Contributions to the evolution of next generation WLANs

Muhammad Shahwaiz Afaqui

Directors:
Dr. Eduard Garcia-Villegas and Dr. Elena Lopez-Aguilera

Wireless Networks Group, Department of Network Engineering

Universitat Politechnica de Catalunya (UPC)
Barcelona-Spain

shahwaiz.afaqui@entel.upc.edu

March 2017

This thesis is dedicate to the loving memory of my mother, Fehmida Iqbal (1956-2016).
There is not a single day that goes by when I don't miss you.

Abstract

The explosive growth in usage of IEEE 802.11 based WLAN networks has resulted in dense deployments in diverse environments and has made the concept of anytime - anywhere data connectivity a realm of commercial reality. The IEEE 802.11 standard (that was initially designed to target small office/home office) has evolved as a key enabling technology to cover medium to large scale enterprises, public area hots spots, apartment complexes etc. Such environments are characterized to encompass multiple small cells with many access points and serve large numbers of stations (refereed to as clients). Improved coverage and higher data rates are the primary achievements, where many cells coexist to create an environment containing multiple Overlapping Basic Service Sets. This small cell deployment is also considered as a key component of the next generation wireless communication to provide greater end user experience.

Adjacent access points can choose different frequency bands (if available) for operations in order to avoid interference for the client stations placed at the cell edge. However, the interference created by overlapping cells using similar frequency can adversely result in reduced performance. Moreover, the overly protected contention-based medium access mechanism of IEEE 802.11 also limits the possibility of concurrent transmissions. The increased number of access points deployed in complex untrusted network environments can also induce network management challenges that incorporate inconsistent security.

The work presented in this thesis originates from the need to understand some of the key challenges affecting legacy IEEE 802.11 protocols under high density scenarios and to design mechanisms that improve network performance within overlapping cells. Through our work, we have contributed to the evolution of IEEE 802.11 standard by demonstrating network enhancements in three important dimensions: availability, capacity and interference management. Throughout the thesis, methods are proposed that require minimum modifications to be made over the exiting IEEE 802.11 protocols. Yet, with the help of extensive evaluation, the proposed schemes have shown considerable performance improvements.

The contributions made in this thesis significantly advance the state-of-the-art for IEEE 802.11 WLANs along the lines of the aforementioned three dimensions. In order to better understand the security threat that a jammer entails, first this thesis demonstrates the impact of a jammer on IEEE 802.11 and proposes a novel malicious entity detection

scheme, called Beacon Access Time, that is required before taking appropriate countermeasures to improve the availability of IEEE 802.11.

Next, a new IEEE 802.11 standard called IEEE 802.11ah, is evaluated as an alternative to densely deployed overlapping Wi-Fi cells. This amendment aims to improve on legacy IEEE 802.11 by enhancing the coverage as well as supporting increased number of associated stations. Also, recent technological additions to IEEE 802.11 standard with the intent to improve operations within high density environments, in the form of future IEEE 802.11ax amendment, are also explored.

To enhance network capacity, a technique named Dynamic Sensitivity Control, is introduced which dynamically adapts carrier sensing and improves the area throughput within dense WLAN deployments by limiting the impact of increased interference (by increasing the spatial reuse). Detailed simulation results indicate that this scheme allowed multiple concurrent transmissions to coexist and, thus, increases the overall network throughput and fairness over the cost of rise in frame error.

Finally, an access point controlled four-way handshake mechanism is proposed that can improve and enhance the performance of dense deployments by reducing interference and frame error rate.

Different contributions proposed throughout this thesis provide solutions for amicable operations of densely deployed Wi-Fi cells. The importance of the work presented in this thesis is also validated through our contributions to the IEEE 802.11ax task group.

Acknowledgements

First and foremost, I would like to thank Almighty God for providing me this opportunity and bestowing upon me the strength, knowledge, and ability to accomplish this milestone.

This thesis is an outcome of my long and valuable professional journey at BarcelonaTech and its completion can be compared to a tedious mountain climb filled with numerous unforeseen difficulties which required endurance and tenacity to reach the summit. This work would not have been possible without the advice and support of many people, both from the academic environment and outside, whom I shared the best and the worst moments. I would like to acknowledge my appreciation and offer sincere thanks to these people whom I am deeply indebted.

I would like to express my heartfelt gratitude to my advisors, Dr. Eduard Garcia-Villegas and Dr. Elena Lopez-Aguilera, who have been extremely kind, helpful, enthusiastic, motivating and patient during the rough road to finish this thesis. Their guidance has been invaluable not only in terms of the research development, but even so in my personal development as a researcher and a professional. Their timely and valuable feedback to the research articles always resulted in improved versions of scientific documents. They always tried to get the best out of me by encouraging to achieve higher standards and provided constructive critics and comments in every stage of the thesis. I am very proud to have them as my thesis supervisors.

I greatly acknowledge the esteemed Professor Josep Paradells for providing me the opportunity to work in the RescueCell project. Even though, the work done in RescueCell project is not added as a part of my thesis, it helped to polish my research abilities. I would also like to take this opportunity to thank my colleagues at the Wireless Network Group.

I would like to thank my family to whom I owe a great deal. They have always been there for me in every step and helped me to remain focused on my goal. To my late mother, who always taught me to be a better man. To my wonderful father, Professor M. Iqbal Afaqui, who has been a constant source of inspiration and always encouraged me to be curious about things. His continuous struggle to give us the best home and education is very much appreciated. To my dear sister (Ayesha) and brothers (Naokhaiz, Dilawaiz and Ahmad) who enriched my life with their love, and friendship, and helped

me to accept the sad things that happen in life. Thank you all for your understanding and encouragement in many ways.

Finally, I would like to thank my wife, Amna Qureshi. She was always there to cheer me up and stood by me through the thick and thin. Her unwavering love, encouragement and editorial support was undeniably the bedrock upon which my Ph.D. journey has been built on.

Contents

List of Figures

List of Tables

List of Abbreviations

3GPP 3rd Generation Partnership Project.

5G Fifth Generation.

AC Access Categories.

ACK Acknowledgment.

AFA Adaptive Frequency Agility.

AID Association ID.

AIFSN Arbitration Inter-Frame Space Number.

AP Access Point.

ARQ Automatic Repeat Request.

BAT Beacon Access Time.

BCC Binary Convolutional Coding.

BDT Bi-directional TXOP.

BI Beacon Interval.

BSS Basic Service Set.

BSSID Basic SSID.

BYOD Buy Your Own Device.

CCK Complementary Code Keying.

CCMP Counter Mode CBC MAC Protocol.

CFP Contention Free Period.

CP Contention Period.

CRC Cyclic Redundancy Check.

CS Carrier Sense.

CSAT Carrier-Sensing Adaptive Transmission.

CSD Criteria for Standard Development.

CSI Channel State Information.

CSMA/CA Carrier Sense Multiple Access with Collision Avoidance.

CST Carrier Sense Threshold.

CSTI CS Time.

CTS Clear To Send.

CW Contention Window.

DCF Distributed Coordination Function.

DIFS DCF Inter-frame Space.

DL MU-MIMO Downlink Multi-User MIMO.

DoS Denial of Service.

DS Distribution System.

DSC Dynamic Sensitivity Control.

DSRC Dedicated Short Range Communication.

DSSS Direct Sequence Spread Spectrum.

DTIM Delivery TIM.

DVB Digital Video Broadcasting.

EC-GSM Extended coverage GSM.

EDCA Enhanced Distributed Channel Access.

EDCF enhanced DCF.

EMO European Mobile Observatory.

ERC European Radio Communications Committee.

ERP Extended Rate PHY.

ETSI European Telecommunications Standards Institute.

FBE Frame Based Equipment.

FC Frame Control.

FCC Federal Communications Commission.

FEC Forward Error Correction.

FER Frame Error Rate.

FFT Fast Fourier Transform.

FHSS Frequency Hopping Spread Spectrum.

FSS Frequency Selective Scheduling.

GDP Gross Domestic Product.

GI Guard Interval.

HC Hybrid Coordinator.

HCCA HCF Controlled Channel Access.

HCF Hybrid Coordination Function.

HE-PPDU High Efficiency PLCP Protocol Data Unit.

HetNet Heterogeneous Network.

HEW High Efficiency WLAN.

HSPA High Speed Packet Access.

HT High Throughput.

IE Information Element.

IEEE Institute of Electrical and Electronics Engineers.

IFFT Inverse Fast Fourier Transform.

IoT Internet-of-Things.

IR Infrared.

ISM Industrial, Scientific and Medical.

ITS Intelligent Transport System.

L-SIG Legacy Signal.

LAA-LTE License Assisted Access.

LBE Load Based Equipment.

LBT Listen Before Talk.

LDPC Low Density Parity Check.

LLC Logical Link Control.

LPWA Low Power Wide Area Network.

LRLP Long Range Low Power.

LSQ Least Squares.

LTE Long Term Evolution.

LWA LTE Wi-Fi Link Aggregation.

M2M Machine-to-Machine.

MAC Medium Access Control.

MCS Modulation and Coding Schemes.

MIMO Multiple Input Multiple Output.

mmWave Millimeter Wave.

MPDUs MAC Protocol Data Units.

MPTCP Multi-Path TCP.

MSDU MAC Service Data Unit.

MU-MIMO Multi-User MIMO.

Multi-RAT Multiple Radio Access Technologies.

NAV Networks Allocation Vector.

NB-IoT NarrowBand IoT.

NDP Null Data Packets.

NORTSDSC RTS/CTS disabled DSC nodes.

OBSS Overlapping BSS.

OBSS PD OBSS Preamble Detection.

OFDM Orthogonal Frequency Division Multiplexing.

OFDMA Orthogonal Frequency Division Multiple Access.

OSI Open Systems Interconnection.

OT Occupation Time.

PAR Project Authorization Request.

PCF Point Coordination Function.

PCS Physical Carrier Sensing.

PDR Packet Delivery Ratio.

PHY Physical.

PHYCCA Physical Clear Channel Assessment.

PHYED Physical Energy Detection.

PHYPD Physical Preamble Detection.

PIFS Point Interframe Space.

PLCP Physical Layer Convergence Procedure.

PPDU PLCP Protocol Data Unit.

Pre-RSNA Pre-Robust Network Association.

PS Power Saving.

PS-Poll Power Save-Polling.

PSR Packet Sent Ratio.

QMF Quality Management Frames.

QoE Quality of Experience.

QoS Quality of Services.

RA Resource Allocation.

RAA Rate Adaptation Algorithm.

RAW Restricted Access Window.

RD Reverse Direction.

RDG Reverse Direction Grant.

RF Radio Frequency.

RID Response Indication Deferral.

RIFS Reduced Interframe Space.

RPS Raw Parameter Set.

RRM Radio Resource Management.

RSNA Robust Network Association.

RSS Received Signal Strength.

RSSI Received Signal Strength Indication.

RT RTS Threshold.

RTS Request To Send.

RTSDSC RTS/CTS enabled DSC nodes.

RU Resource Unit.

RXVector Receiver Vector.

S1G Sub 1 GHz.

SIFS Short Interframe Space.

SIG Signal.

SINR Signal to Interference plus Noise Ratio.

SISO Single Input Single Output.

SOHO Small Office/Home Office.

SPF Speed Frame Exchange.

SS Spatial Stream.

SSID Service Set Identifier.

SST Sub-Channel Selective Transmission.

ST Silence Time.

STA Station.

STBC Space-Time Block Coding.

SU Single User.

TBTT Target Beacon Transmission Times.

TDMA Time Division Multiple Access.

TGax Task Group AX.

TID Traffic Identifier.

TIM Traffic Indication Map.

TMF Time Management Frames.

TPC Transmit Power Control.

TSF Timing Synchronization Function.

TVWS TV White Spaces.

TWT Target Wake Time.

TXOP Transmission Opportunity.

U-NII National Information Infrastructure.

UDP User Datagram Protocol.

UMTS Universal Mobile Telecommunications System.

UPC Universitat Politecnica de Catalunya.

VCS Virtual Carrier Sense.

VoIP Voice over IP.

WAVE Wireless Access in Vehicular Environments.

WEP Wired Equivalent Privacy.

Wi-Fi Wireless Fidelity.

WIMAX Worldwide Interoperability for Microwave Access.

WLAN Wireless Local Area Network.

WNM Wireless Network Management.

WUR Wake Up Radio.

1

Introduction

1.1 Background

We live in the age of data, where the physical world surrounding us has transformed into raw data and information is digitally captured (at data sources) and transfered via point-to-point or point to multi-point digital communication networks. Network interfaces (i.e. a software interface to allow networking over hardware) have changed our perception about the world and societies to an extent that it is hard to visualize interactions that are not network oriented. Entire communities are being connected, so that people have the opportunity to participate in society with the exchange of data.

Wireless communication (that commonly use radio waves to transfer information between two or more points that are not connected by an electrical conductor) is by far the fastest growing segment of digital communications due to reduced cost in data delivery, ability to provide connectivity virtually anywhere and fast access to remote information. These digital communication networks, due to diverse benefits, are being employed in different sectors of the society, such as, residential, enterprise, transportation, health care, manufacturing industry, agriculture and so on. Decades of exponential growth in commercial wireless data services and data pouring from anywhere, anytime and any device has lead to the so-called *"big data"* era, where wireless networks are the critical contributors.

According to Cisco [26], the global mobile data traffic was 7.2 Exabytes (where one Exabyte is equivalent to one billion Gigabytes) per month at the end of 2016, up from 4.4 Exabytes per month at the end of 2015. Also, Cisco predicts that by 2021, there will be 11.6 billion mobile-connected devices, that would far exceed the world's projected population in 2021 (i.e. 7.8 billion). Moreover, massive investments in technology and interoperability by the telecommunication industry has underpinned the capital flows in the global economy. This is reflected by European Mobile Observatory (EMO) report [39] that highlights the fact that global economic footprint of the wireless mobile sector is €3.1 Trillion in the year 2015, that is 4.1% of global Gross Domestic Product (GDP), bypassing the aviation industry which is 3.5% of global GDP.

The surge in mobile data traffic is mainly attributed to the popularity of mobiles, laptops, tablets and other devices (that support broadband applications) which enable ubiquitous access to the Internet. Moreover, the explosion in wireless traffic is also driven by plethora of new applications (e.g. social networking, machine-to-machine communications, video conferencing and streaming). Wireless technologies have become a model of communication, entertainment and education. From music to video streaming, through email to social media, to controlling home appliances from anywhere, wireless technologies have bought numerous benefits and have revolutionized the life style of people.

Nowadays, the demand for higher data rates in wireless networks is unrelenting that has triggered existing wireless communication technologies to expand their capacities and capabilities to provide anywhere anytime connectivity. In addition, the need for improved data rates, decreased latency and better Quality of Services (QoS) has also resulted in the design and development of new wireless standards aimed to provide connectivity in versatile environments. As exemplified by Martin Cooper, the pioneer of cellular communication and visionary of wireless industry, the capacity of wireless networks has doubled every 30 months for the past 40 years to cater the demand of users and can be attributed to: a) Design of better modulation schemes; b) Improvement in using wider spectrum; c) Greatest of all increase due to link efficiency caused by reduced transmit distances and smaller cell sizes. These attributes are still valid today, where enormous gains have been achieved from smaller cell size and enhanced spatial reuse due to higher spectral efficiency.

Different wireless standards, such as Long Term Evolution (LTE), IEEE 802.11 based Wireless Fidelity Wireless Fidelity (Wi-Fi), IEEE 802.16 based Worldwide Interoperability for Microwave Access (WIMAX), High Speed Packet Access (HSPA), Universal Mobile Telecommunications System (UMTS) and so on, have been proposed to improve the usability and performance of mobile communications. In these wireless networks, the challenge to meet the throughput and processing requirements for billions of connected devices is addressed by providing more resources such as spectrum, baseband processor and transmitters. With the advent of Internet-of-Things (IoT), a paradigm which will allow real-time interactions between smart/legacy things (such as actuators and sensors) and mobile clients via wireless networks, it is expected that 28 billion IoT devices will become online by the year 2021 [34]. The resulting demand of wireless connectivity to the added massive IoT devices along with traditional mobile stations will place added strain over exiting network technologies (which, currently are operating over maximum limits). As highlighted by Nokia [27], new wireless network innovations are required as the current mobile and Wi-Fi networks are not growing quickly to meet the increased demand of the capacity.

In recent years, remarkable progress in link layer performance has been witnessed, where different wireless standards utilize efficient modulation schemes and multiple antenna array. However, sustaining the link layer performance is increasingly becoming difficult due to small form factor of mobile devices and the restriction in performing complex operations due to power constraints. Providing reliable wireless communication to massive number of stations is not a small task. Different factors, such as mobility, interference, power consumption, performance consistency, scarcity of

available channel and security affect the system level performance of wireless networks. Transmissions over channels shared by different technologies also interfere with each other and challenge the network capacity. To make the situation worse, maintaining connectivity over wireless channel it self posses problems of path loss due to fading and obstruction. Therefore, current wireless networks are not capable of sustaining future demands of high traffic volumes.

In order to counter the above mentioned issues, new innovative techniques are required to meet the requirements of future wireless networks. Methods to expand network capacity could be achieved by the combined usage of availability of new spectral resources, intense spectrum reuse and methods to increase capacity over each MHz of used spectrum. While the availability of spectral resources appears the most simple solution, it is an expensive alternative. Improved spectrum reuse results in more cells being deployed that increase the spatial efficiency by making more resources available. The spectral efficiency could be achieved by adapting more complex methods, such as beamforming, Multiple Input Multiple Output (MIMO) and channel aware scheduling. To summarize, new mechanisms that employ cross layer optimization techniques can be useful to enhance the performance of future wireless networks.

Another important strategy to cope with the future traffic demands is the development of heterogeneous access networks, where different type of radio access networks could be used together (as shown in Figure 1.1). Consequently, the next generation wireless standard, called Fifth Generation (5G), is being designed to encompass Heterogeneous Network (HetNet) architecture consisting of a single holistic network with Multiple Radio Access Technologies (Multi-RAT). Multiple connectivity protocols and spectrum would be managed from a common core (management system) where, traditional macro-cellular systems (such as LTE etc.) that can provide long range could be used for outdoor coverage, whereas low power wireless systems with high capacity (such as Wi-Fi) can be deployed to cater indoor traffic needs. 5G HetNet is expected to achieve ubiquitous connectivity that would guarantee QoS, Quality of Experience (QoE) along with efficient use of spectrum and energy with low cost.

The fundamental need for wireless communication is the Radio Frequency (RF) spectrum. Mobile networks operate over licensed spectrum and typically pay huge amount to government regulatory bodies for exclusive use. However, even a license does not guarantee interference-free operation due to the co-existence of mobile operators on similar or neighboring RF bands. Meanwhile, Wi-Fi takes advantage of un-licensed spectrum, that is the main reason for the cost benefits. However, in order to operate over un-licensed band, it is obligatory for the Wi-Fi technologies to follow the regulations set by governments. Therefore, in HetNets, both licensed and unlicensed band equipment can be made to operate cooperatively so as to serve the wide variety of wireless applications based on the different environmental needs. A station can be served by both licensed and unlicensed subsystems, where the throughput of the systems can be the sum of the licensed and unlicensed subsystem throughput.

Since major part of the traffic is generated and consumed indoor (50% of voice calls and 70% of data traffic originates from indoor [24]), the indoor connectivity solutions could be instrumental

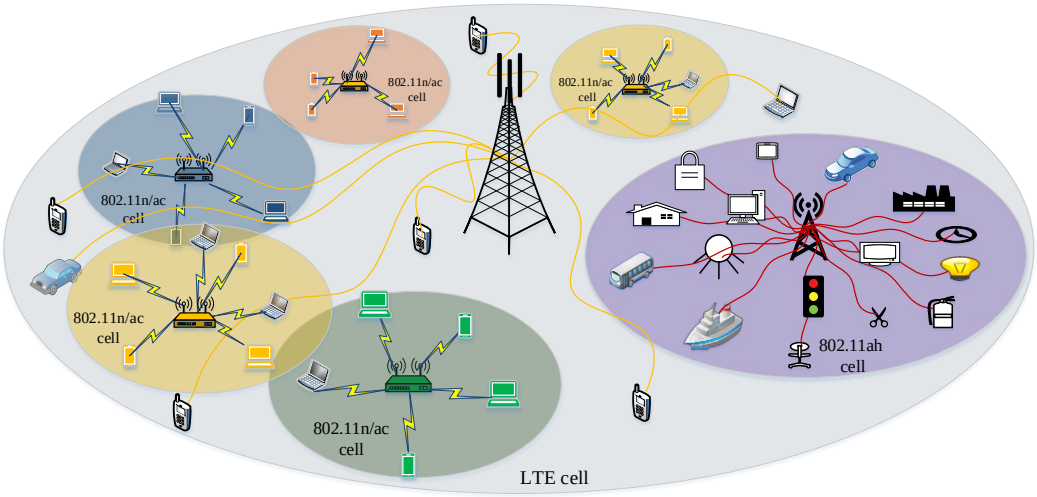


Figure 1.1: Wi-Fi and LTE heterogeneous network.

in addressing the capacity requirements for 5G. It is envisioned that the use of Wi-Fi (which is the dominant technology in sub-6 GHz unlicensed band) in conjunction with cellular networks would provide significant improvement in network capacity and coverage.

IEEE 802.11 based WLANs, that are the most successful indoor wireless solutions and were initially designed to target Small Office/Home Office (SOHO), have evolved as a key enabling technology to cover medium to large scale enterprise, public area hot-spots and apartment complexes etc. Such environments are characterized to include multiple small cells with many Access Points (APs) and serve large number of stations (referred to as clients), where increase in coverage and high data rates are the primary achievements. The IEEE 802.11 has defined series of standards that are providing increasingly higher data rates at each generations.

The popularity of Wireless Local Area Network (WLAN) has increased significantly in recent years because of their ability to provide increased mobility, flexibility, ease of use along with reduced cost of setting up and maintenance. Following facts about the number of WLAN chipset shipped in recent years clearly indicate the popularity of IEEE based WLAN networks; 1.5 billion WLAN chipset were shipped in 2012 [21], whereas 2.6 billion chipsets were expected to be shipped during 2014 [75]. This trend is expected to continue in the following years where 18 billions more chips are expected to be shipped between 2015 and 2018 [75].

Despite the benefits, communication performance of current Wi-Fi networks are hindered by the density of stations, capacity demands, simple security features and lower coverage. This is due to the fact that Wi-Fi operates on Industrial, Scientific and Medical (ISM) 2.4 GHz and National Information Infrastructure (U-NII) 5 GHz band that include fewer number of non-overlapping channels. Besides, this unlicensed spectrum is also shared with other wireless technologies (such as Bluetooth, Zigbee etc.). Due to the requirements of continuous coverage and the rapid increase in associated stations, WLAN access points now span floors and buildings and are configured to operate over similar bands due to scarcity of available channels. Thus, the current Wi-Fi deployments can not fulfill the higher

throughputs and better quality of experience expected by different multimedia applications. To reduce the impact of interference problem, the coverage area of WLAN Basic Service Set (BSS) [1] is reduced (by decreasing transmit power) that results in decreased range. Also, due to contention-based nature of Medium Access Control (MAC) layer, IEEE 802.11 network faces interference problems. Despite the increase in available bandwidth and multiple antennas (at the AP as well as the stations), the inefficient sharing of spatial resources by the MAC layer results in reduced transmission opportunities by the stations. The widespread deployment of IEEE 802.11 and their operations over the unlicensed bands has made then an attractive target for potential attackers. Legacy IEEE 802.11 standard has introduced protocols to improve encryption and authentication. However, most of the security features primarily address the confidentiality and access control. The issue of improving network availability in the presence of misbehaving stations has not been included in IEEE 802.11 standard.

In this thesis, we explore the key performance challenges associated with future IEEE 802.11 networks. Through our work, we have contributed to the evolution of IEEE 802.11 standard by introducing a mechanism to detect malicious entities within Wi-Fi networks, by proposing to utilize a new Wi-Fi amendment (called IEEE 802.11ah) as an alternative to dense deployments and by designing a new adaptation technique for the upcoming Wi-Fi standard for dense deployments (called IEEE 802.11ax) which allows more concurrent transmission to geographically co-exist (that result in increased throughput). The problems highlighted in this thesis are not new. However, the proposed features will allow IEEE 802.11 networks to augment the cellular networks in fulfilling the expectations in supporting massive traffic demand of future wireless networks .

1.2 Evolution of IEEE 802.11 standard

The Institute of Electrical and Electronics Engineers (IEEE) has been actively involved in the standardization of electrical equipment designed for digital communications. For each standardization process, the IEEE creates a project that is assigned a number. In 1989, the IEEE created a project called IEEE 802.11 for the adaptation of single worldwide accepted wireless standard. Motivated by the emergence of Internet connections (such as DSL and cable models) and the availability of regulation free transmission bands, the IEEE 802.11 aimed to design a standard that would allow the delivery of data to computers through high speed wireless connections. In order to certify the interoperability of WLAN products with IEEE 802.11, a non-profit organization (called Wi-Fi alliance) was created in 1999. It is a combination of standardization, testing and trade organizations.

Recent years have witnessed a major surge in WLAN deployment in geographically-limited environments that encompass multiple Overlapping BSS (OBSS) due to the popularity of IEEE 802.11-based WLANs. The IEEE 802.11 standardization committee has actively continued to release new draft amendments to incorporate latest technological advances. These forgoing additions are made to defy practical challenges faced due to massive Wi-Fi deployments in heterogeneous environ-

[1] A BSS is the area or cell that an WLAN AP covers and all non-AP stations communicate in centralized manner to the AP.

ments. As compared to the cellular technologies, IEEE 802.11 standards/amendments are released to be backward compatible and, thus, pile atop of each other by adding and removing key technical aspects. However, the backward compatibility (despite of numerous benefits) incurs in multitude optimization challenges, because various devices in 802.11 networks are highly correlated and an issue in one area quickly ripples to other areas. The physical layer of IEEE 802.11 has greatly evolved within each amendment to accommodate new technologies, but the core functionality of its MAC layer (including carrier sensing, backoff time, protocol headers, ACK frames, various inter-frame shifts and so on) has remained same, where different temporal approaches (such as frame aggregation, block acknowledgment, backoff optimization, etc.) assist in reducing the required MAC operation time.

The IEEE 802.11 covered specification for lower layers of the Open Systems Interconnection (OSI) model, and specified the Physical (PHY) and the data link layer. The data link layer within IEEE 802.11 is further divided into two sub-layers: Logical Link Control (LLC) and MAC. In the following sections, we describe the history of IEEE 802.11 standard evolution with the help of various important IEEE 802.11 amendments proposed in the last two decades.

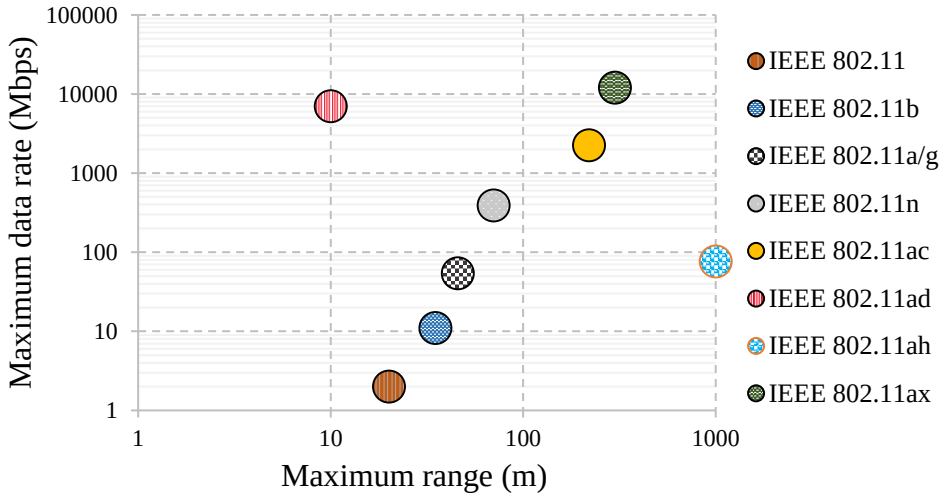


Figure 1.2: Evolution of IEEE 802.11 standard.

1.2.1 Legacy IEEE 802.11

After years of research, in 1997, the IEEE 802.11 adapted the original standard. This standard included forward error correction technique and specified three alternative physical layer technologies: Diffused Infrared (IR) operated at 1 Mbps, Frequency Hopping Spread Spectrum (FHSS) worked at 1 Mbps or 2 Mbps and Direct Sequence Spread Spectrum (DSSS) provided data rates of 1 Mbps and 2 Mbps. At the MAC layer, two protocols were defined: Distributed Coordination Function (DCF) and the Point Coordination Function (PCF). The DCF operated by using the well-known carrier sense paradigm, with an exponential backoff mechanism devised to ensure minimum probability of simultaneous transmission attempts by multiple stations. In other words, the critical features of DCF

were to support the operations over the shared unlicensed bands in the presence of interference. PCF provided a centralized contention-free channel access based on a polling mechanism. At the data link layer, different mechanisms were introduced: Authentication/Deauthentication, Association, disassociation and reassociation, Wired Equivalent Privacy (WEP) and basic power saving by reducing transmission overhead during Forward Error Correction (FEC)/Automatic Repeat Request (ARQ) and scheduling of multiple frame transmissions. The greatest drawback of this standard was the low data rate levels. The frequency band used by this amendment was 2.4 GHz.

1.2.2 IEEE 802.11a

The scope of this project was to allow high speed IEEE 802.11 operations over NII 5 GHz band. This amendment was ratified in July, 1999 and utilized Orthogonal Frequency Division Multiplexing (OFDM) to achieve data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps. These improved data rates were also achieved by utilizing greater number of non-overlapping channels at 5 GHz (i.e. 24 in Europe). However, due to channel conditions, the coverage of IEEE 802.11a was reduced that resulted in the increase of system deployment costs (due to the requirement of a large number of AP per unit area). This standard employed Single Input Single Output (SISO) systems.

1.2.3 IEEE 802.11b

This amendment was ratified along with IEEE 802.11a. However, due to its operation over 2.4 GHz, it received much more attention by the manufacturers. The scope of this project was to enhance legacy IEEE 802.11 to support higher data rates at 2.4 GHz. At the physical layer, this amendment only used DSSS and provided data rates of 1, 2, 5.5 and 11 Mbps while operating in SISO mode. New coding schemes where introduced, where Complementary Code Keying (CCK) was used to encode transmissions over 5.5 and 11 Mbps data rate. At the same time, IEEE 802.11b was backward compatible with legacy IEEE 802.11 at 1 and 2 Mbps transmissions.

1.2.4 IEEE 802.11g

The scope of this amendment was to develop a high speed physical layer extension of IEEE 802.11b amendment. Using this amendment, the IEEE 802.11 working group envisioned the convergence of IEEE 802.11a and IEEE 802.11b. Moreover, this standard was designed to be backward compatible with IEEE 802.11b. IEEE 802.11g was ratified in June 2003, and included CCK encoding and DSSS modulations along with OFDM operation. IEEE 802.11g introduced different features at physical and MAC layers: Extended Rate PHY (ERP), mandatory support of the short preamble type, protection mechanisms that deal with interoperability aspects

Although this amendment provided the highest data rate of 54 Mbps at the physical layer, the MAC layer throughput was far from the foregoing value (i.e. 40-50%). In return, the amendment was unable to support simultaneous and high quality video streaming for multiple stations. Also, the emergence of new use cases such as data sharing in house or offices, wireless printing and Internet

access in shops motivated the IEEE 802.11 working group to add new technological improvements to provide near gigabit type throughput over the WLANs.

1.2.5 IEEE 802.11i

The scope of this amendment was to enhance the security features within legacy IEEE 802.11 MAC. Ratified in June, 2004, IEEE 802.11i defined two classes of security algorithms: Robust Network Association (RSNA) and Pre-Robust Network Association (Pre-RSNA). IEEE 802.11i improved the confidentiality, integrity, and mutual authentication through these security classes. However, these methods did not resolve the availability issues of IEEE 802.11, where a station is unable to access the shared medium due to intentional or unintentional excessive channel occupancy by other competing stations.

1.2.6 IEEE 802.11e

In the legacy IEEE 802.11 standard, support of QoS was not envisaged. By rectifying the IEEE 802.11e amendment in June, 2005, the MAC layer of legacy IEEE 802.11 was enhanced with the inclusion of QoS support where differentiated classes of service were defined. A new MAC scheme, called Hybrid Coordination Function (HCF), was introduced, which was backward compatible with DCF and provided a built-in mechanism for supporting real-time services. HCF defined contention-based channel access mechanism, called Enhanced Distributed Channel Access (EDCA), which was an enhanced version of DCF with added features to provide prioritized QoS to different traffic types to multiple Access Categories (AC)s. Each traffic type was assigned different channel access parameters (that were fixed in legacy IEEE 802.11) within the MAC of each station. Each AC uses its own set of channel access parameters which control the access to the shared wireless medium. These parameters are: Arbitration Inter-Frame Space Number (AIFSN), minimum and maximum Contention Window (CW_{min} and CW_{max}), and the maximum length of a single Transmission Opportunity (TXOP).

The contention less part of HCA is called HCF Controlled Channel Access (HCCA), which provided QoS-enabled centralized polling based channel access to stations.

1.2.7 Standard specification: IEEE 802.11-2007

The IEEE 802.11 working group published the standard specifications, called IEEE 802.11-2007, that included all the revision of legacy IEEE 802.11 (in the form of amendments) until June 2007.

1.2.8 IEEE 802.11k

Published in June 2008, the IEEE 802.11k amendment aimed to improve the provision of data from the PHY and MAC layer (by defining a series of measurement requests and reports), which could assist the upper layers to perform different Radio Resource Management (RRM) mechanisms. The RRM features assisted stations to understand the RF environment in which they existed. IEEE

802.11k allowed key RRM measurement parameters to be exchanged between AP and stations so as to understand the network performance. IEEE 802.11k measurement reports include location information, detail of neighboring AP, channel load and noise histogram.

1.2.9 IEEE 802.11r

Ratified in June 2008, IEEE 802.11r extends the 802.11 base specification to support fast handoff (procedure that enables connection transition of Wi-Fi stations from one base station to a geographically adjacent base station due to movement) in the MAC protocol. It defined mechanism to allow fast security and QoS sensitive transitions between different IEEE 802.11 cells.

1.2.10 IEEE 802.11y

In order to allow IEEE 802.11a type operations over 3.65 to 3.7 GHz (lightly licensed spectrum), this amendment was published in June, 2008. This standard streamlined the adaptation of new spectrum in future for IEEE 802.11.

1.2.11 IEEE 802.11n

Through the IEEE 802.11n, IEEE 802.11 offers wireless higher data rates along with greater and reliable coverage than IEEE 802.11a/b/g networks. This standard was accepted in September 2009. One of the greatest advances in IEEE 802.11n was spatial multiplexing introduced through MIMO, which allowed multiple data streams to be transmitted simultaneously. IEEE 802.11n supported up to four times capacity increase by using up to four antennas. At the physical layer, MIMO was introduced to operate alongside OFDM, where MIMO operations induced robustness and range to weak links through spatial diversity. In addition, various channel bonding schemes were introduced to provide higher bandwidths to achieve increased transmission rates. At the MAC layer, frame aggregation was introduced with the addition of multiple protection schemes (designed to allow coexistence of IEEE 802.11n devices with IEEE 802.11 legacy stations). In frame aggregation, multiple data frames are combined into an aggregate frame that helps by reducing channel contention and backoff delays by transmitting aggregated frame with a transmission opportunity over the shared channel. This scheme, in return improves spectral efficiency.

1.2.12 IEEE 802.11p

This amendment defined a new mode of operation, called Wireless Access in Vehicular Environments (WAVE), that aims to support communication between fast moving vehicles. The maximum communication range envisaged was 1000m. This amendment includes the exchange of data between high speed vehicles and also vehicle to infrastructure in the licensed Intelligent Transport System (ITS) band of 5.9 GHz. At the physical layer, Dedicated Short Range Communication (DSRC)

was defined, that operated with 75 MHz bandwidth. At the MAC layer, EDCA is used with where parameters are set such that traffic of all the stations receive equal priority.

1.2.13 IEEE 802.11w

Ratified in June 2009, this amendment targeted to protect wireless connections and network-sensitive information exchanged within management frames. The mechanisms or protocols to protect management and action frames are very similar to the methods for data protection proposed in IEEE 802.11i.

1.2.14 IEEE 802.11v

The wireless management frames introduced by this amendment allowed network assisted power savings (i.e. a mechanism that restricts the use of power by batter driven devices) and network assisted roaming. This amendment also defined the Time Management Frames (TMF) to enable stations to discover, and adjust for, any of the additional MAC processing delays present in the hardware.

This standard was published in September 2011.

1.2.15 IEEE 802.11ad

This amendment, ratified to the IEEE 802.11 standard in December 2012, performed wireless communications over the Millimeter Wave (mmWave) band. By efficiently utilizing vast available spectral resources and directional medium usage, IEEE 802.11ad aimed to provide multi-Gbps over new application scenario for Wi-Fi. At the MAC layer, this amendment proposed a hybrid MAC approach, where a contention-based channel access, a time scheduled channel allocation and a dynamic channel time allocation schemes were proposed. The later two schemes were Time Division Multiple Access (TDMA) and polling based, respectively.

1.2.16 IEEE 802.11ac

IEEE 802.11ac provided increases data rate compared to 802.11n, which is achieved through the use of expanded channel bandwidth (by bonding across available channels) and higher-order modulation. A new optional technique, called Downlink Multi-User MIMO (DL MU-MIMO), was used that allowed multiple frames to be sent from the AP to multiple receivers simultaneously through multiple spatial streams (i.e. multi-user beamforming). The MAC layer modified the transmission of opportunity mechanisms that performed simultaneous multiple downlink streams for multiple receivers.

1.2.17 IEEE 802.11ae

The amendment described QoS mechanism (called Quality Management Frames (QMF)) for prioritization of management frames. Due to the in-band signaling of IEEE 802.11, this amendment aimed to define separate AC for management frames. This standard was ratified in December 2012.

1.2.18 Standard specification: IEEE 802.11-2012

The IEEE 802.11 working group published the standard specifications, called IEEE 802.11-2012, that included all the revision of legacy IEEE 802.11 (in the form of amendments) until June 2012.

1.2.19 IEEE 802.11af

IEEE 802.11af defined WLAN operations on TV White Spaces (TVWS). Due to favorable propagation conditions of TVWS band (i.e. 470–790 MHz in Europe), the coverage area of AP increased. The physical layer of IEEE 802.11af is similar to IEEE 802.11ac, with additional ability to support both contiguous and non-contiguous channel bonding of up to four channels. An additional guard band was added so as to protect transmission of TV users in adjacent channels. This standard was ratified in February 2014.

1.2.20 IEEE 802.11ah

This standard intended to modify the current IEEE 802.11 standard (at PHY and MAC layer) in order to extend it to operate below 1 GHz for ubiquitous access in less interfered frequency band and to support large number of associated stations within the network. Please refer to Chapter 3 for further information. This amendment was ratified in December 2016.

1.2.21 Standard specification: 802.11-2016

In December 2016, the IEEE standards Association rolled out new specifications for the fundamental IEEE 802.11 standard (called IEEE 802.11-2016). It included all the revision of legacy IEEE 802.11 (in the form of amendments) until December 2016, excluding IEEE 802.11ah.

1.2.22 IEEE 802.11ax

This future standard is currently being developed by the IEEE 802.11 working group, which will enable efficient usage of spectrum along with an enhanced user experience within dense interference limited environments. Please see Chapter 4 for more detail. It is expected that this amendment will be published in 2018.

1.2.23 IEEE 802.11ba

Through this amendment, the IEEE 802.11 working group wants to formally include Wake Up Radio (WUR) features in the standard specifications. The task group of IEEE 802.11ba started its work in July 2016 and the draft is expected to be accepted by 2019.

1.2.24 Other new emerging standards

IEEE 802.11ak[1] amendment is being designed to provide a new service discovery mechanism for WLAN and the external network. This amendment is expected to be published in March 2017.

IEEE 802.11aq is being designed to provide protocols that enhance the ability of IEEE 802.11 to operate as transit links within bridge networks (similar to Ethernet). This amendment is expected to be ratified on January 2018.

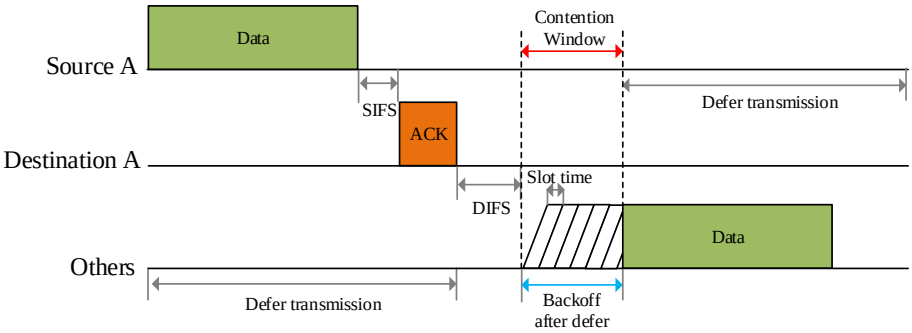
IEEE 802.11 working group is also working to address the needs of a station to identify its absolute and relative position to other station or stations (to which it can be associated) for better network management by introducing IEEE 802.11az. This amendment is expected to be ratified in March 2021.

1.3 Performance challenges for IEEE 802.11 networks

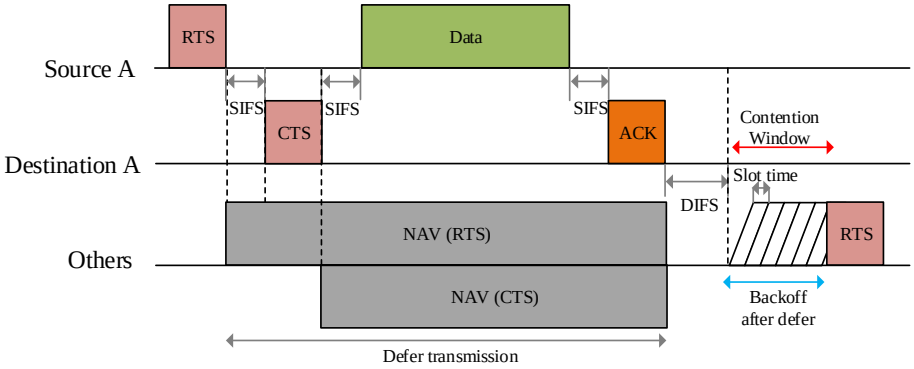
The IEEE 802.11 based WLANs have increasingly become popular means of Internet communication in homes offices and public places due to their ease of deployment and cost efficiency. The need for higher data rates and improved coverage has led to massive and uncoordinated deployments of WLAN AP in geographically-limited areas. As a consequence, an environment encompassing multiple OBSS is created, which is interference-limited and is also vulnerable to saboteurs who intend to disrupt its normal operation. In addition, a station can also decide to misbehave in order to gain certain measurable benefits (such as higher throughput, increased battery life, and so on). While IEEE 802.11 standards committee has introduced IEEE 802.11i amendment for security mechanisms at the network layer, the threats posed by denial-of-service attacks by malicious entity have not yet been fully explored. An intelligent malicious device can also exploit the MAC protocol and can create significant throughput reduction for other contending stations. In addition, due to over simplified MAC protocols, the high density deployments themselves create performance uncertainty related to provision of services when many devices co-exist in close proximity to gain access of shared resources.

Furthermore, since the Wi-Fi operates on ISM unlicensed radio bands of 2.4 GHz and 5 GHz, there are few number of available non-overlapping channels (i.e. 2.4 GHz encompasses just 3 or 4 and 5 GHz includes 24 with some restrictions applied, such as only indoor transmissions, implementation requirement of transmit power control or dynamic frequency selection) to be used in the

[1] Official IEEE 802.11 working group project time line- January 2017: Available at: http://www.ieee802.org/11/Reports/802.11_Timelines.htm



(a) Basic handshake based frame transmission.



(b) Four-way handshake based frame transmission.

Figure 1.3: Contention based MAC operations of IEEE 802.11.

design of high density deployments. The usage of 5 Ghz band was only initiated with IEEE 802.11a standard, where all the other standards were designed to operate on 2.4 GHz (i.e. IEEE 802.11b/g/n). Given the high density deployment of WLANs (operating under different settings and standards), the ubiquitous deployment of APs make coverage a mere design issue. However, due to the scarcity of available channels, spatial reuse via effective management of interference (particularly co-channel) becomes a prime challenge to enhance the overall network throughput.

In contrast to cellular mobile networks, such as Universal UMTS 3G and LTE 4G, the medium access method of IEEE 802.11 based Wi-Fi network is contention oriented. This is because IEEE 802.11 architecture was initially designed to replace the indoor local area network. Thus, it is not surprising that legacy IEEE 802.11 MAC reveals several performance impairments in complex scenarios.

The contention based MAC layer of IEEE 802.11 is a distributed access mechanism which utilizes Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) for physical carrier sensing. The physical carrier sensing method, called Physical Clear Channel Assessment (PHYCCA), is used to observe the channel conditions before transmission (e.g. if the energy level detected on the shared channel is greater than a predefined threshold, it means that the channel is occupied and, thus, the transmitter should abstain from transmission).

While accessing the channel, one of the two situations can occur:

- If the channel is sensed idle by the intended transmitter for more than DCF Inter-frame Space (DIFS), it initiates transmission.
- If the channel is sensed busy during or after DIFS, the station waits for a random backoff interval again before sensing the channel.

Each station generates a random backoff time within a Contention Window (CW) size before attempting to transmit again. The CW starts with a minimum value of CW_{min}, called W_0. After each unsuccessful transmission, the CW value is doubled upto the maximum CW_{max}. The relation between CW_{min} and CW_{max} is given by:

$$CW_{max} = 2^m \times CW_{min} \tag{1.1}$$

where, m is the maximum increasing factor.

If a station intending to transmit, detects the channel busy, the backoff timer is frozen and resumed only when the channel is detected idle for more than DIFS period. The backoff timer is decreased while the channel is sensed idle. The random backoff procedure is also followed between transmission of two consecutive new transmissions from the same transmitter, even if the channel is sensed idle.

The CSMA/CA based DCF protocol is a distributed method that is employed independently at each IEEE 802.11 station. As shown in Figure 1.3, two techniques are used for frame transmission in DCF: the basic two-way handshake and four-way handshake. In two-way hand shake, an acknowledgment (ACK) frame is transmitted by the successful reception of packet by the receiver after a Short Interframe Space (SIFS). A transmission with ACK not received is deemed a collision by the transmitter. SIFS is assigned a value that is shorter than DIFS so as to restrict stations to detect the channel to be idle until the end of the ACK. In the optional four-way handshaking mechanism, Request To Send (RTS)/Clear To Send (CTS) frames are used to reserve the channel before data transmission. Between two consecutive frames in the sequence of RTS, CTS, Data frame, and ACK frames, SIFS time interval is used. Four-way handshake requires the transmitter and receiver to interchange their roles several times, which requires neighboring stations to be silent during the entire exchange. Upon receiving either RTS or CTS, stations in the transmission range of both the transmitter and receiver set a timer, called Networks Allocation Vector (NAV). Stations that receive these frames do not start any transmission until this timer expires. This technique was introduced to reduce the performance degradation caused by the presence of hidden terminals. However, due to the drawback of increased transmission overhead due to RTS/CTS frame exchange (which is significant when short data frames are used), the four-way hand mechanism is rarely used in Wi-Fi devices.

The advantage of DCF is that it guarantees the same probability of channel access for all the stations intending to transmit over the shared channel. In addition, the aim is to coordinated the channel access to minimize or eliminate the incidence of collision and maximum spatial reuse (i.e. allow maximum simultaneous transmission to co-exist) at the same time.

Unfortunately, the IEEE 802.11 MAC mechanisms are unable to guarantee basic data services in case of overwhelming network congestion and interference problems. All CSMA/CA based MAC protocols suffer from well-known hidden and exposed terminal problems. Hidden node problem refers to stations that are unable to sense each other transmission, however, their concurrent transmission results in collisions at the corresponding receivers. The four-way handshake mechanisms used to counter hidden stations, is also not suitable for dense deployments where stations associated to neighboring Wi-Fi cells are also restricted to transmit due to the NAV timer set based on the received RTS/CTS frames.

Exposed station problem occurs when a station refrains from transmission on sensing the channel busy, even though the concurrent transmissions would probably succeed. Hidden node cause increase in collisions and exposed station results in reduced spatial reuse. Both of the foregoing problems have adverse effects on dense deployments.

The distributed DCF MAC also faces the fairness problems, where each station must rely on its own direct experience in estimating congestion, that often leads to asymmetric views. The primary focus of this dissertation is the development of solutions that will address the above mentioned problems, so that the high density IEEE 802.11 deployments can be made resilient against malicious devices along with the ability to increase area throughput.

1.4 Objectives of the Ph.D.

Despite the expected challenges, it is anticipated that the IEEE 802.11 based Wi-Fi standards will be the dominant indoor systems in the coming years with the introduction of new amendments and techniques, that will facilitate in achieving improved capacity under diverse environments. Thus, in this thesis, we consider design and evaluation of mechanisms that would lead toward better management of Wi-Fi stations.
The high level objectives that we intend to answer within this thesis are listed hereinafter,

1.4.1 To investigate the impact of adversaries on IEEE 802.11 networks and to evaluate a novel malicious entity detection mechanism that requires minimum modifications to be made on the existing protocols.

The IEEE 802.11 protocols were designed with the assumption that all stations that want to communicate, would follow specific predefined rules of engagement to transmit and receive data. These were not designed to withstand adversaries attacks intended to interrupt transmission. Particularly for the case of dense deployments, such attacks result in failure to forward packets for many nodes who have the adversary in the nearby vicinity.

While various security issues have been studied, the threats posed by denial-of-service attacks created by real malicious device (jammer or cheater) within IEEE 802.11 dense infrastructure has not been fully explored. Furthermore, the challenge of detecting a station deliberately misusing the

MAC protocol to gain bandwidth at the expense of other stations is also an open research topic. An adversary with the intent to disrupt the network can use low priced and readily accessible RF jammers. Such attacks can be simple in nature but can have devastating consequences.

Thus, in order to design a reliable malicious entity detection mechanism, it is of utmost importance to first evaluate their impact on a real IEEE 802.11 network, then understand the operability of the adversary and finally design the scheme (based on the foregoing information) that is able to correctly detect. An important aspect in the design of the required scheme is that the detection can be performed by the dedicated devices as well as the inclusion of algorithms within already existing devices. The later approach is much more cost efficient and contains minimum overhead.

1.4.2 To explore a new IEEE 802.11 amendment proposed for long range communication (IEEE 802.11ah) as an alternative to densely deployed legacy IEEE 802.11 networks.

As mentioned in the previous sections, dense deployment of WLAN leads to multiple OBSS, that create contention and increase interference, which lead to reduced area throughput. Furthermore, due to the scarcity of available channels, assigning similar channels to different closely located cells can incur in frame collisions.

Lately, a new standard IEEE 802.11ah is published, which intends to support low cost mode of operations with greater coverage area and support for thousands of associated stations. This standard includes technological advances that would enable WLAN to operate at Sub 1 GHz (S1G) frequency and along with methods to allow around 8000 stations to connect to a 802.11ah AP (where only 2007 stations were allowed to connect to AP in legacy IEEE 802.11 networks). We visualize the advent of this standard as a potential complement to dense legacy IEEE 802.11 networks.

1.4.3 To explore a new IEEE 802.11 proposed amendment for dense deployments (IEEE 802.11ax) and design of simple yet optimal self adaptation mechanism to improve spatial reuse within densely deployed networks.

The need for improved performance and efficient methods to share the limited resources has resulted in extensive research being done on spatial reuse, interference and efficient resource sharing. While the new IEEE standards (i.e. IEEE 802.11n and IEEE 802.11ac) were developed by the IEEE standardization committee with intention to improve the peak aggregate (by improving technology) multi-station throughput of the network, mitigation of increased interference incurred (due to the existence of many AP and non-AP devices) has not been addressed in any of the current WLAN standards. As a consequence, the capacity demand associated to WLAN for indoor deployments can not merely be achieved by only improving the peak rate; there is a need to improve the average per user data rate as well. Furthermore, the channel access method in the aforementioned standards is also over-protective, which leads to reduced spatial reuse within dense deployments.

In order to improve matrices that can elevate the user experience by reducing interference as well as to provide improved aggregate multi-station throughput, IEEE 802.11ax amendment (which is a successor of IEEE 802.11ac) is being developed by the IEEE 802.11 working group with the aim to significantly improve WLAN efficiency along with system level performance in dense deployments. In particular, based on the challenges of dense deployments, this standard is intended to utilize techniques in dense deployments that would reduce Frame Error Rate (FER) and allow improvement in spatial reuse by mitigating/reducing interference that would in return increase the area throughput.

Optimizing spatial reuse and network throughput within interference limited environments has been widely studied with context to wireless communication. Since in dense deployments, MAC protocol plays an important role in the achieved performance (in terms of fairness, delay and throughput), it is mainly desired to allow as many concurrent transmissions as possible with minimal increase in collisions (interference). These are the main design objectives of IEEE 802.11ax, which will define standardize modifications of both PHY and MAC layer to improve end user experience in densely deployed WLAN environments.

- **Design of simple yet optimal self-adaptation mechanism to improve spatial reuse within densely deployed networks.**

  Considering the fact that the demand of capacity will rise in the coming years, we foresee this standard to play pivotal role in the further growth and acceptance of IEEE 802.11 networks.

  As a contribution to the IEEE 802.11ax proposed amendment, we first analyze the impact of overly protecting carrier sensing mechanism in high density legacy IEEE 802.11 based networks (which is one of the few studies conducted for dense networks). Then, we evaluate and propose a novel distributive mechanism for improvement of carrier sensing in dense deployment, that leads to increased area throughput and fairness due to optimized spatial reuse.

- **Investigate an intelligent method to alleviate interference problems with in dense deployments without degrading the overall performance**

  The increase in area throughput by introducing carrier sensing modifications in dense deployments leads to increase in concurrent transmission over the cost of slight degradation of channel conditions (in terms of collisions). In order to tackle the foregoing problem, we intend to intelligently utilize techniques proposed for IEEE 802.11 to reduce the impact of collisions in densely deployed networks.

  As a contribution of the 802.11ax amendment, we analyze the intelligent utilization of a conventional IEEE 802.11 legacy protocol that can help in mitigating the interference problem in dense deployments.

1.5 Research methodology

Due to the complex and dynamic nature of wireless networks, it is required that the analytical modeling should be followed by real world experimentations by either utilizing real hardware or

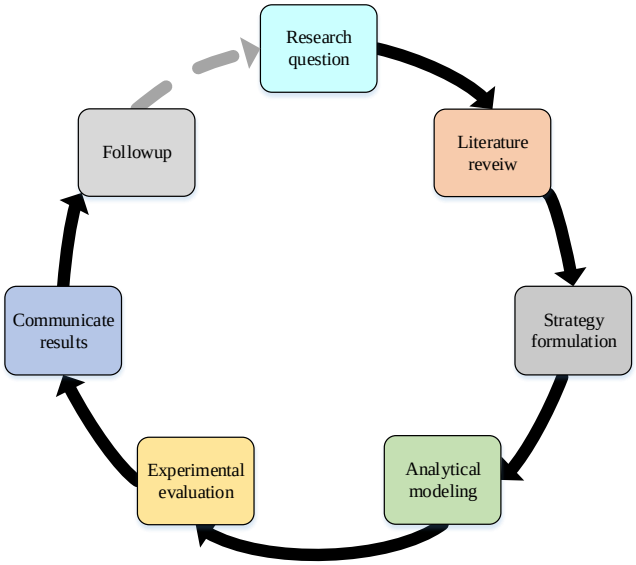


Figure 1.4: Research methodology.

using mature simulation tools that mimics the behavior of real world wireless networks. In this dissertation, network performance results are based on combination of theoretical model, system level simulations and experimental results.

The methodologies used in this thesis to achieve the foregoing objectives are based on design, creation and experimentation strategy. The design and creation aspects are used in the design and evaluation of self-adaptive algorithms to improve spatial reuse (i.e. first sub-objective defined in 1.4.3). Furthermore, the same strategies are also employed in order to design mechanisms to reduce interference within densely deployed networks that utilize the foregoing self-adaptive algorithm (i.e. second sub-objective defined in 1.4.3). Experimentation strategy is used to evaluate and compare malicious entity detection scheme(i.e. objective defined in 1.4.1).

The research methodology followed in this thesis is reflected in Figure 1.4. In the first part, research question was set based on the objectives presented in section 1.4. It included identification of the problem, understanding possible outcomes for a solution and methods to formulate the hypothesis. Each intended objective was followed by a phase consisting of a thorough revision of the related literature (to gain knowledge of relevant research area, to apprehend the problem and to identify possible avenues in the area of interest). In the next phase, strategy based on merits was formulated. Key issues were identified, isolated and addressed through the design of particular techniques. In addition, metrics were also defined that would assist in the evaluation procedure. In the next two phases, a thorough evaluation of the proposed scheme was performed by analytical modeling and implementing the proposal (by leveraging simulation environments and/or real experiments). In the next step, validation of the research was done with the help of publication in international conferences and/or journals. An iterative procedure was followed afterwards, where new ideas were added to existing solutions published in the previous work. Comments received from reviewers were used

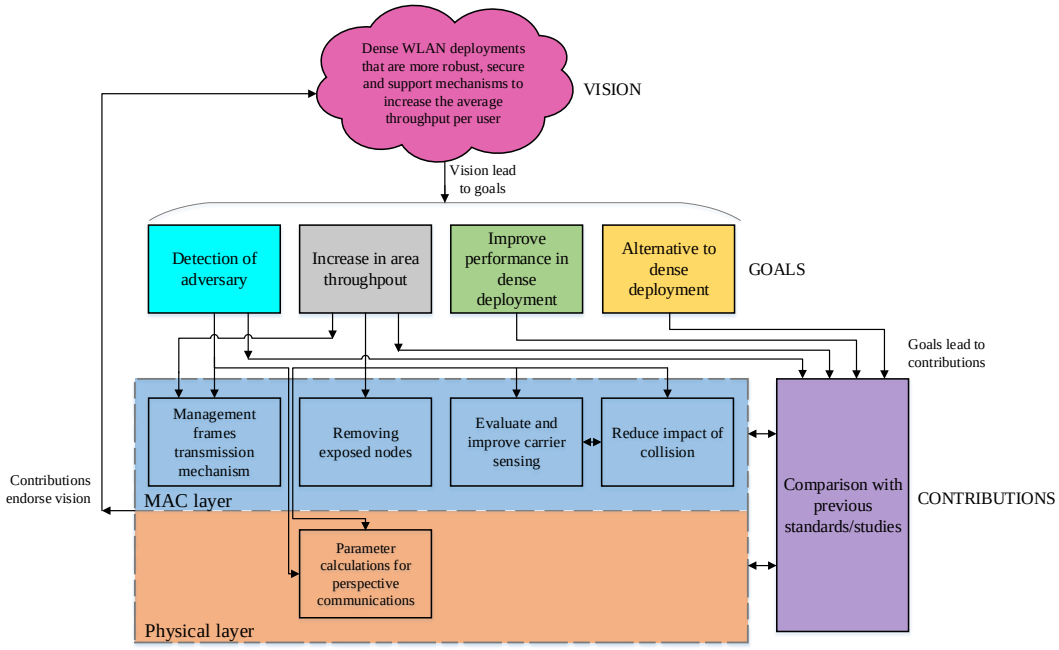


Figure 1.5: Vision, goal and contributions.

to refine the work.

1.6 Contributions and publications

The objective of PhD thesis is to investigate the potential problems and investigate solutions for amicable operation of Wi-Fi deployments. Given that, it is not feasible to cover all types of deployments and also due to the importance of capacity enhancement in 5G networks, the scope of the thesis is limited to densely deployed IEEE 802.11 based networks that utilize DCF based MAC protocol. Figure 1.5 highlights the vision, goals and contributions associated with this thesis.

Majority of the work presented in this thesis has been published or submitted for publication. The publications consist of four parts: a malicious entity detection algorithm, an alternative solution to dense deployments, a standard being designed for dense IEEE 802.11 deployments and a mechanism to optimize spatial reuse (to improve throughput) within ultra dense networks.

1.6.1 Malicious entity detection algorithm

The first article investigates the impact of different adversaries in IEEE 802.11 based WLAN networks. It considers the design and implementation of a novel adversary detection method (that is built on previous work by Dr. Eduard Garcia-Villegas) which is able to correctly detect a malicious device. It analytically proves the viability of the proposed scheme and utilizes simulation as well as a real test bed to build upon the validity of the scheme. In order to signify the importance of the afore-

mentioned contribution, it also encompasses a thorough comparison with the existing mechanisms in literature.

- **Paper 1.** Eduard Garcia-Villegas, **Muhammad Shahwaiz Afaqui**, and Elena Lopez-Aguilera, "A novel cheater and jammer detection scheme for IEEE 802.11-based wireless LANs", published in *Computer Networks: The International Journal of Computer and Telecommunications Networking, Impact factor: 1.446*, Vol. 86, No. C, pp. 40–56, July 2015.

1.6.2 IEEE 802.11ah standard: An alternative to dense deployment

Papers 2 provides a brief but updated overview of the IEEE 802.11ah standard and perform a novel MAC layer comparison of IEEE 802.11ah standard with the previously proposed amendments of IEEE 802.11. Paper 3 discusses the main PHY and MAC layer amendments proposed for IEEE 802.11ah. It investigates the operability of IEEE 802.11ah as a backhaul link to connect devices over a long range. Additionally, it provides a comparison of IEEE 802.11ah standard with previous notable IEEE 802.11 amendments (i.e. IEEE 802.11n and IEEE 802.11ac) in terms of throughput (with and without frame aggregation) by utilizing the most robust modulation schemes.

- **Paper 2.** Victor Baños-Gonzalez, **Muhammad Shahwaiz Afaqui**, Elena Lopez-Aguilera and Eduard Garcia-Villegas, "IEEE 802.11ah: A Technology to Face the IoT Challenge", published in *Sensors, Impact factor: 2.033*, Vol. 16, No. 11, Art. No. 1960, Nov. 2016.

- **Paper 3.** Victor Baños-Gonzalez, **Muhammad Shahwaiz Afaqui**, Elena Lopez-Aguilera and Eduard Garcia-Villegas, "Throughput and Range Characterization of IEEE 802.11ah", submitted to *IEEE Latin America Transactions, Impact factor: 0.436* 2017.

1.6.3 IEEE 802.11ax standard: Amendment for dense deployments

The popularity of IEEE 802.11 based WLANs has increased significantly in recent years because of their ability to provide increased mobility, flexibility, and ease of use, with reduced cost of installation and maintenance. This has resulted in massive WLAN deployment in geographically-limited environments that encompass multiple OBSSs. In the following article, we introduced IEEE 802.11ax, a new standard being developed by the IEEE 802.11 Working Group, which will enable efficient usage of spectrum along with an enhanced user experience. We expose advanced technological enhancements proposed to improve the efficiency within high density WLAN networks and explore the key challenges to the upcoming amendment.

- **Paper 4. Muhammad Shahwaiz Afaqui**, Eduard Garcia-Villegas and Elena Lopez-Aguilera, "IEEE 802.11ax: Challenges and Requirements for Future High Efficiency WiFi,", published in *IEEE Wireless Communications, Impact factor: 4.148*, Vol. PP, No. 99, pp. 2–9, Dec. 2016.

1.6.4 Mechanism to optimize spatial reuse in dense deployments

With the rise in popularity of IEEE 802.11 based WLAN networks, Wi-Fi capable devices keep proliferating by conquering new scenarios and use cases. The need to provide high throughput Internet connection to these progressively growing number of devices has led to high density deployments (both unstructured/unplanned as well as planned). Despite the benefits achieved by Wi-Fi deployments in diverse environments (in terms of data rates, coverage and cost), legacy IEEE 802.11 was not designed to withstand the challenges faced in high density deployments, where frame loss (due to co-channel interference) and overprotected channel access mechanism can seriously degrade the overall performance. Paper 5 provides evaluation of Dynamic Sensitivity Control (DSC) Algorithm proposed for IEEE802.11ax that increases spatial reuse within ultra dense Wi-Fi networks. This algorithm dynamically adjusts the Carrier Sense Threshold (CST) based on the average received signal strength. Paper 6 proposes the intelligent utilization of AP controlled four-way handshake uplink access to improve and enhance the performance of DSC enabled network, leveraging two of the mechanisms under the consideration of the TGax to enhance spatial reuse in future IEEE 802.11ax devices. Paper 7 introduces a DSC-AP scheme for IEEE 802.11ax that increases spatial reuse and limits the effects of increased interference at a Wi-Fi AP within dense deployments. The proposed scheme dynamically tunes CST of an AP based on the received signal strength from its associated stations and surrounding APs. This paper extends the work presented in Paper 5 by presenting simple analytical justification for dynamically adopting CST threshold of each station.

- **Paper 5. Muhammad Shahwaiz Afaqui**, Eduard Garcia-Villegas, Elena Lopez-Aguilera, Graham Smith, and Daniel Camps, "Evaluation of dynamic sensitivity control algorithm for IEEE 802.11ax", published in proceedings of *IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1060–1065, Mar. 2015.

- **Paper 6. Muhammad Shahwaiz Afaqui**, Eduard Garcia-Villegas, and Elena Lopez-Aguilera, "Dynamic sensitivity control algorithm leveraging adaptive RTS/CTS for IEEE 802.11ax", published in proceedings of *IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, Apr. 2016.

- **Paper 7. Muhammad Shahwaiz Afaqui**, Eduard Garcia-Villegas, Elena Lopez-Aguilera, and Daniel Camps "Dynamic sensitivity control of access points for IEEE 802.11ax", published in proceedings of *IEEE International Conference on Communications (ICC)*, pp. 1–7, May 2016.

A mathematical model which utilizes frame collision probability is presented in Paper 7, that indicates the throughput performance of a CST varying station. It indicates the importance of optimal CST selection and motivates the use of received power as a valid and viable local information to set CST. In addition, Paper 8 proposes and evaluates a simple but efficient self adaptation (fully distributive) mechanism that improves spatial reuse within a densely deployed WLAN network which is coherent with the development guidelines for IEEE 802.11ax standard.

- **Paper 8. Muhammad Shahwaiz Afaqui**, Eduard Garcia-Villegas, Elena Lopez-Aguilera, "Dynamic Sensitivity Control for IEEE 802.11ax", submitted to *Computer Networks: The International Journal of Computer and Telecommunications Networking, Impact factor: 1.446*, undergoing second revision, Jan. 2017.

1.6.5 Other publications

In addition to the aforementioned peer reviewed publications, the following submission were presented at the TGax, that have assisted in the standardization efforts of the IEEE 802.11 working group.

- **Presentation 1. Muhammad Shahwaiz Afaqui**, Eduard Garcia-Villegas, Elena Lopez-Aguilera , Graham Smith, and Daniel Camps, "Simulation Based Evaluation DSC in residential scenario, IEEE 802.11-15/0027, January 2015.

- **Presentation 2. Muhammad Shahwaiz Afaqui**, Eduard Garcia-Villegas and Elena Lopez-Aguilera, "Proposal and simulation based evaluation of DSC-AP Algorithm", *IEEE 802.11ax submission*, IEEE 802.11-15/0371, March 2015.

- **Presentation 3. Muhammad Shahwaiz Afaqui**, Eduard Garcia-Villegas, and Elena Lopez-Aguilera, "DSC leveraging uplink RTS/CTS control", *IEEE 802.11ax submission*, IEEE 802.11-15/0580, July, 2015.

- **Presentation 4. Muhammad Shahwaiz Afaqui**, Eduard Garcia-Villegas and Elena Lopez-Aguilera, " DSC calibration results with NS-3", *IEEE 802.11ax submission*, IEEE 802.11-15/1316, Nov. 2015.

- **Presentation 5.** Eduard Garcia-Villegas, **Muhammad Shahwaiz Afaqui** and Elena Lopez-Aguilera, "Drivers of the dynamic CCA adaptation", *IEEE 802.11ax submission*, IEEE 802.11-15/1427, Dec. 2015.

1.7 Impact of research work

The work done in this thesis has improved the state-of-the-art associated with high density WLAN networks. We have highlighted key challenging issues pertinent to dense deployments and have proposed algorithms that increase robustness and efficiency within the aforementioned scenarios. Furthermore, the proposed solutions assist in creation of new avenues for further research in IEEE 802.11 based dense networks. Following are the major impact of our contributions,

- By utilizing the sheer principle that transmission of beacon signals has greater priority over any other transmission within WLAN network, we devised a method to detect an adversary. New algorithms can be designed that utilize basic design features of IEEE 802.11 MAC which,

if used intelligently, can be used in the detection process. Furthermore, feedback systems and cooperation among devices can further improve the proposed algorithm.

- We exposed IEEE 802.11ah standard as a potential alternative to dense deployment due to its enhanced features to associate greater number of stations and by providing greater area coverage. We provide MAC layer comparison of IEEE 802.11ah with previous IEEE 802.11 standards.
- We introduce a high efficiency Wi-Fi standard being designed to increase capacity within high density and outdoor Wi-Fi deployments. We point out the necessity and scope of the proposed amendment and describe the most important technological improvements that will form the basis of the next generation of WLANs. As a contribution, we also highlight the expected co-existence challenge of IEEE 802.11ax with LTE-U. Also, we expose the expected opportunities and challenges for TGax within IoT scenarios.
- With the ability to vary carrier sensing threshold at each device based on local information, we show that the area throughput within dense deployments can be increased (by allowing many concurrent transmission to co-exist). With design and simulation results, we exposed the benefits of the proposed dynamic algorithm. As submission/contribution, we have presented our findings for the highlighted problem and its relevant solution in TGax.
- To the best of our knowledge, neutralizing the negative effects of dynamic PHYCCA modifications by intelligently adapting RTS/CTS mechanism is one of the fist studies. This solution leads to further possibilities of throughput increase and improved spatial reuse.

1.8 Overview of the thesis

Remainder of this dissertation is organized as follows: Chapter 2 highlights the problem caused by malicious entity in WLAN networks and proposes a novel method to detect an adversary. Chapter 3 illustrates the IEEE 802.11ah amendment that can act as an alternative to dense Wi-Fi deployments. Chapter 4 provides a thorough description of the IEEE 802.11ax amendment proposed for dense deployments. Methods (being considered to become part of the IEEE 802.11ax standard) that can increase the area throughput of high density networks are presented in Chapter 5. Chapter 6 presents the concluding remarks. This chapter summarizes the main contribution of this thesis, and also describes possible ways of extending this work in the near future.

2

Intrusion detection in IEEE 802.11 networks

The extensive proliferation of IEEE 802.11 networks has made them an easy and attractive target for malicious devices/adversaries which intend to misuse the available network. Being broadcast in nature and due to its operation over the unlicensed band means that any malicious stations can easily capture and analyze traffic or even create hindrance for stations to perform normal network access. As a consequence, IEEE 802.11 standard has time and again been criticized for not including comprehensive security solutions to protect all the entities within the network.

IEEE 802.11 in its current form, does include security protocols such as WEP, WPA, IEEE 802.11i and IEEE 802.11w, that use cryptographic checks for data and management frames. However, these protocols only deal with vulnerability related to unauthorized access and confidentiality breach. The nonexistence of methods to provide continued provision/availability of service in the face of intentional Denial of Service (DoS) leaves a big security loophole in IEEE 802.11 networks. These DoS attacks can easily be executed by transmitting continuous stream of forged frames that result in gradual slow down of the network to an extent where the network becomes unavailable for authenticated clients.

Since the IEEE 802.11 networks use distributed medium access control techniques where each station is assigned a transmission opportunity in a de-centralized manner, the performance of IEEE 802.11 networks is also impacted by selfish devices that configure their MAC parameters to gain unfair channel access. Similar to DoS attack, IEEE 802.11 protocol has no mechanism to force the stations to follow the rules to access the channel.

Particularly for the case of dense Wi-Fi deployments (as highlighted in Figure 2.1), where network performance (in-terms of throughput and fairness) is already compromised due to increased interference from many overlapping BSS, the security challenges posed by DoS and the operations by selfish stations can result in further degradations. Also, the wide spread deployments of Wi-Fi networks in government, corporate and IoT environments implies the presence of sensitive information

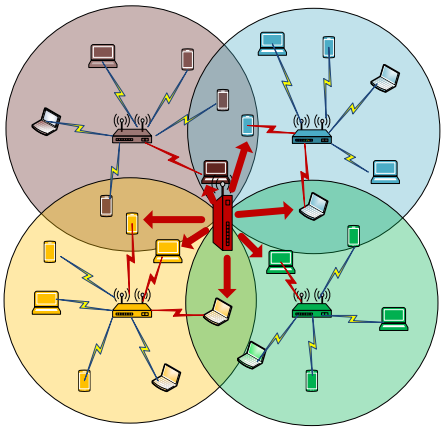


Figure 2.1: Impact of DoS attack in dense deployments.

over the air that needs to be protected from security attacks. Given the necessity and ubiquitousness of 5G HetNet dense connections (encompassing harmoniously knit LTE and Wi-Fi air interface) to provide massive capacity with reduced cost per transmitted bit, providing unrivaled security measure is one of the top design and implementation priority.

An adversary following the IEEE 802.11 protocol, with the intention to disrupt the normal operations of dense deployment can increase its transmission rate and cause collisions at stations concurrently receiving from other sources. This problem is further complicated by the presence of numerous hidden stations in densely co-located Wi-Fi cells, where transmitters might be unable to hear transmissions by stations in neighboring BSS and continue to retransmit frames up-till retry limit of the backoff procedure. Thus, adding to the problem, these retransmissions result in cascading effect, where an adversary can launch a wide spread attack in high density IEEE 802.11 deployments from a single location.

In order to tackle DoS and selfish behavior in dense deployments, it is utmost important to first employ a mechanism that helps in the detection of malicious entities and then take the appropriate countermeasures. This detection procedure can be instrumental in countering the cascading performance degradation effect that an adversary can induce in ultra dense networks. Its important to highlight the fact that performance over unlicensed channels is dependent on the individual security features provided by the wireless technologies. Therefore, this dissertation first explores the possibilities to enhance performance of densely deployed IEEE 802.11 based WLANs through enhanced resilience against adversary attacks. In the forthcoming chapters, the performance is further augmented by techniques that improve the Wi-Fi protocol, so as to enable them to provide high performance in dense scenarios.

In this chapter, we introduce a novel malicious entity detection method for IEEE 802.11 networks. We propose a new metric, the Beacon Access Time (BAT), which is employed in the detection process and inherits its characteristics from the fact that beacon frames are always given preference in IEEE 802.11 networks. The method to detect a malicious entity relies mainly on the observed change in BAT. Most of the previous detection schemes, summarized in section 2.2, take into account the

transmission Packet Delivery Ratio (PDR), CS Time (CSTI) and Received Signal Strength (RSS). To the best of our knowledge, no previous work has been done to detect a malicious entity in IEEE 802.11 WLANs based on beacon frame analysis. Furthermore, our proposed technique is also the first mechanism that has proved to be capable of detecting jammers as well as cheating devices within Wi-Fi networks.

The majority of the work presented in this Chapter has been published in [38].

2.1 Motivation

The success of IEEE 802.11 has attracted more and more users to employ these networks, while increasing the potentials for attackers to operate. The first legacy IEEE 802.11 amendment (that was ratified in 1997 and accepted in 1999) contained WEP security mechanism. WEP enforced confidentiality, access control and data integrity with the goal to protect the privacy of user data from eavesdropping. A secret key was used, where the difficult of discovering the key was based on its length. Therefore, the critical design flaw made WEP practically futile to implement (where a brute force search approach made it trivial to detect the network key in a reasonable time).

Due to WEP vulnerabilities, the IEEE working group ratified IEEE 802.11i in 2004. The aim of this amendment was to provide enhanced security features for WLAN networks by introducing mutual authentication, confidentiality, data integrity and key management protocols. IEEE 802.11i specified two classes of security algorithms: RSNA and Pre-RSNA. RSNA implemented two new data confidentiality algorithms known as acrfulltkip and Counter Mode CBC MAC Protocol (CCMP). It also included 802.1X authentication and four-way handshake authentication and key management protocols. Pre-RSNA included WEP (so as to make IEEE 802.11i backward compatible) and IEEE 802.11 entity authentication (that included open system authentication and shared key authentication).

The design of IEEE 802.11i was based on improving the vulnerabilities of WEP. By using CCMP, this amendment was able to provide an effective mechanism for data confidentiality and integrity. However, IEEE 802.11i extended the use of legacy management action frames, that resulted in the transmission of sensitive information inside management frames. To rectify this problem, a task group was established in 2005 (called TGw) that proposed a new amendment in 2009. This new amendment, called IEEE 802.11w, specified protection of selected management frames of subtype deauthentication, disassociation and action using the IEEE 802.11i security mechanisms. This amendment also aimed to provide solutions to mitigate certain type of well known and easy to implement DoS attacks (such as Deauthentication attack etc.). The only vulnerabilities that IEEE 802.11w possessed was that an intelligent malicious entity could forge management frames, and create authentication protocol attacks to prevent stations from maintaining their connections.

Despite the benefits, IEEE 802.11i and IEEE 802.11w are prone to complicated DoS attack. This is due to the fact that none of the IEEE 802.11 amendments was designed to provide network availability under adverse conditions (i.e. situations where a malicious entities manipulates the network to either gain undue benefits or to totally disrupt the normal operations). Also, the shared access na-

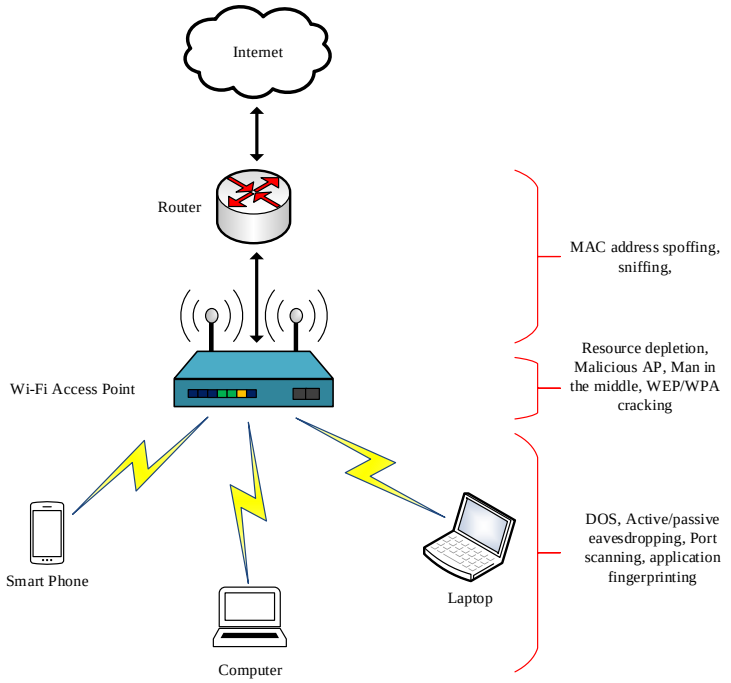


Figure 2.2: Types of attacks on IEEE 802.11 network.

ture of IEEE 802.11 DCF based MAC protocol particularly made these attacks effective were collisions created by DoS can not be distinguished from normal collisions.

With time, the wireless attacks on IEEE 802.11 have become more sophisticated and are evolving to counter every new development made in the above mentioned amendments. Figure 2.2 shows few of the attack strategies being employed at different stages of the Wi-Fi network. The most prominent of these attacks are layer-1 attacks which are seldom considered a threat because they are typically generated from non-Wi-Fi devices sharing the same ISM bands such as micro wave ovens, cordless phones, etc. These non-Wi-Fi devices, when located within a WLAN's coverage area, unintentionally radiate unwanted energy that can affect the whole network. Furthermore, most of the people are not familiar with the interference abilities of such devices and the people who are familiar do not have the control over their placement.

These attacks are further aggravated when done purposefully. An attacker/adversary with the intent to disrupt the network can use low-priced and readily accessible RF jammers. Such attacks can appear to be simple in nature but can have devastating consequences for corporate companies since those security breaches can break down the core communication line within a company (e.g. critical voice over Wi-Fi communication lines which require continuous Wi-Fi connections and e-mail services) that can result in reduced productivity. The ease to attack IEEE 802.11 networks is indicated by [35] where the authors demonstrate the use of off-the shelf hardware that can be used to severely disrupt the network.

In [105], Xu et al. define an adversary as a *jammer to be an entity who is purposefully trying*

to interfere with the physical transmission and reception of wireless communications. Although, we agree with this definition, for the sake of simplicity, we will also consider those accidental interferer's (e.g. baby monitors, cordless phones, etc.) as jammers, given their adverse effects.

2.1.1 IEEE 802.11 MAC Anomaly

The jammer spreads energy over the targeted spectrum, where it becomes difficult to extract the desired signal from interfering signals. Furthermore, due to CSMA/CA based channel access, the Wi-Fi networks become an easy target by these adversaries, where a jammer can even utilize low power to disrupt the network.

IEEE 802.11 standard [45] provides different operating modes: Distributed Coordination Function (DCF), Point Coordination Function (PCF), Hybrid Coordination Function (HCF) with HCF Distributed EDCA and HCF Controlled Channel Access (HCCA). The DCF is the mode currently employed in most deployments and uses CSMA/CA contention-based MAC algorithm. In this case, before initiating a transmission, a station senses the channel to determine whether it is busy during a period of time called the DCF Inter-frame Space (DIFS). If the medium is sensed busy, the transmission is delayed until the channel is idle again, and a slotted binary exponential backoff interval is chosen in the range [0, CW-1], where CW is the contention window. The value of CW is set to its minimum value, CW_{min}, in the first transmission attempt and increases in integer powers of 2 at each retransmission, up to a pre-determined value CW_{max}. For each data frame successfully received, the receiver transmits an ACK frame after a Short Interframe Space (SIFS) period. The protocol described above is called the basic or two-way handshake mechanism. In addition, the specification also contains a four-way frame exchange protocol known as the RTS/CTS mechanism.

Due to CSMA/CA characteristics, this contention-based MAC mechanism is very sensitive to DoS attacks based on jamming techniques. This kind of attacks consists in the transmission of a powerful signal in the frequency band employed by IEEE 802.11 devices. Thus, the medium is always sensed busy during the jammer signal by IEEE 802.11 clients. Obviously, jammer influence will lead to very harmful effects in MAC protocol performance. Jamming attack in IEEE 802.11 can prevent the nodes to perform legitimate MAC operations or can cause the collision of frames that force repeated backoff which can even jam the complete transmission process. The jamming signal interferes and corrupts the desired signal in reception, while causing the co-channel transmitters to reschedule the transmission for longer periods of time. Different factors are incorporated in the effectiveness of interference that a jammer creates namely distance between a jammer and a wireless device, transmission power of jammer and the network devices, and the MAC protocol used within the network.

2.1.2 Different Jammer Strategies

Different attack strategies can be employed by a jammer while trying to interfere with other communicating nodes. In [105], the authors have differentiated jammers based on their attack model. They have defined four types of jammers namely constant jammers, deceptive jammers,

random jammers and reactive jammers. According to the authors, a constant jammer continues to transmit radio signal without following any MAC layer protocol, a deceptive jammer continuously transmits regular frames without any gap, thus deceiving other communicating nodes to believe that a legitimate transmission is occurring, a random jammer transmits for a time and goes to sleep, where both the transmission time and the sleep time can be random, and a reactive jammer that starts transmitting jamming signals as soon as it detects activity on the shared medium and goes to sleep when there is no one transmitting.

An intelligent jammer can also exploit the standard DCF that is used to coordinate nodes for medium access within IEEE 802.11. In [80] Pelechrinis et.al. define intelligent jamming models and methods used to jam IEEE 802.11 networks. In [113], the authors investigate the fabricated CTS attack to the MAC scheme of IEEE 802.11 and propose a mechanism to prevent such attack. This attack is based on a jammer acquiring the use of shared channel by transmitting a fabricated CTS signal, which contains large NAV to falsely defer transmissions from other users for longer duration.

A jammer can also be a cheating device that misuses the IEEE 802.11 MAC constraints in order to attain bandwidth gains. This device can have the ability to choose PHYCCA threshold, backoff window size and/or inter-frame space. By increasing the PHYCCA threshold, the cheating device can improve its opportunity to transmit and thus can effectively disable channel sensing. It can continue to transmit over the medium, while causing other transmitting stations (STA) to undergo collisions and thus to backoff from transmitting. The cheating device can also observe collisions but the backoff period is kept shorter (is not frozen because carrier sensing is already disabled). The authors in [82] extensively explain how a selfish station with higher PHYCCA can experience bandwidth gains.

Similar bandwidth advantages can also be achieved by utilizing a smaller contention window, which helps the cheating node to backoff for smaller periods than average, when collisions occur. The cheating device can also maneuver to cheat the IEEE 802.11 MAC constraint by reducing its DIFS. By reducing the DIFS, the cheating station can gain quick access to the medium, thus depriving other stations from their fair share.

Therefore, finding solutions to eliminate jamming is very important in IEEE 802.11 networks. This solution can only be found by first enabling the network to detect the jammer and then to find an appropriate solution to counter such threats.

2.2 Related Work

Jamming detection relies mainly on observed characteristics and relates them to each other to make a decision. Xu et al. [105] use PDR and Packet Sent Ratio (PSR) metrics. Different jamming attack models that may require different detection strategies are also defined in [105]. PSR corresponds to the number of frames transmitted by the sender divided by the actual number of frames that the transmitter wanted to transmit. The intended and the actual number of frames sent are different in the presence of a jammer. The jamming signal occupies the medium for long periods deferring legitimate transmissions and thus causes the buffer at the MAC of the transmitters to overflow (causes

new frames to be discarded and old frames to be timed out). At the receiver side, PDR is computed. It is defined as the ratio of successfully received frames at the receiver to the total number of frames transmitted by the sender. If a jammer is present near to the receiver, frames might not be decodable at the receiver, and thus PDR value is degraded.

In [81], the authors utilized the propagation characteristics of the wireless channel to expose the presence of jamming devices. The authors use PDR to estimate the presence of a jammer. Whereas the authors in [62] proposed a least-squares (LSQ) based localization algorithm that estimates the jammer's location.

The malicious activity of a jammer can also be detected by measuring RSS along with the calculated PDR. In [52], the authors propose a scheme to detect a jammer based on PDR along with RSS and a mechanism to reduce the impact of jammer in IEEE 802.11 networks. The authors have justified the presence of a jammer by utilizing consistency check when RSS is high and the PDR is low. This scheme uses the jammed channel by adapting the modulation and coding scheme of each node based on successful transmission probabilities. The authors prove that the rate adaptation algorithm (RAA) improves the PDR and link utilization in presence of a jammer. Similarly, recent works have also investigated the impact of jamming strategies on IEEE 802.11 RAA; in [83], the authors characterize the effect of power control and rate adaptation to mitigate the effect of jammers; in [74], the authors have investigated the vulnerability of different RAA against jamming attacks and propose new methods to mitigate them. In [35], authors have utilized cumulative-sum algorithm to detect abrupt changes in Signal to Interference plus Noise Ratio (SINR). They show that the output of their proposed algorithm increases in the presence of a jammer. Moreover, they propose to use the ratio of corrupted packets over correctly decoded packets as the cumulative-sum metrics to detect MAC layer attacks along with the SINR based cumulative-sum algorithm to detect physical layer attacks.

In [105], the authors also proposed the measure of the CSTI (the time a station waits for the channel to become idle) when a jammer is present near to the transmitter. But the CSTI value does not only increase in the presence of a jammer, it can also rise with high number of transmitters. The authors in [37] define a jammer detection method based on the inspection of the number of transmission attempts per frame and use it to correspond to CSTI. The authors define a ratio T_f that is based on the total number of frames that have been sent to the channel and the total number of transmissions that were deferred to avoid collision. The access point measures load (occupation time) and T_f periodically; if T_f is above the value expected for that load, a jammer is present. The authors propose to utilize cell breathing method to reduce the effect of the jammer on an AP. If the load on an AP is high, the cell size of that AP is reduced (so as to allow a minimum number of nodes to connect to that particular AP), while the nodes may be able to connect to other APs that do not have a jammer present in its vicinity. In [82], [87] and [94], the authors propose cheater detection methods in WLANs. The mode of detection in [82] and [87] is based on extensive monitoring and analysis of shared frames by the AP with the help of additional modules. In [94], the authors have designed a lightweight fair-share cheater detector mechanism that does not rely on the idle time distribution, but the proposed mechanism is only theoretically analyzed and the authors have not discussed the

Table 2.1: Functionality Comparison

	Jammer detection	Cheater detection	Principle of detection	Implementation requirements	Approach
BAT-based detector	Yes	Yes	Difference between TBTT and actual beacon transmission time	Additional software required at AP	Centralized
Xu et al. (2005) [105]	Yes	No	RSS and PDR based consistency check calculations	Extra signaling required for sending heart beat beacons	Distributive
Garcia-Villegas et al. (2010) [37]	Yes	No	PHYCCA channel busy indication, TxDeferred transmission and load	Additional software required at AP	Centralized
Pelechrinis et al. (2009) [81]	Yes	No	PDR calculations	Extra signaling required for generation of probe signal to calculate PDR	Distributive
Liu et al. (2012) [62]	Yes	No	PDR calculations	Extra signaling required for generation of probe signal to calculate PDR	Centralized
Fragkiadakis et al. (2013) [36]	Yes	No	SINR calculations	Additional hardware required (monitors) for SINR calculations	Local and distributive collaborative
Ju and Chung (2012) [52]	Yes	No	RSS and PDR based consistency check calculations	Extra signaling required for generation of probe signal to calculate PDR	Distributive
Pelechrinis et al. (2009) [82]	No	Yes	Throughput monitoring module and low power probing module	Additional software required at AP	Centralized
Raya et al. (2004) [87]	No	Yes	Traffic traces collected to analyze scrambled frame or manipulated protocol parameters	Additional software required at AP	Centralized
Tang et al. (2014) [94]	No	Yes	Collision estimation and fair share detector for real-time backoff misbehavior detection	Theoretical analysis, no practical implementation	Centralized

actual implementation aspects of their scheme.

Table 2.1 summarizes the main characteristics of the approaches found in the literature and offers a sneak peek of our proposal, the BAT-based detector. It provides the functionality comparison of the proposed system (which is explained in detail in the following sections) with some of the notable existing malicious entity detection systems. The comparison was done based on the detection capabilities, principle of detection, implementation requirements and approach followed by each detection method. It is pertinent to highlight that no single technique was found to detect both the jammer and the cheater together.

Note that additional hardware is required in [36] to measure SINR within the network. In [37], the authors propose to use PHYCCA channel busy indication for detection process. But this method has an apparent drawback that the channel busy time can increase in the presence of a jammer as well as with increased number of active users. Detection methods in [105], [81] and [62] require extra signaling, which entails and increased overhead. The cheater detection schemes [82] and [87] require extensive monitoring that can lead to increased complexity at the AP. The cheater detection scheme proposed in [94] is based on theoretical analysis and thus cannot be compared with our proposed scheme. In comparison to these schemes, our proposed BAT-based scheme is a novel idea

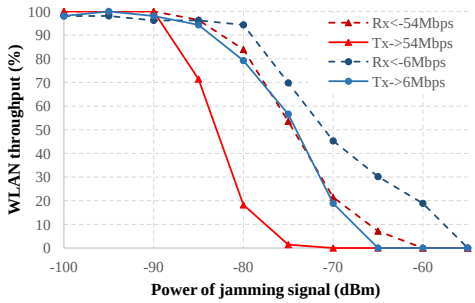


Figure 2.3: Throughput of an IEEE 802.11 link when the receiver/transmitter is under jamming.

of detection and only requires the need to monitor beacons transmission at the AP; it is a cell-centric scheme and does not require additional signaling nor imposes hardware constraints.

2.3 Understanding the Impact of Realistic Jammer

As anticipated in the previous section, the effects of a jammer on WLAN depend on several factors, such as the strength with which the jammer signal is received, the modulation and coding scheme used by the WLAN STAs, the frame size and the role of the attacked device (transmitter or receiver). In this section, we provide information about several experiments to study these factors when an IEEE 802.11 link is interfered by a channel-oblivious, memoryless, continuous jamming device.

2.3.1 Effect of a Jammer

In order to understand the implications of jamming signals on two stations connected through a WLAN link, a detailed study was preformed by previous students at Wireless Network Group. However, in this section we provide an overview of the above mentioned contributions that substantiate the need to understand the after-effects of a jamming attack (performed in section 2.3.2).

The authors first utilized signal generator as a jamming device and found swept sine function as the most effective signal. The swept sine signal was used to hinder User Datagram Protocol (UDP) traffic between two stations. The outcome of the above mentioned experiment are presented in Figure 2.3. First of all, the effects of the jammer start being observable when the power of the jamming signal is close to the receiver sensitivity (-87 dBm for 6 Mbps); then, as the power of the jamming signal is increased, it gradually degrades the performance of the WLAN link to the point at which frames cannot be successfully decoded. This point requires more energy when a robust modulation is used (cf. 6 Mbps vs. 54 Mbps lines in Figure 2.3). After different experiments, we can also conclude that the frame size used by the STAs does not show a definite influence on the effects of the jammer.

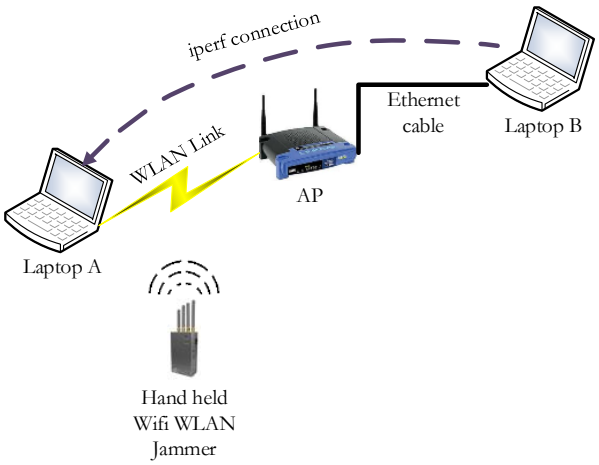


Figure 2.4: Experimental setup to understand the impact of a jammer in IEEE 802.11 network

2.3.2 Recovery after a Jammer Attack

After observing the harmful effects of the jammer, even at relatively low transmission power, in this section we study what happens afterwards, that is, when the jammer is deactivated. In order to do so, we run several experiments in which we switch on a jammer only for a given time and then observe how the WLAN recovers its operation. More precisely, we evaluate the time required by the STAs and AP to re-associate after a jamming attack by varying different set of hardware and software combinations. Figure 2.4 elaborates the setup used to perform the experiments. A simple Wi-Fi network was established in an isolated environment. Both ends of the radio link (AP - STA) were subjected to the interference created by the jammer. Two different APs equipped with different radio chipsets (Linksys WRT54G based on Atheros AR9103 and TP-Link WR1043ND using Broadcom BCM2050) were used in order to analyze the impact of the jammer on two different hardwares. Both the APs were running in IEEE 802.11g mode and operated on channel 1 (i.e. 2.412 GHz). Two laptops (laptop A and laptop B) were used in the experiments that had built-in IEEE 802.11a/b/g NICs. Laptop B was connected to the AP through Ethernet cable and, additionally, it was equipped with PCMCIA based IEEE 802.11a/b/g NIC that was used to sniff wireless traffic. Laptop A was connected to the AP through IEEE 802.11g based wireless connection. A UDP stream was established with the help of *iperf* network testing tool between laptop A and laptop B. UDP datagrams were generated from the client (i.e. laptop B) and were sent to the server (i.e. laptop A).

The jammer used in these experiments was a portable handheld broadband jamming device named CVSAL3405, which is capable of interfering in the following bands: 895-1000 MHz, 1195-1300 MHz and 2395-2500 MHz. The total output power on its three omni-directional antennas was 450mW, enough to prevent any communication within a radius of 20m over the specified bands. It is fitted with an On-Off button to switch on and off the interference. The jammer had the characteristics of ignoring the IEEE 802.11 MAC procedures and could constantly transmit energy on the

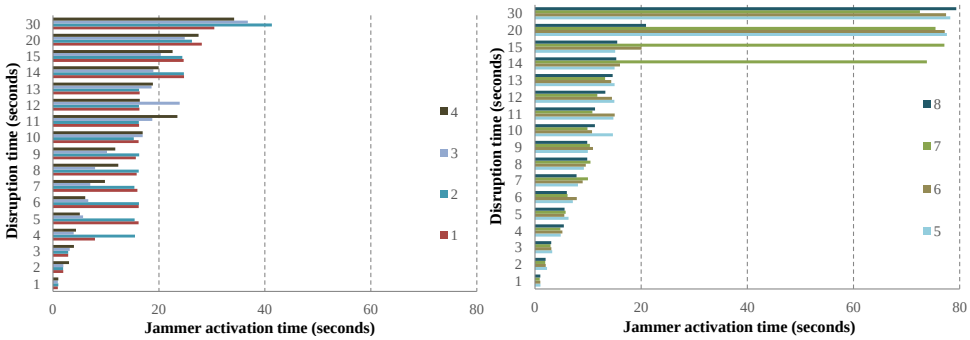
channel when switched on. In the experiments, the jammer was switched on (for a particular time) while frames were being sent from laptop B to laptop A. Once the jammer was activated, the wireless link was completely broken. When it was switched off again, laptop A and the AP tried to recover their link. The sniffer was used to capture the frame stream and to analyze the sequence of events that followed a jamming attack.

In order to make the experiments more observant, two different operating systems (i.e. Microsoft Windows 7 and Linux Ubuntu 12.0.4) were used at laptop A. Additionally, the experiments were also repeated for the cases where the laptop A was using the built-in NIC and in other experiments it was using an external USB Wi-Fi device (i.e. TP-LINK TL-WN822N) instead. Linux operating system was also used in laptop B for all the experiments. Table 2.3 portrays the combination of AP, operating system and NIC (used by laptop A) within our Wi-Fi network.

Table 2.2: Combination of hardware and software used to perform the experiments.

Combination	Operating System used at laptop A	NIC used by Laptop A	AP used in Wifi Network
1	Linux	Built-in	Linksys
2	Linux	Built-in	TP-Link
3	Linux	USB	Linksys
4	Linux	USB	TP-Link
5	Windows	Built-in	Linksys
6	Windows	Built-in	TP-Link
7	Windows	USB	Linksys
8	Windows	USB	TP-Link

For a particular experiment, the jammer attack lasted for a fixed specific time. For each combination of hardware and software, different experiments were performed where each one had different jammer activation time. The trace of frames captured by the sniffer before, during and after the attack depicted the impact of the jammer on the Wi-Fi link and was used to find the disruption time caused by the jammer. This disruption time was calculated by finding the difference between the last acknowledged UDP datagram sent before the jammer was activated and the first acknowledged datagram after the jammer was deactivated. In few of the experiments, the UDP data stream was dropped. In those cases, the instant at which association or re-association succeeded was considered to calculate the disruption time. Figure 2.5 shows the results of the experiments when eight different combinations of software and hardware (see Table 2.3) were used. As the jammer activation time was increased, the disruption time also increased. It is interesting to note that when the attack lasted for 10 or more seconds, the disruption time increased more rapidly than the jammer activation time. Additionally, the disruption time for the case when the laptop A utilized Linux operating system was less than the case where the laptop A used Windows operating system. Furthermore, with jammer activation time higher than 14 seconds, the network manager of Windows operating system assumed the interface to be down and waited for some time before sending the association request to the AP, while Ubuntu's network manager immediately tried to re-establish the link even after long disruption times. This finding is more evident in Figure 2.5 when the jammer



(a) Laptop A utilizing Linux operating system. **(b)** Laptop A utilizing Windows operating system.

Figure 2.5: Disruption time in connection of laptop A to AP caused by the jammer.

was active for 30 seconds: the reassociation strategy employed by Ubuntu's network manager make it more resilient towards jammer activity.

Finally, no differences were observed when the AP device was changed. This leads to the conclusion that, since association and re-association are client-driven mechanisms, a simple strategy implemented in the client's wireless driver or network manager software can help communications to recover early after a jammer attack.

2.4 Design of a Novel Detection Mechanism

The objective of this section is to present the novel adversary detection scheme called BAT. The proposed approach provides a high detection accuracy under varying number of stations operating over different transmission rates and frame sizes. In addition, the design flexibility and simplicity of proposed mechanism can allow easy adaptation of cooperative adversary detection scheme in managed networks, that can help to improve the detection accuracy in dense deployments.

2.4.1 Beacon Access Time

One of the most effective jammer detection mechanisms described in section 2.2 was based on CSTI measurements [105]. However, CSTI is highly dependent on the load of the cell due to the CSMA scheme defined by the IEEE 802.11; for example, the presence of a large number of legitimate transmitters will increase the measured CSTI given that a stations transmission may be deferred by an uncertain number of preceding frames that underwent a shorter backoff, had a higher priority, etc. As discussed in the following, if we measure CSTI but only for Beacons, we can keep those measurements between definite bounds, regardless of the cell load, due to the fact that beacons are prioritized over other transmissions.

Beacon frames serve a variety of functions, the most obvious of which are to identify an AP and to describe its capabilities. Notwithstanding, one of beacons' most relevant functions corresponds

to their contribution to the Timing Synchronization Function (TSF) [45]. STAs in the same BSS are synchronized to a common clock. In an infrastructure BSS, the AP becomes the timing master for the TSF by periodically transmitting beacon frames that contain the AP's timestamp in order to synchronize the timers of other STAs in that BSS. Due to this function, beacons must be prioritized over other frames.

Beacons are sent according to the Beacon Interval (BI) parameter (typically around 100ms), defining a series of Target Beacon Transmission Times (TBTT). At each TBTT, the AP schedules a beacon frame as the next frame for transmission, i.e., the beacon is pushed to the first position of the AP's transmission queue, overtaking any other pending frame. The transmission of a Beacon complies with the IEEE 802.11 standard access, and hence it might be delayed due to CSMA deferrals. However, beacon transmission queue's CW is kept to 0, which effectively disables the backoff procedure, and uses PIFS instead of DIFS. This gives beacons priority over any other transmission in the BSS

Table 2.3: Constants for IEEE 802.11g/n and a/n.

		IEEE 802.11g/n	11a/n
σ	Slot time	9μs	9μs
SIFS	Short Interframe Space	10μs	16μs
PIFS	Point Coordination Function InterFrame Space	SIFS+σ=19μs	25μs
DIFS	Distributed Coordination Function Interframe Space	SIFS+2× σ=28μs	34μs

and, in consequence, if at TBTT the medium is busy, the beacon is the first frame to be transmitted in the BSS after the channel is released.

For the above reasons, we define BA) to implement our malicious entity (cheater or jammer) detection scheme. At the AP, BAT is measured from the time at which the beacon is generated and placed at the head of the transmission queue (i.e. at TBTT), until the actual frame transmission start time. Figure 2.6 depicts the relationship between BAT, TBTT and Beacon Interval.

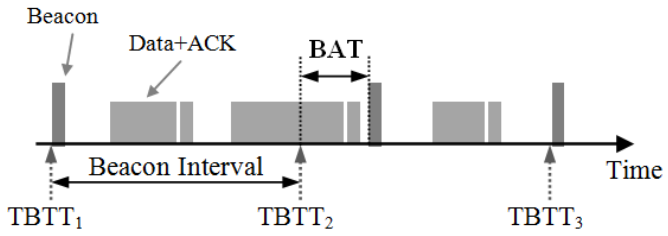


Figure 2.6: Representation of Beacon Acess Time (BAT).

2.4.2 Evaluation of BAT

In this section we study the different parameters that affect BAT under normal operation of the AP and its associated STAs, that is, when no jammer or cheater is present. In this case, BAT values will depend on the physical transmission factors associated with the active stations: number of stations, size of transmitted frames, physical transmission rate and offered load.

An analytical model to predict the BAT behavior is presented in [38], which is used along with simulations, to indicate the effects of BAT on different parameters.

2.4.2.1 Simulation Environment

We employ a custom-made event-based simulation software tool implemented at the Universitat Politecnica de Catalunya (UPC). Our simulation program has been written in C++ programming language and follows all of the IEEE 802.11 MAC protocol details, emulating as closely as possible the real operation of each element (user stations and access points). It allows the evaluation of different parameters, such as throughput and BAT values, in heterogeneous scenarios. Moreover, it includes the emulation of non-legacy stations and a jammer element. The correct operation of the simulation tool was verified by comparing the results obtained with the information published in [19], under identical simulation conditions. It has also been employed in published papers [63] [64].

2.4.2.2 Simulation and Analytical Results

The scenarios considered for this evaluation consist of a single AP serving a varying number of stations operating at different bit rates and transmitting frames with different payload sizes. All the figures included in this section present analytical and simulation results.

Figure 2.7 presents the complete trend of BAT values when different number of stations are used employing different rates and payload sizes within a cell under saturation conditions. In this case, stations employing higher transmission rates or shorter payload sizes result in smaller BAT value. It would take less amount of time to finish the transmission, and thus the AP would have to wait for shorter periods before sending its beacon frame in the event that the medium is sensed busy at a given TBTT.

BAT value is also dependent on the number of stations actively competing for the medium with the AP within a cell. The effect on the BAT value is more observant when less than 10 STAs are communicating to an AP. On the other hand, BAT performance tends to converge as the number of transmitting stations increases. This is due to the fact that the probability that the channel would be sensed busy at corresponding TBTT is closer to 1 when more than 10 STAs are active in a cell. This dependency on the number of stations is more evident when large frames are used, whereas the BAT value shows a faster convergence when stations send shorter frames. If an AP finds the medium frequently occupied by large frames, the average BAT value converges slower due to the increased variance in measured BAT samples. On the contrary, when small frames or no frames at all are found at TBTT, BAT measurements are less variable and thus convergence is faster.

From Figure 2.7 we also observe that the analytical model results coincide with simulation results with an error below 2%. BAT performance also depends on the cell load. Figure 2.8 corresponds

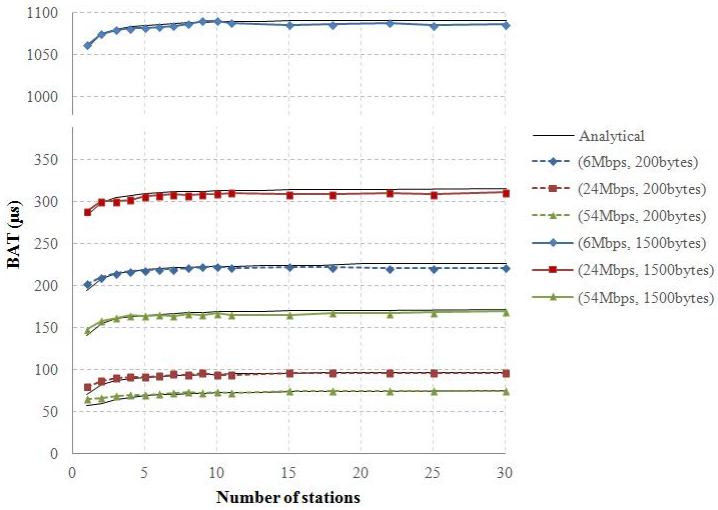


Figure 2.7: BAT values for different number of stations, transmission rates (6, 24 and 54 Mbps) and payload sizes (200 and 1500 Bytes).

to the scenario where 8 STAs are communicating to an AP with a constant physical transmission rate of 18 Mbps and a constant payload size of 1500 Bytes. In this case, the traffic offered by the stations is increased gradually to the saturation point. Saturation load conditions begin at the value of 12.6 Mbps. The BAT values before this point show a linear increase and after the above mentioned point, the values of BAT increase more steadily. Thus indicating the fact that the BAT values become steadier when cell load is increased and saturation is achieved.

Figure 2.8 also shows that analytical and simulation results present the same performance trend when offered load by the stations in the cell increases gradually.

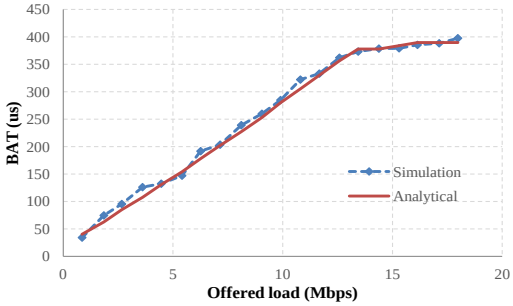


Figure 2.8: BAT values vs. offered load with 8 STAs at 18 Mbps.

2.5 Evaluation of BAT based Cheater and Jammer detector

In the previous sections we have proved that BAT can be predicted by an AP under normal operation of the WLAN, provided that the statistics of the traffic are known. In this section, we evaluate the effectiveness of a jammer detection mechanism based on BAT measurements. By means of simulations, we study how the presence of a jammer or a cheater STA makes BAT measurements deviate from the expected values. It is important to mention here that with downlink traffic, BAT is kept constant (it remains constant at PIFS) and thus the presence of a jammer will easily be detected. Conversely, the worst case scenario (i.e., the most interesting scenario) is found when all traffic is uplink. For these reasons, our evaluation only considers uplink traffic.

2.5.1 Evaluation of BAT in the Presence of a Cheater

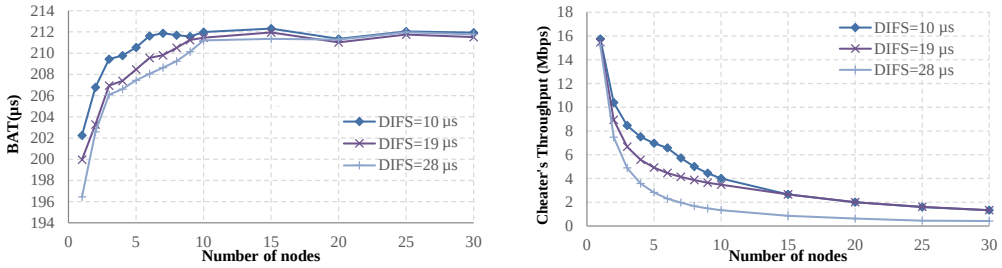
In this section, we observe the impact of a cheater in IEEE 802.11 networks and analyze its effect on the BAT value. Within this analysis we simulate scenarios where up to 30 STAs are communicating to a single AP (on the uplink) with a constant physical transmission rate of 24 Mbps and a constant frame size of 1000 Bytes. One of the stations acts as a cheater where it misuses the IEEE 802.11 MAC constraints in order to attain bandwidth gains. Also, the traffic offered by the stations is kept near saturation point.

2.5.1.1 Cheating Device with Varying DIFS

In the normal operation of IEEE 802.11 MAC at 2.4 GHz frequency band, the value of DIFS is set to the default value of 28μs (i.e. these MAC intervals depend on the physical layer). If IEEE 802.11a/n/ac is used at 5 GHz band, this value is increased to 34μs. A cheating device can be able to attain the access of the shared channel much more quickly if it can reduce its DIFS value. In this way, the cheater can prioritize its communication as compared to other stations.

We simulate the scenarios where we vary the number of stations from 1 to 30. The smallest Inter frame space used in IEEE 802.11 operating at 2.4 GHz is the SIFS and its default value is 10μs. The DIFS value for the cheater is increased from 10μs to 28μs. Again, for 5 GHz specifications, the SIFS interval is set to 16μs. Figure 2.9a indicates that the BAT value decreases when the cheater's DIFS is increased because having a larger DIFS value reduces its priority to access the channel. The BAT value is also increased as the number of stations increases. However, when there are more than 10 STAs, the BAT value converges, making it difficult to detect the cheater. This is due to the fact that with more stations, the probability to find the channel busy when a TBTT arises is greater.

Figure 2.9b indicates the throughput obtained by the cheater, when it reduces its DIFS value from the default (i.e. 28μs). The throughput of the cheater is increased when the DIFS value is decreased and is maximum when DIFS value is set to SIFS (i.e 10μs). Despite its clear advantage over other stations, the cheater still needs to contend for the medium and its throughput will therefore decrease as the number of competing stations increases.



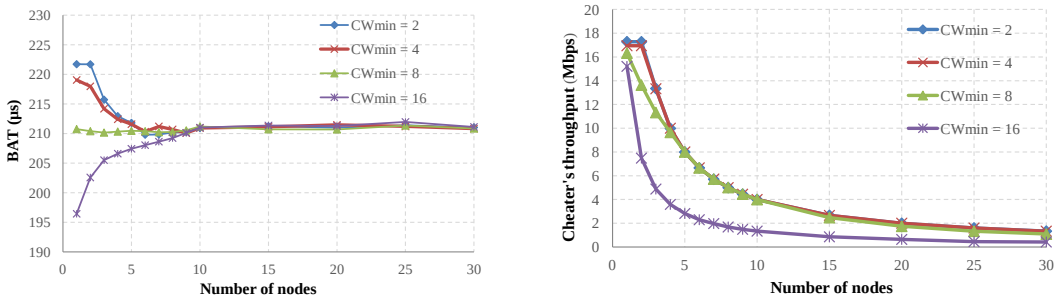
(a) Evolution of BAT values.

(b) Throughput of the cheater.

Figure 2.9: Simulation results showing BAT and throughput with the increase in number of nodes and the presence of a cheater varying its DIFS.

2.5.1.2 Cheating Device with Varying Minimum Contention Window

Following a DIFS period, stations willing to transmit a frame will backoff for a random number of time slots chosen between 0 and the value of the CW. The default value of minimum CW, CW_{min}, is 16. A cheater can utilize lesser CW_{min} value than 16 which can reduce its backoff time and thus increase its access probability. Figure 2.10a indicates the fact that the BAT value is greater when the



(a) Evolution of BAT values.

(b) Throughput of the cheater.

Figure 2.10: Simulation results showing BAT and throughput with the increase in number of nodes and the presence of a cheater varying its CW_{min}.

cheater uses a lower CW_{min} value. It is due to the fact that the cheater reduces its average backoff time after collision and is likely to gain the access to the shared medium much more quickly, as compared to the other stations. As in the case of reduced DIFS, the change in trend of BAT values is much more observant when less than 10 STAs are communicating within a cell.

The throughput of the cheater is considerably increased with the reduced CW_{min}, as shown in Figure 2.10b. It is also notable that the throughput of the cheater decreases with an increase in the number of stations and converges to the performance observed when the cheater employs the default CW_{min} value.

It is apparent from our simulation results that a cheater can cause detectable changes in the BAT

Figure 2.11: Characteristic diagram of On-Off jammer.

value of the AP, provided that the number of active STAs is not very large (e.g. smaller than 10). This change in BAT value depends on the strategy being employed to achieve bandwidth gains.

2.5.2 Evaluation of BAT in the Presence of a Jammer

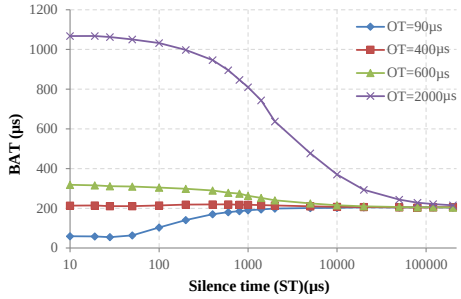
In order to understand the impact of jammers on BAT value, we simulate scenarios where one jammer injects false messages periodically. This jammer is placed randomly within the cell and is able to affect the transmission of both the AP and the STAs. Similar to [36], we use an On-Off jammer that jams/transmits continuously for a certain time (called Occupation time, or OT) and sleeps for a certain time (called Silence time, or ST), thus enabling a more thorough analysis than a simpler continuous jammer. We analyze the impact of the jammer by tuning its occupation and silence times. Figure 2.11, shows the implementation characteristics of the On-Off jammer. We simulate scenarios with 10 STAs communicating to a single AP (on the uplink) at a constant physical transmission rate of 24 Mbps and a constant frame size of 1000 Bytes. The jammer is present in the vicinity of the AP and therefore interferes with both transmitters and receivers.

2.5.2.1 Variation in Silence Time

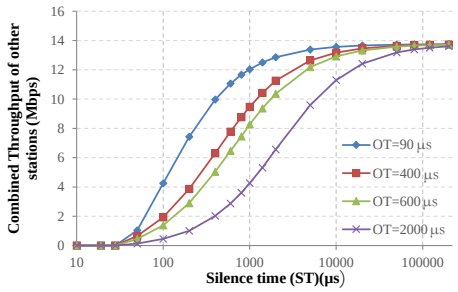
In order to understand the impact of silence time on the AP's BAT, we simulate cases where the silence time of the jammer is increased. In order to make our findings more concurrent, we utilize 4 different values for the occupation time. For a particular simulation scenario, the occupation time is kept constant, whereas the silence time between transmissions is increased from 10μs (i.e. SIFS) to 200ms.

Figure 2.12a illustrates the impact on BAT value when silence time of the jammer is increased. Logically, the BAT value is greater when the jammer occupation time is higher. As the silence time between transmissions is increased, the BAT values for all the combinations converge because the effect of the jammer is minimized. Increase in silence time allows channel to be more frequently available to legacy stations. Figure 2.12b depicts the effect on combined throughput of all legacy stations, in the presence of the jammer. It is also apparent that the throughput of the stations increases as the effect of the jammer is reduced. The combined throughput of all the stations for different jammer settings, converge to a single point when silence time becomes too large as to have any impact.

Figure 2.12a indicates that the least amount of variations in BAT value is for the case when 400μs of occupation time is used along with the varying silence time. That is, a jammer can remain unnoticed while utilizing the occupation time of 400μs, but still can be able to reduce the throughput of other legacy stations. This behavior is explained in the next section.

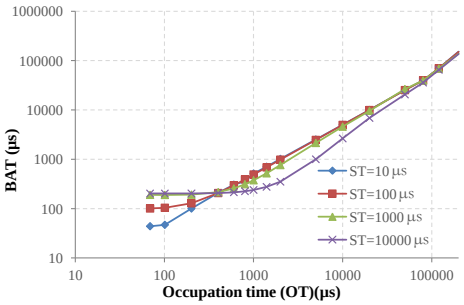


(a) Evolution of BAT vs. silence time (log scaled axis).

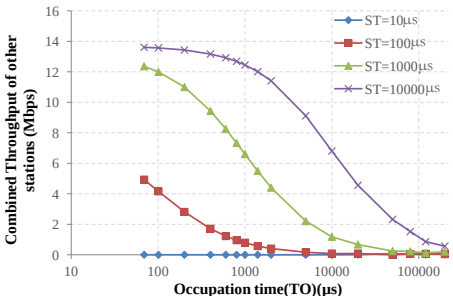


(b) Combined throughput of legacy stations vs. silence time.

Figure 2.12: Simulation results showing the effects on BAT and throughput in the presence of a jammer varying its silence time.



(a) Evolution of BAT vs. occupation time (log scaled axis).



(b) Combined throughput of legacy stations vs. occupation time.

Figure 2.13: Simulation results showing the effects on BAT and throughput in the presence of a jammer varying its occupation time.

2.5.2.2 Variation in Occupation Time

In order to understand the impact of occupation time over BAT values, in this simulation scenario we increase the occupation time of a jammer from 70μs to 200ms. We use 4 different constant silence times for each of the graphs plotted in Figure 2.13a. The trends indicate that, as the occupation time increases, BAT value is raised. At the occupation time of 400μs, the BAT values for all the trends converge. This is due to the fact that at 400μs occupation time the jammer mimics the behavior of a compliant station (i.e. sending 1000 Bytes frames at 24 Mbps).

Figure 2.13b indicates that, as the occupation time for the jammer increases, the combined throughput of all compliant stations decreases. It decays slowly in the case where we have a greater silence period. This is because having a greater silence period gives time to other stations to communicate with the AP. At 200ms occupation time, the throughput of the combined stations approaches 0.

Analysis of Figure 2.13a indicates that, as the occupation time is increased, the impact of silence time is reduced. But it is interesting to mention the case where the silence time is set to be 100μs:

Figure 2.13b shows that the combined throughput of legacy stations for the case of 100μs silence time is considerably reduced as compared to the silence time of 1000μs or 10000μs while causing similar BAT measurements.

2.5.2.3 Tunning the most effective On-Off jammer

In order to compare the impacts of change in silence and occupation time on the jammer, we analyze Figures 2.12a, 2.12b, 2.13a and 2.13b. We indicate the situation where the jammer can be most deceptive. It is evident that, when the jammer utilizes an occupation time of 400μs and silence time of 100μs, it mimics the behavior of normal station (i.e. there is no considerable variations in the BAT value) and thus remains un-detected. Although these jammer settings do not completely prevent communications in the attacked WLAN, they reduce its capacity by a 85%. Despite its apparent simplicity, an effective On-Off jammer that runs unnoticed to the BAT-based jammer detector must be aware of the frame length distribution of the attacked stations and try to mimic their behavior; this will actually require a rather sophisticated device. In conclusion, the BAT-based jammer detector will detect any type of jammer other than a well tuned reactive or intelligent jammer; for detecting the latter, it would be required that all stations in the WLAN participate in the detection, whereas our approach lies completely on the AP.

2.6 Conclusion

Due to high performance and low cost of operations, IEEE 802.11 based WLAN is the most widely used wireless standard. Unfortunately, due to its distributed MAC, the normal operations of IEEE 802.11 network relies on the behavior of stations to follow the set rules for transmissions. A selfish station can misbehave by modifying its MAC parameters to take advantage over other stations in a shared network. In addition, smart jamming devices can maliciously emit forged frames to disrupt legitimate communications. In this chapter, we first investigate the impact of different jammers in IEEE 802.11 based WLAN networks by utilizing both simulations and real Wi-Fi devices. While previous studies have considered the impact of malicious devices on WLAN network, we provide a clear insight about the problem in hand. We then define a new metric called BAT, and evaluate different parameters that impact BAT under normal conditions. We then study the detection performance of the proposed technique. By extensive simulation-based experimentation, we prove that: one, BAT can be predicted by an AP under normal condition; and two, BAT values become considerably different in the presence of a jammer and thus the AP can sense the presence of a malicious entity and take necessary actions. With the help of simulations, we analyze BAT detection behavior in the presence of a selfish node (i.e. a cheater) that wants to quickly acquire access of the shared channel. The results indicate that the cheater can be sensed by the AP using BAT. The results also verify that the BAT predictions are useful to detect the presence of a jammer in IEEE 802.11 based WLANs.

3

Analyzing the long range low power IEEE 802.11ah amendment

In recent years, license exempt radio communication have become attractive solutions due to their low cost and omnipresent access. The success of IEEE 802.11 based WLAN network is also partially based on its operation over the license exempt bands (i.e. 2.4 GHz and 5 GHz). However, as highlighted in Section 1.3, the increase in capacity demands due to enormous growth in global data traffic has lead to dense deployments of wireless networks that cover large number of devices. In addition, the concept of IoT (where many electronics devices sense, monitor and report real time data) has also fueled the data traffic, where several new wireless technologies (such as, LoRa, Sigfox, Weigthless, Telensa, NWave, ZWave, RPMA, and so on) have been proposed with the intent to provide connectivity over license free bands.

The most essential part of IoT infrastructure is the wireless communication system that acts as a bridge for the delivery of data and control messages between leave stations and central processing unit. However, the existing wireless technologies lack the ability to support a huge amount of data exchange from many battery driven devices spread over a wide area. Also, the cost of using license spectrum to support the IoT devices (by using standards like GPRS, LTE, WiMAX, NB-IoT, EC-GSM etc.) is too high that intuitively leads to the adaptation of IEEE 802.11 network as alternative access method.

In-spite of the increase in supported data rates in the current IEEE 802.11 standard, the next generation Wi-Fi networks are expected to face three major challenges. First, the popularity of WLAN networks will lead to massive unmanaged deployments with inherent interference/contention problems. Second, the rise in number of data craving applications, such as real time audio/video streaming, will result in significant increase in throughput requirements. Third, the requirement for WLAN networks to support complex outdoor communication scenario would result in added strain on the legacy protocols. For the first two problems, the future IEEE 802.11 amendment would have to improve over the contention and channel utilization problem along with mechanisms to improve per

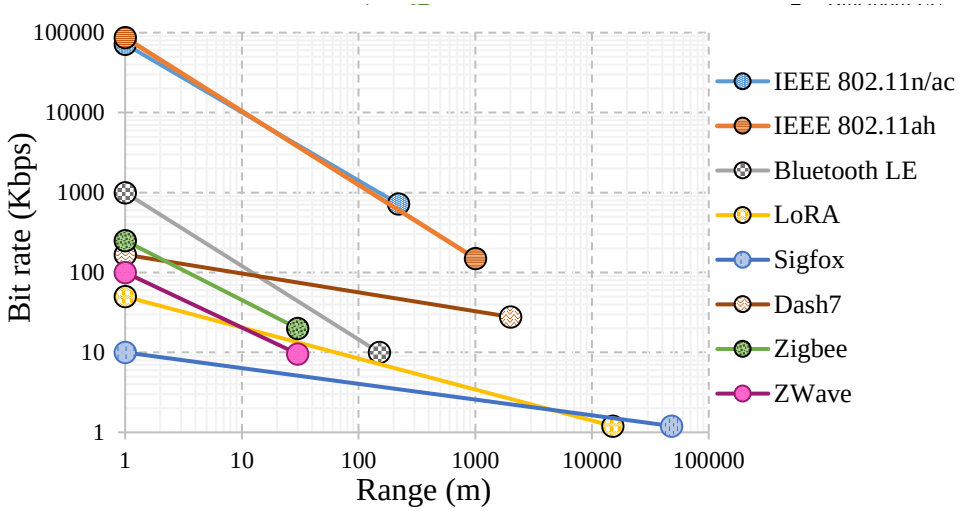


Figure 3.1: Comparison (in logarithm) of IEEE 802.11ah with legacy IEEE802.11 and different potential IoT wireless technologies.

user throughput methods. However, for the third problem, the IEEE 802.11 standard in its current form can not provide adequate performance efficiency due to the major challenge associated in operation of huge number of devices in contention based media over larger distances. In addition, the power of end user devices, severe interference caused by unmanaged overlapping networks, absence of power saving mechanisms and usage of unstable channel bands with poor signal penetration will add to the poor outdoor coverage performance.

In order to tackle the above mentioned problem and to support indoor as well as outdoor communication of large number of devices, the IEEE standards committee is in process to announce a new standard, called IEEE 802.11ah. This amendment is expected to operate over Sub 1 GHz (S1G) license exempt ISM band, where the transmission range of devices will be extended to a kilometer. Furthermore, each AP of 802.11ah amendment is expected to support more than 8000 associated devices, where group based contention procedure is used that divides all the stations into several groups and each group is assigned a non-overlapping period for transmission (thus avoiding collisions from numerous simultaneous attempts to send frames) [89]. Apart from supporting the IoT paradigm, the aforementioned characteristics even point out the possibility of IEEE 802.11ah amendment as a viable alternative technology to densely deployed legacy IEEE 802.11 based Wi-Fi networks.

In this chapter, we present the IEEE 802.11ah amendment that will enable new use and scenarios, such as Machine-to-Machine (M2M), smart cities, smart grid, smart agriculture and so on. These deployment scenarios correspond to dense deployments, where increased number of non-AP stations can result in overall loss in network throughput performance. Since future Wi-Fi networks is envisioned to be deployed in diverse indoor/outdoor environments, the objective of this chapter is to explore key innovations that will enable IEEE 802.11 standard to increase coverage with reduced

interference on other networks.

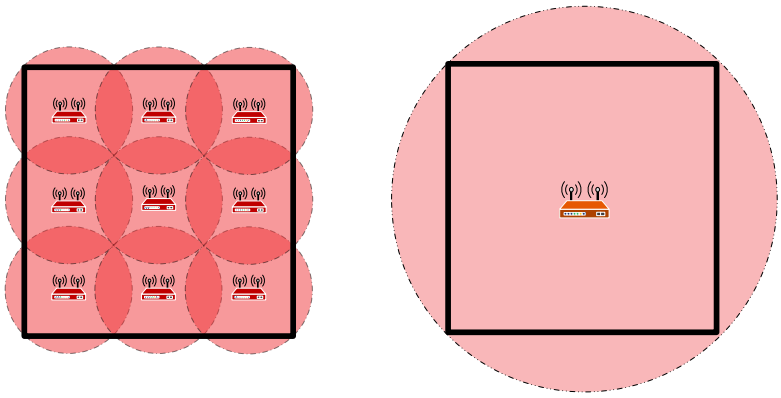
Most of the content presented in this chapter has been published in [16] and [73].

3.1 Motivation

The key to the concept and success of smart cities (an application area of IoT paradigm) which aims to improve the quality of life and alleviate public services in urban centers, is particularly based on exponential growth of different radio technologies. Smart cities take advantage of communication networks and sensors (i.e. IoT devices) to optimize various logistical operations (e.g. transport, electrical, etc.) to improve the quality of life of people residing in the cities. In today's smart cities, cellular and wireless sensor networks are the dominant technologies used to relay information towards a central processing office. Since the amount of information generated over such scenario is assumed to be huge and increasing (due to the increase of connected devices), there is a need to adopt universally accepted, cost effective and scalable communication technology within IoT frame work. IEEE-based WLANs (due to their ease of deployment and cost efficiency) could be used as viable alternative technology for smart cities only if the limitations of high power consumption and limited number of associated stations are overcome. Apart from WLANs, different standards have been proposed for communication process of IoT. This is particularly motivated by the range, data rate and mobility problems associated with Bluetooth and Zigbee (which are part of IoT ecosystem due to their availability in common consumer devices). Unlinke Bluetooth, the scalability problems are not common in Zigbee. However, the short transmission range is overcome by multihop facility that yields poor reliability. Low Power Wide Area Network (LPWA) technologies (such as LoRa, Sigfox, Weightless-P, RPMA, Dash7 etc.) have also been proposed to cover the requirements for IoT. However, these technologies lack the ability to provide QoS and are restricted by low data rates.

In recent years, tremendous proliferation of IEEE 802.11-based WLAN has been witnessed. The wider acceptance of IEEE 802.11 has resulted in mass deployments in diverse environments (e.g. homes, offices, streets, campuses, etc.) where different devices (e.g. smart phones, laptops, tablets, wearables, etc.) utilize the aforementioned standard as a major access method to connect to the Internet. A simple one-hop infrastructure deployment of legacy IEEE 802.11 (consisting of one AP and less than 100 non-AP stations) to support these massive number of devices results in the creation of high density WLAN, faces a well known saturation throughput loss [19] problem. The enormous contention problem created by the CSMA/CA protocol being employed by all stations within high density environment results in poor channel utilization. Moreover, in dense Wi-Fi deployments, even the interference from nearby co-channels can degrade the performance.

Lately, a task group of IEEE 802.11 (called TGah) was working on the draft version [44] of a new standard (called IEEE 802.11ah) which was proposed to support IoT devices as well as to extend the range of Wi-Fi enabled stations. This new standard is intended to support low cost mode of operation, with greater coverage area, and thousands of associated nodes per cell. The advantage of IEEE 802.11ah amendment over legacy IEEE 802.11 and other competing LPWA standards is illustrated



(a) Densely deployed overlapping legacy IEEE 802.11 cells.

(b) Outdoor large range of IEEE 802.11ah.

Figure 3.2: Comparison of legacy IEEE 802.11 with IEEE 802.11ah in providing coverage over $1km^2$ area.

in Figure 3.1. With improved range and high capacity gains, IEEE 802.11ah amendment appears an attractive alternative that can support numerous use cases. In 2016, Wi-Fi Alliance announced the Wi-Fi HaLow (which is certification program for a selected subset of features of IEEE 802.11ah) specifications for products incorporating IEEE 802.11ah technology.

The macro coverage of IEEE 802.11ah is enabled by using of S1G transmission band, which enables coverage to be provided to dense clustered deployments of non-AP stations. Apart from being a wireless technology for IoT devices, IEEE 802.11ah is intended to be highly suitable for long range wireless communication with resilience against large delay spread within multipath environments. Therefore, the key use cases of interest associated with IEEE 802.11ah standard (highlighted in section 3.3.3) are outdoor extended range hotspots and outdoor Wi-Fi network for cellular offloading, that suggest the viability of IEEE 802.11ah as an alternative to dense deployments. As highlighted in Figure 3.2, a wider coverage range with the ability of managing a large number of non-AP stations can result in IEEE 802.11ah to be an attractive alternative for ultra dense Wi-Fi deployments.

In this chapter, we highlight the key technological enhancements proposed for IEEE 802.11ah standard. We first point out the necessity of the long range amendment. We then elaborate the use cases and provide an overview of key technological features proposed for IEEE 802.11ah amendment. Next, we compare the IEEE 802.11ah with previous IEEE 802.11 amendments. Lastly, we highlight some of the important challenges expected for IEEE 802.11ah

3.2 Related Work

The upcoming IEEE 802.11ah amendment proposes to open new avenues for WLAN operations over license-exempt bands. It aims to organize communication between various devices used in IoT applications (such as smart grids, smart meters, smart houses, health-care systems and smart industry etc.). Furthermore, the proposed amendment also intends to be highly suitable for long

range outdoor Wi-Fi communication. The IEEE 802.11ah aspires to improve the operability of legacy IEEE 802.11 standard by introducing methods to allow access of massive number of stations over large coverage area.

In order to expose the key mechanisms of the upcoming IEEE 802.11ah amendment, the authors in [3] provide a comprehensive overview. Similarly, the authors in [50] and [6] explain in detail the distinct features of IEEE 802.11ah. In [86], the authors highlight the importance of IEEE 802.11ah standard as one of the key enabling technologies for low cost, energy efficient and massive deployment for IoT devices in the future. Furthermore, the authors evaluate maximum achieved throughput in three different Modulation and Coding Schemes (MCS) of IEEE 802.11ah using significant assumptions. In [50], the authors show results indicating the performance of IEEE 802.11ah in terms of rate and range. In addition, they provide a comparison of IEEE 802.11ah and IEEE 802.11b/n for three indoor cases without taking into account outdoor scenarios, which are also an important use case for IEEE 802.11ah. The work in [15] also provides as extensive overview of IEEE 802.11ah amendment. Furthermore, the authors summarize standardization procedures as well as the technical challenges expected in the adaptation of IEEE 802.11ah standard. Authors in [29] define different innovative use cases for IEEE 802.11ah standard. Among the proposed use cases, the authors highlight the case where IEEE 802.11ah standard will allow the increase in range so as to provide outdoor connectivity to many devices (placed within homes, campus or shopping malls etc.).

Since, the DCF protocol is expected to create severe contention and hidden node problems in large range networks, the IEEE 802.11ah proposes to use a novel optional medium access control protocol, called Restricted Access Window (RAW). This method allows the grouping of stations with similar characteristics into RAW group. RAW groups are allowed to contend for access in pre-assigned time slots within a beacon interval (refer to Section 3.3.6.4). Authors in [61, 77, 109] have indicated methods to improve RAW based group access mechanism, where the size of contending group and duration of RAW are varied to acquire optimal performance. The problem of hidden terminal within IEEE 802.11ah network is explored by authors in [28, 106], where devices detected to be hidden from each other are proposed to be distributed into different groups.

Authors in [98] describe the implementation of MAC and PHY layer of IEEE 802.11ah within NS-3 simulator.

3.3 Overview and Fundamentals of IEEE 802.11ah Amendment

Through IEEE 802.11ah amendment, the IEEE 802.11 standardization committee is in process of extending the application area of WLAN networks by improving the transmission range along with the ability to support large number of stations. Unlike the previous IEEE 802.11 amendments (i.e. 802.11a/b/g/n/ac) that were designed to provide high data rates over smaller coverage area (i.e. 150-200m), the IEEE 802.11ah amendment aims to support large number of devices with lower data rates over longer transmission range, with added advantage of having the ability to even provide greater bandwidths at longer distances. It is expected that Wi-Fi APs, that are currently widely deployed, will

also include the support of IEEE 802.11ah in future.

In the following sections, we highlight the need and significance of this new WLAN standard.

3.3.1 Basic necessity

The IEEE 802.11ah project, approved in 2010, was driven by the availability of unused wireless resources at the S1G channel (except for TV white spaces), which have favorable propagation characteristics as compared to 2.4/5 GHz. In addition, saturation of 2.4/5 GHz band caused by the irregular/unmanaged dense deployments, the range anomaly encountered by current WLANs and the need for ubiquitous wireless access resulted in IEEE standards committee to explore operations that could reduce congestion. Since, the design of IEEE 802.11ac standard was also under progress at the same time, it was envisioned by IEEE 802.11 working group that the features proposed for IEEE 802.11ah could be based on IEEE 802.11ac, that would help in the design of WLAN chips operating over quadruple band.

3.3.2 Project Definition and Scope

IEEE 802.11ah proposes to incorporate power efficient and improved MAC mechanisms (to support large number of stations with extended range) in WLAN networks. Also, the PHY layer is rebuilt and optimized for operation over S1G. However, the higher network layers remain consistent with the existing IEEE 802.11 standard. Since all the previous evolutions of IEEE 802.11 have been towards providing higher data rates (that results in decreased transmission range and increased power consumption), this standard is being designed to address low-powered devices, long range links and scalable solutions. The amendment aims to target high number of devices present indoor as well as out-door with low to moderate traffic demands. Furthermore, it intends to incorporate power saving mechanisms (to accommodate the IoT requirement) along with enhanced channel access and throughput features (to maintain and improve on the existing Wi-Fi experience).

Thus, the scope of IEEE 802.11ah amendment is to modify the PHY and MAC layer of legacy IEEE 802.11 standard to operate below 1 GHz band (for extended range and ubiquitous access in less interfered band) with the ability to support large number of associated stations. To be more precise, IEEE 802.11ah aims to connect around 8000 devices per AP (placed indoor as well as outdoor) with coverage in the km scale. Also, the standard defines multitude of bit rate variations (from 150 Kbps to 346.67 Mbps) to support a wide variety of services and applications. At the same time, IEEE 802.11ah aims to leverage the already existing Wi-Fi and IP ecosystem for connectivity to the available network/Internet, for effortless configuration and for easy pairing of APs and stations. To summarize, the scope of IEEE 802.11ah standard can be described by the following points,

1. **Improved power saving**
   In-order to support IoT devices with power constraints, this new amendment is expected to provide mechanisms for longer sleep times and reduced requirements for wakeup.

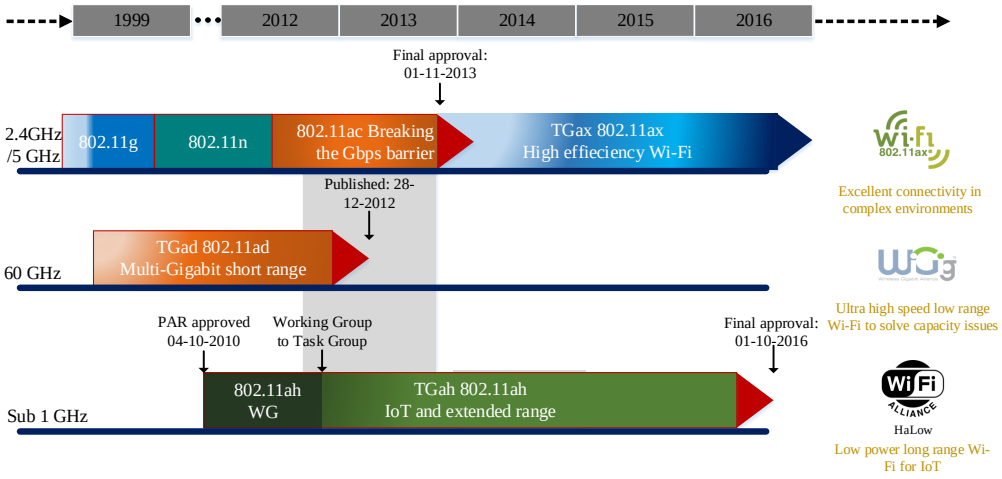


Figure 3.3: Evolution path of IEEE 802.11.

2. **Enhanced channel access mechanism**
   To address the problem of contention/collisions due to massive number of associated station per AP, IEEE 802.11ah intends to define group-based channel access method, where each station has prior information of when it will be able or have to access the shared channel.

3. **Reduce channel occupancy overheads**
   By reducing the overhead induced by the current frame exchange (i.e. header length etc.), IEEE 802.11ah aims to enhance the throughput of associated clients.

3.3.3 Application Environments and Use Cases

The general characteristics of IEEE 802.11ah standard make it attractive for various applications. In the following section, we provide details of three important use cases of the aforementioned standard.

3.3.3.1 Smart Sensors and Meters

In this use case, the IEEE 802.11ah AP connects to a large number of sensor devices that operate at indoor as well as outdoor environments. Therefore, this use case is characterized by high contention (where thousands of station contend for the shared channel) and stations without mobility. The connected devices are mostly battery driven and execute short-burst of transmissions. The AP to station ratio is expected to be of 1/6000. In this use case, traffic offered per device is of tens of Kbps or less. The most common environment for this scenario are large indoor spaces and outdoor in urban, suburban and rural environments. Figure 3.4, shows the characteristics of the foregoing use case.

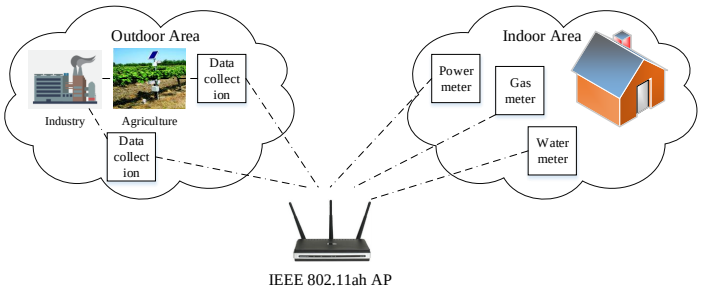


Figure 3.4: Smart sensors and meters use case.

3.3.3.2 Backhaul Connection for Sensors

By exploiting its large coverage, IEEE 802.11ah networks would also be used as backhaul to provide intermediate step in communication between short range wireless technologies and distant data collectors. For example, IEEE 802.15.4 sensor devices show extended battery life, however, their transmission range and available data rates are very low (few Kbps). Thus, a scenario in which IEEE 802.15.4 routers gather data from leaf devices and forward information to servers using IEEE 802.11ah links can be used to cover the communication gap between servers and low range wireless networks. This use case is addressed to outdoor industrial and rural environments with lower than 1 Mbps of offered traffic per station, along with stationary or low mobility devices. The AP to station ratio is of 10/500. Figure 3.5 provides a glimpse of the foregoing use case.

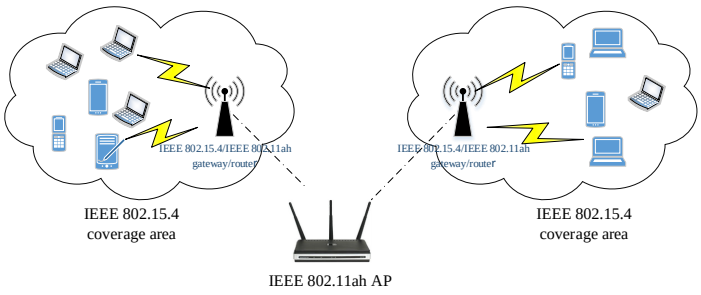


Figure 3.5: Backhaul use case.

3.3.3.3 Extended Range Hotspot and Cellular Offloading

Both high throughput and long transmission range make IEEE 802.11ah an attractive method for expanding hotspot range and for traffic offloading of cellular networks (which is a significant issue for operators and vendors due to mobile traffic explosion and cost associated with it). This use case is addressed to outdoor use in urban and suburban environments with lower than 20 Mbps of bit rate requirement along with pedestrian mobility. The AP to station ratio is of 1/50. Figure 3.6, shows the characteristics of the aforementioned use case.

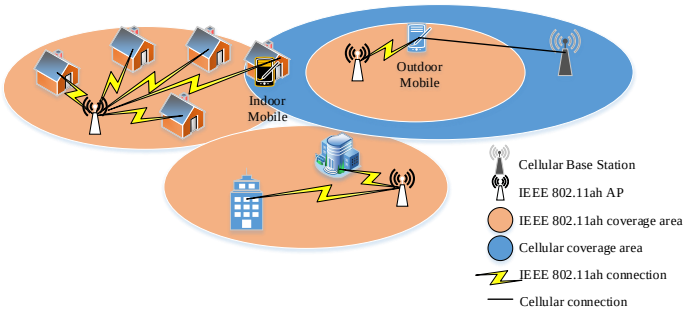


Figure 3.6: Extended range hotspot and cellular offloading use case.

Table 3.1: Functionality Comparison of different IEEE 802.11 standards.

	802.11a/g	**802.11n**	**802.11ac**	**802.11ah**
Antenna Configuration	1 × 1 SISO	4 × 4 MIMO	8 × 8 MIMO	4 × 4 MIMO
Highest order Modulation	BPSK to 64-QAM	BPSK to 64-QAM	BPSK to 256-QAM	BPSK to 256-QAM
Channel Bandwidth	5, 10 MHz(11a), 20 MHz(11a/g)	20 and 40 MHz	20, 40, 80 and 160 MHz	1, 2, 4, 8, and 16 MHz
FFT size	64	64 (20 MHz), 128 (40 Mhz)	64, 128, 256, and 512	32, 64, 128, 256, and 512
Year Approved	1999/2003	2009	2014	2016
Minimum and Maximum Bit rate	6 and 54 Mbps	6.5 and 600 Mbps	6.5 and 6933.3 Mbps	0.15 and 346.67 Mbps
Maximum supported stations	2007	2007	2007	around 8000

3.3.4 Notable Physical and MAC Layer Features

In order to meet the requirements defined by different use cases in previous section, IEEE 802.11ah amendment proposes modifications to be made at the PHY and MAC layers of the legacy IEEE 802.11ac, so as to allow operation below 1 GHz. Due to scarce availability of S1G bands, the PHY layer modifications are intended to improve the spectral efficiency. Furthermore, because of the intention of having numerous IoT devices contending for the shared resources, the MAC of this new amendment is designed to administer scalable operations. In addition, the proposed MAC features assist to improve power efficiency among stations that have limited energy resources. It is pertinent to mention here that due to the redesigned MAC and PHY layer, the new standard is not anticipated to be backwards compatible. Table 3.1 summarizes the key features of IEEE 802.11ah and compares them with previous proposed amendments of IEEE802.11.

In the following section, we give a brief description of PHY and MAC layer enhancements pro-

Table 3.2: Physical layer parameters of IEEE 802.11ah.

Parameter	Value	Parameter	Value
Carrier Frequency	863 - 868 MHz (Europe), 902 - 928 (US)	**Bandwidth**	1, 2, 4, 8, 16
Number of data/total sub-carriers per OFDM symbol	24/32 (1MHz), 62/64 (2 MHz),108/124 (4 MHz),234/256 (8 MHz),468/512 (16 MHz)	**Preamble type**	Short (1MHz), Long (2, 4, 8, 16 MHz)
Number of Spatial Streams (ss)	1-4	**Subcarrier spacing**	31.25 (kHz)

posed for IEEE 802.11ah standard.

3.3.5 Physical Layer

The PHY layer of IEEE 802.11ah inherits its main characteristics from IEEE 802.11ac, but is adapted to operate at S1G frequency band. It is designed to operate by utilizing OFDM along with MIMO including Multi-User MIMO (MU-MIMO) over the downlink. Additionally, it supports various MCSs (i.e. from MCS0 to MCS10). However, given limited capabilities of associated stations devices and low data transfer requirements for certain applications, high-order modulations or even multiple streams are not likely to be widely supported. Based on this argument, support of MCS 0 to MCS 10 for 1 and 2 MHz channel bandwidth, along with a single spatial stream is mandatory for each non-AP station. However, for AP, it is mandatory to support MCS 0 to MCS 7 for all supported channel bandwidths along with a single spatial stream. Table 3.2 highlights the key PHY layer characteristics of 802.11ah [16].

In the following section, we describe the main PHY layer amendments proposed for IEEE 802.11ah that substantiates its operation for the IoT devices.

3.3.5.1 Available Spectrum

Due to limited availability of license exempt spectrum in 1GHz and owing to the intention of enabling Wi-Fi devices to gain access of channel for short-term transmissions, the basic channel width utilized in IEEE 802.11ah is 1 MHz. However, channel bonding can be applied to bond two or more adjacent available channels in order to create 2 MHz or greater channel, so as to achieve the capability of providing higher data throughputs. For global interoperability, 1 and 2 MHz modes are mandatory to support low bandwidth operations. Table 3.3 highlights the available 1 MHz channel count allocated for IEEE802.11ah within different countries. It is expected that early commercial devices will support up to 4 MHz.

It can be observed from Table 3.3, that higher mode operations are possible in the China and United States, where IEEE 802.11ah amendment could be even used to provide higher bandwidths.

Table 3.3: 1 MHz bands allocated by different countries for IEEE 802.11ah.

Regulatory domain	Europe	United States	Japan,	China	Korea	Singapore	Australia
Number of 1 MHz channels	5	26	11	24	6	8	13

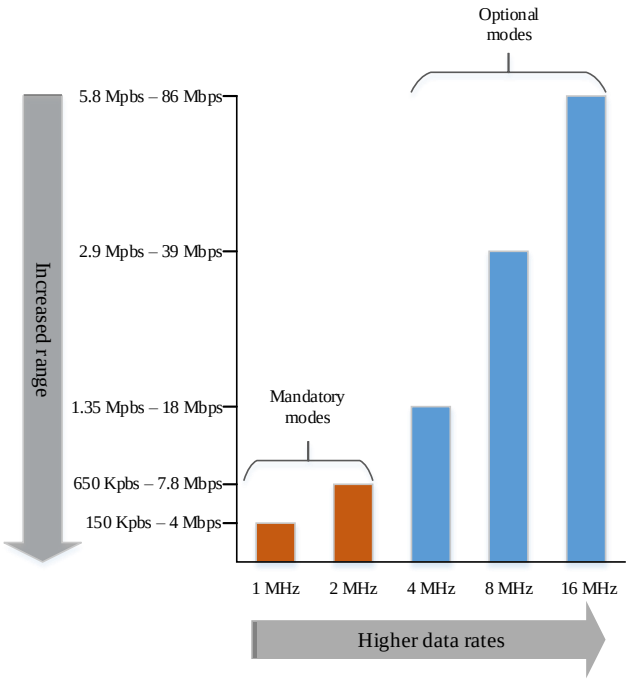


Figure 3.7: Different transmission modes to extend range and enable new application areas.

3.3.5.2 Transmission Modes

One of the main requirements for this amendment is to extend the range of operation and thus to facilitate devices (placed at greater distances) that require low data rates. This aforementioned requirement is fulfilled by combined usage of 1 MHz wide transmission and a new MCS (called MCS 10). This scheme is effectively MCS0 with an addition of 2x repetition (where OFDM symbols repetition is performed with sub-carrier permutation). Apart from 1 MHz, IEEE 802.11ah standard also supports 2, 4, 8 and 16 MHz where the PHY layer is effectively 10 times down-clocked version of IEEE 802.11ac, i.e. OFDM symbol in IEEE 802.11ah standard is 10 times longer than IEEE 802.11ac. Table 3.4 shows the different MCS levels supported by IEEE 802.11ah. These data rates correspond to the use of a single spatial stream, where the N times increase can be expected by using N streams.

Figure 3.7 signifies the benefits achieved in utilizing different transmission modes[1]. Low cost battery operated sensor stations can benefit by using 150-Kbps over 1 MHz channel. These IoT devices can transmit for short duration with lightweight messages, and can remain in sleep state for

[1]The expected data rates correspond to the usage of a single Spatial Stream (SS)

Table 3.4: Data rates (in Mbps) corresponding to different MCS levels for single spatial stream (where the shaded cells represent mandatory modes of operation).

	Modulation	Coding rate	1 MHz	2 MHz	4 MHz	8 MHz	16 MHz
MCS0	BPSK	0.5	0.30	0.65	1.35	2.925	5.85
MCS1	QPSK	0.5	0.60	1.30	3.00	6.50	13.00
MCS2	QPSK	0.75	0.90	1.95	4.50	9.75	19.50
MCS3	16-QAM	0.5	1.20	2.60	6.00	13.00	26.00
MCS4	16-QAM	0.75	1.80	3.90	9.00	19.50	39.00
MCS5	64-QAM	0.67	2.40	5.20	12.00	26.00	52.00
MCS6	64-QAM	0.75	2.70	5.85	13.50	29.25	58.5
MCS7	64-QAM	0.83	3.00	6.50	15.00	32.50	65.00
MCS8	256-QAM	0.75	3.60	7.80	18.00	39.00	78.00
MCS9	256-QAM	0.83	4.00	NA	20.00	43.335	86.67
MCS10	BPSK	0.5	0.15	NA	NA	NA	NA

most of the time.

3.3.5.3 Restricting the Effects of Fading

In order to tackle time and frequency selective fading over narrow band channels, the IEEE 802.11ah implements a new feature called Sub-Channel Selective Transmission (SST). This scheme allows stations to rapidly switch among specific set of sub-channels during transmission (see Figure 3.8), where the channel is selected based on measurements indicating short term fading conditions and/or the level of interference from other stations.

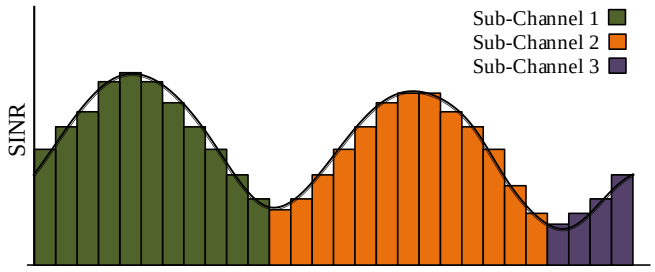


Figure 3.8: Sub-channel selection based on channel conditions.

IoT devices that usually don't require the use of maximum bandwidth (due to power constraints) benefit from this scheme where sub-channels are used instead of the complete channel. SST is implemented by the inclusion of special SST information element in the Beacon frame, through which the AP informs the stations of the sub-channels assigned for uplink and downlink. The width of sub-

channels used in SST is less than or equal to 2 Mhz. The AP periodically transmits sounding frames over the allowed sub-channels, that help a station to decide in selecting sub-channel(s) for transmission. In particular, this selection procedure is based on the channel conditions and the location of the IEEE 802.11ah station.

3.3.6 MAC Layer

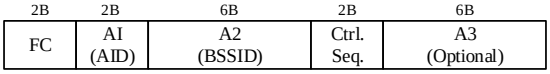
The MAC layer of IEEE 802.11ah includes improvements to specifically address the requirements of long range communications and IoT use cases. It is is optimized to encompass low power mode of operation, redefining short frame transmissions to reduce overhead caused in channel occupancy time and methods to support large number of devices over a single cell. In the following section, we describe in detail the MAC layer enhancements proposed by the IEEE 802.11ah.

3.3.6.1 Compact Frame Format to Increase Throughput

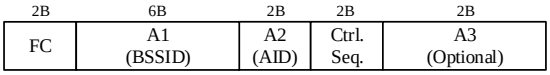
IEEE 802.11ah stations in most of the use cases are expected to operate at low data rates and intend to exchange small data frames. Specifically for IoT devices, the overhead associated with frame headers (e.g. MAC header) may be considerable when compared to the size of the payload. This problem is worsened with the massive overhead created by frame exchange of increased number of associated stations with the IEEE 802.11ah AP. In order to counter overheads and to increase the efficiency and thus the overall throughput, the MAC design of IEEE802.11ah introduces compact frame formats. These formats result in reduced power occupancy and power consumption for both the transmitter and receiver. In the following paragraphs, we describe header compression methods used in IEEE 802.11ah.

1. **Short MAC Header Format**
   The significant change in the new header design is the inclusion of only two mandatory address fields as compared to four addresses fields present in the legacy MAC header. Two address fields are enough for the frame exchange to occur between AP and associated stations. The QoS and High Throughput (HT) fields are shifted into Signal (SIG) in PHY header and Duration/ID field is removed (because virtual carrier sensing is not supported when short MAC header are used). Figure 3.9 provides a comparison between the MAC headers devised for IEEE 802.11ah and the one used for legacy IEEE 802.11. Thus, the short MAC header is able to reduce the overhead (from 30 Bytes to 14 Bytes).

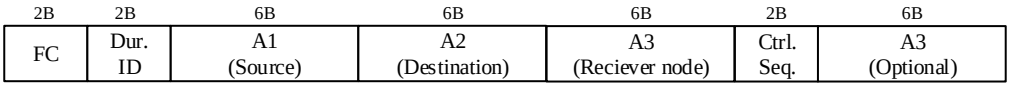
2. **Short MAC Control Frames**
   Apart from the duration field, the MAC control frames in legacy IEEE 802.11 do not carry any necessary payload and are used to indicate different MAC events. To reduce the overhead induced by control frames, the IEEE 802.11ah utilizes Null Data Packets (NDP) which contain PHY header without data, MAC header or FCS. Different control frames (e.g. CTS, ACK, Power Save-Polling (PS-Poll) frame, etc.) are modified to NDP frame format to reduce protocol overhead.



(a) IEEE 802.11ah Downlink MAC header format.



(b) IEEE 802.11ah Uplink MAC header format.



(c) IEEE 802.11 legacy MAC header.

Figure 3.9: Comparison of MAC header format between IEEE 802.11ah and legacy IEEE 802.11.

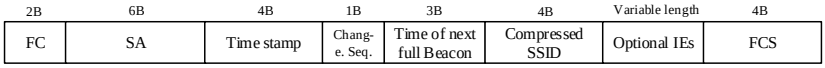


Figure 3.10: Short beacon frame defined for IEEE 802.11ah.

NDP frames were first introduced by the IEEE 802.11ac amendment to be used for channel calibration required for beamforming. Since the received sounding symbols in the PHY header were used for calibration, the NDP frames did not have any payload. IEEE 802.11ah builds on NDP frame proposed for IEEE 802.11ac, where instead of including no information, some useful data is added in the SIG field of the PHY header that indicates the purpose of the NDP frame. For example, in the NDP frame, the SIG field includes ACK ID corresponding to ACK frame.

3. **Short Beacon Frames**

Beacon frames in legacy IEEE 802.11 are usually transmitted with the lowest rate (to be received by stations located at the cell edge) to announce the presence of an AP. These beacons contain Service Set Identifier (SSID) and Basic SSID (BSSID)[1] information along with the supported data rates, security requirements and parameter set to indicate the channel number. In addition, the AP can also include the Traffic Indication Map (TIM) in the beacon and transmit periodically to polling stations that have data available at the AP, but are in power saving mode. Therefore, beacon frames also tend to create unnecessary overhead by excessive medium occupancy and by the power consumed by the AP to transmit as well as the associated stations to receive.

To reduce this overhead, IEEE 802.11ah defines two beacon types: full and short. The purpose of short beacon frames is to announce the presence of AP and synchronize with stations. These beacon types are intended to be transmitted more frequently than the full version.

[1] A BSSID is an identifier that describes the BSS.

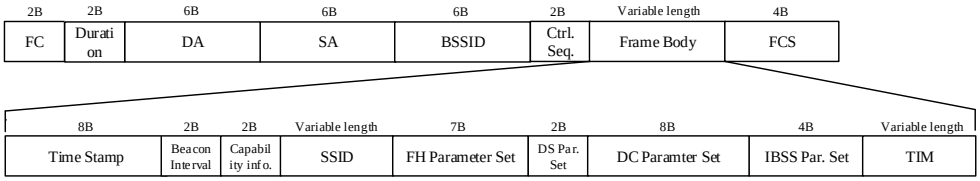


Figure 3.11: IEEE 802.11 legacy beacon frame.

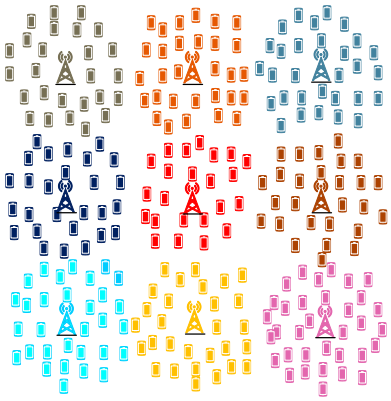


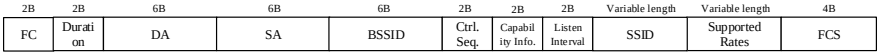
Figure 3.12: IEEE 802.11ah BSS color scheme.

As compared to legacy beacon (shown in Figure 3.11), the short beacon frame proposed by IEEE 802.11ah (shown in Figure 3.10) does not include some of the fields. The destination field is removed because beacons are always broadcast. The BSSID is also not included because it is the same as source address. The time stamp field used for synchronization with the associated stations, is reduced to 4 Bytes (from 8 Bytes), which includes information indicating the time to next beacon. The SSID information element with variable length is replaced with a fixed size compressed SSID field of 4 Bytes. Compressed SSID is a hash function of full SSID.

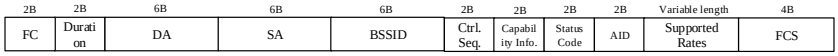
3.3.6.2 Improving Spatial reuse (BSS color)

One of the drawbacks of extended range of IEEE 802.11ah is that multiple BSS can overlap and result in added interference which results in the increase of collisions/interference. To improve the co-existence of multiple overlapping BSS, TGah has introduced a technique, referred to as BSS color, that allows the improvements in the spatial reuse (the total number of possible concurrent transmission in the network).

It is an innovative scheme to increase throughput and medium efficiency of dense WLAN networks, where each BSS is assigned a specific color (in terms of bits designated in Legacy Signal (L-SIG) field of physical header). A station upon receiving frames from neighboring BSS, can abandon the reception process assuming the channel to be idle during that transmission and thus increase its transmission opportunities. However, if the BSS color indicates that the detected transmission is by stations within the BSS, the station defers its transmission. This scheme was initially proposed for



(a) Association request frame.



(b) Association reposne frame.

Figure 3.13: Frames exchanged between non-AP stations and AP by legacy IEEE 802.11 for association

IEEE 802.11ah standard, but has also shown remarkable improvements when used for IEEE 802.11ax use cases (see Section 4.4). With the help of Figure 3.12, we describe the effects of BSS color, where different stations within multiple BSS operate by utilizing various color bits.

3.3.6.3 Support of large number of associated stations

Since IEEE 802.11 was only designed to cover small to moderate networks sizes, the fundamental limit to support large number of stations is dependent on the allocated space for different fields in the management frames. Following paragraphs describe two important modifications proposed in IEEE 802.11ah to enhance the possibility of large number of associated non-AP stations per AP.

- **Hierarchical Grouping based Association ID field**

  In legacy IEEE 802.11, the connection and association mechanisms are applied at the link layer. The basic connection process of station with AP is accomplished through the exchange of frames such as: Probe request, Probe response, Authentication request, Authentication response, Association request and Association response. Once the station identifies a compatible WLAN network (on which it is already authenticated), it initiates the association request. Upon successful association, the station receives from AP, among several other parameters, a parameter called Association ID (AID) which is part of association response frame sent by the AP. The AID is used to identify the station and for delivery of buffered frames for stations in power saving mode. Through Figure3.13, we describe the frame structurer of association process. The 16 bits AID field in the association response frame is assigned a value between 1 to 2007 (even though it is 16 bits long), where the two most significant bits are set to 1 and rest 2008 to 16,384 values are reserved.

  In order to increase the number of associated/supported stations, IEEE 802.11ah utilizes a novel hierarchical AID structure. The AID assigned by the AP during association consists of 13 bits and thus the number of stations that it can associate is up to $2^{13} - 1$ (= 8,191). AID structure consists of four hierarchical levels (i.e. page, block, sub-block, and station's index in sub-block).

  IEEE 802.11ah utilizes the aforementioned AID structure to group stations based on similar characteristics (e.g. traffic pattern, location, battery level etc.).

- **Enhanced traffic indication map field**

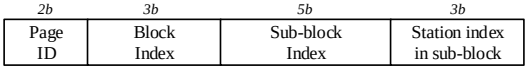


Figure 3.14: Structure of AID in IEEE 802.11ah MAC.

The legacy IEEE 802.11 envisioned the use of battery powered WLAN devices and introduced the TIM field (shown in Figure 3.11) that indicates the presence of buffered traffic at the AP for a station. Figure 3.15 shows the TIM information element. The essential part of TIM is the

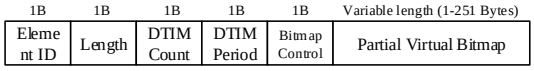


Figure 3.15: Traffic Indication Map information element.

virtual bitmap, which is composed of 2008 bits. Each bit is connected to the association ID (with 251 Bytes, a maximum of 2007 AIDs can be supported with one TIM). If traffic is buffered for an AID (station), the bit corresponding to it is set to 1 and vice versa.

In case there is a large number of power saving stations in the network, the TIM partial virtual bitmap for IEEE 802.11ah can become huge. To solve this problem, TGah proposes to use encoded TIM structure to correspond to the hierarchical AID structure. A new technique called TIM and page segmentation is introduced, where the AP can divide the complete virtal bitmap page into numerous page segments. Each page segment contains a subset of AIDs. Thus, a hierarchical classification of stations into groups along with the definition of two categories of beacon is designed. The two types of beacons are: Delivery TIM (DTIM) beacon and TIM beacon. Every station is expected to listen to the DTIM beacon, which includes information about the buffered data for each group of stations. The TIM beacon informs a group of stations about the amount of buffered traffic available at the AP for a particular station and are transmitted frequently.

A new information element (IE), called segment count is introduced in the DTIM beacon that carries the description of a segment page. In order to wake up at the appropriate TIM beacon transmission, the station computes the page segment assignment in the TIM segment using the page count field and page bitmap field of the segment count IE. TGah has also introduced the concept of TIM station (that need to receive the TIM information for regular wake up intervals) and non-TIM stations (that are not required to receive anything and only wake up when they need to transmit).

The TIM and Page segment method is particularly helpful in reducing the channel occupancy time of beacons. The grouping of stations can be based on similar features or location. This method also helps in reducing contention from a large number of overlapping transmissions caused by greater number of expected hidden stations. In addition, stations can remain in sleep mode for longer durations that can help to conserve limited power resources for battery driven stations.

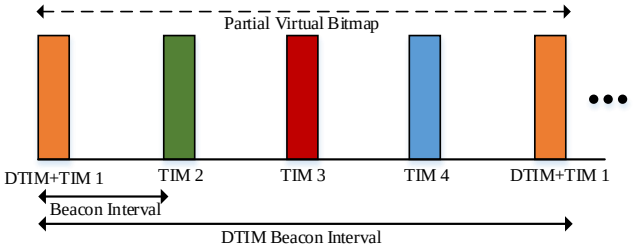


Figure 3.16: TIM and Page segment mechanism

3.3.6.4 Channel Access to Support Large Number of Contending Stations

Apart from supporting the existing EDCA, the IEEE 802.11ah defines a new (optional) contention-less channel access period called RAW. This access method is designed to reduce collisions by improving the channel efficiency. The idea of RAW is based on spreading the uplink attempts of stations over a much longer time and to allow only few devices to transmit on the medium over a particular instance. This technique is particularly useful to provide near contention-free channel and is driven by the existence of large number of hidden stations in high density networks.

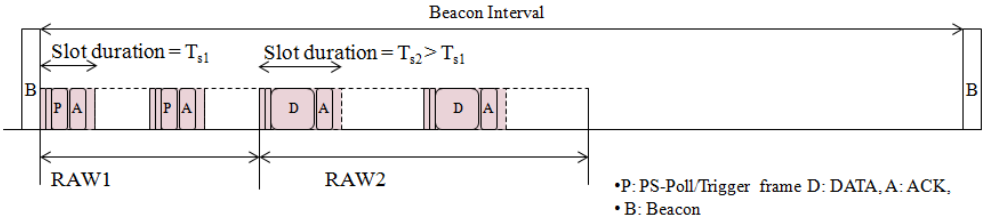


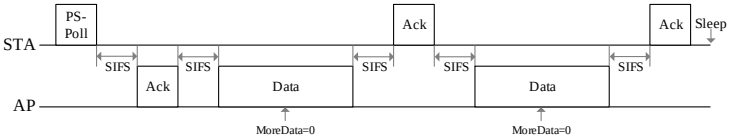
Figure 3.17: Basic RAW time diagram.

Each station calculates the number of time slot N_{RAW} based on the RAW duration T_{RAW} and time slot duration T_{Slot}. There are $N_{RAW} - 1$ equal time slots in a RAW that correspond to different stations. Each station determines the index of the time slot, i_{Slot}, on which it is allowed to transmit based on the following equation:

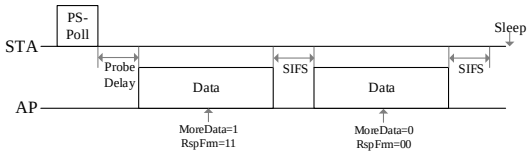
$$i_{Slot} = (x + N_{Offset}) \mod N_{RAW} \tag{3.1}$$

where x represent the AID of the station and N_{Offset} is used to improve fairness among stations.

The AP coordinates the uplink channel access of the stations by defining RAW time intervals in which specific class of devices are given exclusive access of the medium. A new information element, called Raw Parameter Set (RPS) is included in the beacon, through which the AP informs about the restricted medium access intervals. A new management frame, called Resource Allocation (RA), is defined that enables AP to adaptively manage RAW allocations. This frame contains the scheduling information that can help stations to learn the time slot during which they are allowed to access the medium. AP broadcasts RA to all non-AP stations that belong to the RAW group which is identified



(a) Power saving sequence of legacy IEEE 802.11.



(b) Power saving sequence of IEEE 802.11ah.

Figure 3.18: Speed frame exchange technique.

by the RAW group field of a previously transmitted RPS element.

During a RAW slot, stations use EDCA to access the channel. Through Figure 3.17, we show the basic working of RAW mechanism.

3.3.6.5 Power Saving Mode for TIM based stations

In order to support numerous IoT devices (that are desired to operate over limited power resources and are expected to continue unabated processing without the need of battery replacements for weeks or months), the TGah has placed paramount importance on developing and enhancing power saving mechanisms. In the following section, we discuss few of the notable power saving modes used by the IEEE 802.11ah standard.

1. **Speed Frame Exchange**

   In legacy IEEE 802.11, power conservation without sacrificing connectivity is achieved by maximizing the time spent by the transceiver in sleeping mode, called Power Saving (PS) mode. During the sleep mode, AP buffers frames for sleeping stations (where the AID provides a logical link between the frames and sleeping stations). The information about the buffered frames is communicated to the stations through TIM beacons. If a station detects the presence of buffered data, it switches to active state and sends a PS-Poll control frame to retrieve frames (station contends for the medium using DCF and transmits PS-Poll frame after the completion of backoff period). In reply to the PS-Poll, the AP immediately responds first with a ACK frame which is followed by a buffered data frame.

   In order to reduce contention , IEEE 802.11ah proposes to use Speed Frame Exchange (SPF) method, which enables an AP and non-AP station to exchange a sequence of uplink and downlink frames during a reserved TXOP. The client station wakes up after sleep, contends for the access of the shared medium, sends data to the AP, and the AP replies with a short inter-frame gap which allows the station to go to sleep mode immediately. Therefore, SPF allows the station

to save the time wasted in two way acknowledgment and longer inter frame spaces. Figure 3.18 compares the power saving sequence of legacy IEEE 802.11 and the IEEE 802.11ah.

This scheme helps to extend battery life of stations by keeping them awake for shorter duration of time. Furthermore, the foregoing scheme improves channel efficiency by minimizing the frame exchanges required for uplink and downlink data transmissions.

2. **Improvements in BSS Max Idle Period**

   In order to save power consumed by station during regular wake up to listen to DTIM beacon or periodic keep alive messages, legacy IEEE 802.11 has already defined a feature, called BSS Max Idle Period. It is a timing frame during which the AP, in spite of not receiving any packet due to inactivity by the associated stations, does not de-associate it. This timer value is transmitted through association and re-association frames. As a consequence to BSS Max Idle, the stations can remain in sleep mode for longer durations without the need to transmit the keep alive messages.

   IEEE 802.11ah standard improves the BSS Max Idle period mechanism of the current IEEE 802.11 standard. Instead of using same Max idle period for all nodes (i.e. 18.64 hours), IEEE 802.11ah aims to utilize different periods for different devices (i.e. from 18.64 hours to 4660 hours which corresponds to 194 days) based on their operational characteristics.

3. **Wireless Network Management (WNM) sleep mode**

   This mode of operation, which is already part of legacy IEEE 802.11, allows a station to inform the AP about the duration of time through which it intends to remain in sleep mode. During the sleep mode, the station is not intended to wake up and listen to every DTIM beacon. Instead, the station sets up a listen interval based on several DTIM and thus is able to reduce its power consumption by remaining sleep during multiple DTIM cycles.

   Similar to Max Idle period, IEEE 802.11ah aims to extend the WNM-sleep mode from 1.82 hours to 189 days.

3.3.6.6 Power Saving Mode for non-TIM based stations

Apart from stations that regularly wake up on the basis of TIM information, TGah proposes to create a new category of stations, called non-TIM stations, that require longer doze durations and without beacons. For Non-TIM stations, IEEE 802.11ah has defined a new mechanism, called Target Wake Time (TWT), which allows to reduce signaling overhead by scheduling channel access time of each station. The non-TIM stations negotiate a transmission time allocated in a periodic RAW.

TWT function permits an AP to define a specific time or set of times for individual stations to access the medium. The non-AP and AP stations exchange information that includes an expected activity duration to allow the AP to control the amount of contention and overlap among competing stations. A new information element, called TWT IE, is included in the DTIM beacon and regular long beacons, which is shown in Figure 3.19.

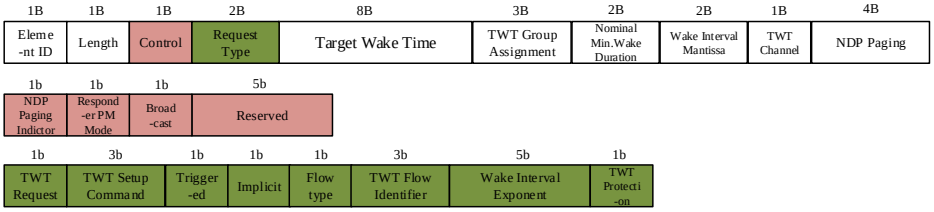


Figure 3.19: TWT information element.

The most important parameters in TWT information element are:

- **Control**

  The control bits indicate the usage of broadcast by TWT.

- **Request Type**

  This field includes the flow identifier that identifies the specific information for a particular TWT request made by a station and is also used for broadcast TWT. Also, the TWT protection field indicates the RAW based protection of a TWT by the AP. In addition, this field includes the period of TWT interval (which is an exponential variable).

- **Target Wake Time**

  It describes the time at which the first TWT interval initiates.

- **Nominal Minimum Wake Duration**

  It describes the minimum values of TWT service period.

- **TWT Channel**

  This field describes the channels on which the station is allowed to transmit during a TWT service period.

The TWT assigned by an AP can be periodic as well as aperiodic. Station can sleep outside the TWT service period. Within TWT, Null data packet is used by the AP and the station to inform about the status of the buffer. Each station uses legacy channel access method to transmit frames within a TWT service period. Different stations can be assigned same TWT, where NAV procedure is used to avoid collisions.

3.4 Comparative Analysis of IEEE 802.11ah with Previous IEEE802.11 Amendments

In the preceding section, we reveal the distinctive characteristics of IEEE 802.11ah amendment that differentiates it from previous IEEE 802.11 standard. With the help of PHY and MAC layer

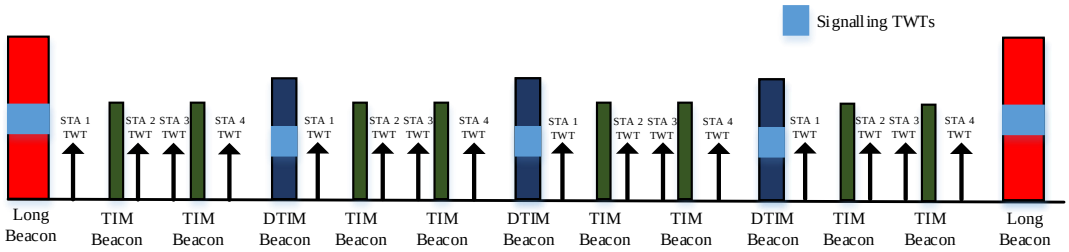


Figure 3.20: TWT mechanism.

comparisons, in this section, we indicate the ability of IEEE 802.11ah amendment to bridge the gap between traditional mobile networks and the demands of IoT devices.

3.4.1 MAC Layer Comparison

The key design feature for the IEEE 802.11 MAC is based on the channel access principle that enforces each station to sense the channel to be idle before initiating transmission, in order to avoid collisions. The MAC operation was designed based on DCF (already explained in previous chapters) protocol that utilizes the aforementioned principle. Despite the robust and adaptive nature of DCF in varying conditions, the initial MAC features were designed for best effort applications and thus did not require complex resource scheduling or management algorithms. However, the massive deployment of IEEE 802.11 networks has resulted in the need to include traffic differentiation and other sophisticated network management schemes. Furthermore, different versions of the IEEE 802.11 standard have been proposed with time, which include additional PHY and MAC features to accommodate the technological advances along with the ability to adapt to ever growing use cases.

Table 3.5 highlights the key MAC features supported by each amendment. Also, key MAC layer differences between the proposed IEEE 802.11ah amendment and previous IEEE 802.11 standards are described. In particular, we highlight the critical MAC additions and changes being made for IEEE 802.11ah, which will allow this future standard to accommodate the IoT paradigm. The notable features compared in Table 3.5 are explained in the following paragraphs.

3.4.1.1 Backwards Compatibility

Up till IEEE 802.11ac, all the IEEE 802.11 systems have been designed to be backwards compatible and usually employ full inter networking with all the previously developed standards.

IEEE 802.11a and IEEE 802.11b/g operated over different frequencies (i.e. 5 GHz for 802.11a and 2.4 GHz for IEEE 802.11b) and were not compatible. However, several manufacturers made equipment that worked on IEEE 802.11a and IEEE 802.11b simultaneously. IEEE 802.11g incorporated OFDM and employed 2.4 GHz, was backward compatible with IEEE 802.11b (additional overhead was introduced in the packet header for compatibility). IEEE 802.11n was developed for operations over both 2.4 and 5 GHz and used channel parallelization (MIMO) to enhance throughput. It was

Table 3.5: Key MAC features within each amendment.

Notable Features		802.11-2007	802.11n	802.11ac	802.11ah
Backwards compatibility		*X*	*X*	*X*	
DCF		*X*			
PCF		*X*			
HCF	HCCA	*X*	*X*		*X*
	EDCA	*X*	*X*	*X*	*X*
TXOP	Forward	*X*	*X*	*X*	*X*
	RD protocol		*X*	*X*	*X*
	BDT				*X*
RID					*X*
Frame Aggregation			*X*	*X*	*X*
Block Acknowledgment		*X*	*X*	*X*	*X*
MU Aggregation				*X*	*X*
NDP			*X*	*X*	*X*
Group-ID				*X*	*X*
BSS color					*X*
Dynamic Bandwidth Management				*X*	
SST					*X*
TIM		*X*	*X*	*X*	*X*
DTIM			*X*	*X*	*X*
TWT					*X*
Grouping of stations					*X*
Hierarchical AID					*X*
Dynamic AID					*X*
RAW					*X*
Group Sectorization					*X*
Relay Operations					*X*
Power saving at AP					*X*
Low power mode of Operations					*X*

backwards compatible with IEEE 802.11a/b/g and defined three modes transmission (i.e. legacy mode, mixed mode and greenfield mode). In mixed mode, both IEEE 802.11n and IEEE 802.11a/b/g devices were allowed to inter-operate in same BSS over the cost of two preamble transmissions by the IEEE 802.11n stations (legacy preamble and the IEEE 802.11n preamble). IEEE 802.11ac was designed to follow the mode of operation set by IEEE 802.11n.

Unlike all the previous amendments, in IEEE 802.11ah, backwards compatibility is not considered due to the use of a completely different frequency band.

3.4.1.2 Distributed Coordination Function

DCF is the basic random access MAC protocol of IEEE 802.11 standard that includes CSMA with Collision Avoidance, a sort of listen before talk mechanism. Furthermore, it encompasses binary exponential backoff rules to manage the retransmission of collided frames. It works as follows. For

more detail of DCF, please refer to Section 1.3.

3.4.1.3 Point Coordination Function

PCF is an optional centralized MAC protocol that supports time bounded and collision free channel access. It uses polling scheme to determine which station can initiate data transmission. This technique is designed for infrastructure based network only, where different stations can optionally participate in PCF and respond to the received poll. Despite the ability of PCF in improving performance under heavy traffic loads and the ability to support Quality of Service guarantees, this scheme is not enabled within hardware implementations. Power consumed and added delay in polling are the main disadvantages of this scheme. However, HCCA (described in Section 3.4.1.4) extends the PCF method.

3.4.1.4 Hybrid Coordination Function

HCF, which improves on the aspects of both the contention based DCF and AP controlled PCF, is a QoS aware MAC protocol that includes appropriate service differentiation mechanism.

Initially, the legacy IEEE 802.11 was designed only for best effort traffic and did not support real time traffic. In order to support the increasing demand for QoS, the IEEE 802.11e was proposed. This standard, was included as part of IEEE 802.11-2007, was developed with the intention to support prioritized and QoS sensitive applications such as Voice over IP (VoIP), video conferencing, streaming etc.

HCF has two basic channel access methods, the enhanced DCF (EDCF) and HCCA. Also, HCF defines two phases of operation between consecutive beacons called Contention Period (CP) and the Contention Free Period (CFP). EDCA is used only within CP whereas HCCA can operate between both of the two phases.

1. HCCA

   HCF Controlled Channel Access operates in similar manner to the PCF and uses the same polling mechanism to assign deterministic TDMA based channel access to QoS enabled stations. A QoS aware Hybrid Coordinator (HC) is defined at the IEEE 802.11e AP, which gains control of the channel after sensing channel to be idle for Point Interframe Space (PIFS) interval. HC controls the access of associated stations and allocates TXOPs. Stations willing to transmit have to negotiate with the HC within CFP.

   HC induced complexity is the main drawback of HCCA channel access method.

2. EDCA

   Enhanced Distributed Channel Access (EDCA) is an extension of the DCF mechanism that tries to implement service differentiation by classifying the traffic into different categories with different priorities. In EDCA mode, a traffic class can make itself a higher prioritized traffic class based on statistically reducing its transmission delay by declaring an AC that has higher priority for contending shared channel.

Frame are transmitted by stations based on DCF and by setting the AC by each station. Each AC within a station has different EDCA parameters (i.e. AIFSN, CW and TXOP) and contends independently to each other for channel access.

A station with frames to be sent, waits until the medium is idle and for an additional period of time defined by the AIFSN parameter (as compared to background traffic, the value of this parameter is smaller for voice traffic that enables quick medium access to the time sensitive voice traffic). After the AIFS period, the stations generates a random backoff period between the CW_{min} and CW_{max} for each contending AC. The TXOP parameter defines the maximum length of single transmission and is explained in the next section.

3.4.1.5 Transmission Opportunity

1. For IEEE 802.11-2007

   TXOP defines a period of time for which a station accessing the channel is allowed to transmit multiple frames without using channel access procedure for all the frames. In EDCA, a station can not transmit a frame that extends beyond a time frame called TXOP limit. A frame that is considered to be too long to be transmitted in single TXOP is fragmented into multiple small frames.

2. For 802.11n/ac/ah

   In these amendments, the TXOP procedure is enhanced, where a station (both AP and non-AP) holding TXOP, can grant part of its unused TXOP time to another station (both AP and non-AP), so as to enhance the channel utilization. This mechanism is known as Reverse Direction (RD) protocol. In legacy IEEE 802.11, it was not possible to apply TXOP mechanism in bi-directional network services (such as VoIP, video conferencing etc.), that resulted in performance degradation due to random backoff.

   Stations using RD protocol are categorized into RD initiator and RD responder. A station that holds a TXOP, called the RD initiator, sends a Reverse Direction Grant (RDG) to the RD responder. RDG is included in HT control field of the MAC header and is sent along with the data to the RD responder. Upon receiving the RDG, the RD responder replies with an ACK frame marked with RDG. The RD initiator waits for SIFS or Reduced Interframe Space (RIFS)[1] time for the transmission to commence from the RD responder, after receiving the marked ACK.

3. For 802.11ah

   IEEE 802.11ah has introduced bi-directional TXOP (BDT) that can help non-AP S1G station (i.e., sensors etc.) to minimize energy consumption. This technique allows the combination of transmission and reception (both at uplink as well as downlink) of frames within a single TXOP

[1] Although shorter in length, RIFS is functionally equivalent to SIFS. It results in improved efficiency through shorten gap between frames.

by S1G AP and S1G non-AP stations, where the decrease in the required frame exchange enables stations to extend their battery life time. In addition, this mechanism assists in efficient use of contention based channel accesses.

Stations participating in BDT utilize information present in the Frame Control (FC) field, Physical Layer Convergence Procedure (PLCP) header Signal field and in the NDP frames to indicate the commencement of BDT procedure. No implicit handshake is required initiate of BDT, where the BDT initiator transmits a PPDU, that is either NDP PS-Poll ACK or contains a response indication field set to long response, to the BDT responder.

Despite being similar to RD protocol, the BDT scheme operates without the need of transmitting ACK frames within the exchange procedure. The AP and no-AP stations frame exchange is separated by SIFS, where each received frame acknowledges the reception of the last frame sent in the opposite direction. If both initiator and the responder have equal number of frame to be transmitted, they are exchanged in turns within a TXOP. However, if one of them has no and the other has frames to be transmitted, NDP ACK or NDP Block ACK frames are used for acknowledgment. Therefore, BDT allows stations to save power by initiating sleep mode as soon as the communication with AP is finished.

3.4.1.6 Response Indication Deferral (RID)

This method is an extension of virtual carrier sensing mechanism originally defined in legacy IEEE 802.11 (i.e. NAV). While using the short header, the NAV procedure is disabled because it does not include the Duration/ID field which is required to set the NAV. RID method is proposed by TGah to cover the NAV operations when short frame headers are used.

Both NAV and RID indicate countdown timers used to show the channel idle time. However, the two schemes differ in the procedure to set the counter (while NAV is set after the complete and correct reception of a frame, RID can be set after the complete header of the frame is received). RID counter is modified based on the Receiver Vector (RXVector)[1] of the length parameter included in the SIG field of the PHY header. Unlike NAV that contains accurate information about the expected transmission duration, RID method predicts the duration based on the type of response indicated by Response Indication field of the PHY header. Four type of responses (named Normal response, NDP response, no response and long response) are defined to describe the channel states. Using the no response, the RID is set SIFS plus time needed to transmit either ACK of Block ACK. NDP response sets RID equal to SIFS plus the duration of NDP frame. To indicate that the channel is idle, no response if used that sets the RID to zero. Long response, is used along with BDT, sets the RIS to SIFS plus the duration of the longest possible transmission duration.

[1] when the PHY layer receives a frame, its extracts the PSDU from the PPDU and forwards it to the MAC layer along with a set of parameters (such as rate, length, preamble type, service, modulation type and RSSI) called RXVector

3.4.1.7 Frame Aggregation

It is a mechanism to combine multiple data frames into one larger aggregated data frame for transmission. Frame aggregation improves network efficiency and throughput by reducing the transmission time for preamble/frame header and by reducing the wait time during CSMA/CA random backoff period for successive frame transmissions. However, as a drawback, this scheme increases the delay, where stations have to wait longer times to access the channel.

1. For 802.11n
   It employs two steps of accumulation to increase the size of the data frame to be transmitted. The first, which is at the top of the MAC, assembles MAC Service Data Unit (MSDU) and is called A-MSDU. Another, at the bottom of the MAC, adds MAC Protocol Data Units (MPDUs) and is called A-MPDU.

   The receiver address and the sender address of each aggregated MSDU matches the transmitter address and the receiver address of MPDU MAC header. All A-MSDU belong to the same Traffic Identifier (TID). The maximum length of A-MSDU is 7395 Bytes. Since only one MAC address is generated for all aggregated frames, the transmission overhead is reduced. However, A-MSDU is not efficient in noisy environments due to the fact that an entire A-MSDU is rejected if only one MSDU is corrupted. The A-MSDU is completed either when the size of waiting frames reach the maximum A-MSDU size threshold or when the maximum delay of the oldest frame reaches a pre-assigned values. The default value for the maximum delay is 1μs and could be assigned value based on AC used.

   The maximum supported length of A-MPDU is 65535 Bytes. All MPDUs within an A-MPDU are addressed to the same receiver. Also, there is no waiting/holding time to form an A-MPDU. The maximum number of frames in an A-MPDU is 64. A-MPDU is more resilient against noise since each MPDU within A-MPDU has its own MAC header and Cyclic Redundancy Check (CRC). On the contrary, this also lead to added overhead, specially for the case when small MSDU are used.

2. For 802.11ac/ah

   Enhanced frame aggregation methods are used. All frames follow the A-MPDU format; the maximum size of A-MPDU is increased for IEEE 802.11ac (i.e. 1,048,575 Bytes).

3.4.1.8 Block ACK

Block Acknowledgment (ACK) mechanism enables the transmission of a single ACK frame by the station that received a series of frames in a TXOP. It results in efficient use of airtime as compared to traditional positive ACK sent for every received frame.

Block ACK contains a bitmap (of 128 Bytes) that indicates the reception of up to 64 MSDUs. IEEE 802.11e has defined two Block ACK procedures: immediate and delayed. In the delayed procedure,

the receiver is given more time to do computing on the received frames.

1. For 802.11n

   Block ACK method is enhanced in IEEE 802.11n to incorporate aggregation. It is introduced to reduce the drawback associated with aggregation, where frame error rate becomes higher as the size of frame increases. Block ACK method is modified to support multiple MPDUs in an A-MPDU. The sender only resends the MPDUs that have not been correctly received by the receiver and are not acknowledged by it.

2. For 802.11ah

   Block ACK response includes the preferred MCS and the bandwidth information. IEEE 802.11ah also introduces the fragment Block ACK procedure. Fragments obtained from the partition of a MSDU can be acknowledged either using immediate acknowledgment by responding with NDP Block ACK frames, or following the normal Block ACK procedure.

3.4.1.9 MU Aggregation

It is a method to support aggregation of MPDUs addressed to multiple receivers into a single PDU and is only used for transmission from AP to multiple STAs. AP selects stations with similar conditions to aggregate to achieve optimal spectrum efficiency.

3.4.1.10 Null Data Packet

Null frame is a frame meant to contain no data but flag information. They are widely used in IEEE 802.11 WLANs for control purposes such as power management, channel scanning, and association keeping alive (e.g. in the absence of data frames, a station transmits null packets to the AP as keep alive messages so as to avoid disconnection). More details of NDP was provided in Section 3.3.6.1.

3.4.1.11 Group ID

The IEEE 802.11ac amendment defines a mechanism to group stations (called Group ID management). This mechanism enables a receiver to determine whether the data payload is single- or multi-user. More specifically, the Group-ID field is utilized by a receiving node to decide if it is targeted in the followed MU-MIMO transmission. Multiple users can be assigned same Group-ID, where stations present in a group are considered together for co-scheduling of transmission using the MU-MIMO beam forming mechanism.

3.4.1.12 BSS color

It is an innovative scheme to increase throughput of dense WLAN networks, where each BSS is assigned a specific color (in-terms of bits designated in L-SIG field of physical header). See Section 3.3.6.2 for details.

3.4.1.13 Dynamic Bandwidth Management

IEEE 802.11ac has also introduced dynamic bandwidth management to optimize the use of available bandwidth. This scheme allows the transmitter and receiver to select an interference free channel before initiating transmission.

3.4.1.14 Sub-Channel Selective Transmission

This feature has been introduced by IEEE 802.11ah. It allows stations to rapidly select and switch to different channels between transmissions to counter fading over narrow sub-channels. Details on SST were presented in Section 3.3.5.3.

3.4.1.15 Traffic Indication Map

In legacy IEEE 802.11, the Beacon frame contains this element through which the sleeping power saving stations are informed of the presence of buffered traffic intended for them at the AP. This element is sent in the form of a bitmap, where each bit represents the AID of stations. A bit is set in TIM when corresponding station has buffered data at the AP. The Delivery TIM (DTIM) serves a similar purpose, indicating the presence of buffered multicast frames. Details were provided in Section 3.3.6.3.

3.4.1.16 Target Wake up Time (TWT)

TWT is a function that permits an AP to define a specific time or set of times for individual stations to access the medium. For detail, see Section 3.3.6.6.

3.4.1.17 Hierarchical AID

IEEE 802.11ah proposed hierarchical network organization where stations are grouped together based on their similarities. Each station is assigned a four level AID structure encompassing page, block, sub-blocks and station fields. As an important outcome, this mechanism helps in supporting increased number of stations. Further details were provided in Section 3.3.6.3.

3.4.1.18 Dynamic AID Reassignment

This mechanism allows the AP to change the page/group of a station due to a change in its traffic characteristics or for load distribution among the channels.

3.4.1.19 Restricted Access Window (RAW)

It is a new near contention-free channel access mechanism that is designed to reduce collisions by improving the channel efficiency. The AP coordinates the uplink channel access of the stations by defining RAW time intervals in which specific class of devices are given exclusive access of the shared medium. Details were provided in section 3.3.6.4.

3.4.1.20 Group Sectorization

This scheme is developed by IEEE 802.11ah that allows stations to transmit in different sectors (positions) around the AP in a time division multiplexing manner (i.e., after each Beacon, a different sector is given access to the shared medium). The Beacons transmitted by a sectorized BSS carry sector option element and each station is allocated a group ID based on sectorization operation.

3.4.1.21 Relay Operations

IEEE 802.11ah has defined a mode of operation to utilize relays within the network to facilitate the exchange of frames between stations and APs over greater distances. Relays also allow stations to utilize higher data rates and TXOP sharing.

In relay mode, the distance between station and AP could be tripled because the relay mode allows maximum of two hops. In addition, using this mode allows stations placed near the AP to transmit at higher MCS levels than the stations that are provided coverage through relaying. Therefore, even though transmission speed reduces with the increasing distance, stations that are directly connected to the AP are not impacted.

3.4.1.22 Power saving at AP

IEEE 802.11ah proposes to include the AP power saving features for battery operated AP. An AP Power Management RAW is defined that can indicate to associated stations the time intervals during which AP would be in sleep mode.

3.4.1.23 Low Power Mode of Operations

IEEE 802.11ah enables a station to inform the AP about the duration of time it intends to remain in sleep mode. During the sleep mode, the station is not intended to listen to Beacons and then it is able to reduce its power consumption.

3.5 Expected challenges posed to long range Wi-Fi

With the increase in saturation levels over the licensed channels used by cellular operators, it is logical to visualize the massive adaption of Wi-Fi standard within different application areas in coming years. It is evident from previous sections, that IEEE 802.11ah can meet the specific demands of IoT (low power, scalability and range). IEEE 802.11 is well suited to meet the needs of smart homes, smart cities and industrial market.

Despite the advantage of adapting IEEE 802.11ah, in the following section, we enlist few of the challenges expected for the future long range Wi-Fi amendment.

3.5.1 Vulnerability to saboteurs

Since IoT devices are generally limited in terms of memory and processing capabilities, they are vulnerable to DOS attacks. Also, as highlighted in Chapter 2, the IEEE 802.11 networks have unique vulnerabilities that make them an ideal avenue for attacks by malicious entities. The significant extended operation range of IEEE 802.11ah also increases the distance from which a malicious station can attack and disrupt the normal operation of the network.

In its current form, the IEEE 802.11ah aims to utilize security mechanisms similar to the IEEE 802.11n/ac, that can be inadequate to protect IEEE 802.11ah IoT stations against malicious stations.

3.5.2 Regulatory restrictions

As shown in Section 3.3.5.1, different countries have allocated various S1G ISM bands, where different spectrum bandwidths are available. Particularly for the case of US, up to 26 MHz of spectrum is available in the 902–928 MHz band. On the contrary, only 5 MHz channel bandwidth is available in Europe. While this small available channel can allow Wi-Fi-enabled devices to get guaranteed access for short-burst data transmissions, such as meter data, it can not be sufficient to full-fill the requirements for back-haul/Wi-Fi offloading use case because of limited data rate (i.e. 5 MHz channel can translate to maximum of 73 Mbps approximately by using 4 spatial streams, that might not be enough for Gbps throughput requirements of Wi-Fi offloading and for future 5G networks). At the same time, the S1G transmission channel visualized to be used by the IEEE 802.11ah is subject to various regulations requirements (such as the maximum allowed transmission power and duty cycle, permissible channel spacing, etc.) set by different regulatory authorities (i.e. European Telecommunications Standards Institute (ETSI) &European Radio Communications Committee (ERC) for Europe and Federal Communications Commission (FCC) for US).

According to the European regulations, every station operating over the S1G is expected to comply with a maximum duty cycle limit of 2.8%. This regulation for the S1G band is also expected to be accompanied with the Listen Before Talk (LBT) algorithm (its is a mechanism that forces radio transmitters to first sense the environment before initiating transmission) and Adaptive Frequency Agility (AFA) scheme (it is a medium access control that defines the mechanism to avoid transmission over already occupied channels). Stations that do not support LBT and AFA are subjected to stricter duty cycle regulation of 0.1 or 1%.

As highlighted by authors in [100], under unsaturated traffic conditions, gradual throughput degradation for uplink traffic can be observed when the number of associated stations are greater than 500 due to duty cycle limitation. Particularly for the case of downlink traffic, that includes frequent beacon transmissions, the duty cycle limitation can severely reduce the network performance.

3.5.3 Synchronization problems

As highlighted in the previous sections, IEEE 802.11ah has defined novel mechanisms that allow stations to sleep and, in return, reduce power consumption. Despite the benefits, increased sleep

durations can lead to drifts in clock that can cause major synchronization problems in the network. In order to avoid possible lags with the network, the longer the station remains asleep, the further advance in time it is expected to wakeup. Therefore, channel synchronization can induce significant overhead for IEEE 802.11ah where massive number devices enter and leave the network. Also, the increased sleeping durations can leave non-AP stations unreachable to the AP because it is unable to check the TIM information.

3.5.4 Competition from other LPWA technologies

IEEE 802.11ah standard with its characteristics, holds great promise to provide long range communication to wide area network without excessive reliance over the wired network. However, IEEE 802.11ah is not the only technology trying to cover the requirements for IoT communications. Upon its arrival, IEEE 802.11ah would have to face enormous competition from other LPWA technologies operating over the S1G ISM band.

However, the advent of Tri-band devices supporting sub 1 GHz, 2.4 GHz, and 5 GHz would greatly improve the possibility of IEEE 802.11ah amendment to become a success.

3.5.5 Interference from other LPWA technologies

The usage of different kinds of LPWA technology on same spectrum might lead to additional interference and suboptimal usage of the spectrum. The massive increase in number of connected IoT stations operating over the shared ISM band will undergo higher level of interference, both as self-interference as well as cross-technology interference. It is already shown by authors [54], that interference will have negative effect on the coverage and capacity among LoRa and Sigfox networks. The contention based MAC of various IoT technologies are either based on Aloha or CSMA (Aloha: Sigfox, LoRa, Slotted Aloha: RFID, NB-IOT, Non-Slotted CSMA/CA: Wi-Fi, Zigbee [55]). These systems operate well in environments with few contending stations. However, they suffer from congestion as the traffic load and the number of devices increase.

3.6 Conclusion

In this chapter, the main characteristics of the upcoming IEEE 802.11ah amendment are presented. With the ability to offer ultra-low power consumption, support for massive number of associated stations per AP and large coverage area, this future standard has the potential to become a ubiquitous standard for IoT.

The contents of this chapter are updated to comply with the published IEEE 802.11ah standard. First, we introduce the IEEE 802.11ah amendment proposed for WLAN that will operate on an unlicensed S1G and will support large number of associated devices connected over long range. Then, we introduce the main PHY and MAC layer features proposed for IEEE 802.11ah. Next, we compare the IEEE 802.11ah standard with previous notable IEEE 802.11 amendments in terms of range,

throughput and MAC features (that are included and excluded within each version). In the last part of the chapter, we highlight the important challenges expected for the long range variant of Wi-Fi.

4

Exploring the high efficiency IEEE 802.11ax amendment

With the rise in popularity of IEEE 802.11 based WLAN networks, more and more Wi-Fi capable devices are proliferating the market that are being deployed in diverse environments. The need to provide high throughput Internet connection to these progressively growing number of devices has led to high density unstructured/unplanned as well as planned networks. Despite the achieved benefits (in terms of high data rates, increased coverage and low incurred cost), legacy IEEE 802.11 was not designed to withstand the challenges faced in high density deployments, where packet loss (due to co-channel interference) and overprotected channel access mechanism can seriously degrade the overall performance. The capacity design and achievable aggregated as well as per user throughput within dense WLAN networks are extensively being challenged by Buy Your Own Device (BYOD) policies, mobility, increased number of Wi-Fi capable devices and bandwidth hungry applications.

While the IEEE 802.11 standard based WLAN has immensely been successful up till now in catering the needs for indoor wireless access, each Wi-Fi standard upgrade has focused on enhancing link or aggregate throughput rather than efficient use of spectrum and user experience (such as latency). Recently, the IEEE 802.11 working group has continued efforts to identify requirements for increasing individual user performances in high-density areas, as well as power efficiency for battery powered devices by creating the IEEE 802.11ax Task Group, TGax (which aims to improve performance in dense environments). TGax is contemplating the design of a new standard (referred to as IEEE 802.11ax) that aims to revamp the legacy PHY and MAC layer protocols so as to improve user experience (in terms of fairness, delay and throughput) within high density networks. This proposed amendment intends to significantly increase spectral frequency reuse and to manage interference from neighboring OBSS.

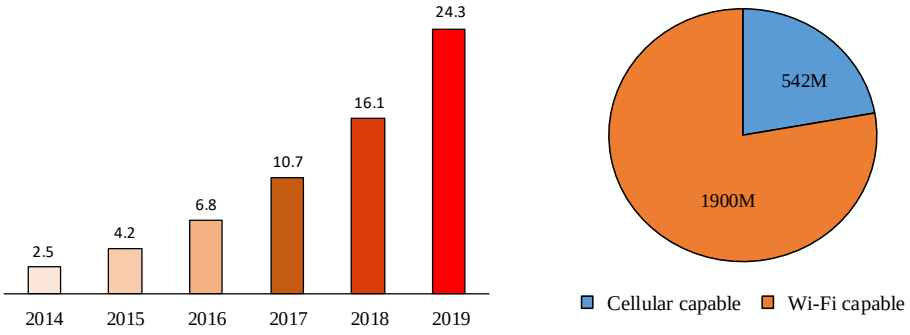
After exposing a mechanism that helps to increase the availability of WLAN networks (which in return improves the performance in dense deployment) and proposing to use IEEE 802.11ah as an alternative technology to densely deployed Wi-Fi cells in previous chapters, the present chapter fo-

cuses on the high efficiency IEEE 802.11ax amendment. Despite the increased outdoor connectivity by IEEE 802.11ah, there is a need to manage the massive number of existing densely deployed Wi-Fi networks. In addition, no single technology is capable of meeting all the requirements of 5G (presented in Section 1.1), several radio technologies would be used in tandem, so as to enable the connection of everything (encompassing numerous use cases). The basic goal of IEEE 802.11ax amendment is to improve network throughput by countering inter-network interference and to adapt robust transmission mechanisms that improve capacity for large number of connected devices (which is one of the main driving force for 5G paradigm).

In order to evaluate and design mechanisms that can lead to increased WLAN performance in dense deployments, we first need to understand the requirements envisaged for IEEE 802.11ax amendment. Thus, the goal of this chapter is to introduce key technological features being explored by TGax and to highlight important opportunities and challenges for the aforementioned amendment. The presented work is published in [10] and [11].

4.1 Motivation

Wireless networks have witnessed continuous and increasing popularity that has attracted ever growing number of users. This has resulted in considerable increase in data consumption over all the networks. As highlighted in Figure 4.1a, by 2019, the global data traffic is expected to increase 10 times more from the level measured in 2014.



(a) Exabytes per month of Mobile data traffic.

(b) Connected devices(by 2019).

Figure 4.1: The strategic importance of Wi-Fi technology [25].

Since major part of the traffic is generated and consumed indoor, the indoor connectivity solutions can be instrumental in addressing the aforementioned capacity requirements.

IEEE 802.11 based WLANs, which are one of the most popular and successful indoor wireless solutions, have evolved as a key enabling technology to cover medium to large scale enterprise, public area hot-spots, apartment complexes etc. Such environments are characterized to include multiple small cells with many APs and serve large number of clients, where increase in coverage and high

data rates are the primary achievements.

Recent years have witnessed a major surge in WLAN deployment in geographically limited environments (encompassing multiple OBSS). The strategic importance of Wi-Fi technology (in terms of the expected number of Wi-Fi capable devices) so as to fulfill the traffic demand by the year 2019 is highlighted in Figure 4.1b. Following facts about the global market size of Wi-Fi clearly indicate the popularity of IEEE based WLAN networks; it is estimated by [68], that the global worth of Wi-Fi market is USD 14.8 Billion in 2015 and it is projected to increase up to USD 33.6 Billion by 2020.

The IEEE 802.11 has actively continued to release new draft amendments to incorporate latest technological advances to defy new practical challenges. As compared to the cellular technologies, IEEE 802.11 standards/amendments are released to be backwards compatible and thus pile atop of each other by adding and removing key technical aspects. Most recently, the IEEE standardization committee has approved IEEE 802.11ax Project. TGax is currently working on the extension of the IEEE 802.11ac standard, but this time aiming to improve the system capacity and not only by increasing the supported data rates at link level. More specifically, this new project is intended to improve the efficiency in scenarios that are interference limited (due to high density of IEEE 802.11 devices). As mentioned in IEEE 802.11ax working document [1], one of the main objectives of the proposed amendment is to increase the spectral reuse and improve interference management in OBSS to achieve higher throughputs. The current IEEE 802.11 standard, when applied to dense scenarios, can result in limited spatial reuse because they utilize overprotected channel access methods.

In this chapter, we introduce the future high efficiency Wi-Fi (i.e. IEEE 802.11ax) amendment. We first point out the necessity of the amendment. We then elaborate the use cases and provide an overview of key technological features proposed for IEEE 802.11ax amendment. Moreover, we identify two major challenges that the next generation of Wi-Fi networks will face: i) co-existence with unlicensed LTE, and ii) adoption of the IoT paradigm.

4.2 Related work

The wide-spread deployments of High Throughput (HT) wireless technologies, such as IEEE 802.11n/ac and the advent of IEEE 802.11ax, can be considered a breakthrough within local area networking (i.e. WLAN) for commodity and community wireless usage over ISM bands. Apart from the PHY layer enhancements, IEEE 802.11ax amendment is considering enhancement to be made at the basic MAC protocol due the vulnerabilities associated with CSMA/CA.

Authors in [31] articulate the need for new generation WLAN protocols. Also they summarize the standardization activities in progress within TGax and discuss the expected features and challenges in the design of PHY and MAC for IEEE 802.11ax amendment. In [18], the author provides an overview of some technological options that were under consideration by the TGax. As a main contribution, the author describes the potential benefits and drawbacks of the mentioned proposals. However, with the release of IEEE 802.11ax draft 1.0, the contents of both [31] and [18] do not match the latest (at the moment of writing) trends in TGax.

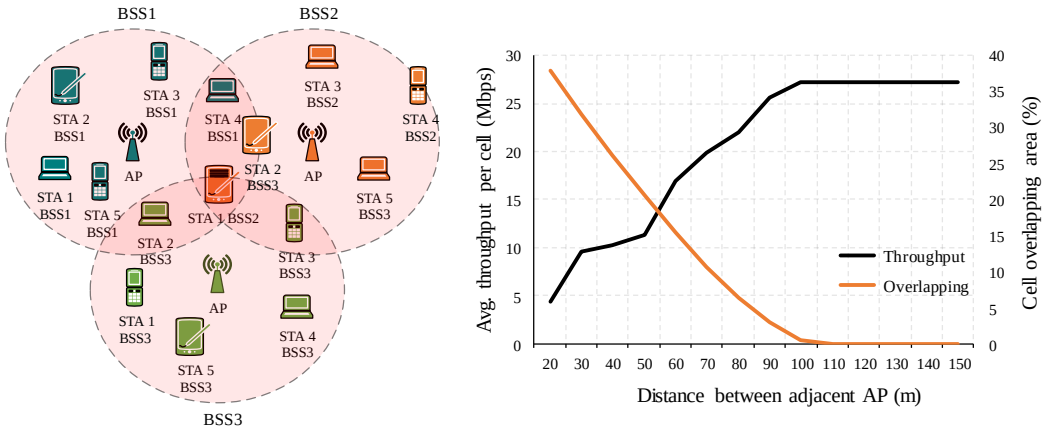


Figure 4.2: High density scenario where numerous Wi-Fi enabled devices co-exists with overlapping BSS problem.

The work presented in this chapter is updated to the latest draft currently under revision by the TGax.

4.3 IEEE 802.11ax Amendment: Vision and requirements for high efficiency Wi-Fi

Since the available number of orthogonal channels for IEEE 802.11 is limited, the OBSS situation in IEEE 802.11 based networks is frequent. The collision avoidance mechanism tends to reduce network throughput and increase transmission delays where, despite an acceptable collision probability, the medium is never fully utilized. Figure 4.2 indicates the OBSS problem. The scenario of three overlapping co-channel cells, each encompassing one AP and five associated stations, is simulated. With the decrease in the overlapping areas, the average throughput within each cell increases (e.g. throughput increase of more than 400% is visible when the overlapping area between adjacent cells decreases from 38% to 7%). The reduction of the overlapping areas could be achieved by applying different techniques introduced by IEEE 802.11ax, as discussed in section 4.4.2. In the following sections, we highlight the need and significance of this new WLAN standard.

4.3.1 Basic necessity

While the current IEEE 802.11 standards (i.e. IEEE 802.11n/ac) were developed with intention to improve the peak aggregate multi-station throughput of the network, proper mitigation of increased interference incurred has not yet been addressed. Furthermore, the channel access method in the aforementioned standards is overly protective leading to reduced spatial reuse. In particular, this future IEEE 802.11ax standard is intended to utilize techniques that would increase the physical bit rate, but also reduce the FER and improve spectral reuse by allowing highly efficient multi-user ac-

cess and by mitigating/reducing interference, which would in return increase the area throughput.

4.3.2 Project definition and scope

Due to the well known performance challenges effecting WLAN in dense deployments, a study group called High Efficiency WLAN (HEW), was initiated within IEEE 802.11 working group in May 2013. The activities of HEW considered improving the spectral efficiency so as to enhance the system throughput/area in high density environments consisting of numerous of APs and/or non-AP stations. After the success of Project Authorization Request (PAR) and Criteria for Standard Development (CSD), this study group was elevated to the status of task group with the aim to design a new IEEE 802.11 standard, called IEEE 802.11ax, in July 2014.

IEEE 802.11ax standard is primarily being designed to provide high efficiency WLAN operation at both indoor and outdoor environments. This standard aims to improve over several performance metrics (such as average per station throughput, area throughput etc.) that directly result in increase of efficiency over several closely placed indoor and outdoor BSS deployments (encompassing large number of stations). Thus the scope of the proposed amendment is to define standardized modifications of both the Physical and MAC layer of legacy IEEE 802.11 standard to improve experience of end users in densely deployed WLAN environments. To summarize, the scope of IEEE 802.11ax standard can be elaborated by the following points,

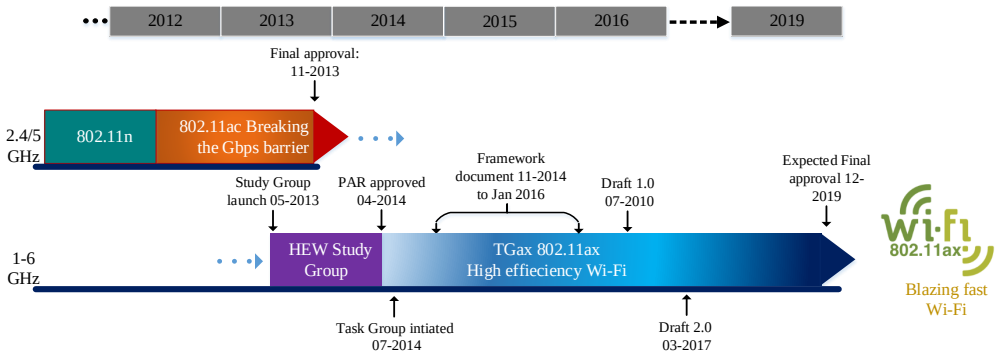


Figure 4.3: Evolution path of IEEE 802.11.

1. **Improved system and user throughputs in dense deployment.**

   Since interference from neighboring devices in dense deployment (consisting of several neighboring AP and non-AP stations) greatly influences the end user experience, the focus of IEEE 802.11ax is on system level performance. This amendment is expected to increase, at least, four times the area throughput while targeting up to ten percent increase on the average throughput per station.

2. **Maintaining and improving power efficiency.**

While enhancing user experience in terms of increased throughput of end users, the aforementioned standard also aims to maintain and enhance the power efficiency by enabling simplified power save modes for each device.

3. **Efficient use of spectral resources.**

   The standard is expected to provide methods that would ensure efficient use of spectrum resources. Furthermore, the standard is also expected to devise schemes that would significantly increase frequency reuse and would also reduce interference induced from neighboring OBSS.

4. **Indoor and outdoor operations over 1 to 6 GHz frequency bands.**

   IEEE 802.11ax is mainly focused on WLAN operations at 2.4 and 5 GHz, but will cater mode of operations between 1 and 6 GHz. It is expected that in future, new unlicensed bands would be made available. This is the motivation for IEEE 802.11ax to operate between 1 and 6 GHz.

5. **Enabling backward compatibility.**

   It is also expected to be backward compatible to support communication with any IEEE 802.11 legacy device. Furthermore, the standard is also presumed to enable the co-existence of legacy stations with IEEE 802.11ax devices operating over similar frequency bands.

4.3.3 Application environment and use cases

Due to the explosive growth in the use of Wi-Fi networks, there is a need to investigate usage model for them in non-traditional environments (such as streets, public spaces, airports, railway stations etc.) for which IEEE 802.11 standard was not specifically designed. The future Wi-Fi will have to take into consideration the environments that are characterized by the overlap of multiple WLANs networks utilizing similar channels for transmissions sharing the scarce and overcrowded frequency resources.

IEEE 802.11ax amendment aims to improve the spectral efficiency and area throughput in real world densely deployed Wi-Fi environments (indoor as well as outdoor) which are affected by the interfering sources and heterogeneous networks. This future standard takes into consideration the environments that are characterized by the overlap of multiple Wi-Fi networks utilizing similar channels for transmissions. IEEE 802.11ax intends to provide self configuration and self adaption abilities to WLAN to increase area throughput. Therefore, TGax has prioritized the following use cases for the development and evaluation of different features.

4.3.3.1 Residential

In this environment, high density OBSS are created when a large number of WLAN APs are installed in close vicinity such as in an apartment building. The hardware used in those SOHO environments share similar characteristics, consisting mainly of low-end/mid-range equipment. In such scenario, increased interference level from neighboring OBSS (due to unmanaged and unplanned deployments) can greatly affect the performance of devices within the network.

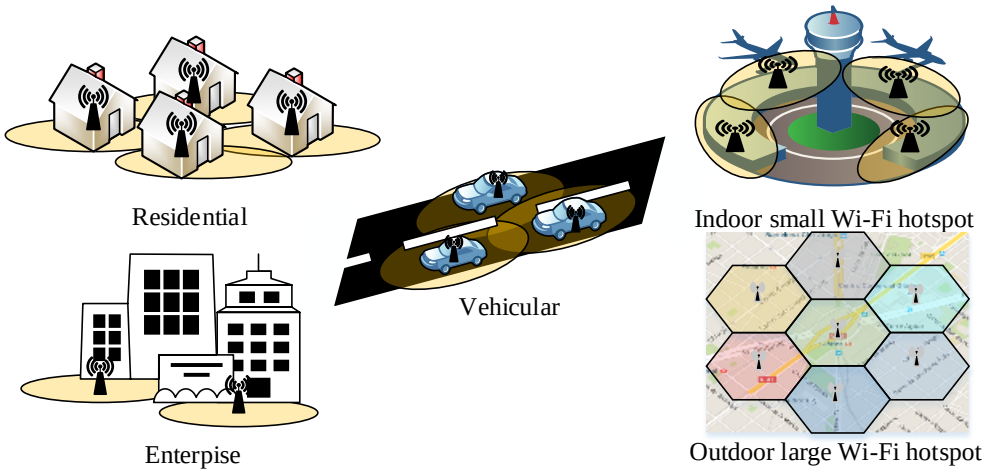


Figure 4.4: IEEE 802.11ax intended environments.

4.3.3.2 Enterprise

Similar to residential environment where Wi-Fi is being densely deployed by home owners to utilize it as a main source to access the Internet , enterprises/organizations are providing Wi-Fi as their primary/only source of access to Internet through a managed network. Furthermore, enterprise environment is characterized to support unified communication encompassing integration of real time communication services of different types. Interference management issues and BYOD policies hold utmost importance in these environments as well as in scenarios where different enterprise networks are present at close proximity.

4.3.3.3 Indoor small BSS Hotspot

This environment represent a scenario with high density of APs and non-AP stations, where the BSS from each operator is deployed in regular symmetry (e.g. shop malls, airports, railway etc.). Different cells of different operators can overlap and cause interference that may degrade the performance within an area.

4.3.3.4 Outdoor large BSS hotspots

Outdoor open area consists of an environment in which large numbers of people (attending an event) utilize their smart-phones concurrently to download and upload data through large sized BSSs. The main objective of this scenario is to model an outdoor deployment (similar to cellular mobile networks) which consist of high density of non-AP stations along with maximum separation among different APs. However, legacy IEEE 802.11 standard was not designed to provide efficient outdoor wireless communication to large number of users. Therefore, in such scenarios, potential interference from different non-AP stations can severely affect the end user experience and reduce the overall performance.

4.3.3.5 Vehicular

In recent years, Wi-Fi networks are introduced and widely deployed in vehicles, where it is used to access the Internet (e.g. different transport systems etc.). IEEE 802.11ax intends to reduce the effect of variable interference of neighboring vehicles as well as to explore possible methods to reduce the restriction on the vehicle to infrastructure communication (i.e. mobility considerations and signal directivity). As an addition to this use case, the TGax also proposes the use of cellular offloading in high speed moving environments to improve user experience.

4.3.3.6 Other notable environments

Campus, factory environments (where several hundred of APs can be concentrated in a small area), small offices (single BSS with limited number of devices encountering unmanageable interference) and IoT use-cases, are also being explored by the TGax as possible use case environments.

4.4 Overview of key technological features of high efficiency Wi-Fi amendment: IEEE 802.11ax

TGax intends to introduce radio technology based on MIMO and OFDMA, so that more bits could be transmitted per TXOP.

In this section, we provide a thorough overview of important features proposed for IEEE 802.11ax amendment. We list different proposals into the following four categories; PHY, MAC, Multi-User and other notable features. With the help of Figure 4.5, we highlight the expected improvements (interms of system throughput) of the four aforementioned categories (where Multi-User techniques indicate the largest gain). It is pertinent to mention that the expected percentage improvement of each proposal is inferred by the studies submitted and discussed at the TGax. Table 4.2 summarizes the main features introduced by TGax as detailed in this section.

4.4.1 PHY layer enhancements

Although IEEE 802.11ax is an evolution of the IEEE 802.11ac standard, it aims to adopt new technologies while being backward compatible. For example, IEEE 802.11ax PPDU intends to include legacy preamble duplicated on each 20 MHz sub-channel so as to solve the backwards compatibility and co-existence challenge. In addition, TGax is also contemplating the design of new preamble types needed to support new features. The noteworthy amendments proposed at the PHY layer for IEEE 802.11ax are explained as in the following.

4.4.1.1 Physical coding decision (LDPC and BCC)

The default forward error correction scheme proposed for IEEE 802.11n and IEEE 802.11ac is based on Binary Convolutional Coding (BCC) with frequency interleaving per OFDM symbol. Using Low Density Parity Check (LDPC) is optional and has not yet got much attraction by the WLAN due

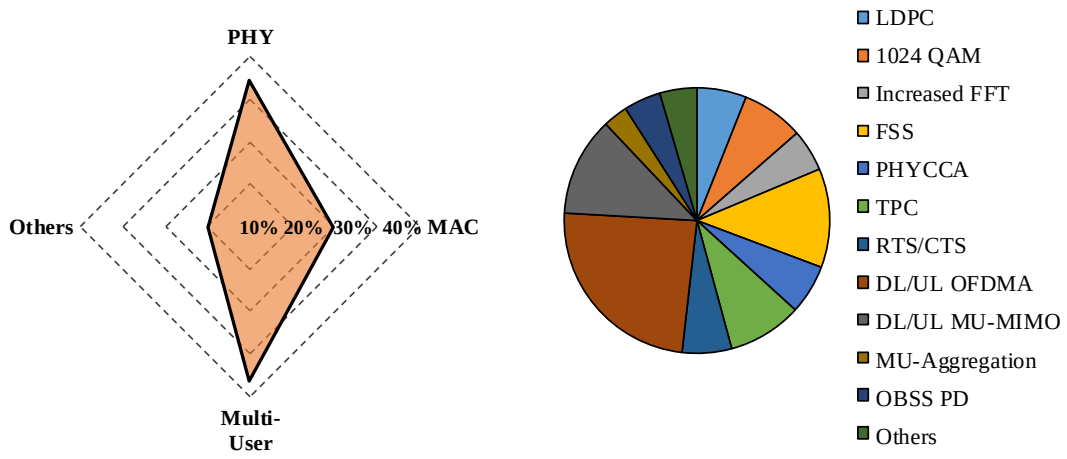


Figure 4.5: Expected improvements by different novel methods proposed for TGax in order to increase the efficiency of WLAN networks.

to high computational cost. However, LDPC codes have shown to provide significant gains (in terms of capacity) when compared to BCC [84].

However, IEEE 802.11ax proposes to use LDPC encoders when using larger bandwidth (i.e. channel bonding) where LDPC sensitivity improvements range from 1.5% to 3% and are dependent on the utilized MCS, and to use BCC in narrower bandwidth where one symbol duration could be saved as compared to LDPC.

4.4.1.2 1024-QAM

As mentioned in design document of IEEE 802.11ax [2], the main goal of the aforementioned standard is to achieve, at least, a four-fold increase in the average throughput available at each station. One of the solutions proposed by the TGax to achieve such improvement is to incorporate a very high modulation scheme (i.e. 1024-QAM) where each symbol encodes a larger number of data bits when using such a dense constellation. 1024-QAM has already been employed in different wireless technologies (i.e. Digital Video Broadcasting (DVB) and long haul microwave etc.) to improve bandwidth efficiency and can be utilized in specific use cases for IEEE 802.11 ax.

4.4.1.3 Enhancement for outdoor communication

The baseband signal in IEEE 802.11 OFDM-based transmissions is generated by using the Inverse Fast Fourier Transform (IFFT) and in reception, data is demodulated by a Fast Fourier Transform (FFT). The IFFT modulation creates non-harmful spectral overlapping of orthogonal sub-carriers.

In order to improve the spectral efficiency of stations over the intended use cases, TGax has defined four times larger FFT size than that used for 802.11ac. This larger FFT size is proposed to increase robustness in outdoor as well as to improve the average indoor throughput. TGax proposes to replace the current payload symbol duration of 3.2μs to 12.08μs [59] with a sub-carrier spacing of

78.1257 (i.e. 256 FFT over 20 MHz) and has indicated 17% improvement over the use of 64 FFT. The foregoing changes facilitate the inclusion of Orthogonal Frequency Division Multiple Access (OFDMA) for 802.11ax amendment.

To subdue the large path loss and channel delay suffered in outdoor large hotspot, TGax defines a new High Efficiency PLCP Protocol Data Unit (HE-PPDU) format, called Extended range Single User (SU) PPDU, in which the fields that contain the information required to interpret packets are repeated (i.e. HE-SIG-A symbols are repeated once in time).

4.4.1.4 Frequency selective scheduling

Channel dependent scheduling is widely used in current wireless networks where differences in channel quality are utilized in the scheduling decision process [14]. OFDMA systems benefit from frequency selectivity in terms of frequency diversity and Frequency Selective Scheduling (FSS). In TGax, FSS is being actively pursued to provide throughput gains to far away stations (with respect to AP) by allocating physical resource blocks with least amount of fading for their transmissions.

In [76], the authors highlight potential gains achieved by Channel State Information (CSI) based frequency selective scheduling with the help of simulations and indicate 42% indoor and 64% outdoor throughput gains.

Furthermore, the IEEE 802.11ax intends to adapt Dual Sub-Carrier modulation (a scheme that modulates the same information on a pair of far apart sub-carriers) to improve FER performance and robustness against narrow-band interferences under dense deployments.

4.4.2 MAC layer enhancements

In order to provide efficient use of spectral resources in dense deployments with the intent to significantly increase spectral frequency reuse and manage interference from neighboring OBSS, TGax is working on the following notable MAC enhancements:

4.4.2.1 Improving Spatial reuse: PHYCCA modifications

The legacy IEEE 802.11 utilizes PHYCCA modules to sense state of the channel (i.e. either busy or idle) by measuring the received energy. The IEEE 802.11ax proposed amendment aims to formally embrace the dynamic PHYCCA modifications. These methods allow multiple concurrent transmissions to co-exist and thus increase the spectral reuse. The intuition to include these modifications lies in the fact that, in dense deployments, stations may end up always assuming the channel to be occupied (due to fixed carrier sensing range), even though multiple concurrent transmissions might still be possible. TGax has been actively involved in the design of PHYCCA modification schemes, where DSC algorithm has been proposed as one of the key innovative technologies that can increase the overall throughput.

The basic idea of DSC scheme is to optimize the existing deployments by appropriately tuning the CST for each node in a distributed manner. DSC tries to confine the increase and decrease of CST

for a station in a bounded area so as to avoid both extremely aggressive and conservative behavior. The throughput gains achieved by DSC are more than 20% [12] on average when combined with optimal channel selection (gain increases beyond 40% when stations use slow bitrates and send long frames).

One of the drawbacks of allowing multiple concurrent transmissions to co-exist in geographically limited area is the increase in hidden nodes, which results in increase of system level Frame Error Rate [9].

4.4.2.2 Improving Spatial reuse: Transmit Power Control

Transmit Power Control (TPC) allows a wireless station to use the minimum power level in the transmit mode required for the correct reception of a frame, regardless of intervening fading and pathloss. In other words, the reduced transmit power levels guarantee the target SINR to correctly decode the received frames at the highest possible transmission rate. It also decreases medium contention (i.e. interference to neighboring cells) and in return, results in higher aggregated throughput levels (with improved overall SINR) by improving spatial reuse.

Therefore, intelligent assignment of dynamically modified transmit power to all the transmitters can decrease frame loss (due to decreased medium contention and improved overall SINR) at the receiver as well as increase spatial reuse. However, starvation problem can still occur in dense network by the usage of heterogeneous transmit power.

Albeit TPC scheme has been standardized in IEEE 802.11h, this scheme was particularly designed to prevent APs (operating at 5 GHz) from interfering with airport radars.

Since interference is the key cause of performance degradation in dense deployments, TGax is contemplating to standardize per link TPC mechanisms with the aim to reduce interference as well as to increase spatial reuse [46].

TPC method in IEEE 802.11ax also constitutes the change of transmit power control of non-AP stations based on the RSSI of beacon signals received from the associated AP. IEEE 802.11ax envisions the utilization of TPC along with PHYCCA modifications so as to avoid excessive interference from stations that reduce their carrier sensing range to allow more concurrent transmissions.

4.4.2.3 Improving Spatial reuse: BSS color

TGax has adopted this innovative scheme introduced in IEEE 802.11ah to increase spatial reuse that enables a station to identify signals from OBSS and allows it to take decisions for interference management or medium contention based on the foregoing information. TGax has renamed this technique as OBSS Preamble Detection (OBSS PD). As highlighted in Section 3.3.6.2, BSS color is an identifier present in the preamble and is used to assist a station in recognizing the BSS from which a frame is originated. A station, that receives an inter-BSS frame with RSSI below the OBSS PD level used by the receiving station does not update its NAV.

In legacy IEEE 802.11, the PD mechanism requires additional PHY resources to constantly monitor the preamble (where, PD threshold is used to decide whether the frame was correctly received).

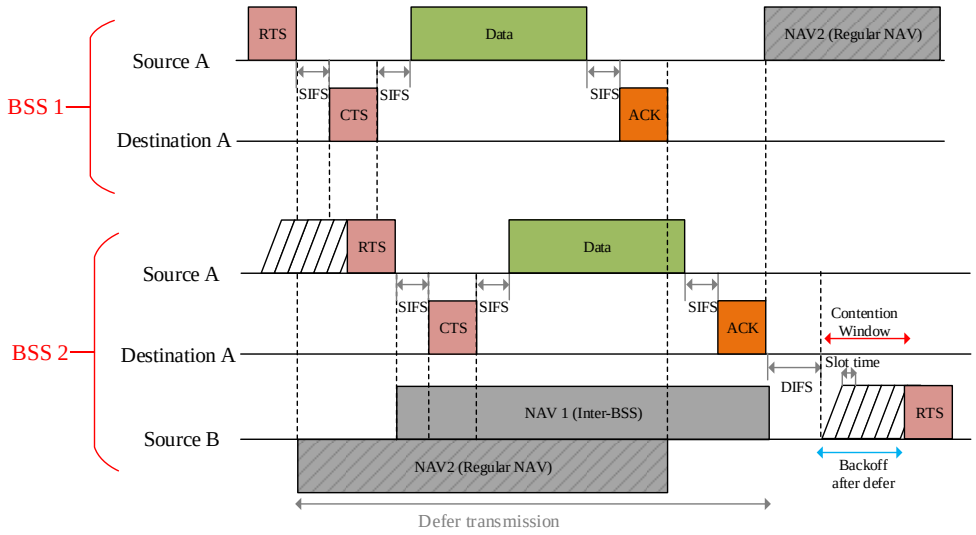


Figure 4.6: Frame exchange sequence for multiple-NAV based spatial reuse scheme.

If the preamble detection was successful, the receiver recognizes it as the start of a valid IEEE 802.11 frame transmission and transits to the receiving state. The PD process was mainly used to discover all the reachable APs. However, due to the complexity of implementation and increased power consumption, this scheme was considered less attractive to be used as the main carrier sensing technique.

4.4.2.4 Improving Spatial reuse: Multiple Network Allocation Vectors

In legacy IEEE 802.11, virtual carrier sensing is used to solve the collision problem associated with hidden nodes. This technique operates by reserving the wireless channel with the help of RTS/CTS handshake (that precede the data frames). The neighboring overhearing stations upon receiving the RTS/CTS frames set a timer, called NAV (refer to Section 1.3 for more details), which blocks them to transmit for a specific time. The underlying shortcoming of this mechanism is that it is not helpful in OBSS scenario and reduces spatial reuse, where the NAV might be set by frames received from one BSS and can be reset by frames of another BSS (legacy NAV operation states that all 3rd party stations receiving RTS/CTS will set the NAV regardless of BSS).

The IEEE 802.11ax amendment proposes to utilize two NAV timers at each station, called Intra-BSS NAV and regular NAV, that are maintained separately. The Intra-BSS NAV is reset or increased only by the frames from the same BSS. Figure 4.6 shows the frame exchange procedure of multiple-NAV scheme. The NAV corresponding to a particular BSS is reset or increased based on the frames received from that BSS. The medium can be considered busy by the virtual carrier sensing mechanisms considering both of the NAVs (i.e. the channel is considered idle only when both the NAVs are zero). These two NAVs can help the station to predict the traffic over its own BSS and enable it to transmit by knowing the state of overlapping traffic.

4.4.2.5 Interference management

Since conventional interference management techniques, when applied to dense deployments, also ease the overall network conditions, IEEE 802.11ax aspires to intelligently utilize RTS/CTS method based on observed channel conditions on per node basis (i.e. an AP can use novel mechanisms to remotely enable RTS/CTS for any of its associated stations). If transmissions are hampered by the suspected existence of hidden nodes (e.g. due to the use of carrier sense adaptation mechanisms such as with DSC), stations can then opt for the usage of the aforementioned method. In [91], the authors highlight the possible mechanism through which an AP can control the RTS/CTS policy for the associated stations.

In Figure 4.7, we indicate simulation results of a network that encompasses DSC and intelligent RTS/CTS mechanism. Uplink transmissions under saturation condition was assumed where each station was continuously transmitting frames of maximal duration (i.e. worst case environment scenario was assumed). The details of simulation environment can be found in Section 5.5.

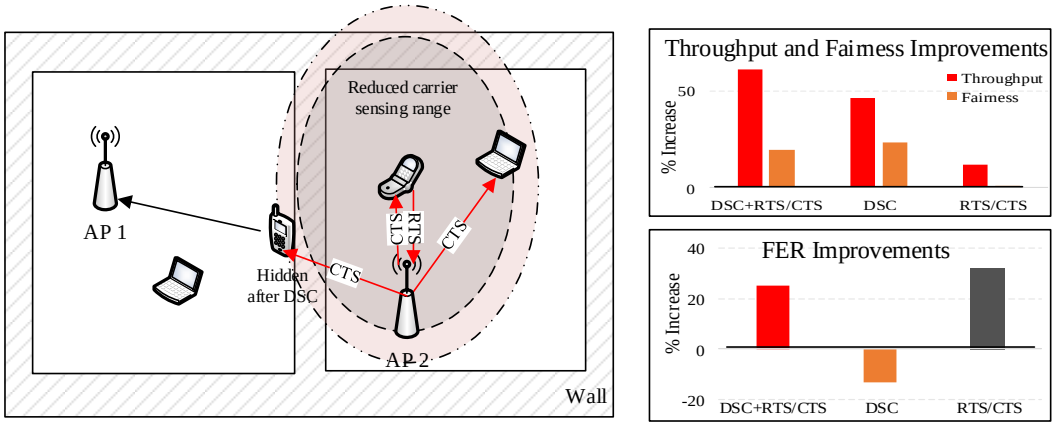


Figure 4.7: TGax proposal for PHYCCA modification and controlled use of RTS/CTS mechanisms.

Figure 4.7 indicates considerable gains when DSC (i.e. around 40% throughput gain) as well as DSC with intelligent four-way handshake mechanism (i.e. around 60% throughput gain) are combined in dense residential environment.

4.4.3 Multi-user enhancements

Authors in [103] provide thorough calculations for some multi-user enhancement proposed for IEEE 802.11ax and signify the importance of frame size and SINR over the proposed multi-user schemes. In this section, we expose the state of the art multi-user techniques that are being investigated by TGax to achieve efficiency gains in high dense deployments. combined in dense residential environment.

4.4.3.1 Downlink and Uplink OFDMA

OFDM is a multiplexing technique that divides the available bandwidth into multiple orthogonal frequency sub-carriers. OFDMA operates on top of OFDM, where the base station allocates the subset of carriers to each user so as to accommodate multiple simultaneous transmissions. OFDMA uses a synchronous medium access that results in reduced contention (i.e. less collisions). This technique is very robust within multipath and frequency selective radio channels. Furthermore, it reduces collision probability (or losses due to interference), which reduces delay and increases throughput. However, to make the most of it, dynamic channel allocation with advanced coordination among adjacent APs is desirable for OFDMA to operate in high density deployments. In [23], the authors indicate benefits of utilizing OFDMA in dense networks.

Thus, IEEE 802.11ax task group has defined the uplink and downlink OFDMA (where the minimum size of Resource Unit (RU) comprises 26 sub-carriers) as the key multi-user feature to improve PHY layer efficiency. Different stations in dense environments that inefficiently contended for the shared resources, are allocated dedicated sub-channels that increase the average end user throughputs. In [85], the authors propose an OFDMA based multi-user access framework for IEEE 802.11ax.

In order to amicably allow the operation of OFDMA, the IEEE 802.11ax proposes the utilization of a specific HE-PPDU format, called HE trigger-based PPDU, which allows the announcement of scheduling decisions. This feature helps to reduce synchronization complexity. The channel allocation mechanism (consisting of methods to allocate available RUs at the downlink and the uplink) is managed by the AP.

At the uplink, the IEEE 802.11ax defines OFDMA based distributed random access mechanism that randomly selects resource units assigned by the AP for transmission of uplink PPDUs. The trigger frame includes a parameter to initiate random access at the uplink.

4.4.3.2 Downlink and Uplink Multi-user MIMO

The concept of multi-user MIMO transmissions, where different data streams are used to serve multiple users simultaneously at uplink as well as downlink (i.e. multiple data streams are transmitted from different users instead of multiple data stream being transmitted by single user), can increase the overall system capacity, as compared to a single user MIMO, where a single user is served by multiple streams. Thus, Multi-user MIMO takes advantage of benefits of space-division multiple access as well as high capacity advantages associated with MIMO.

This technique is particularly useful in the uplink because the complexity on the client side can be kept at a minimum by using only few transmit antenna. However, the AP can have eight or more streams and, thus, could potentially serve many stations simultaneously.

Downlink MU-MIMO has already been introduced in IEEE 802.11ac standard. In [58], the authors provide a thorough and updated overview of different MU-MIMO MAC schemes proposed in literature for IEEE 802.11 standards and amendments.

In MU-MIMO, transmissions to several stations are overlapped in the same time-frequency resources (i.e. several stations simultaneously communicate with a base station equipped with multi-

ple antennas) by exploiting the spatial diversity of the propagation channel.

TGax intends to add uplink MU-MIMO to operate along with downlink MU-MIMO. In uplink MU-MIMO, multiple stations are allowed to transmit simultaneously over the same frequency resources to the receiver. Similar to OFDMA, Trigger based PPDU is used to indicate the transmitting stations when to transmit the uplink MU-MIMO PPDUs.

4.4.3.3 Multi-user aggregation

Multi-user aggregation scheme operates to reduce transmission overheads (i.e. SIFS, DIFS, backoff, etc.) induced by short frames (such as small size PPDU or ACK, etc.) by aggregating different frames addressed to different stations.

Frame aggregation was introduced in IEEE 802.11n to reduce overhead by allowing the transmission of multiple data frames in a single channel access (provided that they have the same destination). IEEE TGax aims to further extend the aggregation procedure by defining multi-user aggregation scheme, that will allow a single access to send frames to multiple recipients. This scheme operates to reduce transmission overheads.

4.4.4 Other notable features

4.4.4.1 Energy efficiency techniques

According to the design guidelines set by TGax, IEEE 802.11ax enabled devices are expected to reduce energy consumed per successful information bit. However, different amendments that are proposed to increase the efficient operation of PHY and MAC layer would work against the aforementioned requirement.

In order to decrease/maintain the utilized energy, TGax is actively pursuing to refine current sleep state and to incorporate power saving techniques, which might allow either to extend sleep time or would allow awake time to be reduced. These mechanisms will assist in high density network conditions as well as for low power mode of operation.

In addition, the TGax is also exploring the possibility to reuse different energy efficiency techniques proposed for the upcoming IEEE 802.11ah standard (such as TWT, where a routine and schedule for sleep is permitted by the AP to the associated stations). Detail of TWT proposition is provided in Section 3.3.6.6.

4.5 Expected challenges posed to high efficiency Wi-Fi

Since IEEE 802.11ax is most likely to be used along side advanced cellular wireless technologies, such as LTE, or its advanced version (LTE-A), in this section, we highlight the expected co-existence challenge. Furthermore, the IEEE 802.11ax amendment is also being explored as a viable communication network to support the IoT paradigm. Therefore, we expose the expected opportunity and challenges for TGax within IoT scenarios.

4.5.1 Challenge of LTE in unlicensed spectrum

As highlighted in section 4.1, densely deployed small cells are an effective means to boost the capacity and coverage demand of end users data traffic. Apart from Wi-Fi networks, other wideband access technologies are considering to start competing in the unlicensed spectrum arena. LTE in unlicensed band has been evaluated by LTE-U forum and 3rd Generation Partnership Project (3GPP) to combat the explosive growth of traffic volume.

The legacy IEEE 802.11 utilizes PHYCCA based LBT process before transmitting a data frame. PHYCCA is composed up of Physical Preamble Detection (PHYPD) and Physical Energy Detection

Table 4.1: Comparison of IEEE 802.11ax amendment with LTE in unlicensed spectrum.

Parameter	IEEE 802.11ax	LTE-U and LAA-LTE
Design architecture	Centralized and distributive	Centralized
Channel bandwidth (MHz)	20, 40, 80, 160	1.25, 2.5, 5, 10, 15, 20
Highest order Modulation scheme	1024-QAM	256-QAM
Access technology	CSMA/CA and OFDMA	TDD based OFDMA
Handover	Client-driven, network-assisted	Network-driven, client assisted
Interference problems	Collisions, hidden and exposed node problem, partially overlapping channels	Co-channel co-tier, cross tier interference, For LAA-LTE (additional interference due to collisions)
Scheduling	Contention based de-centralized EDCA, OFDMA based centralized	For LTE-U (Base Station controlled without contention), For LAA-LTE (Contention based de-centralized, EDCA)
Range	Possible methods under consideration to improve range	Better range characterization as compared to legacy IEEE 802.11
Rate control	Vendor specific algorithms (implicit and explicit feedback based on probing, lack of acknowledgments, etc.)	Constant channel feedback
MAC and PHY layer protocol overheads	In-band signaling (e.g. RTS/CTS, sounding, Null data, etc.), headers, Pilot symbols, etc.	Control channel signaling, LBT (non-adaptive backoff range), CSAT (channel oblivious duty cycle), Pilot symbol, transmission scheduling etc.
Integration with current 4G networks	Requires Mobile Core Integration (MCI) for mobile offload	No requirements
Coexistence with other technologies	Based on LBT	For LTE-U (CSAT and optional LBT), For LAA-LTE (Based on LBT)
Potential market	Belongs to IEEE 802.11 family and is a natural evolution	Motivation for operators to enable/extend services to unlicensed spectrum without the need to integrate with a non-LTE technology

(PHYED) methods. PHYPD method is employed to detect and decode the preamble of other Wi-Fi stations' frames: if energy level of the detected preamble is above the CST, the channel is sensed busy. PHYED (first introduced in IEEE 802.11a to counter the noise generated from OFDM transmitters and later evolved to detect any signal over the shared channel) operates to detect whether any energy (regardless of the type of signal or noise) is present in the channel. The PHYED threshold is generally assigned a value greater than CST (i.e. 20 dB greater).

Unlike Wi-Fi, where devices use a distributed mechanism to contend for access to the wireless medium, LTE relies on base stations as central schedulers for medium access of all associated nodes in a cell. Since operation in unlicensed bands is non-exclusive, medium access inherently needs to employ means for fair spectrum sharing.

In order to shorten the time to market of a first wave of 5 GHz compatible LTE devices, the initial LTE-U framework seeks a minimal impact on current specifications and does not rely on LBT. Instead, LTE-U incorporates a dynamic On/Off scheme called Carrier-Sensing Adaptive Transmission (CSAT). CSAT allows LTE-U transmissions to be scheduled according to a duty cycle (where the off period is selected based on the sensed channel activity). Early studies on co-existence between Wi-Fi and unlicensed LTE indicate inconsistencies within simulation and demonstration results. Some results show that the absence of LBT in LTE-U causes a co-existence issue [17], whereas, other results point to negligible or no impact [95]. However, spectrum regulations defined in ETSI EN 301 893, require the use of LBT in the 5 GHz ISM band across Europe.

The 3GPP variant of unlicensed LTE is called License Assisted Access (LAA-LTE). LAA-LTE, aims to design LTE specifications for global harmonization that allow for fair co-existence with IEEE 802.11. LAA-LTE employs a medium access scheme similar to IEEE 802.11's EDCA. EDCA-like operation utilizes carrier sensing and a priority based backoff mechanism that require changes in LTE specifications. Two types of LBT schemes are defined by LAA-LTE: Frame Based Equipment (FBE) and Load Based Equipment (LBE). These two schemes differ in that the former includes a strict frame structure that should follow the interference avoidance mechanism and channel occupancy. However, LBE is the baseline approach which includes random backoff and variable size of contention window, that is similar to the random access procedure used by Wi-Fi stations.

With context to the co-existence challenge, both CSAT and LBE techniques appear to be aggressive. While CSAT technique might result in overlap of Wi-Fi with LTE transmissions, the nodes using LBE utilize a static range for backoff procedures (unlike Wi-Fi, where exponential backoff process based on contention window is used). Therefore, the co-existence impact on fairness and throughput with respect to LTE, which needs further evaluation, can be considered a current challenge for IEEE 802.11ax standard.

In summary, whereas LAA-LTE and IEEE 802.11 use similar medium access mechanisms and thus, compete in comparable conditions, LTE-U uses a dissimilar approach, not suited for all regulatory domains. However, with the upcoming LTE-U specification introducing LBT into CSAT, co-existence studies between IEEE 802.11ax and LTE-U will need to be revisited. Building on the argument, authors in [67] highlight latest trends regarding those co-existence problems; they propose radio resource management based on comprehensive network monitoring and centralized scheduling within a software-defined networking paradigm to solve the co-existence challenges.

Apart from MAC layer, other notable differences between IEEE 802.11ax and LTE in unlicensed spectrum are highlighted in Table 4.1.

Therefore, LTE being a centralized scheduling scheme, will change the ecosystem within unlicensed spectrum. Furthermore, as highlighted in Table 4.1, the difference in technologies would

lead to no common control channel between LTE and Wi-Fi. The novel techniques proposed within IEEE 802.11ax amendment will help Wi-Fi in combating added interference by and to fairly share the medium with LTE unlicensed.

In spite of the aforementioned co-existence challenge, developing seamless methods to allow the foregoing technologies to operate by aggregating their capabilities can provide users with compelling experience. LTE and LTE Wi-Fi Link Aggregation (LWA) is another proposition put forward by 3GPP. Unlike LTE-U and LAA-LTE, LWA does not introduce a new co-existence mechanism but an interworking framework. The most important aspect of LWA is that it could be enabled with straightforward software upgrades and will allow user data to be simultaneously streamed through both Wi-Fi and LTE interfaces, making use of specific transport protocols such as Multi-Path TCP (MPTCP).

4.5.2 Opportunities and challenges from the IoT paradigm

The IoT communication paradigm envisions the presence of objects equipped with transceivers for digital communication and microcontrollers along with suitable protocol stack that would enable them to connect to the Internet. Therefore, IoT aims to make the Internet pervasive and includes interconnection of consumer electronics and user equipment in homes, offices and cities. The application area of this paradigm lie in different domains, such as home/office automation, industrial automation, medical aids, mobile healthcare, elderly assistance, intelligent energy management, smart grids, traffic management, and so on.

Since the amount of information generated over IoT application areas is expected to be huge and increasing (due to the increase of connected devices), there is a need to adopt universally accepted, cost effective and scalable communication technologies within IoT frame work.

In terms of ongoing enhancements to IEEE 802.11 standard, the proposed IEEE 802.11ah amendment (focuses on operations in the S1G band) is specifically being designed for IoT applications. The key aspects of IEEE 802.11ah, summarized in Table 4.2 and in Chapter 3, are improved energy-saving (e.g. through TWT and longer sleep periods), better coverage (utilizing lower frequency band and more robust modulation and coding), and the ability to simultaneously handle over 8,000 nodes. However, as highlighted by [4], the recent delays in the development process might lead to a situation where IEEE 802.11ah will face heavy competition upon its arrival from other already introduced and promising technologies (such as SigFox, LoRa, BLE, some IEEE 802.15.4 variants, etc.) that seek to operate at the same IoT market.

The aforementioned challenge has resulted in new proposals being explored by TGax to accommodate the IoT use cases. In July 2015, the IEEE 802.11 working group created a new topic interest group, called Long Range Low Power (LRLP) to address the need of M2M, IoT, energy management, and sensor applications. This group intended to develop methods to provide longer range operation of Wi-Fi on the 2.4 GHz band. This new development poses a new co-existence challenge for next generation of WLANs.

In particular, the IEEE802.11ax amendment is not focused on IoT applications. As highlighted in

Table 4.2: Comparison of IEEE 802.11ax amendment with IEEE 802.11ac and 802.11ah amendments.

Parameter	IEEE 802.11ac	IEEE 802.11ah Draft 9	IEEE 802.11ax Draft 1.0
Spectrum	<6 GHz, excluding 2.4 GHz	863-868 MHz Europe and 902-928 MHz US	Between 1 and 6 GHz
Bandwidth	20 to 160 MHz	1 to 16 MHz	20 to 160 MHz
Modulation	BPSK to 256-QAM	BPSK to 256-QAM	BPSK to 1024-QAM
FFT size	64 to 512	32 to 512	256 to 2048
OFDM symbol duration	4/3.6 μs CP	40/36 μs CP	13.6/14.4/16 μs CP
Pilot Sub-carriers	4/6/8/16	2/4/6/8/16	2/4/6/8/16
Subcarrier spacing	312.5 kHz	31.25 kHz	78.125 kHz (smaller value to increase range/coverage for OFDMA systems)
Number of spatial streams	1 to 8	1 to 4	1 to 8
MIMO	SU and DL-MU	SU and DL-MU	SU and DL-UL-MU
Guard interval	Long and short	Long and short	Long, Additional guard interval durations for outdoor channels, Short guard not available
Backward compatibility	IEEE 802.11a/n	NA	IEEE 802.11a/b/g/n/ac
Mechanism to reduce power consumption	NA	TWT	TWT

Section 4.3, its prime objective is to increase efficiency and to allow numerous stations to simultaneously communicate in a geographically limited area. However, the main motivation to choose IEEE 802.11ax for IoT devices is that the proposed amendment is expected to be a de facto Wi-Fi standard in future, built on different chips and devices that would constitute the basic building block of IoT systems. Furthermore, based on different requirements and use cases, it is expected that in future, a mix of technologies would enable the connection to all the devices (i.e. IoT is not a single system, platform or technology but a combination of many technologies). The IEEE 802.11ax standard would be one of the capillary radios to enable the aforementioned connectivity.

Two approaches had been discussed within the LRLP and TGax: i) introducing narrow band OFDMA transmissions with smaller sub-carrier spacing, and ii) accommodating LRLP transmissions in form of single carrier modulations within a new OFDMA scheme, combined with smart link adaptation. In May 2016, the LRLP topic interest group was dissolved, where it was decided by the IEEE 802.11 working group to focus on the issue of low power (leaving aside the long range feature). Currently, the IEEE 802.11 working group is in process to design a new amendment, named IEEE 802.11ba (which is built on the suggestions put forward by LRLP) that aims to enable operations of WUR to prolong the battery lifetime and low latency of IoT devices. WUR is expected to use

narrow-band (i.e. 4 MHz OFDM signals) and low-throughput technology. Thus, this new amendments would enable IEEE 802.11 to avoid non-negligible portion of the wireless medium occupied with wake up frames (or control information) by numerous IoT stations.

Table 4.2 provides an overview of the key technical features of IEEE 802.11ax as compared to IEEE 802.11ac and IEEE 802.11ah amendments. Apart from the methods to improve user experience within dense deployments, TGax has proposed to include longer OFDMA symbols and Cylic Prefix, which can increases the range and coverage. In addition, TWT method is included in the draft version to provide means of reducing power consumption that can be utilized for the IoT devices.

4.6 Conclusion

In this chapter, we have provided a thorough overview of IEEE 802.11ax (a future high efficiency Wi-Fi standard being designed to increase capacity within high density and outdoor deployments). The contents of the chapter are updated to comply with latest draft version of IEEE 802.11ax. After we point out the necessity and scope of the proposed amendment, we introduce the most important technological improvements that will form the basis of the next generation of WLANs. Finally, we highlight the expected co-existence challenge of IEEE 802.11ax with LTE in unlicensed band. In addition, we expose the expected opportunities and challenges for TGax within IoT scenarios.

5

Dynamic Physical Clear Channel Assessment in IEEE 802.11

The popularity and wider acceptance of IEEE 802.11 based WLANs has resulted in their dense deployments in diverse environments. While this massive deployment can potentially increase capacity and coverage, the current physical carrier sensing of IEEE 802.11 cannot limit the overall interference induced and also cannot insure high concurrency among transmissions. In addition, the new IEEE standards (i.e. IEEE 802.11n and IEEE 802.11ac) were developed with the intention to improve the physical rate. However, mitigation of increased interference incurred due to the existence of many AP and non-AP devices has not been addressed in any of the current WLAN standards.

In previous chapters, an overview of IEEE 802.11ah and IEEE 802.11ax amendments was provided, which aimed to improve network performance of legacy IEEE 802.11. The driving force behind IEEE 802.11ah is the need to avoid saturation of the existing cellular networks, so as to provide unlimited, cost effective and license-free spectrum solutions for IoT applications. Despite the possibility to support numerous devices with enlarged coverage area, its is not difficult to foresee overlapping cells (with hundreds and thousands of connected devices) in future that would result in MAC inefficiencies (due to OBSS problem). To build on these challenges, IEEE 802.11ax on the other hand, is particularly being designed with focuses on enhancing the system performance in dense deployment scenarios to reduced congestion caused by HetNet paradigm requirements (such as traffic offloading by cellular infrastructure, and so on). This would be accomplished by efficiently using the unlicensed spectrum, optimizing spatial reuse and introducing robust interference management schemes, along with other MAC enhancements.

Optimization of spatial reuse and network throughput within interference limited wireless networks has been widely studied in literature. Since, in dense deployments, MAC protocol plays an important role in the achieved performance (in terms of fairness, delay and throughput), it is mainly desired to allow as many concurrent transmissions as possible with minimal increase in collisions (interference). Particularly with the inclusion of *Capture Effect* [40], the interaction between PHY

and MAC layer mechanisms is thought to increase spatial reuse by reducing the impact of interfering transmissions (i.e. collisions). In addition, it is also expected that the performance benefits would be acquired with minimum hardware/firmware modifications.

The MAC protocol of IEEE 802.11 encompasses several components that are related to medium access, collision resolution and capacity optimization. Carrier sensing mechanism is used to detect simultaneous transmission and helps to reduce collisions. PHYCCA is an essential ingredient of Wi-Fi networks that employs channel sensing as part of medium access mechanism. In order to resolve contention, binary exponential backoff mechanism defines the rules for retransmissions. In addition, data rate adjustment (such as the auto-rate function) is performed according to the signal quality that results in capacity optimization.

PHYCCA is the crucial component of IEEE 802.11 MAC, that determines the possibility of a station in accessing the shared medium. This mechanism assists in the amicable sharing of a particular communication channel among multiple stations and reduces the likelihood of collision by preventing nodes in the vicinity of each other from transmitting simultaneously. Two stations are allowed to transmit at same time as long as they are sufficiently separated from each other (i.e. the two concurrent transmissions do not interfere with each other). In spite of the simplicity, carrier sense adversely limits the network capacity because of the inadequately restricting simultaneous transmissions. The problem becomes an unprecedented challenge in dense WLAN deployment and results in reduced overall throughput by restricting the effective spatial reuse in the network. In the following chapter, we introduce techniques proposed to enhance the MAC operations (i.e. dynamic carrier sensing mechanism with the ability to improve spatial reuse along with better interference management) of high density IEEE 802.11 network. The presented work constitutes in part the MAC design by TGax in the draft version of IEEE 802.11ax.

In this chapter, we first highlight the problems associated with carrier sensing mechanism in legacy IEEE 802.11 networks. We then use a simple approach to indicate how carrier sense threshold can be derived to maximize spatial reuse in dense environments. Next, we utilize snapshots of a realistic (simulated) densely deployed WLAN network to describe the extent of hidden and exposed node problems. Moreover, we also showcase the benefits achieved by dynamically adapting PHYCCA of each station within the network. Based on the outcome of the aforementioned derivation, we then expose the working of a mechanism to dynamically adapt the carrier sensing of each station within a dense WLAN network based on local information (that is proposed at the IEEE 802.11ax) to increase area throughput of densely deployed WLAN networks). This concept, called Dynamic Sensitivity Control (DSC), allows multiple concurrent transmissions to co-exist which result in an enhanced overall throughput and fairness over the cost of increase in hidden nodes and FER. It is important to highlight that even though the proposed scheme is presented for IEEE 802.11ax amendment, this approach can maintain backward-compatibility with legacy hardware and can be implemented over the current available IEEE 802.11 standards (i.e. 802.11/n/ac).

Since conventional interference management techniques, when applied intelligently within dense deployments, can also ease the overall network conditions, we study the potential benefits of com-

bining intelligent carrier sense adaptation and uplink RTS/CTS control that can increase the performance efficiency by minimizing the negative effects of an adaptive PHYCCA mechanism (i.e. increase in FER).

Majority of the work presented in this chapter is published in [7, 8, 11, 12]

5.1 Motivation

Wi-Fi networks are generally characterized by high peak rates but lower efficiency towards small packet sizes and by limited coverage. The first problem has been solved by the inclusion of frame aggregation (in IEEE 802.11n and newer standards); small cell paradigm (containing ubiquitous deployments of APs) has automatically solved the later issue. Despite the increase in overall throughput due to lesser clients per AP and increased possibilities of concurrent transmissions, most of the APs in dense deployments are assigned same transmission channels (due to the scarcity of available channels) and due to uncoordinated/unmanaged deployments. The aforementioned problem leads to increased co-channel interference that results in significant rise in frame collisions. Thus, effective management of interference that would result in improved spatial reuse is the primary challenge to increase the area throughput within densely deployed WLAN networks.

In IEEE 802.11, DCF is the dominant/default contention based medium access scheme, that defines two modes of operation; the basic two way handshake mechanism and the optional reservation scheme based on four-way handshake (called RTS/CTS). Before initiating a frame transmission, each station utilizes LBT to sense the channel. The CSMA/CA protocol enforces stations to contend to gain access of the shared medium resources (terminals seeking to transmit, first sense the channel state and initiate transmission only when no other transmission is underway). That is, DCF provides all stations (i.e. AP or non-AP) with equal medium access probability. In consequence, in saturation conditions, that access fairness creates a contention asymmetry between uplink and downlink data traffic.

Carrier sensing in IEEE 802.11 is performed at both PHY and MAC layers. Virtual Carrier Sense (VCS) scheme, which utilizes the NAV timer, is employed at the MAC layer to maintain a prediction of future network traffic and operates by stations observing the Duration field present in the MAC frames (such as RTS, CTS and so on) of the traffic not destined for them. This field is set by the transmitter based on frame length, transmit rate and other PHY layer characteristics.

At the PHY layer, IEEE 802.11 carrier sensing includes PHYCCA procedure (which is a function of PLCP). In order to detect the channel condition, Physical Carrier Sensing (PCS) examines the signal strength of the physical channel prior to transmission (for stations intending to transmit). If the measured RSSI is above a predefined threshold, the station senses the channel to be busy and thus differs its transmission. There are two main purposes of PCS: i) to determine whether a transmission is incoming for a receiving station, and ii) to assess whether the channel is clear based upon the waveform and energy detection.

Both PHYCCA and NAV operate in conjunction and aim to provide defense against possible colli-

sions. Despite the runtime process of updating PHYCCA after every slot time, NAV can assist hidden stations operating in the same BSS, and for stations to reserve medium in advance (for ACK transmissions immediately required after correct reception of frames, and so on).

For the case of OFDM PHY layer, the PHYCCA uses two mechanisms to assess the state of the channel: PHYED and Carrier Sense (CS)[1]. Figure 5.1 describes the steps followed by each station before transmitting on the shared medium. The current IEEE 802.11 specifications [45] list six PHYCCA operation modes to determine whether the channel is occupied by other stations or is idle. These modes, specified by the usage of different combination of PHYED and CS, are listed as : i) Only PHYED is used (PHYCCA reports the medium as busy upon detecting any energy above PHYED threshold), ii) Only CS employed (upon properly decoding an IEEE 802.11 preamble, the PHYCCA indicates a channel busy indication), iii) CS with PHYED (if the energy of the decoded IEEE 802.11 preamble is above PHYED threshold, the PHYCCA will signal a channel busy status), iv) CS with a timer (PHYCCA initiates a timer with duration of $3.65ms$, and reports medium to be busy only if signal is received within the timer duration), v) Combination of CS with a timer and PHYED (PHYCCA reports medium to be busy while the PPDU being received at the antenna has energy above PHYED threshold[2]), and vi) energy above -62 dBm (PHYCCA reports medium to be busy upon detecting energy above -62 dBm). For HT transmissions, IEEE 802.11 specifies the requirement of using PHYED.

The CS scheme (also called preamble detection) refers to the ability of the receiver to detect and decode the incoming IEEE 802.11 preamble. It involves the procedure to match the received preamble with known training signal signatures of other IEEE 802.11 devices. When a valid OFDM transmission is received at a level greater or equal to MCS sensitivity (i.e. preamble is usually sent with minimum MCS rate sensitivity, where it should be greater than or equal to -82 dBm for 20 MHz channel spacing, -85 dBm for 10 MHz and -88 dBm for 5 MHz), the CS mechanism reads the length field of L-SIG portion of PLCP and extracts the duration of the current frame. The PHYCCA is then set to busy state.

Contrary to CS, PHYED is based on the presence of raw RF energy and indicates the occupancy of medium independently to the characteristics of the received signal (i.e. the energy could be from noise floor, interference from non-Wi-Fi or transmissions from Wi-Fi stations that have low power or are corrupted). Therefore, even if the preamble is missed (not detected), the receiver can still sense an on-going transmission and trigger the PHYCCA busy through the PHYED mechanism.

The OFDM PHYCCA leverages valid IEEE 802.11 signal detection and/or ED based on the availability of an OFDM preamble. The receiver should be able to detect and measure the signal power equal or greater than the receivers minimum sensitivity. If no OFDM preamble is detected, the detection process is extended to any energy present over the channel. The detection level is set to +20 dB above the MCS sensitivity (i.e. -62dBm).

Therefore, PHYCCA protocol utilizes carrier sensing measurements. If the measured energy level is above a predefined threshold, the node senses the channel to be busy and thus differs its transmis-

[1] CS is also referred to PHYPD.

[2] Mode (v) combines mode (i) and (iv). A signal should be detected with sufficient energy before the channel is reported busy.

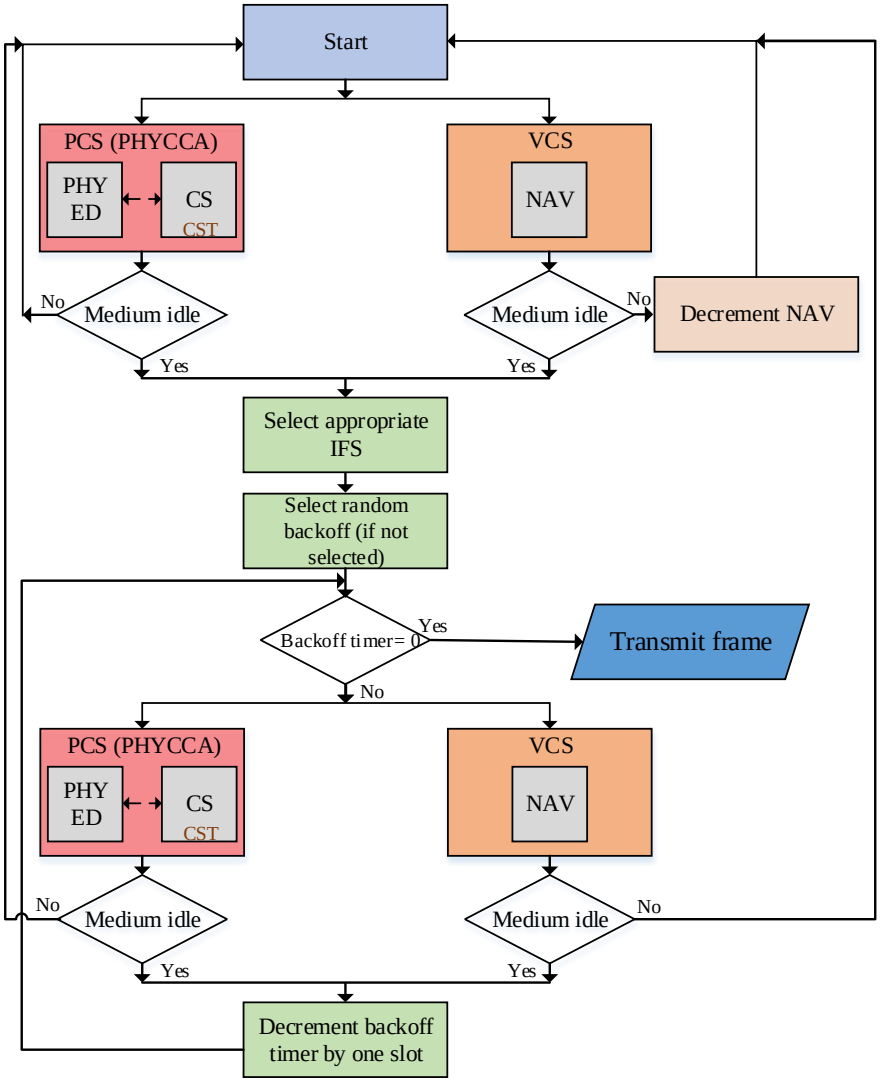


Figure 5.1: IEEE 802.11 channel access mechanism [22].

sion. This predefined threshold is called CST. Note that the CST is (currently) fixed (to the minimum sensitivity of -82dBm, or greater, depending on the bandwidth). TGax proposes that the threshold can be assigned a varying value. A more aggressive (i.e. higher) CST will result in more transmission opportunities at the cost of increased collision probability. Thus CST can be optimally tuned so as to increase efficiency within dense networks.

In order to improve the co-existence among densely deployed WLAN networks and to provide continuous coverage at higher transmission rates, Wi-Fi devices can either be made to minimize their area of influence (by reducing the transmit power) or to increase the CST value so as to accept higher interference. Both of these techniques, if not utilized intelligently, can result in negative effect

on the achievable transmission rates due to higher observed interference levels.

In current IEEE 802.11 standards, the CST is assigned a fixed value, which leads to well investigated hidden and exposed nodes problems. While hidden nodes are the main cause of collisions in WLAN networks (due to transmission of nodes that are present in each others carrier sensing range and are unable to hear each other due to obstruction or distance), the exposed node problem has been found to have greater implications for dense deployments (where stations are unnecessarily silenced due to over protected PCS method).

More formally, assuming P_{XY} is the power of X's transmissions at receiver Y and Sr is the sensitivity (minimum power in reception to decode an 802.11 frame), we define hidden, exposed and contending stations as,

- We consider two nodes X, Y to be hidden from each other if they are not within each other's carrier sensing range CS_R ($P_{XY} < CST_Y$ and $P_{YX} < CST_X$) and a station Z, which is the intended receiver of either X or Y, is placed within both X's and Y's transmission range ($P_{XZ} > Sr_Z$ and $P_{YZ} > Sr_Z$).
- Conversely, nodes X and Y are exposed if they are able to defer each other's transmissions ($P_{XY} > CST_Y$ and $P_{YX} > CST_X$) but are unable to reach each other's intended receivers Z1 and Z2 ($P_{XZ2} < Sr_{Z2}$ and $P_{YZ1} < Sr_{Z1}$) respectively.
- Nodes X and Y are contending when they are able to defer each other's transmission ($P_{XY} > CST_Y$ and $P_{YX} > CST_X$).

The above mentioned definitions of hidden, exposed and contending stations are used throughout this chapter.

The hidden and exposed node problem can severely impact the performance of dense Wi-Fi networks. Particularly for the case of exposed nodes, spatial reuse is greatly affected when stations unnecessarily remain silent due to the over protected PCS method, even though the possibility of multiple concurrent transmissions exists (with small increase in number of collisions). It has been shown in previous studies [47, 111] that intelligent adaptation of tunable PCS threshold at each node (without the need of network level coordination) can yield better aggregate throughput in high density 802.11 networks. As a drawback to the aforementioned adaptation, authors in [112] highlight that severe fairness problems can occur when stations are allowed to modify their CST based on their own FER due to starvation created by hidden nodes.

In dense WLAN deployments, both hidden and exposed stations impact the overall throughput attained by the network. It is easy to visualize from Figure 5.3, that solving the exposed stations results in increase of hidden station problem. Both hidden and exposed terminals waste system capacity through failed transmissions and missed transmission opportunities, respectively. Since, as shown in following sections, the exposed node problem is more prevalent in dense scenarios, controlled methods to restrict the exposed nodes (with restricted increase in hidden nodes) can result in improvements in overall system throughput (through the increase of transmission opportunities for all stations).

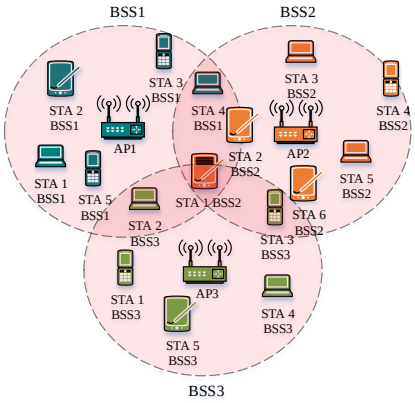
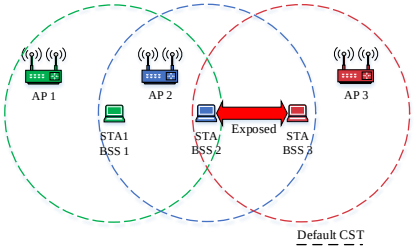
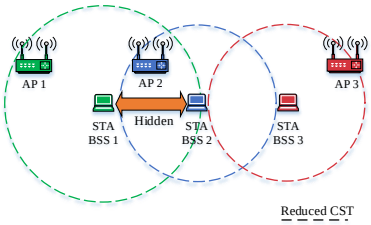


Figure 5.2: High density scenario where numerous Wi-Fi enabled devices co-exist with overlapping BSS problem.



(a) Utilizing default CST generates exposed node problem.



(b) Increasing CST reduces expose nodes, but causes increase in hidden nodes

Figure 5.3: Problems with CSMA/CA based carrier sensing mechanism.

Therefore, intelligent CST adaptation has the potential to improve the area throughput within densely deployed networks, but it requires real-time measurements to provide per station decisions so as to adapt to the particular circumstances faced by each station.(i.e. carrier sensing range is reduced so that the station is able te sense signals from its intended transmitters and, as a consequence, the station is exposed to lesser number of stations). Furthermore, due to the inherent trade-off between collisions and spatial reuse, this algorithm should also confine the increase of FER due to increased number of collisions caused by hidden nodes. With respect to the design constraints related to IEEE 802.11, this algorithm is also expected to operate over all standards (be backward compatible) with minimum required changes in the existing MAC design.

Based on aforementioned requirements, in this chapter, we propose a runtime self adaptation (dynamic) algorithm that modifies the CST of each station. The dynamically adapted CST, based on local measurements (i.e. received power of frames from intended transmitters) results in improved PCS method without the need of any additional frame exchange between the transmitter and the receiver. Importantly, this algorithm aims to improve spatial reuse by using methods to restrict the increase in FER. Intuitively, by avoiding exposed station in a contained manner, the link transmission opportunity within a network increases that in-return leads to improved transmission fairness and optimized concurrent transmissions.

One of the drawbacks of allowing multiple concurrent transmissions to co-exist in geographically limited area is the increase in hidden nodes, which results in increase of system level FER [12]. The

hidden node problem can get further aggravated for stations within high density networks due to obstacles, transmit power, location and mobility.

In order to combat the hidden node problem (so as to reduce collision probability), the legacy IEEE 802.11 has already devised the optional RTS/CTS access mechanism, where RTS and CTS frames are exchanged prior to transmission of data frames. Nowadays, this optional feature is widely adopted (mainly due to large aggregated frames used in IEEE 802.11n/ac/ax), although its use was limited in IEEE 802.11a/b/g due to the additional overhead associated with temporary reservation of the shared medium (i.e. for small data frame size used, this overhead became significant). RTS/CTS is an effective scheme when network traffic is high, where excessive collisions cause network capacity to decrease due to large frames being dropped. On the other hand, RTS/CTS dialog is not adopted when traffic includes small frames (such as voice etc.), where data frame size is smaller than RTS frame that causes increased collision probability. Thus, the problems associated with RTS/CTS method counterbalance its positive aspects in network with mixed traffic conditions and thus an adaptive mechanism is required to enable RTS/CTS through a selective approach.

5.2 Related work

The implication of physical carrier sensing to reduce interference and to increase performance (due to improved spatial reuse) have been extensively investigated by different researchers [97]. In the legacy IEEE 802.11 standard [43], CST values for AP and non-AP stations are set conservatively to prevent concurrent transmissions within a large area, known as carrier sensing range, when multiple nearby transmitters could actually operate simultaneously without causing ample degradation in channel conditions. Therefore, the main optimization problem is to choose a CST value that would allow multiple simultaneous links to operate together and, as a consequence, increase the overall throughput and fairness of the network.

Authors in [66] demonstrate simple modifications that can be made in carrier sensing mechanism to increase the overall throughput in dense networks. They propose changes to be made in DCF over IEEE 802.11 networks that can result in added complexity due to additional signaling over the network. Nevertheless, their proposed scheme can be viewed as a step towards the design of an algorithm that dynamically changes CST of a node based on received power. Similarly in [70], the authors propose cognitive protocol for enabling and disabling virtual NAV and PCS. Their methods require additional information to be added to RTS/CTS control frames and they use a heuristic method to modify the CST.

The increase in performance achieved by optimally adjusting CST is revealed in [5], where the authors propose that for maximum throughput, the CST is linearly dependent on the nodal density. However, the authors have not mentioned the adjustment method and the throughputs are evaluated for regular topologies by adjusting different threshold values. In [108], the authors propose a localized spatio-temporal algorithm that jointly controls contention window and carrier sensing threshold to enhance the spatial reuse and optimize the overall throughput in the network.

Table 5.1: Functionality Comparison

	Hidden/ Exposed node analysis	Fairness analysis	FER analysis	Principle of CST variation	Hardware/Software constrains	Approach
DSC	Yes	Yes	Yes	RSSI based CST adaptation	Additional software required at all stations	Distributed
Kulkarni et al. (2015) [53]	No	Yes	Yes	FER based CST adaptation	Additional software required at all stations	Distributed
Murakami et al. (2015) [72]	No	Yes	No	Physical position based CST adaptation	Software and hardware additions are essential. In addition, feedback mechanism is required	Centralized
Jamil et al. (2014,2015) [47, 48]	No	No	No	RSSI based CST adaptation	Software and hardware additions required	Distributed
Madan et al. (2012) [66]	No	No	No	RSSI based CST adaptation	Requires modification to be made in the 802.11 access mechanism	Distributed
Zhang et al. (2011) [108]	No	No	No	FER based CST adaptation method encompassing frame loss differentiation.	Additional software along with activating four-way handshake mechanism required at all stations	Distributed
Acholem et al. (2010) [5]	No	Assumed constant	No	Local Optimization of the CST over time, based on the current local network density	Mechanism required to estimate the local nodal density	Distributed
Haghani et al. (2010) [41]	No	No	No	RSSI based CST adaptation	Additional software along with feedback mechanism required at all stations	Distributed
Ma et al. (2009) [65]	No	No	No	FER based CST adaptation	Additional software along with feedback mechanism required at all stations	Centralized
Zhou et al. (2007) [110]	No	No	No	RSSI based CST adaptation	Additional software along with feedback mechanism required at all stations	Distributed
Vasan et al. (2005) [102]	No	No	Yes	SINR based CST adaptation	Additional software along with feedback mechanism required at all stations	Distributed

As discussed in Section 5.3.1, a side effect of tuning CST is the variation in the number of exposed and hidden nodes. Hidden and exposed node problem is investigated by [96], where the authors demonstrate that the throughput in network can be increased by tuning CST after every change in network topology. By doing so, the numbers of deferred transmissions are reduced. But the authors have not investigated their scheme in dense infrastructural network.

5.2.1 Related work of CST adaptation using local information

In [110], the authors analytically model the relation of CST with transmission power and data rate within high density WLAN networks. They propose to change the CST based on the Received Signal Strength Indication (RSSI) of received frames, yet they assume fixed total interference in their overall analysis that can be considered a drawback of their proposed scheme. In [41], the authors have also visualized the usage of RSSI to modify the CST of each non-AP station to improve the throughput,

but they require special signaling (called Busy/Idle signal) that is used to monitor the RSSI variations. This technique requires modifications to be made at the AP that can transmit Busy/Idle signal that encompasses the signals channel occupancy information (calculated based on the comparison with the received RSSI and its current CST). Each station (that is also modified) uses this signal together with its own local Busy/Idle signal to determine the current availability of the channel and optimally set its CST.

Authors in [65] propose to use a centralized algorithm which adapts CST of stations based on loss differentiation. Their proposed algorithm operates by gathering feedback information at a central controller (i.e. AP) and adapts CST of all stations. Despite the shared information, the drawback of the proposed scheme is the same constant changed CST that is assigned to all of the stations irrespective of the environment variations. Therefore, the network is unlikely to reach the maximum achievable throughput.

In [102], the authors have investigated a technique to improve network capacity in hotspots by dynamically tuning CST. They analyze an infrastructural Wi-Fi configuration where AP's CST is set according to the minimum measured SINR at the associated stations. Similarly, the CST of the stations is set based on the SINR of frames received at their respective APs. Albeit being one of few studies where carrier sensing is evaluated in the complete infrastructure WLAN dense network, this scheme introduces overheads due to the continuous sharing of SINR information among APs and stations. In spite of this drawback, we consider this study to be very relevant to our current proposed research work and perform comparison with the aforementioned scheme in section 5.6.4.

Authors in [72] have highlighted the overhead involved in dynamic CST adaptation and proposed to use a camera to calculate the positions of nodes, which is in return used to determine the CST for APs. Despite the improvements indicated by the authors, their scheme itself creates an overhead in terms of additional hardware.

Jamil et al., who participate actively in the TGax, evaluated the use of dynamic CST modification in [47] and [48], but they have not proposed any specific algorithm as well as their analysis is based on optimal channel assignment techniques. Meanwhile, authors in [53] propose a FER based heuristic schemes to vary the CST of stations. This scheme increase/decrease CST by comparing FER of the recent window with that of the previous window.

5.2.2 Related work of CST adaptation using alternative approaches

Apart from heuristic modeling, different authors have applied mathematical tools to analyse the complex spatial reuse problem in IEEE 802.11 networks. Park et al. [79] employ non-cooperative game theory to control the CST in order to improve network performance in non-cooperative settings. Graph theory has also been used by different authors to set the optimum carrier sense ranges [78, 107]. Ven et al. [101] use Markov chains to model their network for dynamic CST adjustment. However, the aforementioned schemes lack to distinguish between the sensing and interference area within the CST adaptation procedure.

In comparison to the above mentioned schemes, the DSC scheme is fully distributed mechanism

which takes into consideration the interference and carrier sensing range and dynamically adapts to increase the spatial reuse within highly dense deployments. The argument to have a distributed algorithm (to avoid signaling overhead) that dynamically adjusts the CST is supported by the fact that the level of interference faced by each station within densely deployed network is arbitrary due to the random placements and variability in penetration losses.

Table 5.1 summarizes the main characteristics of some of the PHYCCA adaptation techniques proposed in the literature and compares them with the DSC scheme.

5.2.3 Related work of adaptive RTS/CTS

In order to resolve the hidden node problem associated with DCF, several researchers have envisioned the adaptive usage of RTS/CTS, where the aim has been to reduce the impact of collisions. Although the usage of RTS/CTS method can reserve the channel that can help in reduced frame collisions, the added overhead due to the inclusion of RTS and CTS transmission is not negligible [99] (especially at high data rate transmissions). The benefits associated with enabling and disabling the four-way handshake has already been explored in numerous previous research works (e.g. [49], [51], etc.). Different researchers have proposed the usage of different metrics to enable RTS/CTS exchange (e.g. packet delivery ratio [71], hidden terminal count [90], successful transmitting probability of packets [60], etc.).

Recently, authors in [69] have proposed to utilize RTS/CTS in M2M scenario by serving many stations one after the other to reduce the MAC overhead. Numerous RTS frames are sent in parallel by different stations on different frequency sub-bands while keeping the whole channel available for the CTS, DATA and ACK transmissions. When many RTS messages are decoded by the AP, only one user is able to win the channel access. Stations with unsuccessful RTS requests revoke a backoff procedure before transmitting another RTS frame. In such scenario, RTS frames will seldom collide and therefore major improvements in saturation throughput and delay for loaded networks were exposed by the authors. However, the drawback of this scheme is the need to have many sub-carriers to perform the aforementioned mechanism.

To the best of our knowledge, no previous work explores the benefits of utilizing four-way handshake in high density IEEE 802.11 networks.

5.3 PHYCCA modification mechanism proposed for IEEE 802.11ax - Dynamic Sensitivity Control

In this section, we first highlight the problems associated with carrier sensing mechanism in legacy IEEE 802.11 networks. Next, we evaluate the throughput performance based on frame collision probability of symmetric network with hidden and exposed stations. We then provide analytical justification for dynamically adapting CST threshold of each station based on the received power from the associated station. Next, we utilize snapshots of a real densely deployed WLAN network to

showcase the extent of hidden and exposed node problems. Moreover, we also showcase the benefits achieved by dynamically adapting CST of each station within the network. We then expose the working of Dynamic Sensitivity Control algorithm (i.e. a mechanism that is proposed at the TGax to increase area throughput of densely deployed WLAN networks).

5.3.1 Problems associated with carrier sensing mechanism in legacy IEEE 802.11

As explained in section 5.1, IEEE 802.11 utilizes CSMA/CA based DCF method, where stations are made to listen before transmitting over the shared medium. PCS method is responsible for reporting status of the medium to the MAC layer and leverages PHYCCA module implemented at the PHY layer. The PHYCCA module is able to sense the channel (busy or idle) by measuring the received energy level.

Due to the inherent conservative approach of DCF in assessing interference, it fails in providing an efficient access to the shared medium. For example, if the PHYCCA module reports to the MAC layer that the medium is busy, the station blocks its own transmission so as to yield for other ongoing communication. However, it may happen that the station unnecessarily blocked itself, even though its transmission might have not caused enough interference to corrupt frames on an ongoing communication. This problem (referred to as exposed node problem) has been thoroughly investigated to severely affect the spatial reuse of spectral resources and thus limits the network capacity. On the other hand, if the PHYCCA module reports the medium to be idle, the station can initiate its transmission where the SINR at the receiver determines whether the transmission was successful or not. However, in dense WLAN deployments, concurrent transmissions outside the carrier sensing range of a transmitting station can contribute to ample interference which, in return, can corrupt the ongoing communication. This problem (referred to as hidden node problem) causes collisions and thus reduces the throughput of the network.

Both hidden and exposed node problems result in decreased overall throughput. Exposed node problem for a station occurs due to excessively small CST values, where the transmitter detects far-away transmissions and, as a consequence, it unnecessarily defers its transmission. On the other hand, the cause of hidden node problem is the usage of a high CST at the transmitter, where energy received from a node (hidden) is lower than the CST. Having a conservative approach of assigning CST in the network can cause more exposed nodes to occur that can lead to unnecessary starvation.

In terms of fairness, the IEEE 802.11 MAC protocol implicitly provides equal opportunities to all transmitting stations, where stations placed near the AP tend to occupy less airtime as compared to slower stations placed at greater distances, provided that all stations utilize same frame size. A scheme guaranteeing equal throughput is clearly not feasible in such network where airtime fairness is not achieved when multiple stations with different data rates compete for the shared medium. Maximizing throughput for all stations in also not a viable solution where the high rates stations improve their transmission rate and the slower stations have to counter possible starvation.

Mechanisms that aim to improve the spatial reuse by using asymmetric PCS threshold at each station, encounter the fundamental conflict between optimizing throughput and achieving fairness.

Allocating frequent channel to links influenced by numerous hidden stations might result in reduced channel reuse and the corresponding throughput. Similarly, adapting the PCS thresholds for some stations (that enable any PHYCCA adaptation scheme) can enhance the network throughput dramatically over the cost of reduced throughput (due to access blocking) for legacy stations (that do not use PHYCCA adaptation mechanism). Therefor the overall fairness in the hybrid network can decrease.

Hence maximizing spatial reuse with the aim to increase system throughput must be a careful combination of approaches addressing multiple aspects (e.g. reduced FER, balance between starvation and fairness, etc.) of the network behavior.

5.3.2 Saturation throughput analysis in the presence of hidden and contending stations

In this section, we analyze the theoretical throughput gains achieved by an individual station within densely deployed WLAN network encompassing multiple OBSS. The saturation throughput of Wi-Fi network with n users can be analyzed by Discrete Time Markov Chain model developed in [20]. Authors in [33] have extended the above model to accommodate both hidden and contending stations under non-saturated channel conditions. It is pertinent to highlight that, from the viewpoint of an individual station within densely deployed Wi-Fi network, nodes that are competing within the same cell as well as stations that are exposed to each other fall within the set of contending stations (i.e. all stations within the carrier sensing range, regardless of the cell they belong to).

We utilize the models proposed in [20] and [33] to show the effect of hidden and exposed nodes within a densely deployed network operating under saturation conditions. We first derive the collision probability of each node by taking into account the variations in hidden and contending stations associated with a change in physical carrier sensing. Next, impact on throughput of a station based on the number of hidden, exposed, and contending stations effecting the transmission is presented.

5.3.2.1 System analysis

In [20], the authors used two dimensional markov chain analysis to describe the MAC operations of IEEE 802.11 with help of states and transition between states. MAC state of each station is represented by two variables: the current retransmission state and the remaining backoff time within the considered state. An individual station starts transmission in a generic time slot with probability τ, where each transmission/frame suffers collision with probability p (i.e. frame transmission is assumed successful with probability $1-p$). The model assumes ideal channel conditions where all stations in the symmetric network are in carrier sense range of each other (i.e. there are no hidden stations and capture effect). The saturation throughout can be calculated by using τ and p.

According to [20], under saturation conditions, the probability τ that a stations transmits a frame

in a randomly selected time slot is given by,

$$\tau = \frac{2(1-2p)}{(1-2p)(W_0+1)+pW_0(1-(2p)^m)} \tag{5.1}$$

where, n is the number of competing stations, W_0 and m are the minimum contention widow size and the backoff maximum stage, respectively. Moreover, it is assumed in the modeling that p is the probability that at least one of the $n-1$ remaining stations transmits in a time slot. In general, p is a function of τ by the following expression:

$$p = 1-(1-\tau)^{n-1} \tag{5.2}$$

The fundamental independent assumption of conditional collision probability in the above model implies that each transmission visualizes the system in steady state. Equations 5.1 and 5.2 represent a non-linear system with two unknown τ and p that can be solved using numerical methods with a unique solution.

The above mentioned model (often referred to as Bianchi's model) is extended to account for hidden stations in [33] for non-saturated traffic conditions. The authors use the same chain model, but formulate p (by taking into account the hidden as well as contending stations) as follows:

$$p = 1-(1-\tau)^{c-1}[(1-\tau)^h]^k \tag{5.3}$$

where, n stations in a network are categorized as contending (c) and hidden (h) stations (i.e. $n = c+h$), k is the average slot decrement in a period of time within which transmission from another station initiates and collides with the current transmission (i.e. $k = 2T_{succ}/T$, where, T_{succ} is the time required for the successful delivery of a frame and T is the average slot time) and is related to τ and p by the following expression:

$$k = \frac{2\frac{T_{succ}}{\sigma}}{1+(1-(1-\tau)^n)(\frac{T_{col}}{\sigma})+n\tau(1-p)(\frac{T_{succ}}{\sigma}-\frac{T_{col}}{\sigma})} \tag{5.4}$$

where, T_{col} is the time spent due to a collision and σ is the duration of an idle slot time. Once these values are known, other important relationships can be derived as:

$$P_{tr} = 1-(1-\tau)^n \tag{5.5}$$

$$P_{idle} = 1-P_{tr} \tag{5.6}$$

$$P_{ok} = n\tau(1-\tau)^{n-1} \tag{5.7}$$

$$P_{col} = P_{tr}-P_{ok} \tag{5.8}$$

where, P_{tr} is the probability that there is at least one transmission in the considered slot, P_{idle} is the probability that the slot time is empty, P_{ok} is the probability that a transmission occurred was successful and P_{col} is the probability that transmission resulted in unsuccessful transmission. A frame is successful only when exactly one station transmits over the channel, conditioned to the fact that at least one station transmits.

Finally, the normalized aggregate saturation throughput is calculated as the average amount of payload bits that are successfully transmitted per slot time:

$$S = \frac{P_{ok}E[P]}{T} \tag{5.9}$$

where, $E[P]$ is the average data size.

The average slot time T can be derived as follows: If the medium is idle, the slot time would be equal to σ. If the medium is busy, the slot time would either be the time to perform a failed transmission or the time to complete a successful transmission. Thus the average time slot is:

$$T = P_{idle}\sigma + P_{ok}T_{succ} + P_{col}T_{col} \tag{5.10}$$

For basic access method[1], T_{succ} and T_{col} can be expressed as:

$$\begin{aligned} T_{succ} &= T_{DIFS} + T_{data} + \delta + T_{SIFS} + T_{ack} + \delta \\ T_{col} &= T_{DIFS} + T_{data} + \delta \end{aligned} \tag{5.11}$$

where, T_{DIFS} is the DIFS interval (which is the time a station has to listen after the backoff period to sense the channel state), T_{SIFS} is the SIFS interval (that is the amount of time required for a stations to process and respond with a frame), T_{data} and $Tack$ corresponds to the time required to transmit data and ACK bits (that include MAC and PHY headers) respectively, δ represents the propagation time.

For IEEE 802.11g, T_{data} is given by:

$$T_{data} = T_{preamble/header} + 4\left\lceil \frac{(22 + (L_{header} + L_{data})8)}{4r} \right\rceil + T_{SignalExtension} \tag{5.12}$$

where, $T_{preamble/header}$ is the preamble duration at the PHY layer, L_{header} is the MAC and LLC[2] header, L_{data} corresponds to frame size, r is the data rate and $T_{SignalExtension}$ is the additional time required by high-rate coding in IEEE 802.11g.

For IEEE 802.11n, T_{data} and T_{ack} calculations depend on the type of transmission mode (Non-HT, HT Mixed or HT Greenfield). HT-mixed is considered mandatory, while HT Greenfield, which does not include the non-HT compatibility information, is an optional format. Concerning HT

[1]For RTS/CTS handshake, T_{succ} should include the time required to exchange the RTS and CTS frames and T_{col} only includes the time of an RTS

[2]LLC provides similar functionality as traditional data link control protocol and is the highest layer of IEEE 802.11 OSI reference model.

Table 5.2: System parameters.

Parameter	Values	Parameter	Values
r	24 Mbps	T_{DIFS}	28μs
L_{data}	1000 Bytes	T_{SIFS}	10μs
L_{header}	36 Bytes	δ	0.16μs
$T_{SignalExtension}$	6μs	σ	9μs
W_0	15		

Mixed mode, which is the most commonly used frame format because of its support for both HT and legacy IEEE 802.11a/g OFDM radios, T_{data} is given by:

$$T_{data} = T_{preamble/header} + T_{preamble\_stream} + 4\left\lceil \frac{(T_{sym} \times N_{symbols})}{4} \right\rceil + T_{SignalExtension} \tag{5.13}$$

where,

$$T_{preamble\_stream} = 4(N_{LTF} - 1) \tag{5.14}$$

and,

$$N_{symbols} = \left\lceil \frac{(16 + 6N_{ES} + (L_{header} + L_{data}) \times 8)}{N_{DBPS}} \right\rceil \tag{5.15}$$

where, $T_{SignalExtension}$ is set to 6μs for 2.4 GHz band and 0 μ s for 5 GHz, and T_{sym} corresponds to the symbol duration (3.6μ for short Guard Interval (GI), and 4μ for long GI). N_{ES} and N_{DBPS} depend on the used MCS level and are fixed in the standard specification. N_{LTF} corresponds to the number of long training symbols, which depends on the number of spatial streams, N_{SS}. Without Space-Time Block Coding (STBC), N_{LTF} equals the number of spatial streams, except for three spatial streams, in which case four training symbols are required.

T_{ack} computation follows T_{data} with modifications (L_{header} and L_{data} are replaced with 14 Bytes.)

Instead of modeling the problem based on non-saturation traffic condition used in [33], we build our analysis by solving Equations 5.1, 5.3 and 5.4 numerically. Our work follows the model presented above, where we explore the impact of hidden and contending nodes on the throughput of an individual station. As explained in the previous sections, the value of CST utilized by each station directly effects the existence of hidden and exposed nodes experienced by it. Each station compares the received energy level at any time slot with its CST to detect the channel occupancy.

5.3.2.2 Numerical results

As highlighted in Section 5.3.2, τ and p can be numerically solved from the perspective of an individual station. The main objective of this section is to evaluate the impact of hidden and exposed stations trends over the throughput of a stations that varies its CST. Based on the following definitions, an open source network simulator (called NS-3) was used to extract the average variations in hidden, contending and exposed stations experienced by a station that increases its CST value. The extracted values were used in the saturation throughput model described in the previous section.

The parameters used in calculating the average per user saturation throughput (i.e. equation 5.9

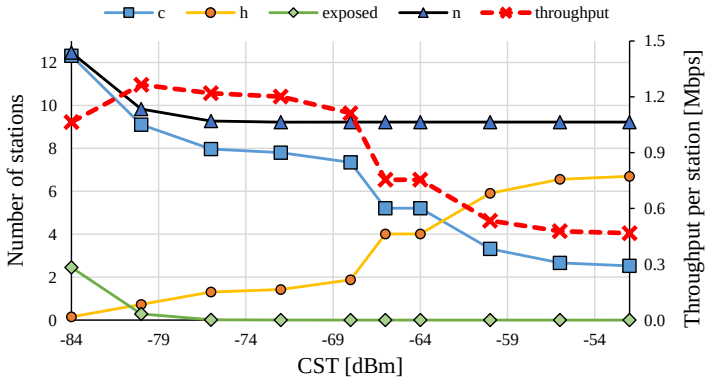


Figure 5.4: Impact of CST variations over throughput performance of a station

averaged for n stations) based on the aforementioned model are highlighted in Table 5.2.

We assume a residential building environment encompassing 100 apartments, where 1/3 of the tenants utilize WLAN cells operating over the same frequency (the details of the environment can be found in Section 5.5). In summary, the setup is an 802.11 network in infrastructure mode with many stations (i.e. 5 per cell) sending uplink traffic to their respective AP.

Hidden, contending and exposed node analysis is performed by measuring the received power at each station from every other station, and comparing it with the corresponding CST in many randomly generated scenarios. Only upstream traffic in saturation condition is assumed because the hidden node problem is more prominent in this scenario (there are fewer number of hidden APs with respect to hidden non-AP stations).

Due to the trade-off associated with hidden, exposed and contending stations, an increase in CST at a station increases the number of hidden nodes while the exposed nodes count decreases. In order to calculate the average number of hidden and contending stations, a constant carrier sensing range is assumed for all the transmitting stations.

Figure 5.4 indicates the throughput trend witnessed by a station, which experiences variations in hidden, exposed and contending stations. The CST value ranges from -84 to -50 dBm. At a CST value of -84 dBm, the presence of both exposed and contending station reduces the protocol efficiency. On the other hand, at -62 dBm, the throughput decrease is evident due to an increase in hidden stations. Thus an optimal CST range (i.e. from -80 to -68 dBm) creates a balance between the hidden and the number of exposed/contending stations that maximizes gain in throughput for the station. Note that throughput increases as we reduce the number of exposed nodes; from that point on, additional increments of CST only produce more hidden nodes without any compensation in throughput.

5.3.3 Communication model to obtain appropriate CST to maximize spatial reuse

Based on our analysis in previous section, it is important to highlight that network capacity of high density Wi-Fi networks can be improved by carefully tuning the CST of each individual station.

In addition, as an important outcome, we identify the main consequences when a node increases its CST as follows: (i) channel access probability increases because the station cares for fewer other transmissions, (ii) interference level from and to other stations increases.

Out of the aforementioned outcomes, increased interference level is the main obstacle in providing high capacity over the shared medium. More specifically, for the case of dense Wi-Fi implementations, which are severely hampered by hidden and exposed node problems and are characterized by being interference limited, the key to achieve high performance lies in limiting the effects of interference but, at the same time, increasing spatial reuse. Thus, it is of utmost importance to study the impact of interference on the carrier sensing.

In this section, we introduce our analytical model for carrier sensing and describe how CST could be tuned by received power, that dramatically improves the throughput of dense WLAN deployments.

According to the simplified two-ray pathloss model (with antenna heights of 1m and gains of 1dB), the power a station receives from the transmitting node can be represented by,

$$P_r = \frac{P_t}{d^\alpha} \tag{5.16}$$

where, α is the pathloss exponent and its normal value for indoor communication is assumed to be in the range of 2 to 4. P_t is the transmitted power. Due to the pathloss constraint, the energy of a received signal should be above a given threshold (called receiver sensitivity, S_r) for it to be correctly decoded,

$$P_r = \frac{P_t}{d^\alpha} \geq S_r \tag{5.17}$$

For the sake of simplicity, let us assume that all stations are equal (i.e. same P_t, S_r, etc.). Using (5.16) and (5.17), the transmission range (i.e. the region around the transmitter where the received signal strength at the transmitter is greater than or equal to the receiver's sensitivity) can be given as,

$$T_r = (\frac{P_t}{S_r})^{\frac{1}{\alpha}} \tag{5.18}$$

In order to determine whether the channel is free or busy due to a nearby transmission, the PHY-CCA method defines the carrier sensing range (i.e. the region around the transmitter where the received signal strength is greater than the CST). Within this range, nodes are able to sense signals over the shared medium, even though the correct reception of frames may still not be possible. The carrier sensing range can be represented as,

$$CS_r = (\frac{P_t}{CST})^{\frac{1}{\alpha}} \tag{5.19}$$

In order to derive the interference range (i.e. the region around a receiver in which any two simultaneous transmissions may result in a collision), we consider the scenario presented in Figure 5.5 where we assume that a node A transmits a packet to node B, but B's strongest interferer, node C (that is hidden from node A), starts another transmission at the same time (power received by B

from A is $P_{AB} = P_t / d_{AB}^{\alpha}$, where d_{AB} is the distance between A and B, and the power received by B from C is $P_{CB} = P_t / d_{CB}^{\alpha}$, where d_{CB} is the distance between C and B). The two signals can overlap in time, but the receiver could be able to decode one of the received packets (let's say from A) due to the *capture effect* (i.e. upon collision, packet with strongest signal will be successfully received, while the weaker signal will have the same effect as noise). This effect is observed when the SINR of the

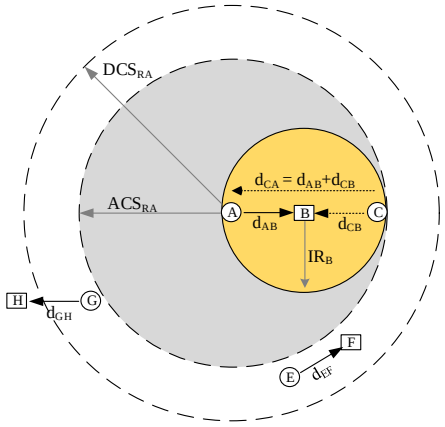


Figure 5.5: Appropriate carrier sensing range that just covers the interference range.

received packet is greater than a given threshold (called capture threshold, C_t). According to [56], this threshold depends, fundamentally, on the modulation used (C_t increases with physical rate). Ignoring thermal noise and assuming all transmitters use same transmit power, we have,

$$SINR = \frac{P_{AB}}{P_{CB}} \geq C_t \implies (\frac{d_{CB}}{d_{AB}})^{\alpha} \geq C_t \tag{5.20}$$

This equation implies that, in order to successfully receive a signal from A, the interfering node C must be, at least, $C_t^{\frac{1}{\alpha}} \times d_{AB}$ meters away from the receiver B. In the limit:

$$d_{CB} = C_t^{\frac{1}{\alpha}} \times d_{AB} \tag{5.21}$$

The transmission range of a node is generally considered to be much smaller than the carrier sensing or interference range. The receiver sensitivity (defining the transmission range) and capture threshold depend on the characteristics of the hardware, whereas the carrier sensing range is tunable (through CST adaptation) and can greatly affect the performance of the network. Being $d_{CA} \leq d_{AB} + d_{CB}$, setting

$$CS_{RA} = d_{AB} + d_{CB} \tag{5.22}$$

the carrier sensing range of A covers B's interference range (presented as IR_B in Figure 5.5); that is, any transmission outside CS_{RA} will not cause a collision in B and could thus be safely ignored when A senses the medium before transmitting to B, avoiding exposed nodes (e.g. nodes E and G). Hence,

to derive the proper CST for A, we first compute the minimum power A receives from C,

$$P_{CA} \geq \frac{P_t}{(d_{AB} + d_{CB})^{\alpha}} \tag{5.23}$$

Combining equations (5.21) and (5.23), we have,

$$P_{CA} \geq \frac{P_{AB}}{(C_t^{\frac{1}{\alpha}} + 1)^{\alpha}} \tag{5.24}$$

Finally, the A's CST that allows an increased spatial reuse and, at the same time, prevents collisions with C is given by

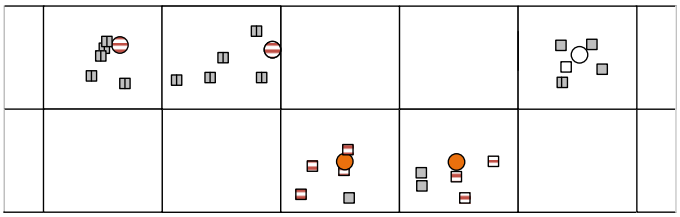
$$CST_A = \frac{P_{AB}}{(C_t^{\frac{1}{\alpha}} + 1)^{\alpha}} \approx \frac{P_{BA}}{(C_t^{\frac{1}{\alpha}} + 1)^{\alpha}} \tag{5.25}$$

where, $P_{BA} = P_t / d_{BA}^{\alpha}$, d_{BA} is the distance between B and A, and $P_{BA} \approx P_{AB}$ due to assumed similar transmit power P_t.

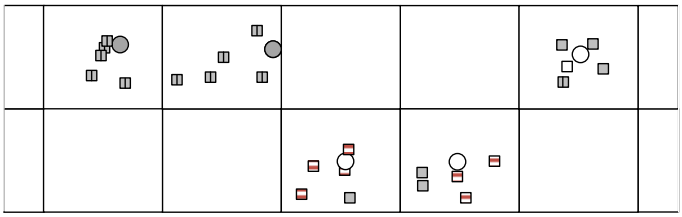
This improved CST value creates a new optimized carrier sense range, which is represented by ACS_{RA} in Figure 5.5. To justify this argument, we consider a typical domestic scenario where we assume that the power received at a node from its transmitter (within a cell) is -55 dBm and C_t is set to be 15 dB. Furthermore, if we assume $\alpha = 3.5$ (which corresponds to the value used by the IEEE 802.11 TGax to develop the pathloss model [88]) and substitute these values in equation (5.25), the CST obtained is ∼-75 dBm, which is greater than the default CST (i.e. -82 dBm) used by the current IEEE 802.11 standard (represented by the DCS_{RA} radius in Figure 5.5). Consequently, it would decrease the carrier sensing range of the node and thus will allow more concurrent transmissions to take place around that transmitter. Correspondingly, we justify our observation that the power received from the intended receivers can be used as a viable and simple solution for a node to set its CST. In Section 5.3.5, we infer the aforementioned concept to design an algorithm that enables every station to set their CST to optimal values based on the power received from their associated stations.

5.3.4 Need to dynamically adjust CST of each station within Dense WLAN deployment

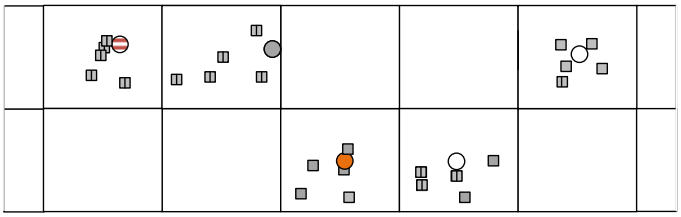
In order to exemplify the extent of hidden and exposed node problem within a densely deployed WLAN network, we utilize Figure 5.6a to 5.6d, which are graphical representations of ten rooms of a particular floor (out of one hundred rooms) within a realistic densely deployed WLAN residential simulation environment. Hidden and exposed node analysis is performed by measuring the received power at each station from every other station, and comparing it with the corresponding CST (formal definitions of both hidden and exposed stations are mentioned in Section 5.3.2.2).



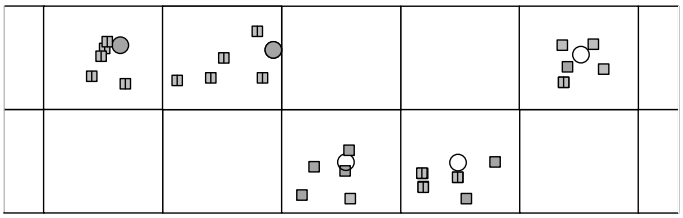
(a) Default CST used by all the transmitters.



(b) DSC applied at APs and default CST used by the non-AP stations.



(c) DSC applied at non-AP stations and default CST used by the APs.



(d) DSC utilized at all transmitters (AP and non-AP stations).

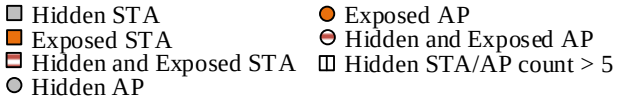


Figure 5.6: Influence on a dense WLAN deployment by the inclusion of algorithm to dynamically modify CST.

5.3.4.1 Impact of CST on Hidden and Exposed nodes count

Figure 5.6a depicts the case where the entire transmitter set utilizes similar CST (-82 dBm). Majority of the nodes (i.e. 87%) are found to have, at least, one hidden pair, and 36% of the stations are found to be exposed to other transmitters.

Hidden and exposed node analysis for the case when DSC is only applied at the APs is presented

in Figure 5.6b. A reduction in the exposed node count is witnessed (i.e. from 36% to 23%) when compared to all station utilizing constant CST. Interestingly for the case of AP, the exposed node count is decreased from 80% to 0%. In addition, hidden node count increased for APs that already had hidden pairs. However, the exposed node count for non-AP stations did not decrease.

In Figure 5.6c, DSC is applied only at the stations. Results highlight that there is significant reduction in exposed nodes count (i.e. from 36% to 6.7%) when compared to the environment where all transmitter use the same CST value. As a consequence, the number of nodes that are hidden from six or more stations is increased (i.e. from 36% to 47%). To be more specific, the number of exposed stations decreased from 23% to 0% due to DSC being employed only at the uplink. On the contrary, some of the APs still suffer from exposed nodes, thus justifying the need to have a method that modifies CST at AP and non-AP stations.

Building upon the aforementioned argument, Figure 5.6d signifies the case when DSC is used by all of the stations. Interestingly, employing a dynamic method to adapt CST of each station within a dense deployment leads to network conditions where each station is allowed to communicate (i.e. exposed node count decreased from 36% to 0%). However the spatial reuse is increased over the cost of increase in hidden nodes (i.e. from 87% to 90% and hidden count for nodes that were already hidden from greater than 5 stations also increased).

These results indicate the important benefits achieved by changing CST of each station based on received power. Furthermore, as a consequence of the mobility of stations and the expected changes in the network scenario, received power is also expected to vary over time, and hence CST tuning should be continuous and dynamic.

5.3.5 Dynamic Sensitivity Control Algorithm

In the prior discussion, we have motivated the need to implement an algorithm to dynamically adjust the CST for each station (AP and non-AP) within dense deployments. The argument to have a distributed algorithm that dynamically adjusts the CST is supported by the fact that the level of interference faced by each station within densely deployed network is arbitrary due to the random placements and variability in penetration losses. Utilizing a constant CST for all stations might create a disparity among stations where some of them will be more severely affected by starvation or interference than others.

In this section, we give an overview of our proposed algorithm that dynamically adjusts CST of all stations (AP and non-AP stations) in infrastructure-based WLANs. Thus, an environment is created where CST of all stations adapt to the heterogeneity of dense deployments. As a consequence, the appropriate CST value allows more concurrent transmissions to take place (without considerable increase in collisions incurred due to increase in the number of hidden nodes) within the network that yields to improvement in the spatial reuse.

The basic idea of DSC scheme is to optimize the existing deployments by appropriately tuning CST for each node in a distributed manner (in order to avoid signaling overhead).

For non-AP stations [13], the CST of each station is varied based on the RSSI of beacon frames

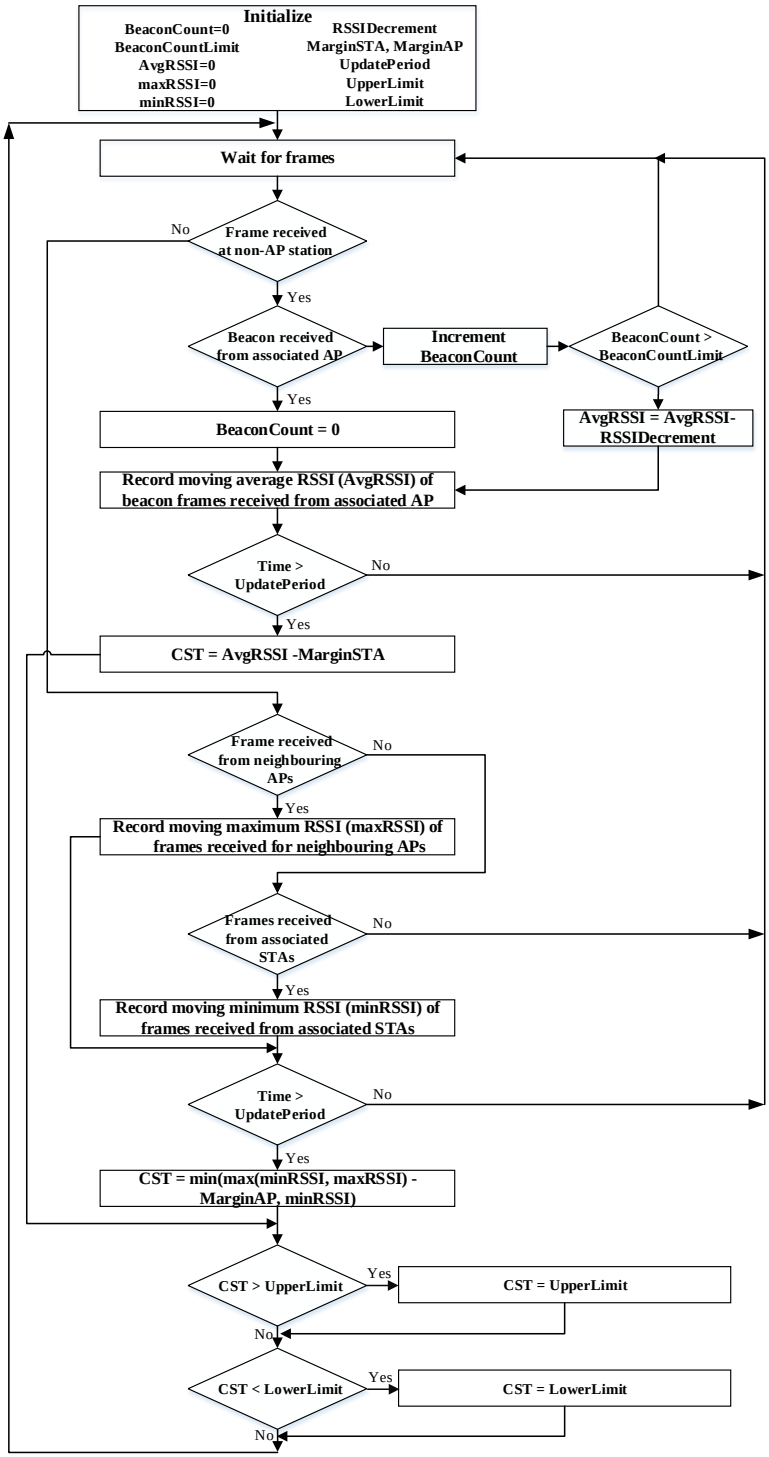


Figure 5.7: Flow chart of DSC algorithm used at each station.

received from the associated AP. Stations, that are placed near to their respective AP can have lower carrier sensing range because interference from concurrent transmissions would have limited implications (due to *Capture effect*), while stations that are placed further away could have higher carrier sensing range so that the probability of correct transmission would be increased by reducing the presence of hidden nodes.

For AP, DSC operates to facilitate more concurrent transmissions to occur by tuning the CST based on the RSSI received from the furthest associated station[1] of the AP. This argument is further augmented by the fact that in residential buildings, associated stations are predominantly placed near their APs. Therefore, the AP is able to confine/reduce its carrier sensing range to include only the links that operate within the cell (i.e. AP is able to serve the needs of all of its stations). In order to cater for a situation where an active interferer (i.e. OBSS station) is nearest to the AP (as compared to associated stations), only then the CST of AP is optimally tuned according to the interferer. In order to avoid excessive fluctuations of the CST and given that, typically, most of the traffic in a WLAN is originated from the AP, the algorithm only considers interference coming from neighboring APs.

Thus, the underlying difference between the DSC for non-AP and the DSC for APs is that the latter keeps track of the furthest receiver and also considers RSSI information from dominant interferers.

In order to understand the basic operation of our DSC algorithm, a flow chart is presented in Figure 5.7. We consider an infrastructure-based dense WLAN scenario where each non-AP station is already associated to its respective AP and the DSC algorithm is executed concurrently over all the stations. Furthermore, we consider two way communications where each station keeps track of different frames (i.e. data, ACK, beacons, etc.) it receives.

Due to distinct behavior of DSC for AP and non-AP stations, the first stage of the algorithm resolves the identity of the node that utilizes DSC. If frames are received by non-AP stations, algorithm waits to receive beacon frames from the associated AP. For each beacon frame received, the non-AP station accumulates the RSSI uptill the *UpdatePeriod*. This *UpdatePeriod* time is a preset value that encompasses multiple Beacon Intervals (BI) (i.e. if it is set to $1s$ and the BI is set to 100 ms, then 10 beacons are expected from the AP). The DSC algorithm maintains a moving average of RSSI (called *AvgRSSI*) of all received beacons within the *UpdatePeriod*. If a beacon frame is not received within a BI, *BeaconCount* (i.e. the number of consecutive beacons missed) is incremented. Later, this *BeaconCount* is compared with $BeaconCountLimit$ (i.e. maximum consecutive missed beacons). If *BeaconCount* is found to be greater than the *BeaconCountLimit*, the existing average RSSI from beacons is decremented by a default value (called *RSSIDec*). The reason for said decrement is to increase the carrier sensing range of non-AP station so as to allow it to improve (i.e. the current carrier sense range may be too small, not including the associated AP and needs to be stepwise increased by correctly detecting beacons from the associated AP). After every *UpdatePeriod*, each non-AP station tunes its CST, where *MarginSTA* is subtracted from the *AvgRSSI* so as to set the CST.

However, when frames are received by an AP, the algorithm waits to receive beacons from neighboring APs as well as data/ACK frames from associated non-AP stations. If the AP receives frames

[1] A single appropriate CST for AP is calculated within a cell so as to avoid the complexity introduced by assigning different CSTs for transmissions to different associated stations

(that it is able to decode properly), it records the RSSI of the frames until the *UpdatePeriod*. The AP maintains a moving maximum RSSI (called *maxRSSI* of the frames received from neighboring APs. By doing so, the AP is able to detect the strongest interfering AP. For its own stations, the AP maintains a moving minimum RSSI (called *minRSSI*) of the frames received and thus is able to identify a non-AP station that is placed at a maximum distance. If no frame is received from any non-AP stations within an *UpdatePeriod*, the AP waits to receive frames and does not change its carrier sensing range. Furthermore, if no frames are received from stations associated to the AP, it does not change its CST even though frames are received from the neighboring interfering APs (i.e. the basic aim of AP is to give preference to its associated stations).

After every *UpdatePeriod*, AP tunes its CST. The AP evaluates the maximum between *minRSSI* and *maxRSSI*. Then *MarginAP* is subtracted from the previous calculated value and is used to set the CST for the AP. The decision to consider the greatest value between the *minRSSI* and *maxRSSI* is based on fact that, in a residential scenario, stations are always placed near their respective APs and the AP should prefer its own stations to set its CST.

MarginAP and *MarginSTA* values are kept constant for all AP and non-AP stations respectively and can correspond to $(C_t^{\frac{1}{\alpha}}+1)^{\alpha}$, depending on the modulation used and following equation (5.25)[1], as explained in Section 5.3.3.

In the next step, the new calculated CST (both for AP and non-AP station) is confined between an upper limit (*UpperLimit*) and lower limit (*LowerLimit*) so that if the AP is located near its associated stations or neighboring AP, it is assigned a CST that falls near the upper limit and vice versa.

The above mentioned DSC algorithm effectively allows more flows to co-exist and, as shown in Section 5.6, results in higher per flow and aggregate throughput while a good level of fairness is maintained for all nodes.

5.3.5.1 Need to confine CST within a bounded region

Since DSC is characterized as a fully distributed algorithm where each station simply attempts to achieve maximum spatial reuse gains, the increase in CST by a station placed near to its transmitter can lead to following consequences: (i) the chance for the station to access the shared channel will increase because it will care for fewer nodes and thus will sense the channel idle more frequently, (ii) as a consequence of more aggressive channel access, the interference from the station to other stations will increase. In addition, interference from other nodes employing DSC to the station under consideration will also increase.

On the contrary, a station placed far away from the associated transmitter can decrease its CST (due to CST being dependent on the received frames RSSI) that can lead to following consequences: (i) the sensitivity of the station will increase, thereby the station will sense greater number of transmission by being over conservative and thus can increase the probability of correctly receiving frames for the relevant station, (ii) Nevertheless, the aforementioned action can lead to decrease in exposed node and reduced spatial reuse that can reduce the overall throughput.

[1] Margin values range between 18 and 25 dB in typical indoor scenarios (i.e. $\alpha \sim 3.5$)

The above mentioned conflicting consequences of increasing and decreasing CST highlight the need to confine the RSSI calculated CST within a bounded area. The aforementioned argument is further supported by results exposed in sub-section 5.6.3, which indicate decrease in overall achieved throughput when DSC is used without CST limits.

The significance to include a method to limit the increase in CST has also been highlighted in [79]; authors have utilized non-cooperative game theoretic framework to design a fully distributive algorithm for the tuning of CST at each station within a CSMA based multihop network. They have devised a pricing method where the CST of stations is confined (i.e. not allowed to increase above a maximum) based on the number of collisions.

5.4 DSC Algorithm leveraging adaptive RTS/CTS to minimize the impact of hidden nodes

One of the drawbacks of allowing multiple concurrent transmissions to co-exist in geographically limited area is the increase in hidden nodes, which results in increase of system level FER [12]. The hidden node problem can get further aggravated for stations within high density networks due to obstacles, transmit power, location and mobility.

In order to combat the hidden node problem (so as to reduce collision probability), the legacy IEEE 802.11 has already devised the optional RTS/CTS access mechanism, where RTS and CTS frames are exchanged prior to transmission of data frames. However, this optional feature has not been adapted in most of the implementations of the WLAN standard due to the additional overhead associated with temporary reservation of the shared medium (i.e. for small data frame size used, this overhead becomes significant). Thus, the problems associated with RTS/CTS method counterbalance its positive aspects and thus an adaptive mechanism is required to enable RTS/CTS through a selective approach.

Since conventional interference management techniques, when applied intelligently to dense deployments, can also ease the overall network conditions, in this section, we propose the adaptive utilization of RTS/CTS mechanism along with DSC scheme so as to neutralize the negative effects of PHYCCA modifications. The IEEE 802.11ax has already shown keen interest in including a method that allows an AP to remotely enable RTS/CTS for any of its associated stations. With the help of system model description, we give substance to the utilization of RTS/CTS along with DSC and even indicate increase in performance efficiency over the already proved DSC scheme. Another motivation to study the foregoing combination is because a major drawback of RTS/CTS scheme is already overcome by the usage of larger frame size (e.g. frame aggregation) available in the new IEEE 802.11 amendments.

In other words, our aim in this work is not to design and evaluate a specific algorithm or heuristic to be implemented in future IEEE 802.11ax devices, but to study the potential benefits of combining intelligent PHYCCA adaptation and uplink RTS/CTS control, leveraging new mechanisms under the consideration of the IEEE 802.11 TGax.

5.4.1 System Model

As highlighted in TGax specification framework document [93], this new amendment intends to define a mechanism by which an AP can configure the use of RTS/CTS for each associated non-AP station. In [91], the authors highlight the possible mechanism through which an AP can control the RTS/CTS policy for the associated stations. We build our propositions on the aforementioned principles.

The legacy IEEE 802.11 standard has defined a configurable parameter called RTS Threshold (RT), that is used to enable and disable the RTS/CTS handshake for each station. If the length of frame to be transmitted is greater than the assigned RT, the four-way handshake is initiated. Traditionally, the RT value was always set to a very high value so as to disallow the usage of the RTS/CTS mechanism.

In this section, we illustrate methods through which we select certain number of stations within the network to utilize RTS/CTS. Different metrics (i.e. FER, SINR, hidden node count, etc.) can be used as selection criteria. FER information is readily available over each station and thus can be used in the decision process. However, it is difficult to measure SINR in real system, especially when the intended and the interference signal arrive asynchronously. Furthermore, both FER and SINR are highly depending on the environment, where mobility and obstacles can induce random variations. Hidden node count at each station can also be utilized to initiate RTS/CTS method because most of the collisions occur due to transmissions from stations that are unable to hear each other. However, detecting hidden nodes at each station is not trivial.

In this work, we use FER as well as hidden node count as the main criterion to enable and disable RTS/CTS. Intuitively, lower FER does mean less frame collisions, indicating a smaller number of hidden terminals. Using FER metric is a practical approach to the problem in hand. Hidden node count, on the other hand, is used to validate the concepts of increase in FER but can not be considered a practically feasible solution.

We consider L APs and M non-AP stations associated to a single AP within each cell (i.e. we have total of $L \times M = N$ non-AP stations). All APs are assumed to be connected to a single distribution system (DS). Furthermore, the coverage area of the cells are assumed to overlap, where each non-AP station is only associated with a single AP. At the MAC layer, all stations utilize DCF-based channel access method, where the stations can opt to use basic or RTS/CTS mechanism. A transmitting station can dynamically adopt its Carrier Sensing Range by utilizing DSC algorithm (previously evaluated in [12]). Due to lack of non-overlapping channels, some of the APs are assigned same channels.

5.4.1.1 Method 1

In this method, we enable RTS/CTS mechanism on O (where $O \subset N$) number of stations based on the criteria that the FER of the selected stations is greater than FER_{Thresh} (i.e. a threshold based on the average FER of the network). All APs are assumed to be able to infer FER information of all associated stations (either by means of an explicit feedback, or through local estimations based on received frames [30]) over the duration of τ_c, where DSC is enabled for all non-AP stations. Figure 5.8 highlights the implementation details of the proposed method, where two separate instances

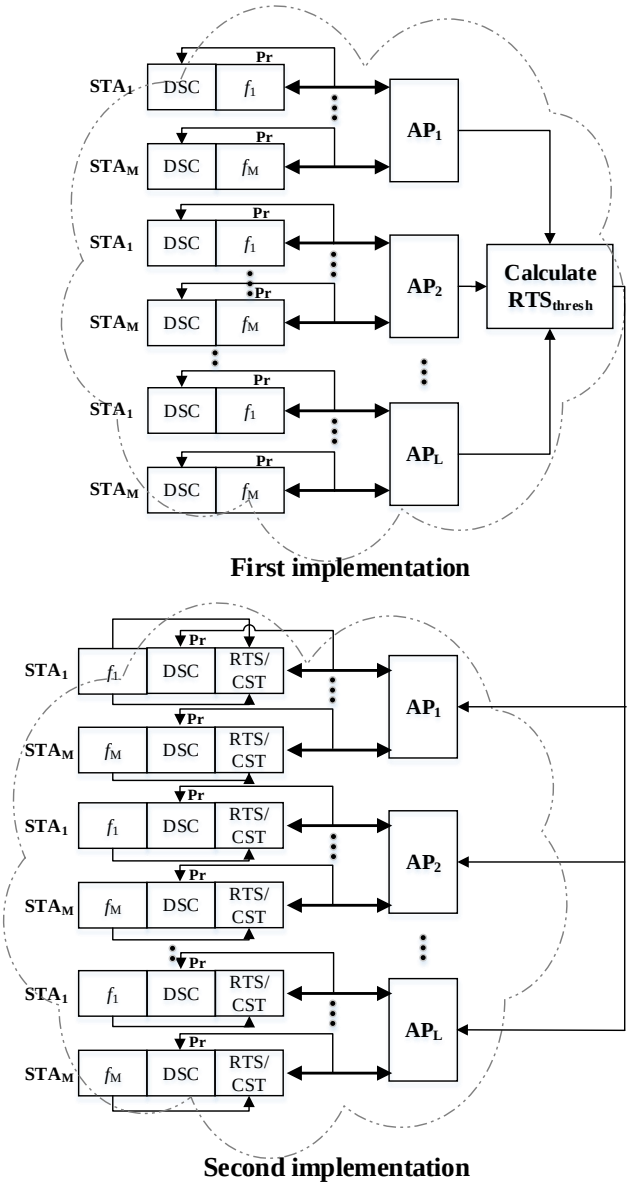


Figure 5.8: Graphical representation of Method 1.

of a network are operated in sequential manner. In the first step, the APs collect the FER information (f_i) of each station for a specific period. Afterwards, they collaborate to find the average FER (called $AvgFER$ in equation 5.26) within the network. Following equation is used to calculate the FER_{Thresh},

$$FER_{Thresh} = \delta \times AvgFER \tag{5.26}$$

where δ is assigned a fixed value. As shown in sub-section 5.7.1.1, δ = 0.6 provides the best performance. In the second step, this FER_{Thresh} is used by each AP to select an RT value for each associated station (i.e. AP activates RTS/CTS by transmitting specific RT values to the associated stations). The RT_i value set for each station by the AP can be explained by the following linear adaptation algorithm,

$$RT_i = \begin{cases} minRT_i, (f_i \geq FER_{thresh}) \\ maxRT_i, (f_i < FER_{thresh}) \end{cases} \tag{5.27}$$

where $minRT_i$ is a value that is less than the frame length used by a non-AP station that, in return, activates RTS/CTS for it and $maxRT_i$ has a value greater than the frame length, that disables RTS/CTS[1].

As an outcome of this method, a percentage of stations only employs the four-way handshake mechanism based on their FER being ranked in the overall network. Figure 5.8 signifies the implementation detail of the foregoing method, where STA represents a non-AP station.

5.4.1.2 Method 2

The drawback of the previous method (i.e. Method 1) is the need for all the APs to collaborate in order to evaluate the $AvgFER$ of all the stations operating within the network.

On the contrary, in this method we maintain the distributed nature of each cell, where every AP selects a fixed percentage (i.e. η) of stations to enable RTS/CTS. The AP ranks the FER of associated stations and selects the percentage of stations that have the highest FER in descending order. The AP then assigns and transmits a specific RT_i value to each station which results in activation or deactivation of RTS/CTS for a station (i.e. RTS/CTS is enabled when RT of station is greater than the frame length used by it and vice versa).

5.4.1.3 Method 3

Since, by utilizing RTS/CTS method, we explicitly want to tackle the problems caused by hidden nodes, in this Method 3, we utilize hidden node count at each station as an enabling criteria. Even though, this method does require additional algorithm being implemented at the stations (where a station can predict the presence of hidden stations by observing the contention levels over the shared medium), we use it to compare with the FER based schemes presented in 5.4.1.1 and 5.4.1.2.

At the beginning, each station shares the hidden node count information with its AP. All the APs then collaborate to select a percentage (i.e. γ) of stations to enable four-way handshake. The selection process involves ranking the hidden node count for each station in descending order and to select stations that have highest number of hidden node count. Each AP then transmits a specific RT_i value for each associated station, which results in activation or deactivation of RTS/CTS for a station (i.e. RTS/CTS is enabled when RT of station is greater than the frame length used by it and vice versa).

[1] If all the non-AP stations utilize similar frame lengths, both $minRT_i$ and $maxRT_i$ can be assigned fixed values.

5.5 Simulation environment

In order to showcase the benefits of introducing DSC within dense WLAN deployments, we present a simulation-based study (utilizing network simulator NS-3) to evaluate the performance of an IEEE 802.11 infrastructure network operated within dense building apartments. We compare the performance when DSC (at both non-AP stations and AP stations) was used within the network with the legacy IEEE 802.11, in which a constant/default CST threshold was used in every node.

In our simulations, we considered the scenario defined by the IEEE 802.11ax TGax in [88], consisting of a multi-floor residential building (see Figure 5.9). It consisted of 100 apartments and had the following specifications:

- 5 floors, 3m height of each floor
- 2×10 apartments in each floor
- Apartment size: 10m×10m×3m
- Building type: Residential
- External wall type: Concrete with windows

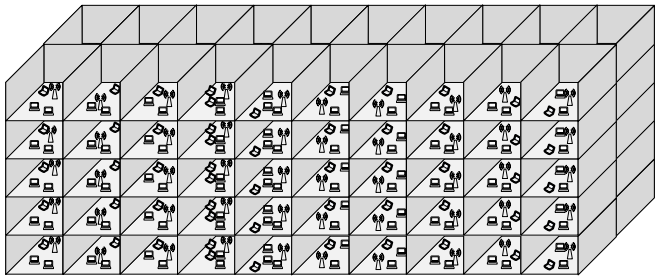


Figure 5.9: Layout of dense deployment of IEEE 802.11 infrastructural network in residential building.

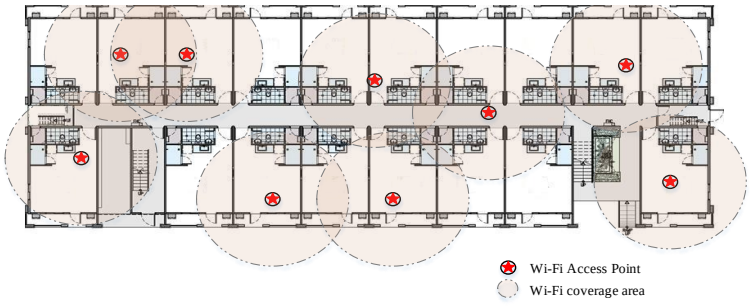


Figure 5.10: Example floor-plan of a single floor portraying dense Wi-Fi deployment.

A single AP was randomly placed within the walls of each apartment. Figure 5.9 indicates a possible indoor floor plan consisting of randomly placed APs. Five non-AP stations were placed around

each AP randomly. Furthermore, APs selected channel 1, 6 and 11 at random so that each channel was shared by 1/3 of the cells. We focus our study on the use of 2.4 GHz band because this band is more restricted in dense environments. The simulation was carried out using NS-3 network simulator in which Hybrid building propagation loss model[1] was used. For the final calculated results, a large enough number of simulations were run in order to have small 95% confidence intervals. A large enough simulation time was chosen to disregard the transient time due to initial association between stations and APs. To make our evaluation more realistic, we consider asymmetric traffic where uplink transmission rate is set to one-fifth of downlink transmission rate. Furthermore, we assume that saturation condition[2] (i.e. stations always have frames to transmit) is established within each cell. Constant Bit Rate UDP flows were used on each transmitting node. It is important to mention here that the comparison between DSC and conventional IEEE 802.11 network was done under the exact same network conditions. We modified the NS-3 simulation package, a) to allow non-AP stations to measure the received energy level of each beacon frame received from the relevant AP, b) to measure the received energy level of any frames by the AP, received from its associated stations as well as from its neighboring APs, c) by improving hybrid building pathloss model to accommodate for floor penetration losses.

The metrics used in our evaluation are: 1) aggregate throughput (total bytes correctly received by the receivers per second); 2) FER; 3) Fairness[3] (calculated according to Jain fairness index); 4) number of hidden nodes; 5) number of exposed nodes. For the hidden node analysis, we considered a pair of hidden nodes (i.e. two nodes that are hidden from each other) as a single entry. This simplification was also used for the exposed node count. The description of PHY and MAC layer parameters used in our simulations are detailed in Table 5.3 and Table 5.4 respectively.

5.5.1 Tunning of DSC parameters

In sub-section 5.3.3, we derived an analytical model to set CST of a station based on received power from its intended transmitter(s). In order to justify our analysis, we demonstrated a simple example where the CST value was set to be approximately 20 dB less than the received power (the difference between the received power of -55 dBm and the newly calculated CST of -75 dBm). This value of 20 dB, which follows from equation (5.25), can be considered as a benchmark around which the optimal value can be selected (fine tuned) for more realistic environments. This optimal value (called Margin) when added to the received power could result in appropriate CST selection of a node and thus results in increased spatial reuse.

Through extensive experimentation, we provide recommended values of different DSC parameters to be used at the non-AP (as seen in Section 5.6.1) and the AP stations (as seen in Section 5.6.1). Those values were found to produce a good balance between the benefits of DSC and its drawbacks,

[1] Hybrid Buildings Propagation Loss Model: NS3-Design document: http://www.nsnam.org/docs/models/html/buildings-design.html.

[2] Saturation is used to explore maximum capacity.

[3] Overall fairness in the network is calculated based on per flow analysis.

[1] In NS3, energy detection threshold corresponds to receiver sensitivity and not the PHYED threshold.

Table 5.3: PHY layer parameters for simulation.

Parameter	Values	Parameter	Values
Wireless Standard	IEEE 802.11n	Frame payload size	1000 and 1500 Bytes
Frequency band	2.4 GHz	Trans. power (STA & AP)	16 dBm
Physical transmission rate	72.2 and 7.2 Mbps	Antenna gain	1 dB
Propagation loss model	Hybrid buildings propagation loss	Noise figure	7 dB
Propagation delay model	Constant speed propagation delay	Energy detection threshold[1]	-78 dB
Shadow fading	disabled	Initial CST	-80 dBm
Wall penetration loss	12dB	Rate adaptation mechanism	not used
Floor penetration loss	17 dB	Channel width	20 MHz
Guard interval	Short	Data preamble	Short
AP and STA number of TX/RX antennas	1/1		

and, hence, are the values used in rest of simulations described in Section 5.6.

Furthermore, *UpperLimit* is set to -40 dBm and *LowerLimit* is set to -82 dBm for every station that utilizes DSC; $2s$ of *UpdatePeriod* is used within the algorithm.

5.5.2 Parameters for adaptive RTS/CTS

In order to evaluate the performance of AP controlled four-way handshake uplink access, the PHY and MAC layer parameter presented in Table 5.3 and Table 5.4 are used along with the activation of RTS/CTS mechanism. Following equation 5.27, the $minRT$ is set to 200 (i.e. a fixed value below the data frame size) and $maxRT$ is set to 999999 (i.e. a fixed value above the data frame size).

Table 5.4: MAC layer parameters for simulation.

Parameter	Values	Parameter	Values
Access protocol	EDCA, AC_BE with default parameters ($CWmin = 15$, $CWmax = 1023$, $AIFSn = 3$)	Retransmission attempts	16
RTS/CTS	disabled	Maximum missed beacons for re-association	100000
Association	100 % STAs associated to AP within an apartment	Active probing	disabled
Traffic type	UDP CBR	Aggregation	disabled
Beacon Interval	100ms		

5.6 Simulation results and discussion on DSC

In this section, we evaluate the performance of the proposed DSC algorithm through an extensive simulation study. We compare the IEEE 802.11 network that utilizes DSC algorithm at all stations (AP and non-AP) with a network that utilizes legacy IEEE 802.11 stations. It is important to highlight that the contention parameters for IEEE 802.11 (i.e. $CWmin = 15$, $CWmax = 1023$) are kept constant throughout the simulation study. These parameters are particularly important in high density environments, where most of the stations spend time in back-off due to collisions. In the following sections, we demonstrate that DSC algorithm provides multifarious benefits in dense IEEE 802.11 implementations.

5.6.1 Recommended parameters for DSC algorithm at non-AP stations

First, we evaluate the DSC algorithm to be applicable at the non-AP stations so as to uncover the combination of recommended values for *MarginSTA* and *RSSIDec*, which provide maximum efficiency. Different combination of values for *MarginSTA* (5, 10, 15, 20 and 25) and *RSSIDec* (4, 5 and 6) are used for the evaluation process.

In this section, we define a network in which all non-AP stations implement DSC and utilize a fixed data rate (24 Mbps). We then compare different metrics to the same network with all stations using constant CST.

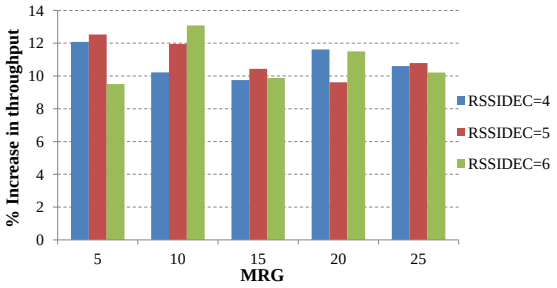
Figure 5.11a. presents the percentage increase in aggregate throughput for all the nodes while utilizing different set of *MarginSTA* and *RSSIDec*. The throughput results indicate around 10% improvements for all the cases over the conventional IEEE 802.11 protocol.

Figure 5.11b. shows the percentage increase in fairness achieved while utilizing DSC algorithm. The proposed algorithm increases the aggregate throughput along with fairness in the system. Maximum fairness benefits are achieved when lower values of *MarginSTA* are used.

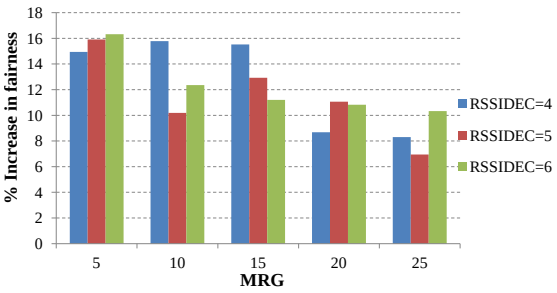
Figure 5.11c. highlights the percentage increase in hidden nodes while utilizing DSC. At higher *MarginSTA* values, the increase in hidden nodes is smaller. Another important outcome is that the presence of exposed nodes is driven to 0.

As a consequence of the increased number of hidden nodes, the overall FER in the network is also increased. These results are highlighted in Figure 5.11d. It is important to mention that higher values of *MarginSTA* and *RSSIDec* result in smaller FER degradation. This is due to the fact that the impact of *MarginSTA* and *RSSIDec* results in lower *CST* and thus the carrier sensing range is increased. As a consequence, the FER is decreased due to less hidden nodes.

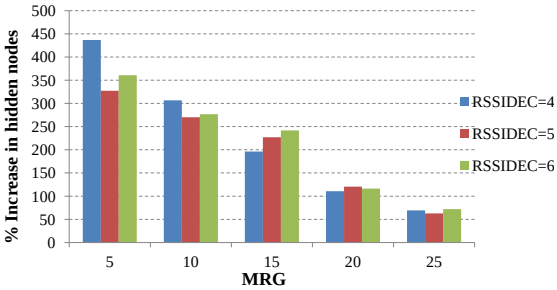
Comparing Figures 5.11a, 5.11b, 5.11c and 5.11d, it is pertinent to mention that the DSC scheme provides improvements in throughput and fairness at the cost of increasing FER and hidden nodes. After closely analyzing the results, we chose *MarginSTA* as 20 and *RSSIDec* as 6 to be the recommended parameters that create a balance between the negative and positive aspects of DSC. We employ these values for DSC algorithm when used at the non-AP station in the remainder of the chapter.



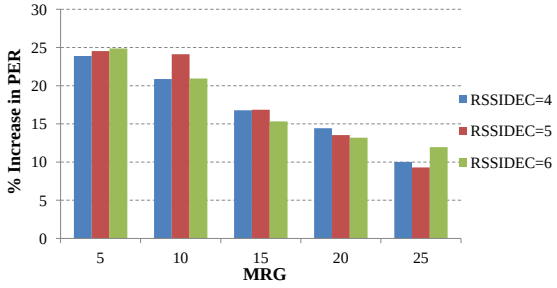
(a) Throughput improvement with DSC at non-AP stations.



(b) Fairness improvement with DSC at non-AP stations.



(c) Increase in number of hidden nodes with DSC.



(d) Increase in FER with DSC.

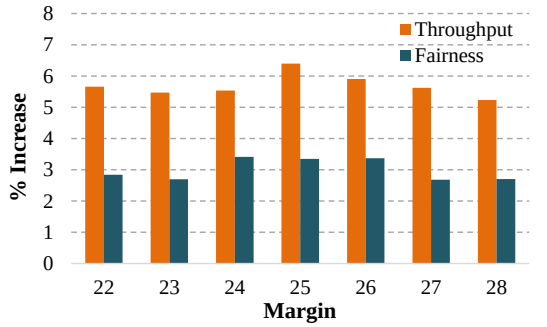
Figure 5.11: Increase of different metrics when DSC is in use for different combinations of $Margin$ and $RSSIDec$.

5.6.2 Recommended parameters for DSC algorithm at AP stations

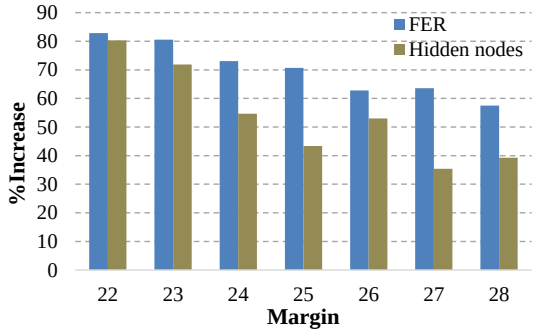
Next, we evaluate DSC algorithm for AP stations to uncover the recommended value for *MarginAP* which provides maximum efficiency in the simulation environment under consideration.

In Section 5.3.3, we derived an analytical model to set CST of a node based on received power from its intended transmitter/transmitters. In order to justify our analysis, we demonstrated a simple example where the CST value was set to be approximately 20 dB less than the received power (the difference between the received power of -55 dBm and the newly calculated CST of -7 5dBm). This value can be considered as a benchmark around which the optimal value can be selected (fine tuned) for more realistic environments. This optimal value, when added to the received power, could result in optimal CST selection of a node and thus results in increased spatial reuse.

In this section, we consider a network encompassing only downlink traffic in which all AP stations implement DSC and utilize a fixed offered load (i.e. 6 Mbps that lead to saturation condition) over every AP to station link. Figure 5.12a presents the percentage increase in aggregate throughput and fairness for all the APs while utilizing different $MarginAP$ values. The throughput results indicate



(a) Throughput and Fairness improvements with DSC at APs.



(b) Increase in FER and number of hidden nodes with DSC at APs.

Figure 5.12: Increase of different metrics when DSC at APs is in used for different $MarginAP$ values.

around 6 % improvements for all the cases over the conventional IEEE 802.11 protocol. The proposed algorithm increases the aggregate throughput along with fairness in the system. Maximum fairness

benefits are achieved when *MarginAP* values of 24, 25 and 26 are used.

Figure 5.12b highlights the increase in FER and hidden nodes while utilizing DSC at AP stations. Higher *MarginAP* values caused less hidden nodes. Another important outcome is that the presence of exposed nodes is driven to 0.

As a consequence of the increased number of hidden nodes, the overall FER in the network is also increased. However, the impact of an increased FER can be reduced by the MAC level stop-and-wait ARQ used in IEEE 802.11 transmissions. It is important to mention that higher values of *MarginAP* induce smaller FER degradation. This is due to the fact that the impact of *MarginAP* results in lower i.e. more conservative *CST* of APs and thus the carrier sensing range is increased. As a consequence, the FER is decreased due to less hidden nodes.

Comparing Figures 5.12a and 5.12b, it is pertinent to mention that the DSC scheme (when utilized at the AP stations) provides improvements in throughput and fairness at the cost of increasing FER and hidden nodes. After closely analyzing the results, we chose *MarginAP* of 25 to be the recommended parameter that creates a balance between the negative and positive aspects of DSC. We employ this value for DSC algorithm at the APs in the remainder of the chapter.

5.6.3 Justification of upper and lower limits of CST in DSC algorithm

As highlighted in Section 5.3.2, the optimal CST of a station is expected to create a balance between the number of hidden and exposed stations that helps to enhance the throughput gains. In this section, we show results that justify the need to have upper and lower limits to confine CST of a station within a bounded region. We expose the performance of a network (employing asymmetric traffic) where variants of DSC algorithm (that include and exclude the *UpperLimit* and the *LowerLimit*) are employed at the downlink as well as at the uplink. The overall performance of DSC with limits (referred to as DSC) and DSC without limits (called DSC with no limits) are compared to the network where default/fixed CST is utilized by each node.

Figure 5.13 reveals near 7% throughput improvement for DSC network utilizing limits over conventional IEEE 802.11 protocol. On the other hand, even without limits, DSC improves throughput and fairness, but to a lesser extent (due to increased interference). However, both variants of DSC algorithms were found to improve the overall fairness in the network.

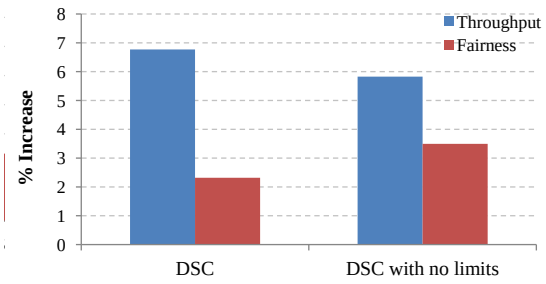


Figure 5.13: Percentage increase in throughput and fairness.

As a consequence of the increased number of hidden nodes, the overall FER in both types of DSC networks increased due to greater collision probabilities. These results are presented in Figure 5.14. It is pertinent to highlight results for DSC with no limits, where FER is considerably increased due to stations transmitting without any restriction or care for other transmissions[1]. This increase in FER results in reduced throughput for DSC with no limits. The hidden node count for both the variants of DSC show similar trends. However, exposed node count for DSC with no limits slightly increased (i.e. instead of complete elimination, few exposed nodes where found within certain simulations) due to the limit-less increase in carrier sensing range by a limited number of far-off placed stations.

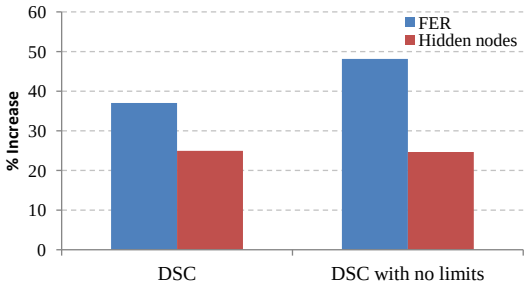


Figure 5.14: Percentage increase in FER and hidden nodes.

The above mentioned results demonstrate the benefits of limiting/confining the variation of CST over each station and are aligned with the outcomes of a non-cooperative game-theoretic framework for decentralized control of physical carrier sensing presented in [79].

5.6.4 Comparing the effectiveness of DSC scheme.

In this section, we test the effectiveness of the proposed DSC scheme by comparing with a protocol suggested in literature (referred to as AP-CST [102]) and with a scenario where constant increased CST (i.e. -65 dBm[2]) is assigned to all stations (this static/fixed scheme is designated with the name FCST). The aforementioned schemes were tested with the same amount of aggregated traffic load asymmetrically shared among AP and non-AP stations (i.e. AP supported K times more traffic). The motivation to compare DSC with AP-CST lies in the fact that both of these schemes were designed to operate over every station (AP and non-AP) within dense WLAN infrastructure network. Moreover, despite of the functional differences, the core functionality of both schemes show similarity where received signal strength of the frames is used as a principle information in adapting the CST. DSC scheme differs from AP-CST on the basis that, instead of varying CST of transmitter based on the RSSI of frames at the receiver (that incurs in feedback overhead due to continuous SINR sharing, where CST of the transmitter is set based on received SINR at the receiver), DSC transmitter adapts its CST based on RSSI of frames received by it from the relevant transmitter (thus not relying on continuous

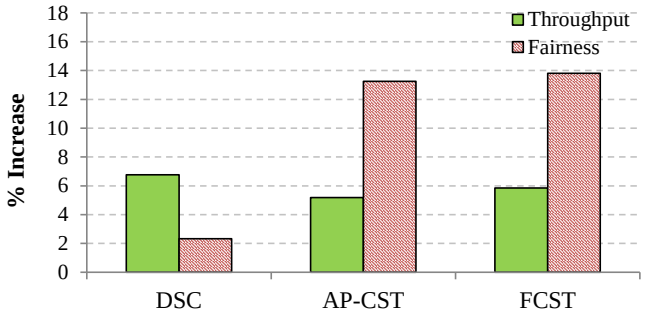
[1] It is important to mention here that increase in FER implies greater delay in transmission (due to retransmissions and larger backoff intervals)

[2] The reason to select this value for comparison is because the average CST value (for all stations) in the DSC enabled network for numerous simulations was found to be around -65 dBm

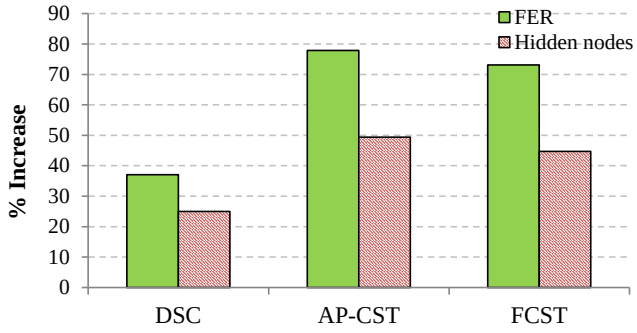
exchange of information between the transmitter and the receiver). In addition to AP-CST, the reason to compare DSC with FCST can be justified with the rational that, in dense residential scenario, stations are relatively placed in close proximity to their respective APs and comparing performance of fixed increased CST (i.e. small carrier sensing range) for all stations can signify the importance to adapt CST on each station based on local circumstances.

Both AP-CST and FCST schemes were also implemented in NS-3 and the comparisons were performed over similar environments (i.e. same network conditions and similar station positions). For AP-CST scheme, the values of pathloss exponent and SINR threshold are assumed to be 3.5 and 15 dB respectively (note that these values are selected in order to be consistent throughout the analysis and correspond to the value assumed in the analysis done in 5.3.3). Two way transmission in saturation conditions is utilized, where percentage improvement of DSC, AP-CST and FCST with respect to stations utilizing default CST (i.e -80dBm) is considered.

Figure 5.15a shows that the three schemes perform better than legacy IEEE 802.11 in terms of



(a) Percentage increase of throughput and fairness.



(b) Percentage increase in FER and number of hidden node.

Figure 5.15: Comparison of DSC, AP-CST and FCST.

throughput and fairness; DSC provides the best throughput (i.e. 417.65 Mbps for DSC, 405.83 for AP-CST and 414.064 Mbps for FCST as compared to 391.167 Mbps for the case when no algorithm in applied), and FCST appears to be the fairest (i.e. 0.67 for DSC, 0.736 for AP-CST and 0.744 for FCST

as compared to 0.65369 for the case when no algorithm is applied). However, in Figure 5.15b, it is clear that all three schemes witness more collisions, with DSC showing the smallest increment.

Fairness benefit achieved for AP-CST is due to the fact that this scheme assigns the minimum achieved CST to each station and thus is not purely dynamic. Moreover, allotting same reduced CST leads to all stations accessing the shared medium in much fairer manner. More specifically, AP-CST and FCST end up being too aggressive so that stations seem to only defer upon transmissions from their own cells (i.e. all stations have the same number of effective contenders) while DSC is more conservative and some stations are also aware of neighboring cells. This reduces collisions and increases throughput.

All of the schemes were found to eliminate the presence of exposed nodes (i.e. out of total 16,110 possible links among the 150 non-AP stations and 30 AP stations, the exposed links are reduced from approximately 110 to 0). With context to hidden station problem caused by an increased CST value, DSC scheme raised the hidden links count from approximately 1060 to 1324 out of the total 16,100 possible links within the network. For CST-AP, this count increased from 1060 to 1783 and for FCST, the number of hidden links increased from 1060 to 1533.

Despite of improvements witnessed in terms of throughout due to increased spatial reuse, AP-CST and FCST schemes were found to only perform better than DSC in terms of fairness over the cost of considerable increase in FER (i.e. 0.1784 for DSC, 0.25 for AP-CST and 0.26 for FCST as compared to 0.1302 for the case when no algorithm is applied).

The aforementioned analysis indicates that DSC exhibits the best balance between the positive and negative aspects of CST adaptation; it shows the highest throughput increase with the smallest FER degradation. It is important to highlight that intelligent utilization of AP controlled four-way handshake (where the AP can selectively enable RTS/CTS only for stations that face greatest collisions within a cell) can be used along with DSC to further improve and enhance the performance (in terms of throughput, fairness and FER) [7]. Building on the argument, as mentioned in Section 4.4.2, TGax is contemplating to use the aforementioned technique to reduce interference/FER.

The aforementioned analysis indicates that DSC exhibits better throughput performance without causing noticeable increase in collisions.

5.6.5 Combining DSC at non-AP stations with Channel Selection and Rate Control

The legacy IEEE 802.11 standard allows operation over channels on the 2.4 GHz ISM and 5 GHz U-NII bands. Although non-overlapping channels can be configured to be used by neighbouring APs, most of the existing dense WLAN deployments utilize the default channel assignment that results in sub-optimal performance of the network. This problem is further aggravated by the fact that the 2.4 GHz band suffers from lack of non-overlapping channels (i.e. only 3 are non-overlapping) and majority of today's Wi-Fi devices utilize the IEEE 802.11n standard over the 2.4 GHz band.

Therefore, default channel assignment and the high density of stations make interference one of the main reasons behind poor performance of WLAN deployments. The network performance is

further degraded by the frequent occurrence of hidden and exposed node problem. Therefore, the network performances can be increased by assigning optimal channel selection by different stations. This efficient assignment of channels can be achieved through different approaches (see e.g. [32, 42, 57]). In general, the goal of optimal channel selection schemes is to introduce maximum possible spectral separation between potential interfering links.

In optimal channel selection, channels are selected at each AP so that the distance between co-channel cells is maximized (so as to avoid/minimize interference between neighboring co-channel cells and thereby maximize network capacity). In this subsection, we evaluate the performance of DSC (at AP and non-AP stations) under optimal channel selection.

In this section, we evaluate the performance of DSC under channel selection and rate control. As mentioned in [92], the DSC algorithm can be combined with an intelligent channel selection to provide increased efficiency. We further assess the DSC algorithm varying the MCS at each non-AP stations.

The rational for this analysis is to show the impact of combined usage of DSC along with optimal channel selection. It should be noted here that optimal channel selection mimics the behavior of a managed network. In other words, we are pointing out that DSC is bound to show better performance in non-residential environments as well.

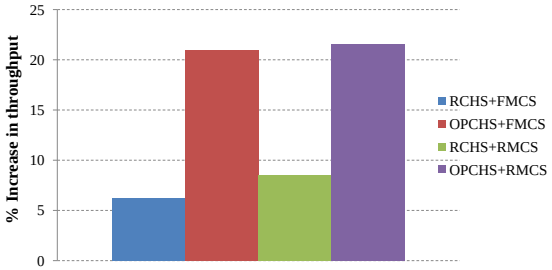
We simulate the following scenarios to expose a comparison between IEEE 802.11 network utilizing and not utilizing DSC algorithm, a) IEEE 802.11n network with Fixed MCS and Random CHannel Selection (RCHS+FMCS), b) IEEE 802.11n network with OPtimal CHannel Selection[1] and Fixed MCS (OPCHS+FMCS), c) IEEE 802.11n network using Random MCS and Random CHannel Selection (RCHS+RMCS), d) IEEE 802.11n network with OPtimal CHannel Selection and Random MCS (OPCHS+RMCS).

Random MCS is added to emulate the presence of inner walls and other obstacles within the apartment/office that will trigger the rate adaptation on stations receiving varying signal quality. For optimal channel selection, three 20 MHz-wide non-overlapping channels (i.e. 1, 6, and 11) are used. For fixed MCS case, the MCS index used is 7 (i.e. PHY rate of 72.2 Mbps) and for random MCS, a random MCS index (following uniform distribution) is selected among 0, 3 and 7 (i.e. 7.2, 28.9 and 72.2 Mbps) for all the nodes in the network.

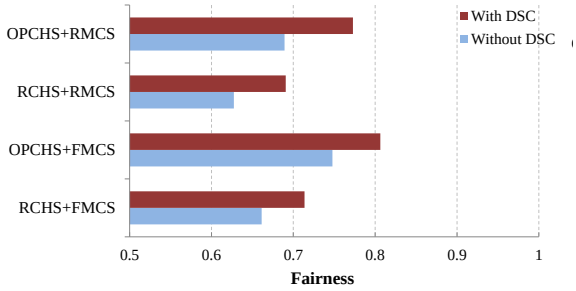
5.6.5.1 Throughput comparison

In Figure 5.16a, we illustrate a comparison of throughput improvements induced by the use of DSC in a dense IEEE 802.11n WLAN. It is worth noting that the scenarios where DSC is combined with optimal channel selection provide maximum throughput gains of more than 20%. Furthermore, note that when MCS is set randomly, the average MCS on the network is lower (i.e. transmissions last longer) and the penalty imposed by exposed nodes is higher. In those cases, DSC has more room for improvement.

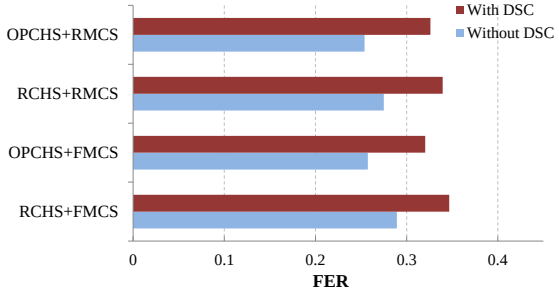
[1] In optimal channel selection, channels are selected at each AP so that the distance between co-channel cells is maximized.



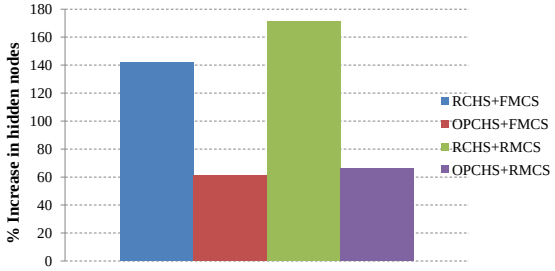
(a) Comparison of four schemes in terms of % increase of throughput while utilizing DSC.



(b) Fairness comparison between four schemes w.r.t average values.



(c) FER comparison of four schemes while utilizing DSC.



(d) Comparison of four schemes in terms of % increase in hidden nodes while utilizing DSC.

Figure 5.16: Combining DSC at non-AP stations with channel selection and rate control

5.6.5.2 Fairness analysis

It is logical to think that DSC may decrease fairness by giving more transmission opportunities to nodes that are near the AP, since they set higher CST values. On the other hand, DSC reduces the number of exposed nodes, which may become starved when they are located between two unsynchronized transmitters. Figure 5.16b indicates that fairness is increased in all the scenarios when DSC is used. This validates our previous conclusion that DSC increases the aggregate throughput by fairly increasing throughput over all the nodes.

5.6.5.3 FER assessment

In Figure 5.16c the average FER value of the four scenarios is presented, while comparing the scenarios with and without DSC. As mentioned in Section 5.6.1, FER is increased when DSC is introduced. FER is slightly improved when optimal channel selection is used.

5.6.5.4 Hidden and exposed nodes comparison

As expected, % increase in hidden nodes is smaller while utilizing optimal channel selection. This result is depicted in Figure 5.16d. With a random channel selection, the increase in hidden nodes is around 150%. On the contrary to hidden nodes, in all of these experiments we witness almost 100% decrease in the number of exposed nodes.

5.6.6 Combining DSC with Channel Selection in asymmetric up-link and down-link traffic

In this sub-section, we evaluate the performance of DSC (at AP and non-AP stations) under optimal channel selection (so as to avoid/minimize interference between neighboring co-channel cells and thereby maximise network capacity).

We simulate IEEE 802.11n network with OPtimal CHannel Selection with DSC (OPCHS+DSC) and compare its performance with the following scenarios, a) IEEE 802.11n network with OPtimal CHannel Selection without DSC (OPCHS+NODSC) b) IEEE 802.11n network using Random CHannel Selection with DSC (RCHS+DSC), c) IEEE 802.11n network with Random CHannel Selection with no DSC (RCHS+NODSC)[1].

5.6.6.1 Throughput comparison

In Figure 5.17, we illustrate a comparison of throughput improvements induced by the use of DSC in a dense IEEE 802.11n WLAN with optimal channel selection. It is worth noting that the scenarios where DSC is combined with optimal channel selection provide maximum throughput gains of more than 30% when compared with a network that utilizes neither DSC nor channel selection. Additionally, approximately 25% improvement was witnessed when DSC network utilizing optimal

[1]This scenario can also be represented as legacy IEEE 802.11 network

channel selection scheme was compared with a DSC enabled network that did not utilize optimal channel selection. Individually, DSC improved throughput by approximately 7% (cf. Figure 5.17) whereas, on a network with an optimized frequency management, DSC was able to increase by up to 12%. This result validates the aforementioned argument that DSC provides increased efficiency when utilized in conjunction with optimal channel selection environment.

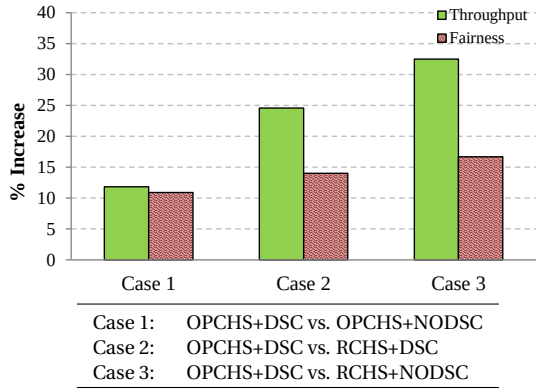


Figure 5.17: Improvements provided by OPCHS+DSC over different combinations of channel selection and DSC.

5.6.6.2 Fairness analysis

Figure 5.17 indicates that fairness is considerably increased in all the scenarios when DSC is used. This validates our previous conclusion that DSC increases the aggregate throughput by fairly increasing throughput over all the nodes.

5.6.7 Interoperability of DSC enabled nodes with legacy 802.11 nodes.

In this sub-section, we investigate the interoperability of DSC enabled devices in the presence of legacy IEEE 802.11 devices that do not implement any algorithm to modify their carrier sensing range. By doing so, we show the effect of DSC enabled stations/cells on other neighboring legacy stations/cells. Since WLAN deployments in residential scenarios are characterized to be unmanaged, DSC enabled devices are expected to co-exist with nodes that might not adopt similar solutions (such environments, also refereed as hybrid cases, can also be envisioned as backward compatibility challenge for the future IEEE 802.11ax standard).

In order to simplify the analysis and make the impact of hybrid scenario more observant, we highlight cases where different percentage of DSC enabled nodes/cells are made to operate along with legacy nodes/cells in network encompassing different traffic patterns.

5.6.7.1 Case 1: (Uplink traffic only) Impact of DSC cells over legacy cells

We first compare the performance of legacy cells (consisting of non-DSC AP and non-DSC stations) with DSC cells, where all nodes implement DSC. The simulation results are shown in Figure 5.18. As the number of DSC cells increase, the average throughput in the network also improved. However, average throughput of DSC cells increased over the cost of a small but noticeable decrease in throughput of non-DSC cells. The overall throughput and fairness within the hybrid network increased due to DSC and because legacy devices became less competitive with the growth of DSC cells. It is also interesting to note that the throughput trends for DSC cells decrease because, with the reduction in the number of legacy cells, the possibility for improvement also reduces; i.e. the advantage that DSC cells have when competing against legacy cells fades when all competition is DSC. That is, with 100% DSC cells, all the stations within the network get fair access of the channel.

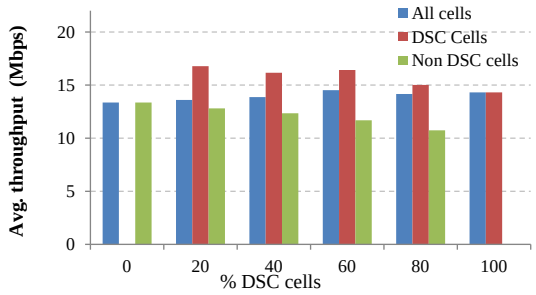
The overall FER in the network increased with the rise in DSC cells (due to increased number of hidden nodes) where FER for non-DSC cells remained approximately constant. In addition, as it is evident and can be inferred to as an outcome of the results, DSC increases fairness and improves spatial reuse by reducing the number of exposed nodes.

5.6.7.2 Case 2: (Uplink traffic only) Impact of DSC nodes over legacy nodes

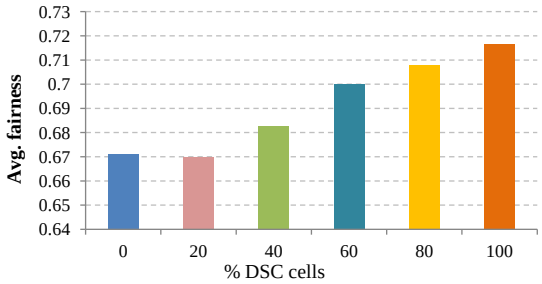
We now consider the performance of a network consisting of heterogeneous nodes (i.e. DSC and non-DSC nodes) that are made to co-exist within each cell and the percentage of DSC nodes is increased through regular intervals. As the number of DSC enabled stations increases, the network conditions become much fairer (as indicated by Figure 5.19). Therefore, the gains achieved by DSC stations decrease. The throughput trends of DSC stations decrease because the possibility of improvement is dependent on the stations that do not dynamically adapt their CST and thus unnecessarily refrain to transmit. However, on the average, the throughput of all DSC network remains greater than for a network composed only of legacy devices. DSC increased the fairness in the network by reducing the presence of exposed nodes. However, due to the aforementioned observation, the number of hidden nodes in the network increases which, in return, causes surge in FER of the network. Furthermore, fairness results point out the co-existence problem between DSC and legacy IEEE 802.11 nodes within the cells.

5.6.7.3 Case 3: (Asymmetric uplink plus downlink traffic) Impact of DSC cells over legacy cells

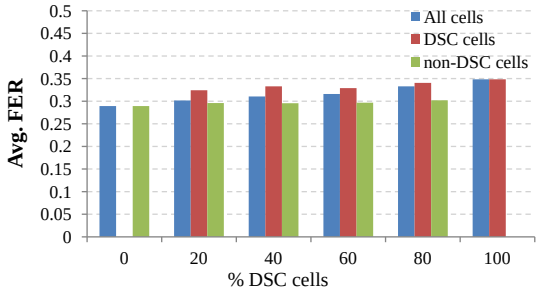
Figure 5.20 depicts the impact of DSC cells in asymmetric traffic conditions (where downlink transmission is much greater than the uplink transmission). Similar to the outcome of the results for Case 1, notable throughput gains were achieved by DSC cells at the cost of slight degradation for non-DSC cells where throughput gains for DSC cells were more evident in hybrid scenarios (i.e. DSC plus non-DSC cells).



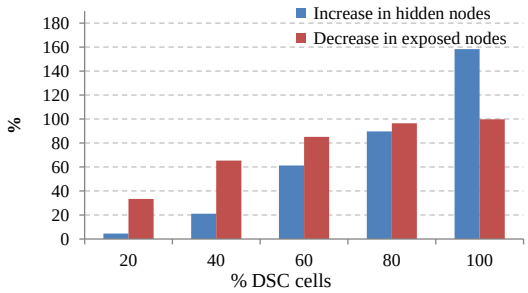
(a) Throughput improvement with DSC.



(b) Fairness enhancement due to DSC nodes.

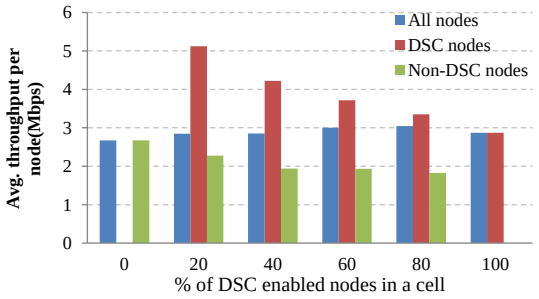


(c) Increase in FER with DSC cells.

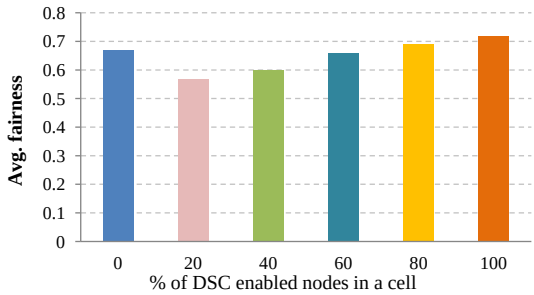


(d) Impact on hidden and exposed node count.

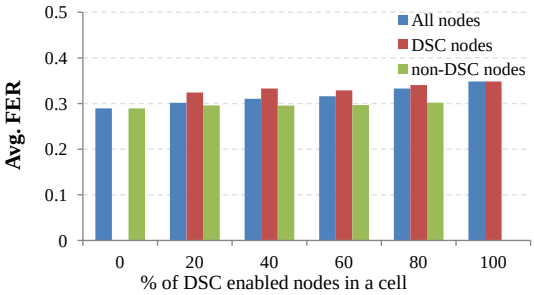
Figure 5.18: Impact of DSC enabled cells on legacy IEEE 802.11 cells under uplink traffic conditions.



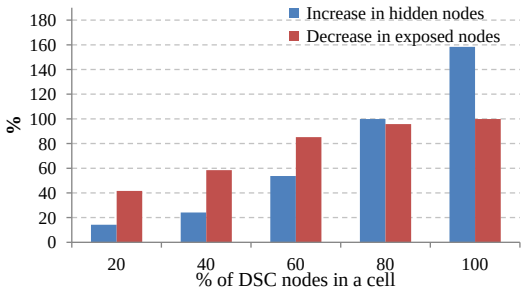
(a) Impact due to the presence of DSC nodes.



(b) Fairness enhancement due to DSC nodes.

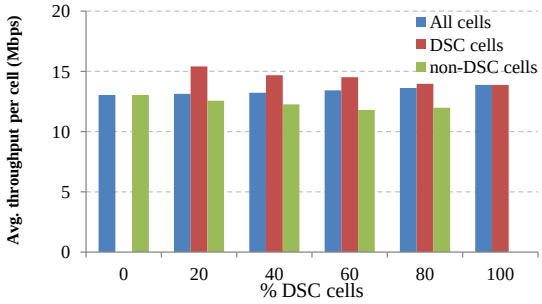


(c) Increase in FER within the hybrid network.

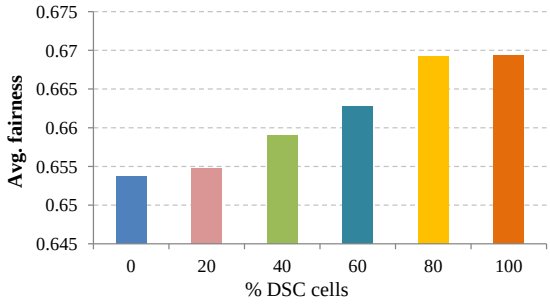


(d) Impact on hidden and exposed node count.

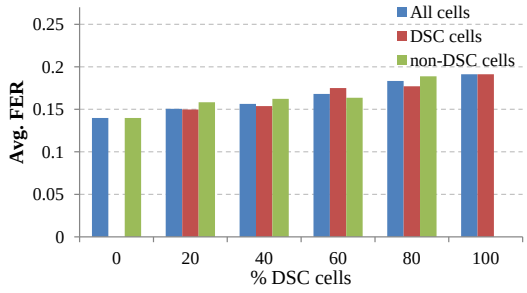
Figure 5.19: Impact of DSC nodes on legacy IEEE 802.11 nodes (where a % of DSC nodes within a cell are DSC enabled) within uplink traffic conditions.



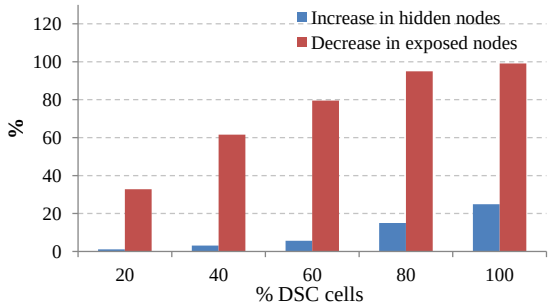
(a) Throughput improvement with DSC cells.



(b) Fairness enhancement incurred due to DSC cells.



(c) Increase in FER with DSC cells.



(d) Influence on hidden and exposed node count.

Figure 5.20: Impact of DSC enabled cells on legacy IEEE 802.11 cells under asymmetric traffic conditions.

5.6.8 Performance evaluation of DSC under worst case environment scenario

In this sub-section, we evaluate the performance benefits of DSC when employed in a scenario (referred to as worst case), where stations are made to transmit large packet size (i.e. 1500 Bytes) by using the lowest connection rate with the simplest modulation and coding (i.e. MCS 0). The rational to select the aforementioned scenario is based on the fact that greater number of stations transmitting packets of larger duration with minimum rate might lead to conditions where significant number of transmitters would be expected to get starved (due to increase in probability of non-availability of the shared medium). Therefore, stations in such environments can greatly improve their performance by varying their carrier sensing range. Since DSC is designed to alleviate the starvation problem by increasing the spatial reuse, selection of the worst scenario can be considered as a vital performance indicator.

Figure 5.20 highlights comparative analysis of a network encompassing uplink traffic in saturation conditions, where each station intends to transmit 1500 Bytes packet to their respective APs using MCS0.

According to the results, DSC was found to increase the aggregate throughput by fairly increasing throughput over all the nodes. Furthermore, the increase in throughput after enabling DSC in a scenario with optimal channel selection is considerable even under difficult network conditions(i.e. 35%). In addition, relatively small difference in FER was observed between the network consisting of optimal channel selection and random channel selection. Although better FER was expected for the case with optimal channel selection, a small difference was measured due to the fact that the slowest modulation used in the corner case under study is also more resilient against noise and interference. However, the inclusion of optimal channel selection with DSC was found to help reduce the number of hidden nodes.

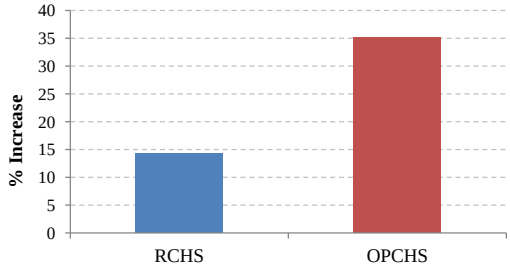
The foregoing results highlight significant improvement achieved due to the inclusion of DSC in worst case environment conditions.

5.6.9 Impact of DSC on a network employing rate adaptation in asymmetric uplink and downlink traffic

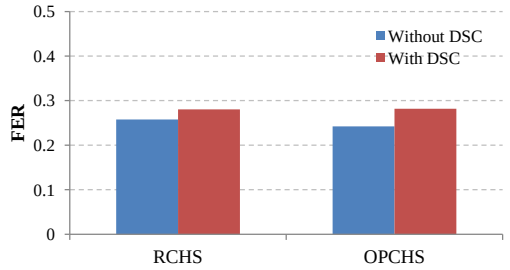
In order to make our analysis more realistic, in this section, we investigate the performance of DSC in a network where all stations utilize rate adaption. Rate adaption is a crucial part of wireless network performance, where different stations adapt the PHY layer configuration to the variability of wireless channel. These variations can be due to different factors, such as interference from other stations, signal attenuation or multi-path fading. IEEE 802.11 based WLAN support multiple rates for adaptive data transmission. In our analysis, we use the widely adopted Minstrel[1] [104] rate adaption algorithm, which adapts the rate based on statistics collected on the probability of successful transmission.

With the help of Figure 5.21, we illustrate the impact of DSC on an IEEE 802.11n networks with

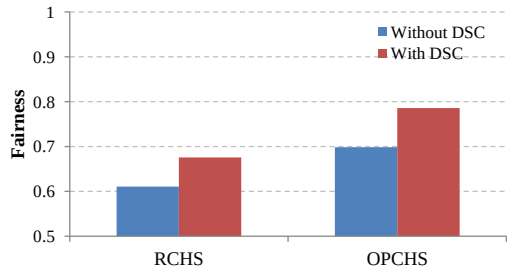
[1]Minstrel is the default rate control in Linux (for NICs supporting soft-MAC through mac80211 kernel module).



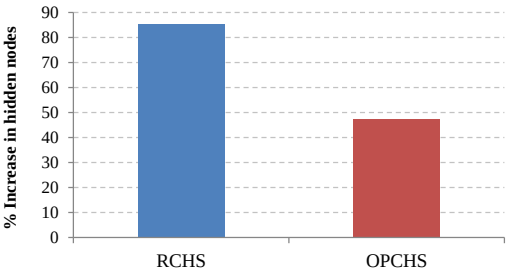
(a) Increase in throughput due to DSC under different channel management schemes.



(b) Increase in fairness due to DSC.



(c) Slight increase in FER due DSC.



(d) Percentage increase in hidden nodes.

Figure 5.20: Performance analysis of DSC under difficult network conditions (i.e. rate of MCS0 and packet size of 1500 Bytes).

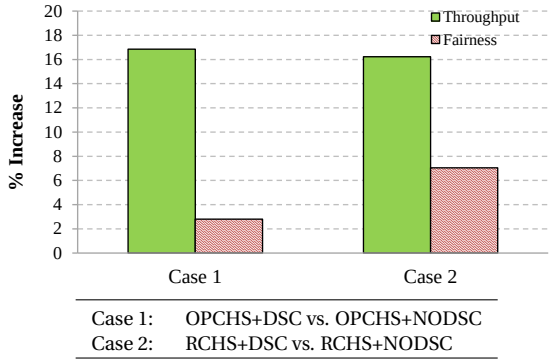


Figure 5.21: Improvements provided by OPCHS+DSC with rate adaptation over different combinations of channel selection and DSC.

rate adaptation. As expected, DSC improves the performance of the network also in the presence of rate adaptation, although to a lesser extent than the worst case studied in Section 5.6.8 (16% increase in throughput vs. 35%). More fairness benefits were witnessed for the random channel selection.

5.7 Simulation results and discussion on DSC leveraging RTS/CTS

In this section, we explore the experimental evaluation of the performance of DSC algorithm when intelligent RTS/CTS control methods are used to mitigate the drawback associated with DSC. More specifically, we compare the IEEE 802.11 network that utilizes DSC algorithm along with intelligent RTS/CTS control mechanism with a network that utilizes only DSC and with a legacy IEEE 802.11 based network. In the following sections, we demonstrate that the combined use of DSC along with four-way handshake can be beneficial in terms of reduced overall FER and can even provide throughput and fairness gains.

5.7.1 Evaluating methods to intelligent enable RTS/CTS

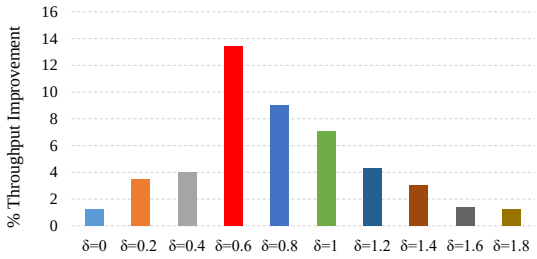
In this section, we evaluate the performance of methods proposed in Section 5.4.1 to intelligently select stations within a network for the RTS/CTS activation. The frame length used within the following analysis corresponded to the maximum allowed MSDU (i.e. 2302 Bytes) for IEEE 802.11.

5.7.1.1 Evaluating method 1

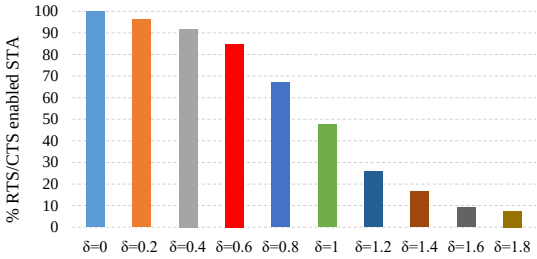
We start by first evaluating the implication of activating a percentage of RTS/CTS enabled DSC stations based on Method 1 (details provided in Section 5.4.1.1). Keeping in view the already proven improvements induced by the inclusion of DSC within densely deployed IEEE 802.11 networks, Figure 5.22a gives substance to the idea of intelligently utilizing RTS/CTS mechanism. Around 14% throughput improvement is witnessed when intelligent RTS/CTS plus DSC enabled network (utilizing δ of 0.6) is compared with only DSC enabled network. In terms of fairness, no notable difference

was found between RTS/CTS plus DSC and DSC only networks.

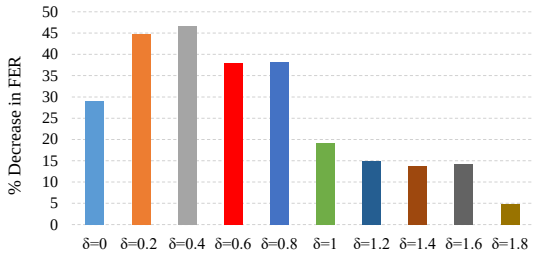
Figure 5.22c highlights considerable reduction in overall average FER of the network.



(a) Percentage increase of throughput.



(b) Percentage of RTS/CTS enabled nodes.



(c) Improvement in overall FER.

Figure 5.22: Comparison of four-way handshake enabled DSC stations utilizing method 1 with DSC-only stations.

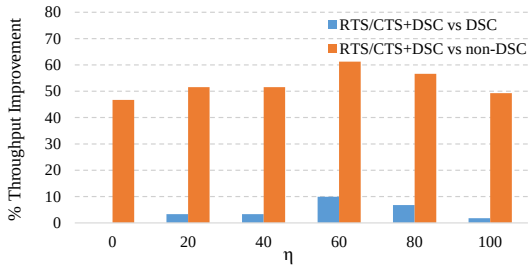
5.7.1.2 Evaluating method 2

We implement the selection process in this section based on the Method 2 presented in Section 5.4.1. The percentage η of nodes utilizing RTS/CTS is gradually increased (i.e. 20, 40, 60, 80 and 100%). Figure 5.23a indicates considerable gains (i.e. above 60%) achieved by only activating RTS/CTS on 60% of the stations when compared to a network that neither utilizes selective four-way handshake, nor uses DSC (i.e. legacy IEEE 802.11 network). With respect to a network only employing DSC, this increase is around 10%. In addition, the fairness improved by 3% for RTS/CTS enabled DSC network.

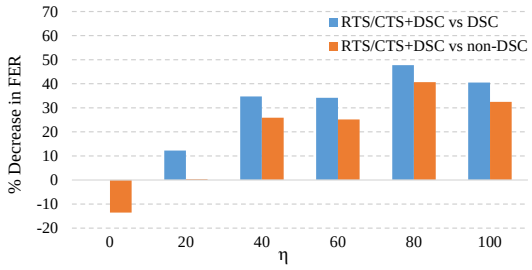
Figure 5.23b signifies the gradual improvements in FER, where around 48% decrease in FER is

witnessed when 80% of DSC enabled stations utilize RTS/CTS (when compared to DSC-only scenario). Interestingly, FER improvement was also found when RTS/CTS enabled DSC network was compared with legacy IEEE 802.11 network, an indicator to the importance of intelligently enabling RTS/CTS.

In order to distinguish among the factors that lead to throughput improvements (i.e. whether the differences were due to DSC with RTS/CTS or RTS/CTS only), we also analyzed the performance of using four-way handshake on selected nodes without using DSC. When a network in which 60% of the non-AP stations within a cell utilized RTS/CTS was compared to a network that neither used four-way handshake nor utilized DSC, only 10% throughput improvement was witnessed. Thus indicating the importance of utilizing DSC with selective RTS/CTS that complement to achieve better performance results (i.e. 60% throughput improvement).



(a) Percentage increase of throughput.



(b) Percentage of RTS/CTS enabled nodes.

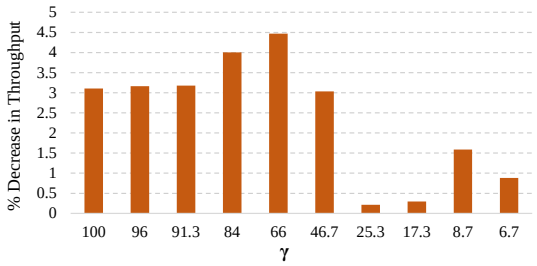
Figure 5.23: Comparison of four-way handshake enabled DSC stations utilizing method 2 with DSC only enabled stations and with a network that utilizes legacy IEEE 802.11 stations.

5.7.1.3 Evaluating method 3

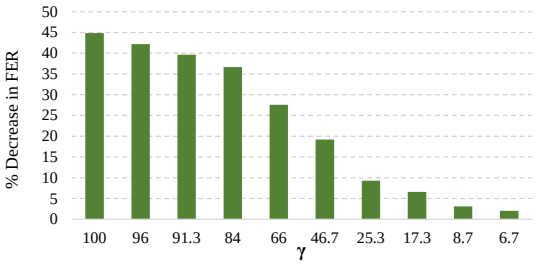
In this section, we evaluate the performance of a network that intelligently varies the percentage γ of stations utilizing RTS/CTS based on the hidden node count. The rational to conduct this study was based on our understanding that DSC increased FER in the system due to the dynamic decrease in carrier sensing range that results in the increase of hidden count number.

In order to make the results more observant and to correlate with a FER based method evaluated in Section 5.7.1.1, we choose the γ as the percentage of stations selected for RTS/CTS in Sec-

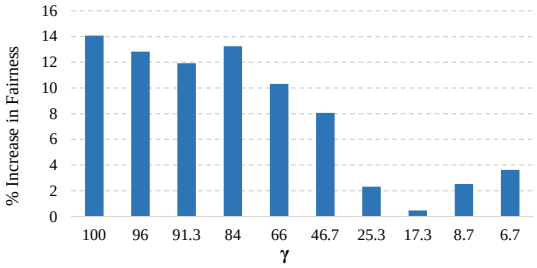
tion 5.4.1.1 (i.e. we chose the same number of stations highlighted in Figure 5.22b by varying different δ values). Intuitively, the number of hidden nodes of a particular station and its measured



(a) Percentage decrease in throughput.



(b) Percentage decrease in FER.



(c) Improvement in overall Fairness.

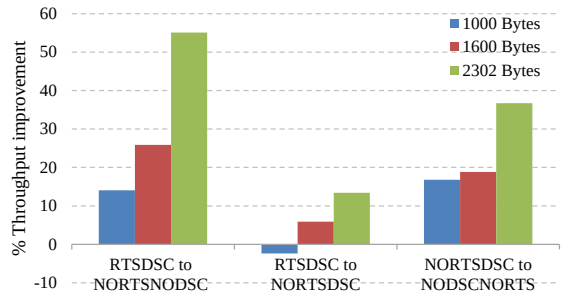
Figure 5.24: Comparison of four-way handshake enabled DSC stations utilizing method 3 with only DSC enabled stations.

FER would be correlated (more hidden nodes mean more collisions and thus a higher FER). In that case, the performance of Methods 1 and 3 should be similar; however, the results in Figure 5.24 show notable discrepancies (lower throughput and higher fairness). A large number of hidden nodes may result in a surprising low FER if those hidden nodes do not have many transmission opportunities.

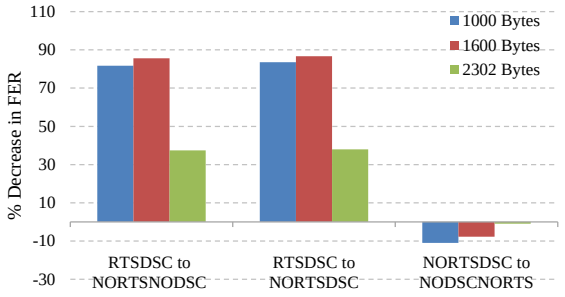
Based on the aforementioned analysis, we indicate that FER is a reliable metric for RTS/CTS selection and can increase the overall performance of a DSC enabled network. Furthermore, it is a general metric that is easy to calculate and can be measured in real environments that can include interference/noise as well as mobility.

5.7.2 Impact of frame size on RTS/CTS enabled DSC stations

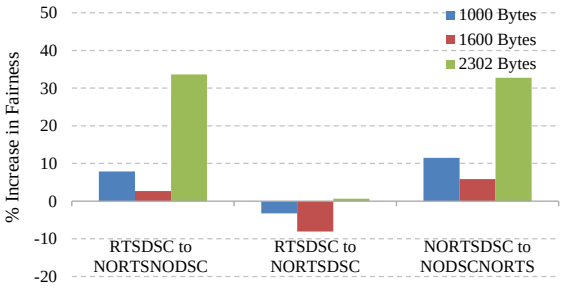
As highlighted in previous section, intelligent method to enable RTS/CTS control can have multifold benefits. In this section, we build on the proposed argument where different frame sizes are used (i.e. 1000, 1600 and 2302 Bytes) for comparative evaluation of a dense WLAN network. In Section5.7.1.1, we exposed maximum benefits when $\delta = 0.6$. We utilize the same δ and apply Method 1 so as to perform the following analysis: we compare the RTS/CTS enabled DSC nodes (RTSDSC) with a network encompassing RTS/CTS disabled DSC nodes (NORTSDSC) and a network that neither utilizes DSC nor uses four-way handshake (NORTSNODSC). Figure 5.25a indicates approximately 55%



(a) Percentage increase of throughput.



(b) Impact on FER.



(c) Improvement in Fairness.

Figure 5.25: Performance evaluation of RTS/CTS enabled DSC stations with varying frame sizes.

improvement in throughput for the largest frame size. RTS/CTS control was found to add to the benefits of DSC for all cases. According to Figure 5.25b, maximum FER improvements were achieved

for small frame size. In terms of fairness, RTSDSC provides substantial benefits when compared to NORTSNODSC network. An important outcome of the aforementioned results is that for large frame sizes, RTS/CTS can be beneficial. On the other hand, for small frames size, RTS/CTS method can be an overhead that can lead to system performance degradation, even in a dense environment, where the number of hidden nodes is large.

5.8 Conclusion

In this chapter, we design a simple but efficient self adaptation (fully distributive) mechanism that improves spatial reuse for all stations within a densely deployed WLAN network that is coherent with the development guidelines for IEEE 802.11ax standard (i.e. design of solution that is applicable to all the previous IEEE 802.11 standard without the need of modifications within legacy protocols).

Furthermore, we utilize NS-3 simulator to evaluate the benefits provided by the aforementioned scheme, as compared to legacy IEEE 802.11 and other CST adaptation mechanisms in the literature. Comparative analysis indicating the advantages of the proposed mechanism is also provided. As one of the major outcomes, we explain the co-existence challenges faced when devices/cells leveraging dynamic CST adaptation are made to operate along with legacy IEEE 802.11 devices/cells. Besides, results signify considerable improvement due to DSC in worst interference conditions (i.e. slow stations transmitting large frames).

Detailed simulation results indicate that DSC (both at the AP and stations) allowed multiple concurrent transmissions to co-exist, thus increasing the overall throughput and fairness over the cost of increased hidden nodes and FER. It is significant to mention that the DSC algorithm described in Section 5.3.5, which is used throughout this chapter, is a generic model and is valid in any scenario (i.e. all use cases of IEEE 802.11ax). However, for each environment, the algorithm would need to be fine-tuned to perform in optimal manner. Different studies have already been presented in TGax, where authors have evaluated the working of DSC under non-residential environment. However, it is expected that overall trends would be similar in different interference-limited scenarios.

In order to counter the increase in FER, we then propose the intelligent utilization of AP controlled four-way handshake uplink access to improve and enhance the performance of DSC enabled network, leveraging two of the mechanisms under the consideration of the TGax to enhance spatial reuse in future IEEE 802.11ax devices. Through extensive simulations we show how an intelligent selection of the set of stations using RTS/CTS access minimizing the negative effects of an adaptive PHYCCA mechanism such as DSC.

6

Conclusions and future work

The dramatic increase in number of smart phones, tablets, wearables, and other smart mobile devices has resulted in tremendous growth in traffic demands (both in terms of total traffic volume and data rate required by individual stations) for current and future wireless networks. In addition, with the emergence of IoT paradigm, there is a strong derive from the different sectors of the economy (encompassing education, health, manufacturing etc.) and utility companies to exploit the benefits of wireless communication. The future wireless networks are expected to manage and satisfy the requirements of billions of connected devices. The foreseen growth in traffic can only be sustained by: a) densification of wireless networks because of scarcity of new available spectrum and the near Shannon's limit capacity achieved by the current cellular wireless technologies (such as LTE Advanced) and b) by deploying HetNets (to improve system resource usage) that include network deployments of nodes which support multi-RAT joint radio operations.

Therefore, higher capacity and data rate along with improved spectral efficiency and reduced power consumption requirements for the future 5G networks are anticipated to be fulfilled by dense HetNet deployments, where IEEE 802.11 based Wi-Fi networks and LTE based cellular networks are envisioned to be the principle technologies with joint operations to provide enhanced indoor and outdoor coverage.

Despite the advantages of future dense HetNet deployments, they are expected to face several major technical challenges. The densification of wireless network can not be merely achieved by rescaling the existing protocols and networks. This is due to the fact that current wireless standards were not particularly designed to efficiently operate in high density. Moreover, due to increased number of APs and complex network architectures, the dense deployments pose serious challenges to network management that include inconsistent security, interference problems and extensive backhauling.

This Ph.D. thesis aims to explore challenges and proposes practical solutions to improve efficiency of the current IEEE 802.11, that are deemed necessary for the drastic performance improvements within dense deployments. Throughout this thesis, it is made clear to the readers that the

current MAC layer of IEEE 802.11 requires numerous modifications so as to enable Wi-Fi to become an important element of the evolution of 5G broadband networks.

In this chapter, we conclude on the main findings in this dissertation. Apart from summarizing the main contributions, limitations and directions of future work are also presented.

6.1 Contributions

IEEE 802.11 based WLAN networks have become integral part of today's indoor communication due to their ease of deployment and cost efficiency. The popularity and wider acceptance of the aforementioned standard has also resulted in their deployments in diverse environments. While, the high density deployment phenomena is due to the ease of installation and low cost, it is also a deliberate design choice to reduce the distance between APs and non-AP stations so as to enable the capabilities of serving high traffic loads. As a consequence, these massive deployments can potentially improve capacity and coverage.

In IEEE 802.11 networks, carrier sensing methods are used to manage the medium access by different nodes communicating within the network. Both AP and non-AP stations utilize the default DCF channel access method (that enforces each station to contend to gain access to the shared medium through CSMA/CA) to exchange control, management and data frames. Before initiating transmission, a procedure called PHYCCA is followed, where each node senses the medium; if the measured energy level of the detected preamble exceeds a predefined threshold, the channel is sensed busy and the node defers communication. A backoff procedure is used to reduce the collision probability between multiple stations. PHYCCA and backoff decrease the probability of transmission collisions at the cost of lower channel utilization.

Regardless of the improvements in network conditions, DCF suffers from significant performance degradation within dense deployments. The presence of numerous closely located transceivers operating over the unlicensed ISM band and the use of predefined fixed MAC layer parameters causes increase in congestion, collisions and interference problems, which lead to overall degradation of network performance. This problem is further compounded by the inherent flaws of DCF, such as the hidden and exposed node problems, which result in a decreased overall throughput. Moreover, due to over simplified MAC operation of Wi-Fi, malicious entities operating within dense deployments can greatly benefit by merely changing the default/predefined parameters to gain frequent access of the medium.

The main focus of this thesis has been to study and propose layer-2 optimization solutions of PHY and MAC layers of the IEEE 802.11 standard, that result in improved performance in dense Wi-Fi networks. We exposed different vulnerabilities of IEEE 802.11 and proposed potential countermeasures for amicable operations of Wi-Fi deployments. In other words, the approach followed in this research work was to revisit the MAC layer of IEEE 802.11, so as to improve network performance in high density deployments without completely modifying the global IEEE 802.11 architecture.

Due to CSMA/CA characteristics, the MAC of IEEE 802.11 is very sensitive to malicious entities

operating over the shared medium. Particularly, for the case of dense deployments, there is a need to find solutions that enable detection of adversaries, so as that the performance of multiple overlapping cells is not compromised. A malicious station can improve its bandwidth, throughput and QoS at the cost of other stations, by modifying legacy IEEE 802.11 MAC. Also, a jamming device can cause DoS attack by either forced channel occupancy (by continuously transmitting and forcing contending stations to backoff), or by restricting the access of other stations to the shared medium (by transmitting bulk of MAC control frames). Therefore, in Chapter 2, implementation and evaluation of a malicious detection scheme for IEEE 802.11 networks was carried out. This scheme was based on the sheer principle that transmissions of beacons have priority over any other transmission and, thus, can be used to monitor the activity within WLAN network area from its AP (i.e. not requiring any modification to legacy client stations). The effectiveness of the detection scheme was evaluated by simulations as well as by experimentation. Results indicated that the proposed scheme was able to detect a cheating device as well as a jammer within the network. Although this study was based on IEEE 802.11a/g devices, this novel scheme could equally be employed to newer IEEE 802.11 standards, such as IEEE 802.11n, IEEE 802.11ac, IEEE 802.11ah and IEEE 802.11ax, because they utilize the same CSMA/CA based MAC layer, which is the source of the weakness exploited by the jammers and cheaters.

Inspite of the fact that dense deployments are generally used to obtain better coverage and performance, extensive management and coordination schemes (which operate in de-centralized manner) are required to address the increased interference problems caused due to excessive transmissions by nearby stations over the shared channel. Moreover, the cost of backhaul to connect the massive number of small cells and reception/interference problem of unplanned and unmanaged indoor deployments with default configurations are also the key stumbling blocks for dense Wi-Fi deployments. In order to explore an alternative for densely deployed Wi-Fi networks, Chapter 3 explores a new IEE 802.11 amendment, called IEEE 802.11ah. This standard intends to modify the current IEEE 802.11 standard (at PHY and MAC layer) in order to extend the coverage by operating over S1G for ubiquitous access in less interfered frequency band and to support large number of associated stations within the network. This IEEE 802.11 amendment is one of the most promising and appealing standards, which aims to bridge the gap between traditional mobile networks and the demands of massive number of connected devices (i.e. IoT). Chapter 3 provides the key technological enhancements proposed for IEEE 802.11ah standard. It points out the necessity of long range amendment and elaborates the important use cases. Next, a thorough comparison between IEEE 802.11ah with previous IEEE 802.11 amendments is described. Lastly, some of the important challenges expected for IEEE 802.11ah are mentioned.

Poor Wi-Fi performance is often attributed to wireless interference in heavy loaded dense scenarios where the degree of contention among stations inevitably lead to high collision levels. Unlike their cellular counterparts, in IEEE 802.11 networks there is neither dedicated frequency nor time for any user. Thus, the MAC protocols of IEEE 802.11 require many modification efforts to enhance the performance in dense deployments. The need for improved operations and efficient methods to

share the limited resources has resulted in extensive research being done on spatial reuse, interference mitigation and efficient resource management in IEEE 802.11.

Apart from proposing standard that increases the coverage area of IEEE 802.11 cells along with the possibility to support thousand of associated stations, the IEEE working group is in process to contemplate standardization of radio resource management technologies to improve performance within dense deployments. A new amendment, called IEEE 802.11ax is being designed, that aims to improve over several performance metrics (such as average per station throughput, area throughput, spectral efficiency, quality of experience, etc.) that directly results in an increase of efficiency over several overlapping BSS deployments. Thus, the scope of the proposed amendment is to define standardized modifications of both the PHY and MAC layer of legacy IEEE 802.11 standard to improve the end user experience in densely deployed WLAN environments. In Chapter 4, a thorough overview of IEEE 802.11ax (a future high efficiency Wi-Fi standard being designed to increase capacity within high density and outdoor deployments) is provided. After pointing out the necessity and scope of the proposed amendment, this chapter introduces the most important technological improvements that will form the basis of aforementioned next generation of WLANs. Since, IEEE 802.11ax amendment would be a de facto WLAN standard in future, where it would be implemented over different chips and devices that constitute the basic building block of IoT, a thorough analysis of the expected opportunities and challenges for TGax within IoT paradigm are also explored.

Due to the scarcity of licensed spectrum, the future small cells HetNets based on cellular technologies perspective are expected to share the same spectrum with macro-cells, that would result in severe co-channel interference. Motivated to achieve capacity growth required due to increased wireless traffic demands in future and to reduce the impact of co-channel interference, standardization efforts are underway by 3GPP to allow the opportunity of cellular mobile networks to operate over the unlicensed 2.4 and 5 GHz spectrum currently being used by Wi-Fi, Zigbee and other communication systems. This development posses a new co-existence challenge for the IEEE 802.11, which is not designed to withstand the centralized scheduling approach of cellular networks. Therefore, Chapter 4 gives a detailed analysis of the expected co-existence challenge of IEEE 802.11ax with LTE-U, that needs to be addressed for the harmonious co-existence of the foregoing multi-RAT technologies.

One of the most important objectives of the IEEE 802.11ax amendment is to enhance spatial reuse in dense WLANs, to enable multiple concurrent non-overlapping transmission to co-exist. The current DCF-based MAC protocol of IEEE 802.11 is configured conservatively and is not efficient in spatial utilization. In high density environments, due to scarcity of available non-overlapping channels, different BSS are assigned similar channels that can lead to increased frame collisions probability. Before initiating transmission, each station senses the medium, if the energy level measured exceeds a predefined threshold, called CST, the channel is sensed busy and the node defers communication. In some cases, this CSMA/CA based conservative MAC protocol unnecessarily prevents the stations to transmit because of the inadequacy to recognize the interference levels at the receiver (even though there is a maximum possibility to correctly decode the frame at receiver) and due to

over conservative fixed CST value. This problem (referred to as exposed node problem) has been thoroughly investigated to severely affect the spatial reuse of spectral resources. On the contrary, allowing concurrent transmissions may lead to increase of interference from hidden nodes present outside the carrier sensing range of a transmitting station. Therefore, more aggressive (i.e. higher) CST results in more transmission opportunities at the cost of increased collision probability. Thus, an optimum OBSS spatial reuse algorithm is required that adapts to the variations over the shared medium and dynamically sets the spatial reuse parameters to selectively allow OBSS transmission, leading to improved network efficiency and throughput. While reducing the presence of exposed stations, this technique is also expected to curtail the increase in hidden stations, so as to restrict the rise in frame collisions. This is due to the fact that interference levels directly impact the achievable data rates, where increase in interference may result in decreased SINR which can force the transmitter to utilize lower MCS levels for transmissions.

Based on aforementioned requirements, a runtime self-adaptation (dynamic) algorithm that modifies the CST of each station is proposed in Chapter 5, called DSC. It has been acknowledged by the TGax, that dynamic sensitivity control is an important issue, that needs to be addressed, to solve the spatial reuse challenge associated with densification of WLANs. However, discussion are ongoing (with consensus yet to be reached) to explore the best way forward.

DSC dynamically adapts CST, based on local measurements (i.e received power of frames from intended transmitters) that results in improved carrier sensing method without the need of any additional frame exchange between the transmitter and the receiver. Importantly, this algorithm aims to improve spatial reuse by using methods to restrict the increase in FER. Intuitively, by avoiding exposed stations in a contained manner, the link transmission opportunity within a network increases and, in-return, it leads to improved transmission fairness and optimized concurrent transmissions. Comparative analysis indicating the advantages of the proposed mechanism is also provided. As one of the major outcomes, the co-existence challenges faced when devices/cells leveraging DSC are made to operate along with legacy IEEE 802.11 devices/cells (that use a fixed CST value) are also explained. Besides, results signify considerable improvement due to DSC in worst interference conditions. In addition, DSC scheme was observed to improve substantially the throughput of the systems that implement adaptive rate control. The proposed scheme was, however, found to increase the hidden node count that results in increase of FER of the overall network. The benefits of the proposed scheme is validated by means of mathematical as well as simulation-based analysis.

Various methods have been proposed to reduce the effect of hidden nodes in IEEE 802.11 networks. However, the legacy IEEE 802.11 has already defined a method to cater the foregoing problem. Apart from providing the default two-way basic access, the DCF function also supports an optional four-way handshake mechanism (called RTS/CTS). This scheme is primarily designed to combat hidden terminal problem, where RTS and CTS frames are exchanged between ACK and data frames transmissions. However, the RTS/CTS mechanism is not commonly used in infrastructure mode WLANs (it is mostly utilized to protect large aggregated frames) due to the bandwidth overhead associated with additional frame exchange. Particularly, this overhead is considerably multiplied when

small frame sizes are used for transmission that can cause increased collisions, and in adverse situations, might make the nodes switch unnecessarily from high data rates to low data rates (due to excessive collisions of RTS and CTS frames in dense deployments).

However, as highlighted in Chapter 5, a preventative method can be used, where RTS/CTS method is only activated when a hidden terminal is sensed in the vicinity by a node. Specifically for the case of dense deployments, RTS/CTS can greatly benefits those nodes that are deprived of channel access due to multiple hidden stations. In addition, since frame aggregation schemes are employed in new standards of IEEE 802.11 (i.e. IEEE 802.11n and IEEE 802.11ac), the bandwidth overhead associated with RTS/CTS might not be a relevant challenge.

Building on the aforementioned argument, Chapter 5 also proposes the intelligent utilization of AP-controlled four-way handshake uplink access to improve and enhance the performance of DSC enabled network, leveraging two of the mechanisms under the consideration of the TGax (i.e DSC and adaptive RTS/CTS) to enhance spatial reuse in future IEEE 802.11ax devices. The decision to enable RTS/CTS exchange could be based on hidden node as well as the FER over each station. Furthermore, a detailed performance analysis on the impact of RTS/CTS based on frame size used for transmission is evaluated. To the best of our knowledge, the evolution of the foregoing mechanism has not been presented in literature yet for densely deployed networks. Through extensive simulations, it is indicated that intelligent selection of the set of stations using RTS/CTS access can minimize the negative effects of an adaptive CST mechanism. As a result of this combination, considerable improvements were witnessed along with increased fairness and reduced FER.

6.2 Limitations and future work

To summarize, this thesis has provided platform for additional research, where key challenges have been identified that would impact the future dense Wi-Fi networks in terms of security, robustness and efficiency. Several layer-2 interaction techniques and adaptive mechanisms, are presented to increase the capacity and efficient use of shared resources within IEEE 802.11-based WLANs. Through this work, we have contributed to the evolution of IEEE 802.11 standards and have proposed procedures that would enable Wi-Fi to become an integral part of 5G paradigm. This final section of the thesis is meant to inspire readers for future research work on dense Wi-Fi networks.

The security and availability issues of Wi-Fi networks are neither easy nor straightforward. Even though WLAN network are being deployed in high density to increase capacity, they are being exposed to growing number of attacks by adversaries which aim to misuse the network. Even though the malicious entity detection algorithm presented in this thesis is a novel method that requires to only monitor beacons, intelligent devices which mimics the behavior of a normal station, can be deceptive to the mechanism. Different radio resource management parameters at the PHY layer, such as abrupt changes in SINR, PDR and RSS, and feedback information from non-AP stations could be used to improve and develop a cross-layer detection mechanism. Particularly, for the case of dense managed Wi-Fi deployments, cooperation of APs could be used, where BAT at each AP could be com-

pared to detect and position the jamming device.

While it is expected that an increase in density of APs is proportional to the enhanced capacity, uncoordinated neighboring cells can not operate with full potential due to OBSS induced interference over the limited available spectrum. In this thesis, we propose the use of IEEE 802.11ah as an alternative to dense deployment. However, due to the sparse channel availability at S1G, methods to analyze the benefits achieved in dense deployments by concurrently utilizing IEEE 802.11ah and IEEE 802.11ax, so that the interference/contention problem could be adequately administered by selecting the best available alternative is a logical extension to the proposal. This argument is particularly important for fulfilling the stringent 5G requirements such as latency, availability, scalability, cost and energy efficiency, where different wireless technologies can work in concert. With reference to Wi-Fi networks, the heterogeneous connectivity can be instrumental to enhance the transmission rates, availability and reliability to improve the overall system capacity.

The spectral efficiency improvement algorithm presented in this thesis is based on distributed adaptation and results in raised interference levels. DSC technique, verified through extensive work, increases the number of concurrent transmissions and therefore improves the area throughput. Inspite of the expectation that achievable transmission rates would be negatively affected by the higher interference levels, results indicate that DSC also provides improvements when adaptive rate control algorithm was applied in the network. The simulation-based evaluation to analyse DSC was focused on the particular case of residential buildings. Therefore, the first extension of this work could be to perform a thorough study of DSC in different environments, where DSC parameters would have to be fine-tuned to provide optimal performance based on the specific scenarios. However, the exception are that the overall trends would be similar in different interference-limited scenarios.In our analysis, we have focused on 2.4GHz band due to limitation on the available number of non-overlapping channels. However, we expect similar gains to be achieved in dense 5 GHz deployments. Since DSC increases throughput of the stations at the expense of higher FER, a comparison of DSC with aggressive contention settings can help to better understand the performance gains. This is due to the fact that when stations do not employ DSC, they spend most of the time is backoff because of excessive collisions from numerous neighbours. Moreover, Chapter 5 exposes the possible co-existence problem between legacy and DSC enabled stations, where a mechanism is required that restricts stations with aggressive CST levels to take unfair advantage of stations using fixed CST. Next, the evaluation of DSC with TPC and BSS color can help to understand the impact of interference management and further improvements in spectral reuse. Lastly, the influence of IEEE 802.11ax MAC modifications on multi-RAT network deployments and the need for cross-RAT cooperation can also be explored as a possible extension.

Another important outcome of the thesis is the intelligent utilization of AP controlled four-way handshake in dense deployments, that can be used along with DSC to further improve and enhance the performance in terms of throughput, fairness and FER and interference. This work can be extended by designing specific algorithms or heuristics to select stations that enable RTS/CTS exchange that lead to overall system performance improvements.

Bibliography

[1] 802.11 HEW SG proposed PAR. *IEEE 802.11ax, IEEE 802.11-14/0165r0*.

[2] Proposed 802.11ax functional requirement. *IEEE 802.11ax, IEEE 802.11-14/1009-02*.

[3] A survey on {IEEE} 802.11ah: An enabling networking technology for smart cities. *Computer Communications*, **58**:53 – 69, 2015.

[4] ABIRESEARCH. IEEE 802.11ah low power Wi-Fi – too late to the party?, 2015.

[5] O. ACHOLEM AND B. HARVEY. Throughput performance in multihop networks using adaptive carrier sensing threshold. In *IEEE SoutheastCon*, pages 287–291, March 2010.

[6] T. ADAME, A. BEL, B. BELLALTA, J. BARCELO, AND M. OLIVER. Ieee 802.11ah: the wifi approach for m2m communications. *Wireless Communications, IEEE*, **21**(6):144–152, December 2014.

[7] M. S. AFAQUI, E. GARCIA-VILLEGAS, AND E. LOPEZ-AGUILERA. Dynamic sensitivity control alogorithm leveraging adaptive rts/cts for ieee 802.11ax. In *IEEE WCNC*, April 2016.

[8] M. S. AFAQUI, E. GARCIA-VILLEGAS, E. LOPEZ-AGUILERA, AND D. CAMPS-MUR. Dynamic sensitivity control of access points for ieee 802.11ax. In *2016 IEEE International Conference on Communications (ICC)*, pages 1–7, May 2016.

[9] M.S. AFAQUI. Simulation based evaluation of dsc in residential environment. *IEEE 802.11ax, IEEE 802.11-15/0027*.

[10] M.S. AFAQUI, E. GARCIA-VILLEGAS, AND LOPEZ-AGUILERA. IEEE802.11ax: Challenges and requirements for future high efficiency Wi-Fi. *IEEE Wireless Communication Magazine*, 2016.

[11] M.S. AFAQUI, E. GARCIA-VILLEGAS, AND E. LOPEZ-AGUILERA. Dynamic sensitivity control for IEEE 802.11ax. *Computer Networks, submitted for possible publication*, **PP**, 2016.

[12] M.S. AFAQUI, E. GARCIA-VILLEGAS, E. LOPEZ-AGUILERA, G. SMITH, AND D. CAMPS. Evaluation of dynamic sensitivity control algorithm for IEEE802.11ax. In *IEEE WCNC*, March 2015.

[13] M.S. AFAQUI, E. GARCIA-VILLEGAS, E. LOPEZ-AGUILERA, G. SMITH, AND D. CAMPS. Evaluation of dynamic sensitivity control algorithm for IEEE802.11ax. In *IEEE WCNC*, March 2015.

[14] M.S. AFAQUI AND A. QURESHI. A review of channel dependent scheduling in wireless networks. In *Multitopic Conference (INMIC), 2012 15th International*, pages 413–416, 2012.

[15] S. AUST, R.V. PRASAD, AND I.G.M.M. NIEMEGEERS. Outdoor long-range wlans: A lesson for ieee 802.11ah. *Communications Surveys Tutorials, IEEE*, **17**(3):1761–1775, thirdquarter 2015.

[16] VICTOR BAÑOS GONZALEZ, M. SHAHWAIZ AFAQUI, ELENA LOPEZ-AGUILERA, AND EDUARD GARCIA-VILLEGAS. Ieee 802.11ah: A technology to face the iot challenge. *Sensors*, **16**(11), 2016.

[17] ALIREZA BABAEI, JENNIFER ANDREOLI-FANG, AND BELAL HAMZEH. On the impact of LTE-U on Wi-Fi performance. In *IEEE PIMRC*, pages 1–6, Sep 2014.

[18] B. BELLALTA. IEEE 802.11ax: High-efficiency wlans. *IEEE Wireless Communications*, **23**(1):38–46, February 2016.

[19] G. BIANCHI. Performance analysis of the IEEE 802.11 distributed coordination function. *Selected Areas in Communications, IEEE Journal on*, **18**(3):535–547, 2000.

[20] G. BIANCHI. Performance analysis of the ieee 802.11 distributed coordination function. *IEEE Journal on Selected Areas in Communications*, **18**(3):535–547, March 2000.

[21] J. BRODKIN. Wifi's future: faster, smarter, and fewer cables, May 2012.

[22] MARCUS BURTON. Certidied wireless network professional: 8011 arbitration, Septmeber 2009.

[23] G. CAIRE AND S. SHAMAI. On the achievable throughput of a multiantenna gaussian broadcast channel. *Information Theory, IEEE Transactions on*, **49**(7):1691–1706, 2003.

[24] V. CHANDRASEKHAR, J. G. ANDREWS, AND A. GATHERER. Femtocell networks: a survey. *IEEE Communications Magazine*, **46**(9):59–67, September 2008.

[25] CISCO. Cisco visual networking index: Global mobile data traffic forcast update, 2014-2019, May 2015.

[26] CISCO. Cisco visual networking index: Global mobile data traffic forcast update, 2016-2021, Feb 2017.

[27] BELL LABS CONSULTING. Ericsson mobility report, 2016.

[28] WAYAN DAMAYANTI, SANGHYUN KIM, AND JI-HOON YUN. Collision chain mitigation and hidden device-aware grouping in large-scale {IEEE} 802.11ah networks. *Computer Networks*, **108**:296 – 306, 2016.

[29] ROLF DE VEGT. Potential compromise for 802.11ah use case document. *IEEE 802.11-11/0457r0*, March 2011.

[30] LARA DEEK, EDUARD GARCIA-VILLEGAS, ELIZABETH BELDING, SUNG-JU LEE, AND KEVIN ALMEROTH. A practical framework for 802.11 {MIMO} rate adaptation. *Computer Networks*, **83**:332 – 348, 2015.

[31] D. J. DENG, K. C. CHEN, AND R. S. CHENG. Ieee 802.11ax: Next generation wireless local area networks. In *Heterogeneous Networking for Quality, Reliability, Security and Robustness (QShine), 2014 10th International Conference on*, pages 77–82, Aug 2014.

[32] I. DOLIŃSKA, A. MASIUKIEWICZ, G. RZĄDKOWSKI, AND M. JAKUBOWSKI. Algorithms for channels assignment in 802.11 networks. In *2016 International Conference on Information and Digital Technologies (IDT)*, pages 83–89, July 2016.

[33] O. EKICI AND A. YONGACOGLU. Ieee 802.11a throughput performance with hidden nodes. *IEEE Communications Letters*, **12**(6):465–467, June 2008.

[34] ERICSSON. Ericsson mobility report, June 2015.

[35] A. FRAGKIADAKIS, I. ASKOXYLAKIS, AND P. CHATZIADAM. Denial-of-service attacks in wireless networks using off-the-shelf hardware. In NORBERT STREITZ AND PANOS MARKOPOULOS, editors, *Distributed, Ambient, and Pervasive Interactions*, **8530** of *Lecture Notes in Computer Science*, pages 427–438. Springer International Publishing, 2014.

[36] A. G FRAGKIADAKIS, V. A. SIRIS, N. E. PETROULAKIS, AND A. P. TRAGANITIS. Anomaly-based intrusion detection of jamming attacks, local versus collaborative detection. *Wireless Communications and Mobile Computing (2013)*, 2013.

[37] E. GARCIA-VILLEGAS, M. GOMEZ, E. LOPEZ-AGUILERA, AND J. CASADEMONT. Detecting and mitigating the impact of wideband jammers in IEEE 802.11 WLANs. In *Proc. of IWCMC*, pages 57–61, 2010.

[38] EDUARD GARCIA-VILLEGAS, MUHAMMAD SHAHWAIZ AFAQUI, AND ELENA LOPEZ-AGUILERA. A novel cheater and jammer detection scheme for {IEEE} 802.11-based wireless {LANs}. *Computer Networks*, **86**:40 – 56, 2015.

[39] GSMA. Mobile industry observatory, 2016.

[40] Z. HADZI-VELKOV AND B. SPASENOVSKI. Capture effect in IEEE 802.11 basic service area under influence of rayleigh fading and near/far effect. In *Personal, Indoor and Mobile Radio Communications, 2002. The 13th IEEE International Symposium on*, **1**, pages 172–176 vol.1, Sept 2002.

[41] E. HAGHANI, M.N. KRISHNAN, AND A. ZAKHOR. Adaptive carrier-sensing for throughput improvement in IEEE 802.11 networks. In *IEEE GLOBECOM*, Dec 2010.

[42] J. HERZEN, R. MERZ, AND P. THIRAN. Distributed spectrum assignment for home WLANs. In *2013 Proceedings IEEE INFOCOM*, pages 1573–1581, April 2013.

[43] IEEE STANDARDS ASSOCIATION. IEEE standard part 11: Wireless LAN MAC and PHY specifications. *ANSI/IEEE Std. 802.11-2012*, 2012.

[44] IEEE STANDARDS ASSOCIATION. Draft part 11: wireless lan medium access control (mac) and physical layer (phy) specifications – amendment draft. *IEEE P802.11ah/D 5.0*, March 2015.

[45] IEEE STANDARDS ASSOCIATION. 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. *ANSI/IEEE Std. 802.11-2016*, 2016.

[46] I JAMIL. Mac simulation results for dynamic sensitivity control (dsc - cca adaptation) and transmit power control (tpc). *IEEE 802.11ax, IEEE 802.11-14/0523*.

[47] I JAMIL, L. CARIOU, AND J.-F. HELARD. Improving the capacity of future IEEE 802.11 high efficiency wlans. In *ICT*, pages 303–307, May 2014.

[48] I JAMIL, L. CARIOU, AND J.-F. HELARD. Efficient mac protocols optimization for future high density WLANs. In *IEEE WCNC*, March 2015.

[49] LAURA HUEI JIUN JU AND IZHAK RUBIN. The effect of disengaging rts/cts dialogue in ieee 802.11 mac protocol. In WEIHUA ZHUANG, CHI-HSIANG YEH, OLAF DROEGEHORN, C.-T. TOH, AND HAMID R. ARABNIA, editors, *International Conference on Wireless Networks*, pages 632–638. CSREA Press, 2003.

[50] V. JONES AND H. SAMPATH. Emerging technologies for wlan. *Communications Magazine, IEEE*, **53**(3):141–149, March 2015.

[51] HUEI-JIUN JU, I. RUBIN, AND YEN-CHANG KUAN. An adaptive rts/cts control mechanism for ieee 802.11 mac protocol. In *VTC 2003-Spring*, **2**, pages 1469–1473 vol.2, April 2003.

[52] KWANGSUNG JU AND KWANGSUE CHUNG. Jamming Attack Detection and Rate Adaptation Scheme for IEEE 802.11 Multi-hop Tactical Networks. *International Journal of Security and Its Applications*, pages 149–154, 2012.

[53] P. KULKARNI AND F. CAO. Taming the densification challenge in next generation wireless lans: An investigation into the use of dynamic sensitivity control. In *Wireless and Mobile Computing, Networking and Communications (WiMob), 2015 IEEE 11th International Conference on*, pages 860–867, Oct 2015.

[54] M. LAURIDSEN, B. VEJLGAARD, I. Z. KOVACS, H. NGUYEN, AND P. MOGENSEN. Interference measurements in the european 868 mhz ism band with focus on lora and sigfox. In *2017 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1–6, March 2017.

[55] A. LAYA, C. KALALAS, F. VAZQUEZ-GALLEGO, L. ALONSO, AND J. ALONSO-ZARATE. Goodbye, aloha! *IEEE Access*, **4**:2029–2044, 2016.

[56] JEONGKEUN LEE, WONHO KIM, SUNG-JU LEE, DAEHYUNG JO, JIHO RYU, TAEKYOUNG KWON, AND YANGHEE CHOI. An experimental study on the capture effect in 802.11a networks. In *ACM WiNTECH*, 2007.

[57] D.J. LEITH, P. CLIFFORD, V. BADARLA, AND D. MALONE. WLAN channel selection without communication. *Computer Networks*, **56**(4):1424 – 1441, 2012.

[58] R. LIAO, B. BELLALTA, M. OLIVER, AND Z. NIU. A survey: MU-MIMO MAC protocols for wireless local area networks. *IEEE Communications Surveys Tutorials*, **PP**(99):1–1, 2014.

[59] D. LIM. Envisioning 11ax phy structure - part ii. *IEEE 802.11ax, IEEE 802.11-14/0801r0*.

[60] JUN LIU, WEI GUO, BAI LONG XIAO, AND FEI HUANG. Rts threshold adjustement algorithm for ieee 802.11 dcf. In *ITS*, pages 654–658, June 2006.

[61] R.P. LIU, G.J. SUTTON, AND I.B. COLLINGS. Wlan power save with offset listen interval for machine-to-machine communications. *IEEE Transactions on Wireless Communications*, **13**(5):2552–2562, 2014.

[62] ZHENHUA LIU, HONGBO LIU, WENYUAN XU, AND YINGYING CHEN. Exploiting Jamming-Caused Neighbor Changes for Jammer Localization. *IEEE Transactions on Parallel and Distributed Systems*, **23**(3):547 –555, 2012.

[63] E. LOPEZ-AGUILERA, J. CASADEMONT, AND J. COTRINA. Propagation delay influence in IEEE 802.11 outdoor networks. *Wireless Networks*, **16**(4):1123–1142, 2010.

[64] E. LOPEZ-AGUILERA, J. CASADEMONT, AND E. GARCIA-VILLEGAS. A study on the influence of transmission errors on WLAN IEEE 802.11 MAC performance. *Wireless Communications and Mobile Computing*, **11**(10):1376–1391, 2011.

[65] HUI MA, R. VIJAYAKUMAR, S. ROY, AND JING ZHU. Optimizing 802.11 wireless mesh networks based on physical carrier sensing. *Networking, IEEE/ACM Transactions on*, **17**(5):1550–1563, 2009.

[66] R. MADAN, A SAMPATH, AND N. KHUDE. Enhancing 802.11 carrier sense for high throughput and qos in dense user settings. In *IEEE PIMRC*, pages 253–259, Sept 2012.

[67] TARAS MAKSYMYUK, MARYAN KYRYK, AND MINHO JO. Comprehensive spectrum management for heterogeneous networks in LTE-U. *accepted for publication in IEEE Wireless Communication*, 2016.

[68] MARKETSANDMARKETS.COM. Global Wi-Fi Market by Business (Model Indoor Wi-Fi, Outdoor Wi-Fi, Transportation Wi-Fi), Product (Access Points, WLAN Controllers, Wireless Hotspot Gateways, Others), Service, Vertical, Region- Global Forecast to 2020, July 2015.

[69] B. MAWLAWI, J.-B. DORE, N. LEBEDEV, AND J.-M. GORCE. Csma/ca with rts-cts overhead reduction for m2m communication. In *IEEE WCNCW*, pages 119–124, 2015.

[70] S. MERLIN AND S. ABRAHAM. Methods for improving medium reuse in IEEE 802.11 networks. In *IEEE CCNC*, pages 1–5, Jan 2009.

[71] M. MJIDI, D. CHAKRABORTY, N. NAKAMURA, K. KOIDE, A. TAKEDA, AND N. SHIRATORI. A new dynamic scheme for efficient rts threshold handling in wireless networks. In *AINA 2008.*, pages 734–740, March 2008.

[72] KODAI MURAKAMI, TATSUYA ITO, AND SUSUMU ISHIHARA. Improving the spatial reuse of IEEE 802.11 WLAN by adaptive carrier sense threshold of access points based on node positions. In *ICMU*, pages 132–137, Jan 2015.

[73] VICTOR BA NOS GONZALEZ, M. SHAHWAIZ AFAQUI, ELENA LOPEZ-AGUILERA, AND EDUARD GARCIA-VILLEGAS. Throughput and range characterization of ieee 802.11ah. *submitted to IEEE Latin America Transactions*.

[74] GUEVARA NOUBIR, RAJMOHAN RAJARAMAN, BO SHENG, AND BISHAL THAPA. On the robustness of ieee 802.11 rate adaptation algorithms against smart jamming. In *Proceedings of the Fourth ACM Conference on Wireless Network Security*, WiSec '11, pages 97–108, New York, NY, USA, 2011. ACM.

[75] O.BAY. Wi-Fi chipset shipments will near 18 billion chipsets during the next five years, May 2014.

[76] K. OTERI. Frequency selective scheduling (fss) for tgax ofdma. *IEEE 802.11ax, IEEE 802.11-15/568r2*.

[77] C. W. PARK, D. HWANG, AND T. J. LEE. Enhancement of ieee 802.11ah mac for m2m communications. *IEEE Communications Letters*, **18**(7):1151–1154, July 2014.

[78] K. J. PARK, L. KIM, AND J. C. HOU. Adaptive physical carrier sense in topology-controlled wireless networks. *IEEE Transactions on Mobile Computing*, **9**(1):87–97, Jan 2010.

[79] KYUNG-JOON PARK, J.C. HOU, T. BASAR, AND HWANGNAM KIM. Noncooperative carrier sense game in wireless networks. *Wireless Communications, IEEE Transactions on*, **8**(10):5280–5289, 2009.

[80] K. PELECHRINIS, M. ILIOFOTOU, AND S.V. KRISHNAMURTHY. Denial of Service Attacks in Wireless Networks: The Case of Jammers. *IEEE Communications Surveys Tutorials*, **13**(2):245–257, 2011.

[81] K. PELECHRINIS, I. KOUTSOPOULOS, I. BROUSTIS, AND S.V. KRISHNAMURTHY. Lightweight Jammer Localization in Wireless Networks: System Design and Implementation. In *Proc. of IEEE GLOBECOM*, 2009.

[82] K. PELECHRINIS, GUANHUA YAN, S. EIDENBENZ, AND S.V. KRISHNAMURTHY. Detecting Selfish Exploitation of Carrier Sensing in 802.11 Networks. In *Proc. of IEEE INFOCOM*, pages 657–665, 2009.

[83] KONSTANTINOS PELECHRINIS, IOANNIS BROUSTIS, SRIKANTH V. KRISHNAMURTHY, AND CHRISTOS GKANTSIDIS. A measurement driven, 802.11 anti-jamming system. *CoRR*, **abs/0906.3038**, 2009.

[84] ELDAD PERAHIA AND ROBERT STACEY. *Next Generation Wireless LANs: 802.11N and 802.11AC*. Cambridge University Press, New York, NY, USA, 2nd edition, 2013.

[85] QIAO QU, BO LI, MAO YANG, AND ZHONGJIANG YAN. An OFDMA based concurrent multiuser MAC for upcoming IEEE 802.11ax. In *IEEE WCNCW*, pages 136–141, 2015.

[86] O. RAEESI, J. PIRSKANEN, A. HAZMI, J. TALVITIE, AND M. VALKAMA. Performance enhancement and evaluation of ieee 802.11ah multi-access point network using restricted access window mechanism. In *Distributed Computing in Sensor Systems (DCOSS), 2014 IEEE International Conference on*, pages 287–293, May 2014.

[87] MAXIM RAYA, JEAN-PIERRE HUBAUX, AND IMAD AAD. Domino: A system to detect greedy behavior in ieee 802.11 hotspots. In *Proceedings of the 2Nd International Conference on Mobile Systems, Applications, and Services*, MobiSys '04, pages 84–97, New York, NY, USA, 2004. ACM.

[88] MERLIN S. IEEE 802.11 tgax simulation scenarios. *IEEE 802.11ax, IEEE 802.11-14/0980r6*, 2014.

[89] J. O. SEO, C. NAM, S. G. YOON, AND S. BAHK. Group-based contention in ieee 802.11ah networks. In *2014 International Conference on Information and Communication Technology Convergence (ICTC)*, pages 709–710, Oct 2014.

[90] T. SHIGEYASU, M. AKIMOTO, AND H. MATSUNO. Throughput improvement of ieee802.11dcf with adaptive rts/cts control on the basis of existence of hidden terminals. In *CISIS*, pages 46–52, June 2011.

[91] S. SIGURD. Uplink rts/cts control. *IEEE 802.11ax, IEEE 802.11-15/0059r1*.

[92] GRAHAM SMITH. Dense apartment complex capacity improvements with channel selection and dynamic sensitivity control. *IEEE 802.11ax, IEEE 802.11-13/1487r2*.

[93] R. STACEY. Specification framework for TGax. *IEEE 802.11ax, IEEE 802.11-15/132r5*.

[94] JIN TANG, YU CHENG, AND WEIHUA ZHUANG. Real-time misbehavior detection in ieee 802.11-based wireless networks: An analytical approach. *Mobile Computing, IEEE Transactions on*, **13**(1):146–158, Jan 2014.

[95] QUALCOMM TECHNOLOGIES. LTE in unlicensed spectrum: Harmonious coexistence with Wi-Fi.

[96] C. THORPE, S. MURPHY, AND L. MURPHY. Ieee802.11k enabled adaptive carrier sense management mechanism (kapcs2). In *Integrated Network Management (IM), 2011 IFIP/IEEE International Symposium on*, pages 509–515, May 2011.

[97] CHRISTINA THORPE AND LIAM MURPHY. A survey of adaptive carrier sensing mechanisms for ieee 802.11 wireless networks. *Communications Surveys Tutorials, IEEE*, **16**(3):1266–1293, Mar 2014.

[98] LE TIAN, SÉBASTIEN DERONNE, STEVEN LATRÉ, AND JEROEN FAMAEY. Implementation and validation of an ieee 802.11ah module for ns-3. In *Proceedings of the Workshop on Ns-3*, WNS3 '16, pages 49–56. ACM, 2016.

[99] I. TINNIRELLO, SUNGHYUN CHOI, AND YOUNGSOO KIM. Revisit of rts/cts exchange in high-speed ieee 802.11 networks. In *WoWMoM*, pages 240–248, 2005.

[100] M. QUTAB UD DIN, A. HAZMI, L. F. DEL CARPIO, A. GOEKCEOGLU, B. BADIHI, P. AMIN, A. LARMO, AND M. VALKAMA. Duty cycle challenges of ieee 802.11ah networks in m2m and iot applications. In *European Wireless 2016; 22th European Wireless Conference*, pages 1–7, May 2016.

[101] PETER M. VAN DE VEN, AUGUSTUS J.E.M. JANSSEN, AND JOHAN S.H. VAN LEEUWAARDEN. Optimal tradeoff between exposed and hidden nodes in large wireless networks. *SIGMETRICS Perform. Eval. Rev.*, **38**(1):179–190, June 2010.

[102] A. VASAN, R. RAMJEE, AND T. WOO. Echos - enhanced capacity 802.11 hotspots. In *IEEE INFOCOM*, **3**, pages 1562–1572, March 2005.

[103] T. WU. Ofdma performance analysis. *IEEE 802.11ax, IEEE 802.11-14/1227r3*.

[104] D. XIA, J. HART, AND Q. FU. On the performance of rate control algorithm minstrel. In *2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC)*, Sept 2012.

[105] WENYUAN XU, WADE TRAPPE, YANYONG ZHANG, AND TIMOTHY WOOD. The feasibility of launching and detecting jamming attacks in wireless networks. In *Proc. of ACM MOBIHOC*, pages 46–57, 2005.

[106] SUNG-GUK YOON, JEONG-O SEO, AND SAEWOONG BAHK. Regrouping algorithm to alleviate the hidden node problem in 802.11ah networks. *Computer Networks*, **105**:22 – 32, 2016.

[107] CHONGQING ZHANG. Investigating the optimum carrier sensing range using transmission relation graph in wireless ad hoc networks. In *Journal of Networks*.

[108] YONGNING ZHANG, C. ASSI, B. ALAWIEH, AND H. ALAZEMI. A spatiotemporal contention resolution for enhancing spatial reuse in wireless networks. *Vehicular Technology, IEEE Transactions on*, **60**(2):680–691, Feb 2011.

[109] 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. *IEEE Transactions on Wireless Communications*, **13**(11):6180–6192, Nov 2014.

[110] ZHI ZHOU, YANFENG ZHU, ZHISHENG NIU, AND JING ZHU. Joint tuning of physical carrier sensing, power and rate in high-density WLAN. In *APCC*, pages 131–134, Oct 2007.

[111] JING ZHU, XINGANG GUO, L. LILY YANG, W. STEVEN CONNER, SUMIT ROY, AND MOUSUMI M. HAZRA. Adapting physical carrier sensing to maximize spatial reuse in 802.11 mesh networks: Research articles. *Wirel. Commun. Mob. Comput.*, **4**(8):933–946.

[112] JING ZHU, B. METZLER, XINGANG GUO, AND Y. LIU. Adaptive csma for scalable network capacity in high-density wlan: A hardware prototyping approach. In *INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings*, pages 1–10, April 2006.

[113] XIAOCHENG ZOU AND JING DENG. Detection of fabricated CTS packet attacks in wireless LANs. *Springer Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, **74**:105–115, 2010.