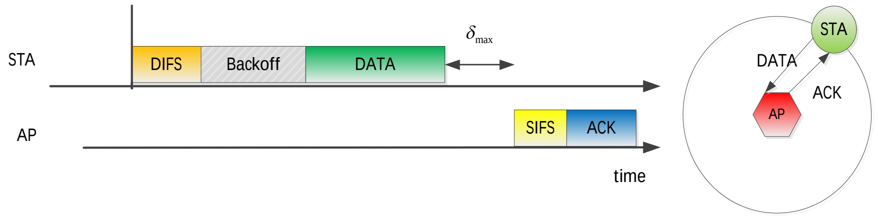

Figure 6.1 *Typical data transmission in a simple IEEE 802.11ah network using the basic scheme: we assume uplink traffic where the STA continuously (full buffer case) sends DATA packets to the access point.*

The duty cycle is usually defined per device, i.e., only the activity of a tagged device is concerned and not the whole network. In the following we investigate the theoretical maximum duty cycle for STA and AP devices in an IEEE 802.11ah network.

6.1.1 STA Duty Cycle

For a simple IEEE 802.11ah network where only one device is sending data to its associated access point (AP), we can easily determine the upper limit of the duty cycle D per device analytically. Fig. 6.1 shows how data is typically transmitted between one station (STA) and one AP using the IEEE 802.11ah basic access scheme. The IEEE 802.11ah timing parameters are shown in Table 2.4.

Here we assume the following:

- We assume uplink traffic where the STA continuously sends DATA packets to the AP.
- Point to point communication between one STA and one AP (no contention).
- No re-transmissions are used: a given data packet is transmitted only once.
- We use a minimum contention window (CW_{min}) of 15 time slots. Consequently, the random back-off time will be chosen between 0 and 15 time slots, which results in an average of $(CW_{min} + 1)/2$ seconds per sent packet.
- Full buffer: The STA always has a packet to be transmitted.

If we assume further that the basic modulation and coding scheme, MCS 0, is used (0.650 Mbps) and the size of data payload is 256 bytes, then to determine the theoretical duty cycle upper limit we need to know the number of times the

Table 6.1 *Upper limit of duty cycle for a STA with different payload sizes for 1 MHz and 2 MHz channel widths*

MCS	1 MHz			2 MHz		
	256 B	512 B	2048 B	256 B	512 B	2048 B
MCS 0	95.08	97.39	99.32	81.45	89.12	96.90
MCS 1	90.74	94.96	98.64	70.07	80.93	94.05
MCS 2	86.98	92.69	97.99	62.39	74.53	91.40
MCS 3	83.53	90.53	97.34	56.84	69.63	88.95
MCS 4	77.84	86.64	96.08	49.38	61.68	84.53
MCS 5	72.85	83.13	94.87	45.33	56.84	80.75
MCS 6	70.92	81.61	94.27	43.84	53.93	78.97
MCS 7	68.70	80.00	93.68	42.25	52.87	77.35
MCS 8	65.55	77.35	92.56	38.81	49.38	74.21
MCS 9	63.72	75.45	91.82	-	-	-
MCS 10	98.71	99.33	99.82	-	-	-

transmission cycle shown in Fig. 6.1, occurs in one hour. Let Q be the number of cycles, which can easily be determined as

$$Q = \left\lfloor \frac{3600}{T} \right\rfloor, \tag{6.2}$$

where $\lfloor x \rfloor$ denotes the largest integer less than or equal to x and T is the total transmission cycle duration given in (6.3).

$$T = DIFS + Backoff + DATA + SIFS + \delta_{max} + ACK. \tag{6.3}$$

Once the number of cycle Q is determined, the theoretical duty cycle upper limit D_{max}^{STA} for a given STA in the network can be expressed as

$$D_{max}^{STA} = 100 \times \frac{Q \times DATA}{3600}. \tag{6.4}$$

The upper duty cycle limit for a STA for different payload sizes and MCS is given in Table 6.1. As it can be seen in the table, the maximum duty cycle is higher for larger payloads and lower MCSs. Intuitively, the duty cycle is higher for 1 MHz channel width as compared to the 2 MHz mode.

Table 6.2 *Upper limit of duty cycle for AP with different uplink payload sizes for 1 MHz and 2 MHz channel widths. Beacon size = 100 Bytes*

MCS	1 MHz			2 MHz		
	256 B	512 B	2048 B	256 B	512 B	2048 B
MCS 0	7.66	4.61	2.08	10.10	5.98	1.81
MCS 1	8.85	5.36	2.30	13.29	8.52	2.76
MCS 2	9.43	5.81	2.46	14.83	10.09	3.50
MCS 3	10.82	6.72	2.74	16.99	12.00	4.46
MCS 4	11.99	7.69	3.09	17.43	13.23	5.43
MCS 5	13.10	8.59	3.43	18.81	14.88	6.72
MCS 6	13.95	9.25	3.70	19.33	15.88	7.33
MCS 7	14.92	9.96	3.95	19.87	16.24	7.88
MCS 8	14.63	10.02	4.08	21.04	17.43	8.95
MCS 9	15.34	10.76	4.37	-	-	-
MCS 10	7.82	5.17	3.06	-	-	-

6.1.2 AP Duty Cycle

In the uplink traffic scenario, the AP activity is mainly related to sending ACKs to the corresponding STA in addition to periodically transmitting beacon management frames. Here we assume that only long beacon frames are transmitted with a period interval of one second. Hence, in principle the AP will broadcast 3600 beacons in an hour. If B_T is the time needed for transmission of all the beacons during an hour, then (6.2) can be modified for AP duty cycle as

$$Q_{AP} = \left\lfloor \frac{3600 - B_T}{T} \right\rfloor. \tag{6.5}$$

Using the same assumptions as in the estimation of the STA duty cycle, the theoretical duty cycle upper limit D^{AP}_{max} of the AP can then be expressed as

$$D^{AP}_{max} = 100 \times (\frac{Q_{AP} \times ACK}{3600} + BEACON), \tag{6.6}$$

where BEACON is the duration of the beacon frame assumed to be sent with the most robust MCS. Generally the typical length of a long beacon in an IEEE 802.11ah network is around 100 Bytes. The maximum theoretical duty cycle for AP is shown in Table 6.2 for different sizes of uplink payload. Here the duty cycle values are less compared to STA duty cycle because only beacons and ACKs are transmitted in downlink.

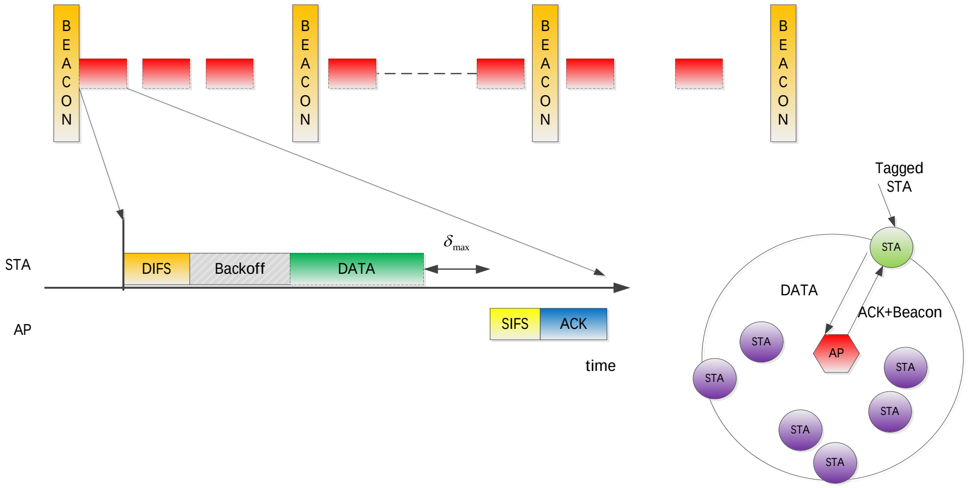

Figure 6.2 *Typical transmission in IEEE 802.11ah network*

6.2 IEEE802.11ah performance under duty cycle limits

In this section we evaluate the performance of an IEEE 802.11ah network while considering the duty cycle limits under different traffic assumptions. The simulation parameters are given in Table 2.4 while we assume an ideal channel and zero path loss for the stations. In the simulations we also assume a maximum number of unsuccessful transmission attempts of 4 for a packet, after which the packet is discarded. Again, we use the Omnet++ simulation tool for our simulations. We analyze the throughput of the system when the duty cycle limit is imposed on each station in the network and compare it to the scenario when no such limitation is applied. In our simulations we consider both the saturated and unsaturated traffic scenarios and present our findings in the following.

6.2.1 Saturated Traffic Analysis

In the saturated scenario each station has full buffer, meaning that it always has a packet to transmit. As soon as one station exhausts its duty cycle limit, it is considered inactive for the remaining period of the hour. Fig. 6.3 shows the saturation throughput of the network when a 1% and 2.8% duty cycle limit is imposed while the throughput with no duty cycle limitation is also shown for comparison. It can be seen that imposing a limit of 1% on the duty cycle of all stations results in a high degradation of network performance and even with saturated traffic the throughput remains below 60 kbps.

Relaxing the duty cycle limitation to 2.8% improves the network throughput and allows acceptable data rates to be achieved. It is interesting to note that when the

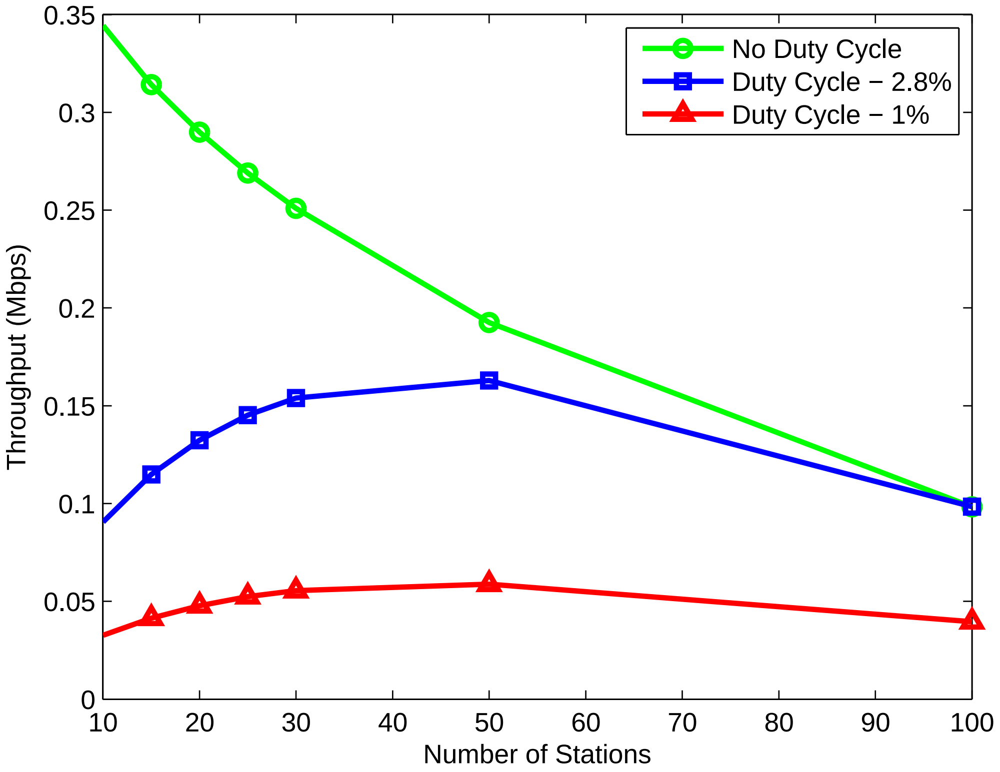

***Figure* 6.3** *Network Throughput in Saturated Traffic for Limited Duty Cycle*

***Table* 6.3** *Traffic Parameters for IEEE 802.11ah Use cases used in the simulation*

Use case	Packet Size (Bytes)	TX Period (sec)
Sensor Networks (IoT)	256	10-60
Home/Building Automation	512	60
Healthcare/Clinic	2048	0.25

number of stations in the network reach 100, the throughput of the network with and without the duty cycle limit becomes the same. This indicates that beyond this network size the duty cycle limit of 2.8% does not affect the system performance since due to increased contention in the network the stations remain below their duty cycle limit and spend most of the time in listening to the channel transmissions.

6.2.2 Unsaturated Traffic Analysis

The unsaturated scenario is of more interest particularly because all practical use cases for the IEEE 802.11ah network have unsaturated traffic assumptions. In this section we consider three use cases of the IEEE 802.11ah amendment described in [13, 38]. The selected use cases encompass a wide range of applications and represent

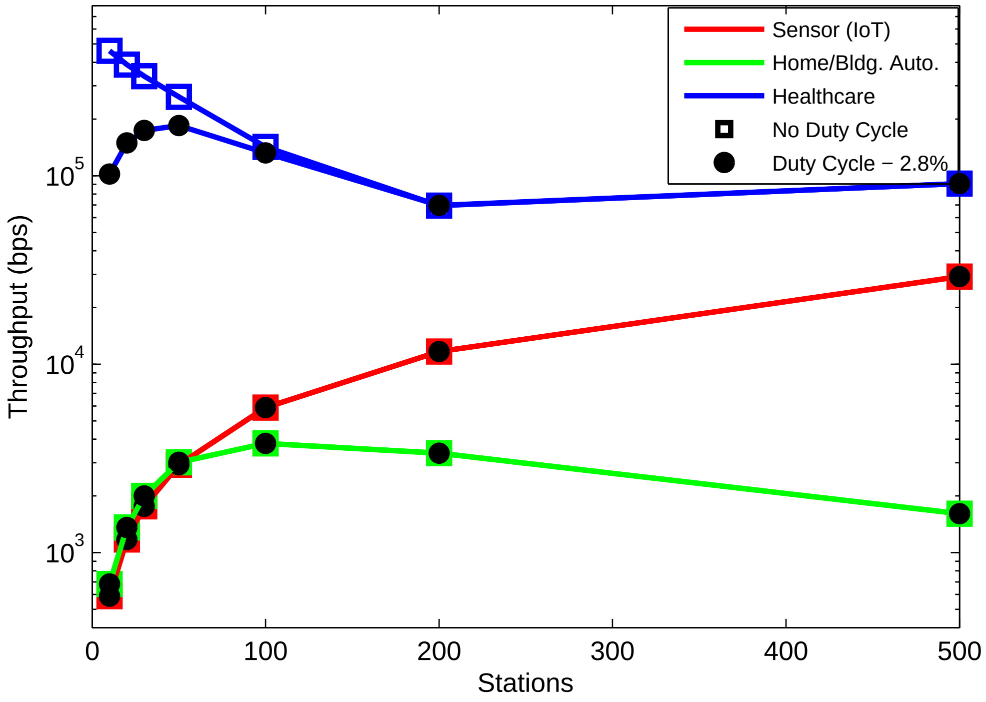

Figure 6.4 *Network Throughput in Unsaturated Traffic with (black circles) and without (squares) the 2.8% Duty Cycle Limit*

typical scenarios in which the IEEE 802.11ah networks will be deployed [12]. For instance in the healthcare usecase, the used values are a good representative of ECG, heart rate and EEG measurements [39].

Fig. 6.4 shows the throughput for up to 500 stations with and without the 2.8% duty cycle limit imposed for different use cases. The black circled markers depict the case when the duty cycle limit is imposed. The payload size and inter-arrival times of packets for stations' uplink data for each use case are given in Table 6.3.

We observe that the throughput of the network with and without the duty cycle limit remains the same for the 'Sensor Networks' and 'Home & Building Automation' use cases. This indicates that in these two use cases, due to a combination of low traffic intensity and payload sizes, the stations do not run out of their duty cycle limit of 2.8%. On the other hand, the performance in case of 'Healthcare' use case is moderately degraded up to a network size of 100 after which the duty cycle limit does not have any effect on the performance due to increased contention in the network, as we saw earlier with the saturated traffic case.

It is also important to consider that after a station exhausts its duty cycle limit, how much time it has to wait to start its next transmission. Naturally, since we

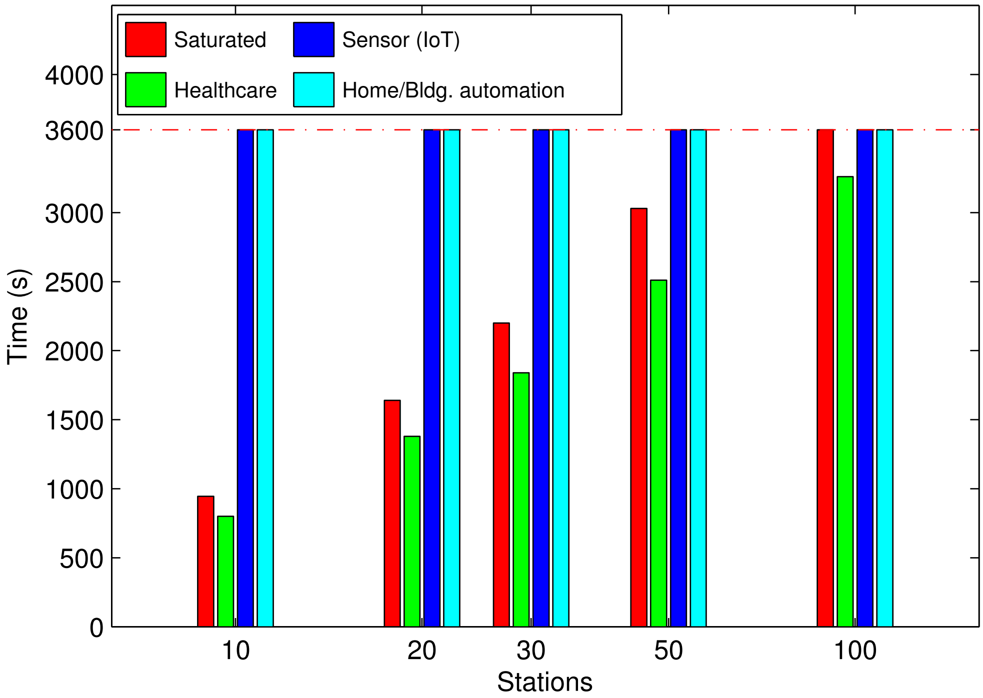

Figure 6.5 *Mean times within an hour for all stations to exhaust the 2.8% Duty Cycle Limit*

have defined the duty cycle limit for one hour, we can examine at what point during the hour the station runs out of its assigned quota of channel access attempts to determine the delay it will experience till its next transmission. Fig. 6.5 shows the average times at which the duty cycle limit is exhausted for all stations in the network for the described use cases. It can be seen that in case of 'Sensor Networks' and 'Home & Building Automation' use cases the duty cycle limit is not exhausted until the end of the hour (represented by red dashed line). In case of saturated traffic the limit is exhausted very quickly as compared to the 'Healthcare' use case.

At this point it is interesting to see the duty cycle of the AP as it has to serve a large number of stations. It is also particularly important because in infrastructure mode, if the AP exceeds its duty cycle limit then no station will be able to transmit its data causing severe degradation of network performance. Considering only the uplink traffic and a long beacon interval of 1 second, the duty cycle of the AP for different network sizes is shown in Fig. 6.6. We can see here that the duty cycle of the AP remains well below 2.8% for every considered use case.

It is however noted that in the presence of downlink traffic and more frequent transmission of beacons, the AP may exhaust this duty cycle limit even under low intensity traffic. The actual capacity limits for this scenario however, still remain an

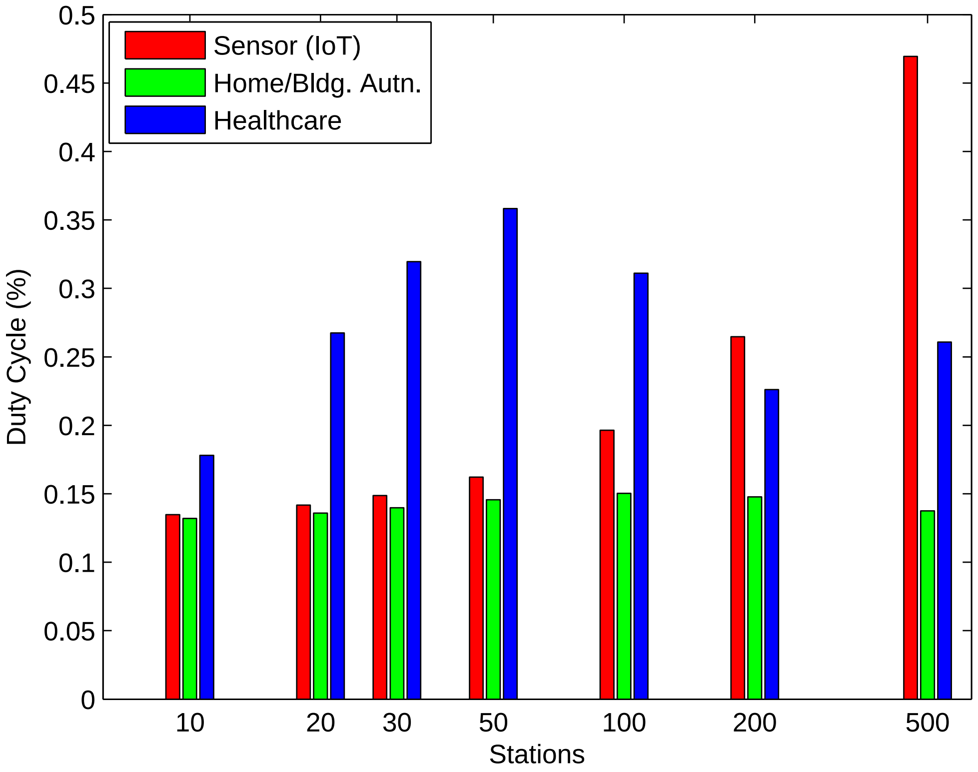

Figure 6.6 *AP Duty Cycle in Unsaturated Traffic with 2.8% Duty Cycle Limit*

uninvestigated issue and form an important subject for our future research work.

7. CONCLUSIONS

In this thesis we first discussed the motivations and requirements behind the development of the new Sub-1 GHz WiFi standard namely the IEEE 802.11ah. We then presented an overview of the recent MAC and PHY features enabled by the new specification. We presented an analytical model for the saturation throughput of RAW mechanism, an important and promising feature of the new standard. We conducted performance analysis of the various novel features of IEEE 802.11ah by means of extensive system level simulations. We also validated our simulations model against our own analytical model as well as another accurate analytical model based partly on mean value analysis. Specifically, we focused on the performance evaluation of the new enhancement schemes of IEEE 802.11ah networks in a practical case of OBSS deployment with high number of associated stations (STAs). This included studying features such as frame shortening, sub channel selective transmission, RAW, group sectorization and TXOP based sectorization and identifying parameters in each of these cases that can be tuned to achieve optimal performance. The reported extensive simulation results clearly demonstrate the importance of these mechanisms in order to substantially improve the system throughput as well as the system and device-level energy efficiency in the emerging M2M and IoT applications.

We also presented and evaluated the performance of novel holding schemes for the IEEE 802.11ah RAW mechanism in the non-cross slot boundary case. The findings in our work provide new insight into the suitability of these schemes with respect to the spatial distribution of nodes around the AP. We proposed two new holding schemes (VARIABLE and HYBRID) and based on that a new grouping scheme (BIN) for RAW mechanism as well. We found out through extensive system level simulations that the proposed schemes perform better than the existing schemes mentioned in the literature.

We also investigated the effects of the duty cycle limitation on the devices operating in the sub-1 GHz ISM bands in an IEEE 802.11ah network. We presented the theoretical maximum duty cycle achievable in an IEEE 802.11ah network considering saturated uplink traffic. We then studied the effects of the imposed limitation of 2.8% duty cycle on network throughput using both the saturated and unsaturated traffic by means of extensive system level simulations. We presented a quantitative measure of the reduction in network throughput performance when various levels of duty cycle limitations are imposed in a network with saturated traffic. We also identified the practical use cases of IEEE 802.11ah network deployment where the duty cycle limit does not appear to be a bottleneck when only uplink traffic is considered. We found that in all of the use cases, at least up to 500 stations can be supported with a 2.8% duty cycle limit without any major degradation in the throughput. However, in the presence of downlink traffic and more frequent beacon transmissions, the duty cycle limitation may severely limit the network performance.

Overall, the findings in this thesis strengthen the understanding and prospects of IEEE 802.11ah as one key enabling technology towards the IoT-centric era and future society with massive amounts of embedded connected devices. These finding also outline the potential challenges in the deployment of the standard and how the new features of the standard can be tuned to overcome these challenges.

BIBLIOGRAPHY

[1] A. Research, "The internet of things will drive wireless connected devices to 40.9 billion in 2020," https://www.abiresearch.com/press/the-internet-of-things-will-drive-wireless-connect, accessed: 2015-02-10.

[2] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," *Internet of Things Journal, IEEE*, vol. 1, no. 1, pp. 22–32, 2014.

[3] T. Adame, A. Bel, B. Bellalta, J. Barcelo, and M. Oliver, "IEEE 802.11ah: the WiFi approach for M2M communications," *Wireless Communications, IEEE*, vol. 21, no. 6, pp. 144–152, 2014.

[4] K. Ashton, "That 'internet of things' thing," http://www.rfidjournal.com/articles/view?4986, Jun. 2009.

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

[6] International Telecommunications Union, ITU Internet Reports 2005, *The Internet of Things. Executive Summary.* Geneva: ITU, 2005.

[7] C. Inc., "Seize new iot opportunities with the cisco iot system," http://www.cisco.com/web/solutions/trends/iot/portfolio.html, Aug. 2015.

[8] ZigBee Alliance, http://www.zigbee.org/en/index.as.

[9] N. Kushalnagar, G. Montenegro, and C. Schumacher, *IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions.* IETF RFC 4919, Aug. 2007.

[10] R. Morrow, *Bluetooth: Operation and Use.* New York: McGraw-Hill, 2002.

[11] "IEEE Draft Standard for Information Technology - Local and Metropolitan Area Networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment-Sub 1 GHz License-Exempt Operation,," *IEEE P802.11ah/D4.0, January 2015*, January 2015.

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

[13] M. Cheong, "Tgah functional requirements and evaluation methodology," IEEE 802.11-11/0905r5, Jan. 2012.

[14] A. Hazmi, J. Rinne, and M. Valkama, "Feasibility study of IEEE 802.11ah radio technology for IoT and M2M use cases," in *Globecom Workshops (GC Wkshps), 2012 IEEE*, Dec. 2012, pp. 1687–1692.

[15] O. Raeesi, J. Pirskanen, A. Hazmi, T. Levanen, and M. Valkama, "Performance evaluation of IEEE 802.11 ah and its restricted access window mechanism," in *Communications Workshops (ICC), 2014 IEEE International Conference on.* IEEE, 2014, pp. 460–466.

[16] B. B. Olyaei, J. Pirskanen, O. Raeesi, A. Hazmi, and M. Valkama, "Performance comparison between slotted IEEE 802.15.4 and IEEE 802.11ah in IoT based applications," in *Wireless and Mobile Computing, Networking and Communications (WiMob), 2013 IEEE 9th International Conference on.* IEEE, 2013, pp. 332–337.

[17] L. Zheng, M. Ni, L. Cai, J. Pan, C. Ghosh, and K. Doppler, "Performance analysis of group-synchronized dcf for dense IEEE 802.11 networks," *Wireless Communications, IEEE Transactions on*, vol. 13, no. 11, pp. 6180–6192, 2014.

[18] Y. Zhou, H. Wang, S. Zheng, and Z. Lei, "Advances in IEEE 802.11ah standardization for machine-type communications in sub-1GHz WLAN," in *Communications Workshops (ICC), 2013 IEEE International Conference on*, June 2013, pp. 1269–1273.

[19] W. Sun, M. Choi, and S. Choi, "Ieee 802.11 ah: A long range 802.11 wlan at sub 1 ghz," *Journal of ICT Standardization*, vol. 1, no. 1, pp. 83–108, 2013.

[20] S. Aust, R. V. Prasad, and I. G. Niemegeers, "IEEE 802.11 ah: Advantages in standards and further challenges for sub 1 GHz Wi-Fi," in *Communications (ICC), 2012 IEEE International Conference on.* IEEE, 2012, pp. 6885–6889.

[21] T. Adame, A. Bel, B. Bellalta, J. Barceló, J. Gonzalez, and M. Oliver, "Capacity analysis of IEEE 802.11 ah WLANs for M2M communications," in *Multiple Access Communcations.* Springer, 2013, pp. 139–155.

[22] "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)*, pp. 1–2793, March 2012.

[23] M. Park, "IEEE P802. 11 Wireless LANs Specification Framework for TGah Rev. 15," *TGah Spec Framework, doc.: IEEE 802.11-11/1137r6*, 2014.

[24] D. Halasz, "Sub 1 GHz license-exempt par and 5c," IEEE 802.11-10/0001r13, July 2010.

[25] R. Porat, S. Young, and K. Doppler, "IEEE P802. 11 Wireless LANs, TGah Channel Model Proposed Text," DCN 11-11-0968-03-00ah-channel-model-text, Tech. Rep., 2011.

[26] E. Khorov, A. Lyakhov, A. Krotov, and A. Guschin, "A survey on ieee 802.11 ah: An enabling networking technology for smart cities," *Computer Communications*, vol. 58, pp. 53–69, 2015.

[27] M. Heusse, F. Rousseau, G. Berger-Sabbatel, and A. Duda, "Performance anomaly of 802.11b," in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, vol. 2, March 2003, pp. 836–843.

[28] W. Ye, J. Heidemann, and D. Estrin, "An energy-efficient MAC protocol for wireless sensor networks," in *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, vol. 3. IEEE, 2002, pp. 1567–1576.

[29] M. Qutab-ud din, A. Hazmi, B. Badihi, A. Larmo, J. Torsner, and M. Valkama, "Performance analysis of iot-enabling ieee 802.11ah technology and its raw mechanism with non-cross slot boundary holding schemes," in *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2015 IEEE 16th International Symposium on a*, June 2015, pp. 1–6.

[30] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," *Selected Areas in Communications, IEEE Journal on*, vol. 18, no. 3, pp. 535–547, 2000.

[31] J. Robinson and T. Randhawa, "Saturation throughput analysis of ieee 802.11e enhanced distributed coordination function," *Selected Areas in Communications, IEEE Journal on*, vol. 22, no. 5, pp. 917–928, June 2004.

[32] C. Hu, H. Kim, J. C. Hou, D. Chi, and S. S. Nandagopalan, "Provisioning quality controlled medium access in ultrawideband-operated WPANs," in *Proceedings IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications*, 2006.

[33] Y. Tay and K. C. Chua, "A capacity analysis for the IEEE 802.11 MAC protocol," *Wireless networks*, vol. 7, no. 2, pp. 159–171, 2001.

[34] L. X. Cai, X. Shen, J. W. Mark, L. Cai, and Y. Xiao, "Voice capacity analysis of WLAN with unbalanced traffic," *Vehicular Technology, IEEE Transactions on*, vol. 55, no. 3, pp. 752–761, 2006.

[35] R. Zhang, L. Cai, and J. Pan, "Performance analysis of reservation and contention-based hybrid MAC for wireless networks," in *Communications (ICC), 2010 IEEE International Conference on.* IEEE, 2010, pp. 1–5.

[36] R. Jain, A. Durresi, and G. Babic, "Throughput fairness index: An explanation," Tech. rep., Department of CIS, The Ohio State University, Tech. Rep., 1999.

[37] ETSI, "Technical characteristics and spectrum requirements of wideband SRDs with advanced spectrum sharing capability for operation in the UHF 870 - 876 MHz and 915 - 921 MHz frequency bands," Tech. Rep., *ETSI TR 103 245 V1.1.1*, Nov. 2014.

[38] M. Park, E. Perahia, and E. Qi, "TGah Use Cases Summary and Aggregated PHY Rates Analysis," IEEE 802.11-11/0299r0, Mar. 2011.

[39] S. Arnon, D. Bhastekar, D. Kedar, and A. Tauber, "A comparative study of wireless communication network configurations for medical applications," *Wireless Communications, IEEE*, vol. 10, no. 1, pp. 56–61, 2003.