

**PERFORMANCE EVALUATIONS ON THE SPATIAL REUSE TECHNIQUES
OF THE NEXT GENERATION WLANS**



M.Sc. THESIS

Ömer Faruk TOPAL

Department of Electronics and Communications Engineering

Telecommunications Engineering Programme

MAY 2019

**PERFORMANCE EVALUATIONS ON THE SPATIAL REUSE TECHNIQUES
OF THE NEXT GENERATION WLANS**



M.Sc. THESIS

Ömer Faruk TOPAL
(504161325)

Department of Electronics and Communications Engineering

Telecommunications Engineering Programme

Thesis Advisor: Prof. Dr. Güneş Zeynep KARABULUT KURT

MAY 2019

**YENİ NESİL KABLOSUZ YEREL AĞLARINDA
SPEKTRAL TEKRAR KULLANIM TEKNİKLERİNİN DEĞERLENDİRMESİ**

YÜKSEK LİSANS TEZİ

**Ömer Faruk TOPAL
(504161325)**

Elektronik ve Haberleşme Mühendisliği Anabilim Dalı

Telekomünikasyon Mühendisliği Programı

Tez Danışmanı: Prof. Dr. Güneş Zeynep KARABULUT KURT

MAYIS 2019

Ömer Faruk TOPAL, a M.Sc. student of ITU Graduate School of Science Engineering and Technology 504161325 successfully defended the thesis entitled “PERFORMANCE EVALUATIONS ON THE SPATIAL REUSE TECHNIQUES OF THE NEXT GENERATION WLANS”, which he/she prepared after fulfilling the requirements specified in the associated legislations, before the jury whose signatures are below.

Thesis Advisor : **Prof. Dr. Güneş Zeynep KARABULUT KURT**
Istanbul Technical University

Jury Members : **Prof. Dr. Mustafa ERGEN**
Istanbul Technical University

Dr. Mehmet Şükrü KURAN
AirTies Wireless Networks

Date of Submission : **3 May 2019**

Date of Defense : **22 May 2019**





To my family,



FOREWORD

This thesis is indented to provide a comprehensive analysis and enhanced mechanisms on about spatial re-usability issues of WLAN networks by considering the practicality concerns.

This thesis is granted by the ITU-AYP-03 project of ITU BAP department. In addition, the thesis is supported and facilitated by the AirTies Wireless Networks Company. Throughout the study, I have made benefit from the extensive knowledge of the company and its resources. For this reason, I would like to give special thanks to my colleagues for their supports and their valuable orientations.

I would like to present my deep thanks to my supervisor Prof Gunes Karabulut Kurt who had always motivated and helped me on being determined along the studies. Also, I would like to thank to my family, my dear, and my close friends for their immeasurable supports.

May 2019

Ömer Faruk TOPAL

TABLE OF CONTENTS

	<u>Page</u>
FOREWORD.....	ix
TABLE OF CONTENTS.....	xi
ABBREVIATIONS	xiii
SYMBOLS.....	xv
LIST OF TABLES	xvii
LIST OF FIGURES	xix
SUMMARY	xxi
ÖZET	xxiii
1. INTRODUCTION	1
2. INTRODUCTION TO THE NEXT GENERATION WLANS	7
2.1 Common Issues of the Current Wi-Fi Standards.....	7
2.1.1 Channel sharing.....	7
2.1.2 Collision and delay issues for the dense networks	8
2.1.3 Spatial reuse limitations	9
2.2 Transition from OFDM to OFDMA.....	9
2.3 Spatial Reuse Enhancements.....	10
2.3.1 BSS color mechanism.....	11
2.3.2 OBSS_PD based SR technique	12
2.3.3 SRP based SR technique	15
2.3.4 Two separate network allocation vector (NAV) mechanism	15
2.4 Evaluation of OBSS_PD Based SR.....	16
2.4.1 Implementation details of the OBSS_PD based SR in simulation environment.....	16
2.4.2 Experimental evaluation of OBSS_PD SR technique	16
3. ADAPTATION OF CARRIER SENSING THRESHOLD TO INCREASE THROUGHPUT IN DENSE 802.11AC WIRELESS NETWORKS.....	21
3.1 Channel Model and Performance Metrics.....	23
3.1.1 Communication model	23
3.1.2 Airtime calculations.....	24
3.1.3 Fairness calculations.....	25
3.2 Adaptive carrier sense threshold algorithm	25
3.3 Performance Evaluation and Simulation Results of the Adaptive Carrier Sensing Algorithm.....	28
3.3.1 Point to point performance of a 802.11ac network	29
3.3.2 Analysis of CST change effect on a simple grid dense network setup...	31
3.3.3 Adaptive algorithm performance evaluations.....	34

4. A COUNTER-MEASURE APPROACH AGAINST CARRIER SENSING ATTACKS IN WLANS	37
4.1 Introduction	37
4.2 Background and Related Work.....	40
4.2.1 Relevant 802.11 functions	40
4.2.2 Related work.....	41
4.3 Analysis of Collision Probability	44
4.4 Impact of CCA Tuning on WLANS.....	47
4.5 Modelling a CCA Attacker Network and Its Effect on WLANs.....	49
4.6 The Proposed Countermeasure Algorithm	51
4.6.1 Selection of counter-measure technique.....	52
4.6.2 Counter-measure with coordinated channel switching.....	54
4.6.3 Counter-measure with coordinated BSS color change	57
4.7 Evaluation of the Proposed Counter-Measure Mechanisms.....	59
4.7.1 Implementation of the used functionalities	60
4.7.2 Performance evaluations.....	60
5. CONCLUSIONS AND FUTURE WORK.....	65
REFERENCES.....	67
APPENDICES.....	71
APPENDIX A.1	73
1.1 Collision Probability Simulation Codes	73
CURRICULUM VITAE.....	81

ABBREVIATIONS

STA	: Station
AP	: Acces Point
WLAN	: Wireless Local Area Networks
Wi-Fi	: The general name of IEEE 802.11 standards
DCF	: Distributed Coordination Function
CSMA	: Carrier Sense Multiple Access
CSMA-CA	: Carrrier Sense Multiple Access-Collision Avoidance
CCA	: Clear Channel Assessment
CST	: Carrier Sense Threshold
OFDM	: Orthogonal Frequency Division Multiplexing
OFDMA	: Orthogonal Frequency Division Multiplexing Access
OBSS_PD	: OBSS Power Detection
PHY	: Physical
MAC	: Media Access Control
BSS	: Basit Service Set
OBSS	: Other Basit Service Set
SR	: Spatial Reuse
SRP	: Spatial Reuse Parameter
OBSS_PD	: OBSS Power Detection
ns-3	: Network Simulator 3
BCC	: BSS Color Change
DSC	: Dynamic Sensitivity Control
PLC	: Physical Layer Capture
RTS	: Request to Send
CTS	: Clear to Send
RSSI	: Received Signal Strength Indicator
SINR	: Signal to Noise Ratio
UDP	: User Datagram Protocol
Mbps	: Mega Bit per Second
CSC	: Channel Switch Count
CSA	: Channel Switch Announcement
PLCP	: Physical Layer Convergence Procedure
PPDU	: PLCP Protocol Data Unit
CBR	: Constant Bit Rate
NAV	: Network Allocation Vector
MCS	: Modulation and Coding Scheme
SDWN	: Software Defined Wireless Networks



SYMBOLS

$\text{OBSS_PD}_{\min}$	: Minimum value of OBSS power detection threshold.
$\text{OBSS_PD}_{\max}$	: Minimum value of OBSS power detection threshold.
$\text{OBSS_PD}_{\text{level}}$	: Current value of OBSS power detection threshold.
TXPWR	: Current value of transmission power.
$\text{TXPWR}_{\text{Ref}}$	: Reference value of transmission power.
$\text{TXPWR}_{\max}$	: Maximum allowed transmission power.
τ_i	: Throughput of flow i .
τ_{sys}^*	: The initial cumulative throughput of the system.
τ_{sys}	: The cumulative throughput of the system.
T_{cst}^*	: The initial carrier sense threshold of the system.
T_{cst}	: The current carrier sense threshold.
ϵ_{cst}	: The step-size for carrier sensing threshold.
δ_n	: The change in the throughput after applying new CST.
$\delta_{\text{threshold}}$	: The threshold for throughput change.
$\Gamma_{i,j,\min}$	: The minimum received signal power of associated STAs.
ϕ_n	: Log-throughput factor for n^{th} iteration.
ϕ_n^*	: Initial value of log-throughput factor.
ϕ_{pt}	: Penalty threshold for log-throughput factor.
p	: Probability of collision.
W_0	: Minimum contention window size.
τ	: Transmission probability in a given slot.
m	: Backoff maximum stage.
N	: Number of station.
c	: Number of contending stations.
h	: Number of hidden stations.
k	: Average slot decrement of hidden stations.
n	: Total number of contending and hidden stations.
σ	: Idle slot duration.
T_{succ}	: Time spent by successful transmissions.
T_{col}	: Time spent by collisions.
$P_{\text{RX}}(d)$	: The received power strength of the legitimate node at distance d .
P_{N}	: The received power strengths of noise.
I_i	: The received power strengths from interferer.
S_{0m}	: The default SINR threshold for the MCS index m .
c_i	: BSS color i .
$S_{j,ci}$	: The cluster of STAs that belong to same BSS.
$\mathcal{R}_A$	: The received power strengths of the attacker at the target AP.
$\mathcal{R}_{S_{j,ci}}$	: The received power strengths of the STAs at the AP.

AP_{ci}	: The AP that has BSS color i
STA_{ci}	: The STAs that have BSS color i
η	: The tolerable RSSI threshold for the spatial reuse operations
CSC_1	: Channel switch countdown value
CSC_2	: Color switch countdown value
t_1	: The value of channel listening duration
t_1	: The interval of channel listening



LIST OF TABLES

	<u>Page</u>
Table 2.1 : The coordinate table of the nodes for the given deployment.	17
Table 2.2 : Simulation parameters for OBSS_PD based SR experiments.	18
Table 3.1 : A summary of notation.	27
Table 3.2 : Simulation parameters for the carrier sensing adaptation experiments	30
Table 3.3 : Achievable throughput values versus received signal strength (RSS).	31
Table 4.1 : Simulation parameters for the countermeasure performance experiments.	63



LIST OF FIGURES

	<u>Page</u>
Figure 2.1 : A basic network deployment scheme, in which the STA2 is moving away.	8
Figure 2.2 : Throughput change vs distance of STA2 for the down-link UDP traffic with saturated offered loads.....	8
Figure 2.3 : Exposed node scheme.....	9
Figure 2.4 : The RU division scheme for 20 MHz channels.....	11
Figure 2.5 : OBSS_PD levels and Classic CCA levels comparison	12
Figure 2.6 : The figure of relationship between OBSS_PD level and TxPower limitations	13
Figure 2.7 : Changes in CSR ranges and Simultaneous transmissions with the OBSS_PD and BSS coloring	14
Figure 2.8 : Frame Capture Model with the OBSS_PD SR mechanism.....	15
Figure 2.9 : The simplified Box5 scenario deployment scheme	17
Figure 2.10 : Throughput of each flow for the CSMA-CA and OBSS_PD SR mechanisms.....	19
Figure 2.11 : Aggregated throughput of each BSS for the CSMA-CA and OBSS_PD SR mechanisms.....	19
Figure 2.12 : Average delay of each traffic flow for the CSMA-CA and OBSS_PD SR mechanisms.....	20
Figure 2.13 : Aggregated average delay of each BSS for the CSMA-CA and OBSS_PD SR mechanisms.....	20
Figure 3.1 : RTS-CTS handshake mechanism	22
Figure 3.2 : A simple AP-STA pair network with inter distance d.	30
Figure 3.3 : The number of Transmission attempts and total airtime utilization rate of the channel vs CST change for network density 9	30
Figure 3.4 : System Throughput and Log-Throughput Factor vs CST change.....	31
Figure 3.5 : The 3×3 simple grid dense network deployment where access points (APs) and stations (STAs) are 5m apart.	32
Figure 3.6 : Overall network throughput vs CST for different network densities (4-9-16-25).....	32
Figure 3.7 : 4 AP-STA pair grid network deployment.....	33
Figure 3.8 : 9 AP-STA pair grid network deployment.....	33
Figure 3.9 : 16 AP-STA pair grid network deployment.....	34
Figure 3.10 : 25 AP-STA pair grid network deployment.....	34
Figure 3.11 : The throughput improvement by the proposed algorithm for different network densities.....	35
Figure 4.1 : The format of a channel switch announcement element.	40
Figure 4.2 : The format of a BSS color change announcement element	41

Figure 4.3 :	The deployment scheme of the standard compliant networks and a misbehaving network for the analysis of collision probabilities.....	45
Figure 4.4 :	Collision probability results for the mathematical model, simulation default and under jamming attack cases versus high number of active STAs.....	46
Figure 4.5 :	Collision probability results for the mathematical model, simulation default and under attack versus low number of active STAs.....	47
Figure 4.6 :	The scheme of backoff process and collisions in the presence of a carrier sense attacker.	47
Figure 4.7 :	The deployments of two high interfere networks	48
Figure 4.8 :	Throughput vs adjacent network RSSI for two interfere networks when UDP uplink traffic is used.	49
Figure 4.9 :	The CSA element view in beacons, where CSA mode is disabled by default	61
Figure 4.10 :	The CSA element view in beacons, where CSC equals to 3	61
Figure 4.11 :	The CSA element view in beacons, where CSC equals to zero, which imply that immediate chanel switch operation.....	61
Figure 4.12 :	The view of BSS Color Change elements in beacons	62
Figure 4.13 :	Enterprise networks deployment with the presence of an attacker ...	62
Figure 4.14 :	Aggregate throughput change when the BSS color change and CSA methods are applied.....	64
Figure 4.15 :	Aggregate throughput results when the proposed countermeasure mechanisms are applied ($\mathcal{R}_A = -77dBm$).	64

PERFORMANCE EVALUATIONS ON THE SPATIAL REUSE TECHNIQUES OF THE NEXT GENERATION WLANS

SUMMARY

The explosive growth in the number of Wi-Fi devices in recent years makes many of the network deployments insufficient due to the architectures of the current Wi-Fi standards. When the WiFi was introduced in 1999, the initial aim was to serve multiple numbers of stations (STA) that can reach minimal data rates. But today, the existing structures of previous WiFi standards becomes insufficient for the demands of STAs in dense networks. Considering these, in 2017, the IEEE Tgax community which is comprise of many academic and industrial staffs, have started developing the next generation wireless networks or IEEE 802.11ax. Furthermore, it is currently in the draft phase, and planned to be finalized by 2020.

Considering the channel unavailability of dense networks, the users suffer from having very low data rates due to the spectrum sharing by the distributed coordinated function (DCF) mechanism of Wi-Fi. According to the DCF mechanism, a STA must go into the backoff process while accessing a channel, which can causes long waits and packet collisions, especially when the number of contending devices are high. Furthermore, according to the carrier sense multiple access collision avoidance (CSMA-CA) protocol, a channel must be sensed idle before initiating a transmission. This sensing process is held by the carrier sensing threshold (CST), which determines the availability of the channel in a given slot. Although this protective behavior of the CSMA-CA provides a collision-free domain, it generally limits the spectral reuses in dense networks.

The two key features of the new standard are the transition from orthogonal frequency division multiplexing (OFDM) to orthogonal frequency division multiple access (OFDMA) structures and the usage of new spatial reuse techniques. The usage of OFDMA is intended to resolve the issues with regard the spectrum sharing and contention. On the other hand, the new spatial reuse techniques, in particular, OBSS_PD based spatial reuse (SR) technique is aimed to improve the spectral capacity utilization in densely deployed networks. The primary aim of this new amendment is to improve the user experiences in dense network deployments in which the STAs can have different needs according to their traffic types.

While the WiFi architecture is improved by the new amendment, the security issues at low layers remain open. Due to the distributed nature of WiFi, the networks can not even detect the existence of a misbehaving node while exposing to an attack. Although it has a severe impact on the performance, the security at the PHY layer has not been sufficiently studied in the research community. In addition to this, a greedy node can easily be created by manipulating the clear channel assessment (CCA) threshold of a normal device which eventually will take over the entire spectrum, and thus will mostly suspend the legitimate network.

Despite the severity of the issue, there are a few relevant studies that are solely focusing on the detecting of the misbehaving nodes. Note here that, the proposed detection mechanisms satisfy the accuracy and practicality concerns. On the contrary, there exist barely any comprehensive study on defending the WiFi networks against the PHY layer attacks which offer neither lightweight nor accurate schemes.

Based on the above-mentioned issues, in this thesis study, we first evaluate the proposed SR techniques of the new amendment in the simulation environment. The benefits of using OBSS_PD SR technique is clearly demonstrated in terms of throughput and packets delay. The performance evaluations conclude that the new SR technique yields a significant gain in throughput and reduces average delays of transmission for the congested networks.

Secondly, we investigate the impact of carrier sensing mechanism and re-design the mechanism for the legacy networks that are aimed to improve the spatial reuse in dense networks. Moreover, in the design of new carrier sensing algorithm, various criteria that are vital for any wireless local area networks (WLANs) are taken into account. These criteria are ensuring of the connectivity and fairness levels of systems. The results of our experiments demonstrate that the new proposed carrier sensing scheme makes significant gains while ensuring the connectivity and fairness among the networks.

Lastly, the studies on the physical (PHY) layer security of WiFi are carried out. In this context, first, the disruptive effect of a malicious node is investigated in denser networks. Besides this, the collision probability performance of legitimate networks in case of attacking is investigated. And, as the main part of the chapter, we propose a novel two-step counter-measuring strategy, which is intended to work after an accurate detection of the greedy networks is accomplished. Ensuring coordination and applicability were the main concerns of the designing process. For this reason, the functions that already defined in the standards are used to accomplish the channel hopping and basic service set (BSS) color changing operations. The performance evaluations show that the proposed strategy is effective in restoring the networks. Moreover, a significant advantage of using the new SR mechanism against an attacker is observed.

All the performance evaluations are carried out in the network simulator 3 (ns-3) platform, which currently does not support the new developing Wi-Fi standard. Therefore, we have developed a code for the new spatial reuse mechanism in the ns-3 simulator.

YENİ NESİL KABLOSUZ YEREL AĞLARINDA SPEKTRAL TEKRAR KULLANIM TEKNİKLERİNİN DEĞERLENDİRMESİ

ÖZET

Son yıllarda kablosuz yerel ağ (WLAN) cihazlarının sayısı ve kullanımı oldukça yüksek değerlere ulaşmaktadır. Bununla beraber, geliştirilen protokol ve sistemler kullanıcıların artan talepleri karşısında zaman zaman yetersiz kalabilmektedirler. Kablosuz yerel ağların tarihsel gelişim sürecine baktığımızda 1999 yılından başlayarak sırasıyla 802.11b, 802.11g, 802.11a, 802.11n ve 802.11ac standartlarının geliştirildiği görülmektedir. En son geliştirilen 802.11ac standardının temeli ise 2013 yılında atılmış ve 2016 yılında yazımı tam anlamıyla tamamlanmıştır.

Bilindiği üzere, 2.4 GHz ve 5 GHz frekans bantlarında oldukça az sayıda birbiriyle girişim yapmayan kanal mevcuttur. Bu kısıtlama da özellikle çok sayıda aktif trafiğin bulunduğu ortamlarda kullanıcıların genellikle oldukça düşük veri hızlarına sahip olmalarına neden olmaktadır.

WiFi mimarisinin kanal erişim mekanizmasının incelenmesi, yukarıda bahsedilen veri hızı düşüş problemini daha anlaşılabilir hale getirecektir. WiFi için geliştirilen standartlarda kanal erişimi için sadece bir mekanizma kullanmıştır; taşıyıcı algılayıcı çoklu erişim (CSMA). Bu mekanizmanın çalışma prensibi incelendiğinde, 2 adet taşıyıcı sinyal algılama tekniği olduğu görülür. Bunlardan ilki sanal taşıyıcı algılama olarak (virtual carrier sensing) isimlendirilen ve alıcı-verici yapısının iletimden önce basit bir karşılıklı RTS-CTS paket iletimi gerçekleştirerek, ortamdaki diğer cihazların başlayacak olan iletimden haberdar olmasını sağlayan mekanizmadır. Diğer mekanizma ise fiziksel taşıyıcı algılama olarak isimlendirilen ve alıcıların ortamda belirli bir seviyenin üzerinde herhangi bir iletimin devam etmekte olup olmadığını anlık olarak kontrol ettiği bir mekanizmadır. Eğer, ortamdaki sinyal seviyesi standard tarafından tanımlanan minimum taşıyıcı algılama eşik (CST) değerinin üzerindeyse, ortam meşgul olarak algılanır ve cihazların kendi iletim paketleri ertelenir. Aksi durumda ise iletimler doğrudan başlatılır. Bu taşıyıcı algılama eşığının değeri şimdiye kadar ortaya konan standartlarda sabit olarak tanımlanmış ve genellikle -82 dBm olarak verilmektedir.

Bahsedilen taşıyıcı algılayıcı mekanizma, her ne kadar paket çarpışmalarını ve paket hata oranlarını düşürmeye yönelik olsa da, oldukça koruyucu yapısı, bir yandan da spektrumun kısıtlı olarak kullanılmasına yol açmaktadır. CSMA protokolunun içerisinde bulunan dağıtık koordinasyonlu fonksiyon (DCF) mekanizmasının yapısı gereği, her bir kullanıcı (STA) paketlerini hedef cihaza bulunduğu kanalı kullanarak gönderirken, bir yandan da kanalın o sırada müsait olduğuna emin olmak durumundadır. Bu noktada da DCF mekanizması, kullanıcılar arasında kanalın adil bir şekilde erişilmesine olanak vermektedir. Fakat, bu mekanizmalar bütünü ayrıca, kanalda eş zamanlı olarak bulunan ve birbirlerinin iletimlerini etkilemeyecek

kadar uzakta olan kullanıcı cihazlarının kanalı eş zamanlı olarak kullanmasına çoğunlukla mücadele etmemektedir, dolayısıyla kanalların hava ortamındaki zaman ekseninde ortamdaki aktif kullanıcılar arasında paylaşılmaktadır. Hava ortamındaki bu paylaşım aslında kanalın veri hızı kapasitesinin paylaşılmasıyla sonuçlanmaktadır. Bu paylaşımların başlıca sebebi ise sabit ve oldukça düşük değere sahip bir CST değerinin standarda uygun tüm cihazlar tarafından kullanılmasıdır.

Şimdiye kadarki öne sürülen standartların gelişim sürecinde, veri hızları ve benzeri metrikler daha çok çeşitli çoklu anten mimarileri, modülasyon teknikleri ve trafik önceliklendirme yapıları kullanılarak iyileştirilmeye çalışıldı. Önceki yıllardaki az sayıda kullanıcı ve trafik sayısı gerçeği dikkate alındığında, öncelikli amacın koruyucu spektrum algılayıcı yapısını muhafaza ederek, birtakım yeni geliştirmeler yapılması oldukça mantıklı gözükmemektedir. Bunun yanında, yukarıda bahsedilen taşıyıcı algılayıcı mekanizmasının yan etkileri az sayıda cihazın kullanımından dolayı ihmal edilebilir seviyelerdeydi. Fakat günümüzde, oldukça yüksek sayıya ulaşan aktif kullanıcı ve trafik sayısı ile beraber, bu koruyucu mekanizmanın yan etkileri oldukça ciddi boyutlara ulaşmaktadır. Özellikle veri hızı ve ortalama paket gecikme performansları açısından ele alındığında uyarlanabilir ve daha esnek bir taşıyıcı algılayıcı mekanizmanın geliştirilmesi yoğun ağlardaki kullanıcıların performanslarının iyileştirilmelerine olanak sağlayabilir.

Esnek ve uyarlanabilir bir algılayıcının tasarımı ve uygulanması sırasında birçok kriter dikkate alınmalıdır. Bunlardan bazılarını inceleyecek olursak,

1) Kullanıcılar arasında adillik (fairness): WiFi gibi dağıtık sistemlerde, kullanıcıların kanallara eşit bir şekilde erişebilmesi gerekir. Yeni bir mekanizma tasarlanırken, önceki standartların sistemlerde sağladığı gibi, kullanıcılar arasında kanal erişim eşitliği sistem genelinde sağlanmalıdır. Bu metrik düşünülmezse geliştirilen sistemlerde, her ne kadar sistem genelinde toplam veri hızı artmış olsa dahi, aynı kapasiteye ve veri hızına sahip olabilecek kullanıcıların, bazılarının çok yüksek, bazılarının ise oldukça düşük kanala erişim imkanına sahip olması, tasarımın başarımlı performansını oldukça indirger.

2) Paket hata oranları ve bağlantırlık (connectivity): Bir diğer önemli kriterde, son kullanıcıların bağlantılarını ve paket hata oranlarını muhafaza edebilmektir. Eşik değerlerinde veya benzeri parametrelerde uyarlanabilir yapılar geliştirilirken, kullanıcıların bağlantılarını sürdürebilmeleri göz önünde bulundurulmalıdır. Aksi takdirde, bazı kullanıcıların yüksek eşik değerleri kullanılması sonucu kopmaları, sistemin başarımlı başka metriklere bakılmaksızın kabul edilemez hale getirecektir. Yine aynı şekilde, paket hata oranlarını belirli bir seviyenin altında tutmak, özellikle Voice ve benzeri, özellikle yüksek gecikme ve paket hata oranlarına toleransı olmayan trafik çeşitlerinin de sorunsuz bir şekilde çalışmalarına olanak sağlayacaktır.

IEEE topluluğu, 2017 yılından itibaren özellikle yoğun ağlardaki kullanıcıların trafik gereksinimleri ve kısıtlamalarını dikkate alarak yeni nesil WLAN olarak nitelendirilen 802.11ax isimli standardı tanıtmış ve halen daha geliştirme sürecini devam ettirmektedir. Bu yeni standard aslında yukarıda anlatılan problemler ve benzeri konular ışığında çözüm olabilecek yapı değişiklikleri ve iyileştirme mekanizmalarını içermektedir.

Yeni geliştirilmekte olan standartta iyileştirme mekanizmalarının daha çok fiziksel katmanı (PHY) ve ortam erişim katmanını (MAC) kapsayacak şekilde yapıldığı

görülmektedir. Özellikle PHY katmanında en köklü değişimlerden ikisi, OFDM yapısının OFDMA yapısına dönüştürülmesi ve spektral tekrar kullanım (SR) tekniklerindeki iyileştirmeler olarak örnek verilebilir. Bu mekanizmalardan özellikle spektral geri kullanım yukarıda bahsedilen klasik WiFi yapısının yoğun ağlarda maruz kaldığı kısıtlama ve problemlere çözüm getirme amacıyla geliştirilmiştir.

Yeni standart 2 yeni SR mekanizmasını kullanıcılara sunuyor. Bunlar temel olarak "OBSS_PD based SR" and "SRG based SR". Bunlardan ilki ve en önemlisi olarak verilen "OBSS_PD based SR", yapısı itibarıyla klasik CSMA-CA protokolunun sağladığı CST tabanlı taşıyıcı algılama sisteminin bir eklentisi gibi gözükmemekte ve oldukça etkili olabilmektedir. Bu mekanizmanın klasik temel algılayıcıdan temel farkı, ortamdaki farklı BSS lere ait iletimleri sınıflandırıp, taşıyıcı algılama kararını buna göre vermesidir. Bunun yanında, yeni standard alınan paketlerin sınıflandırılmasına olanak sağlayan, yeni BSS renkleri konseptini tanıtmaktadır. Buna göre, her BSS kümesi farklı renklere sahip olacak ve bu değerleri iletim esnasında paketlerin başlangıç kısımlarına ekleyecektir. Bu sayede her bir cihaz yeni bir paket alım esnasında paketin kaynağının hangi BSS kümesine ait olduğunu kolaylıkla anlayabilecektir. Bu yeni geliştirilen renklendirme mekanizması doğrudan OBSS_PD SR tekniği içerisinde kullanılmaktadır.

OBSS_PD tekniğini detaylı olarak incelediğimizde, bilinen statik CST parametresine ek olarak yeni bir eşik değeri parametresi (OBSS_PD threshold) tanımlandığını görmekteyiz. Bu yeni parametrenin değeri cihazların iletim gücü ve referans değerlere bağlı olarak hesaplanan alt ve üst eşik değerleri arasında olmak koşuluyla son kullanıcıya bırakılmıştır. OBSS_PD tekniğine göre, eğer gelen sinyalin rengi kendi BSS rengiyle aynıysa, içinde bulunduğu BSS, klasik CST parametresini taşıyıcı algılama kararı esnasında kullanacaktır. Eğer ki gelen sinyalin başlangıcında okunan değer farklı renk ise, OBSS, sistem taşıyıcı algılama yaparken yeni tanımlanan OBSS_PD threshold parametresini kullanacaktır. Böylelikle, klasik CST değeri düşük olduğundan kendi BSS iletimlerine karşın korumacı bir davranış içinde hareket ederken, nispeten daha yüksek değerlere ulaşabilen yeni OBSS_PD eşik değeriyle, farklı BSS lerden gelen sinyalleri daha esnek olarak ihmal edebilecek ve eş zamanlı iletimlere imkan sağlayacaktır.

Bu tez çalışmasının ilk bölümünde, yeni geliştirilen 11ax standardının OBSS_PD SR tekniği baz alınarak, önceki standartlarla arasındaki performans farklarını ve etkilerini çeşitli açılardan analiz edilmeye çalışıldı. İkinci kısımda ise, uyarlanabilir bir CST değerinin önceki standartlar için oldukça etkili olabileceği gerçeğinden yola çıkarak, yeni bir uyarlanabilir CST algoritması yukarıda verilen gereksinimler dikkate alınarak tasarlandı. Tasarım sırasında da CST değerinin değişiminin yoğun ağlardaki performans etkileri pozitif ve negatif yönleriyle birçok başarımlı metriği açısından değerlendirildi. Elde edilen gözlem ve sonuçlar algoritmanın şekillendirilmesi sürecinde kullanıldı.

Tez çalışmaları sırasında öne sürülen yapı ve algoritmaların tamamı simülasyon ortamında uygulanarak değerlendirildi. Simülasyon platformu olarak, "network simulator 3" (ns3) programı kullanıldı. Bu program WiFi ile ilgili araştırma çalışmaları için oldukça popüler olarak kullanılmasının yanı sıra, açık kaynak kodlu ve ayrık olay simule edebilen mimariye sahiptir. Özellikle WiFi ile ilgili olarak, ns-3 içerisinde önceki standartlara oldukça benzer yapıda protokol ve yapılar bulunmaktadır. Buna karşın, simulator programının halen daha yeni 11ax standardının

temel özelliklerini içermediği, dolayısıyla 11ax standardı üzerinde yapılacak değerlendirmeleri desteklenemeyeceği anlaşıyordu. Bu nedenle, değerlendirmeler için ilk adım olarak, BSS renk ve SR teknikleri, önceki standartların modüler yapısına ek olarak yazılıp entegre edildi. Bu çalışma bundan sonraki simülasyon çalışmalarımız için bir zemin hazırlayacak mahiyette oldu.

Bu tez çalışmasının üçüncü bölümünde ise, yine WLAN sistemlerinde bir başka problem olan, PHY katmanındaki taşıyıcı algılama saldırılarının ağ performansı üzerindeki etkisi ve çözüm teknikleri üzerinde çalışmalar yapıldı. Bilindiği gibi, WiFi teknolojisinin sahip olduğu dağıtık yapı, esasen sistemi farklı saldırı çeşitlerine karşı oldukça savunmasız hale getirmektedir. Bu saldırıların birçoğu MAC katmanında da olmasına karşın, PHY katmanında da yeni saldırı türleri ortaya çıkmaktadır. Bu en alt fiziksel katmandaki yeni ve etkili saldırılardan bir tanesi, yüksek taşıyıcı algılayıcı eşik değeri kullanılarak, sistemin adil erişim yapısını manipüle edilmesidir. Aslında bu ve benzeri ataklar, davranış ve etkileri açısından klasik jammer ataklarına benzetilebilir. Böyle bir durumda, sinyal boğucu düğümler, ortamdaki iletimleri ihmal ederek, hedef kanalda sürekli olarak kendi paketlerinin iletimlerini gerçekleştireceklerdir. Bu da standartlara uygun olarak çalışan normal cihazların kendi iletimlerini erteleme ve hatta susmalarına neden olur. Dolayısıyla, özellikle fiziksel katmandaki bozucu saldırıların sistemde oldukça yüksek paket gecikme sürelerine ve veri hızlarında önemli miktarda düşüşe yol açacağı öngörülmektedir. Buna ek olarak, özellikle yeni çıkacak 802.11ax standardının çok yoğun ortamlar için tasarlandığı göz önüne alındığında, bu tarz saldırıların, sistemlerde çok ciddi performans kayıplarına neden olabileceği açıkça anlaşılmaktadır.

WiFi sistemlerinde oldukça yıkıcı etkilere ulaşabilen taşıyıcı algılama saldırılarına karşın, maalesef halen daha, pratik ve kolayca uygulanabilir çözümler geliştirilememiştir. Saldırıların tespiti ile ilgili birkaç çalışma mevcut olsa dahi, elde edilen sonuçlar sonucunda, sistemleri maruz kaldığı saldırılardan kurtaracak veya performansını iyileştirecek karşı tedbirler yetersiz kalmaktadır. Genelde klasik sinyal bozucu saldırılar karşısında kanal değiştirme hareketleri geliştirilmiş olsa dahi, geliştirilen mekanizmaların birçoğu günümüz gereksinimlerini dikkate almaksızın ortaya çıkarılmış ve birçoğunun da uygulanabilirlik açısından oldukça zayıf olduğu görülmektedir. Bu tez çalışması kapsamında, biz bu konudaki mevcut ihtiyaçtan yola çıkarak, WLAN ağlarındaki bu tarz saldırılar karşısında yeni savunma tekniklerinin tasarlanması üzerinde çalışmalarımızı yürüttük. Çalışmalarımız sonucunda, içerisinde iki fonksiyonel mekanizma barındıran bir karşı tedbir (countermeasure) stratejisi belirledik. Bu tekniklerin tasarım sürecinde göz önünde bulundurulmuş başlıca kriterler aşağıdaki gibi listelenebilir,

- 1) Yeni veya ek herhangi bir cihazlar arası protokol tanımlamaktan uzak durarak tasarımlar yapmak; Gerçekte kullanılan son kullanıcı cihazları oldukça kapalı mimariye sahip olduklarını düşünüldüğünde, kolay uygulanabilirlik için mümkün olduğunca daha önceden tanımlanmış fonksiyon ve methodların kullanılması.
- 2) Sistemin maruz kaldığı yıkıcı etkidен hızlı bir şekilde minimum zaiyet vererek kurtarılabilmesi için geliştirilecek tasarımla birlikte sistem genelinde tüm cihazlarda koordinasyonlu bir şekilde operasyon yapılmasının sağlanması.

Öne sürülen savunma mekanizmalarından ilki, saldırı karşısında klasik çözüm olarak mevcut operasyon kanalını değiştirmek, ikincisi de kanal değişimine alternatif olarak uygun koşullarda, hedef BSS kümesinin BSS rengini değiştirerek, yeni

standartın SR tekniğinin avantajlarından faydalanmasını sağlamak ve bu sayede sistemi savunabilmek olarak belirlendi. Bu noktada özellikle belirtmek gerekirse, BSS Renk değiştirme tekniği, oldukça yeni olması sebebiyle, bundan önceki hiçbir akademik çalışma kapsamında kullanılmadığı gözlemlenmektedir.

Yoğun ortamlardaki kanalların kullanım oranları, özellikle 2.4GHz bandı için, oldukça fazla olmaktadır. Dolayısıyla, olası bir bozucu saldırı karşısında, kanal değişimi tekniğini kullanmak sistem performansını kısmi iyileştirebilmesine rağmen, geçilecek kanaldaki cihazların elde ettiği veri hızlarını kanal paylaşımından ötürü oldukça düşürecektir. Bu mekanizmaya alternatif olarak, uygun koşullarda yeni standartın getirdiği SR tekniklerini kullanmak oldukça faydalı olacaktır.

Yukarıda bahsedilen tasarım kriterlerini sağlayabilmek adına yeni ve önceki standartta verilen opsiyone mekanizmalar kullanılmıştır. Bunlar "Channel Switch Announcement" (CSA) elemanı ve "BSS Color Change" elemanlarıdır. Bu mekanizmaların kullanımı sistemi hem pratiklik hemde cihazları arası koordinasyon sağlama açısından oldukça avantajlı getirmiştir.

Mekanizmaların tasarım sürecinde birkaç temel varsayım yapıldı. Birincisi ve en önemlisi, yüksek eşik değerine sahip sinyal bozucu cihazların, sistemde uzun sürelerce statik olarak kaldığı, uyarlanabilir bir mekanizmaya sahip olmadığı ve bir BSS kümesi içindeki 11ax kapasiteli cihazları hedef aldığı varsayıldı. İkincisi, sistemin olası bir saldırıya maruz kalması durumunda, saldıran cihazların tespitini kısa sürede ve doğru bir şekilde yapabiliyor olduğu varsayıldı.

Bu çalışma kapsamında öne sürülen tüm tekniklerin değerlendirmeleri ns-3 simülasyon ortamında yapıldı. Değerlendirmelerin öncesinde, simulator platformu kullanılması planlanan standartlarda tanımlı opsiyonel mekanizmaların eklenmesi, yine standartlara ve platformun mimarisine uygun olarak AP tarafından üretilen "beacon" paketlerinin içine eklenip, testleri yapıldı. Daha sonra öne sürülen algoritmanın entegrasyonu yapılarak, performansları değerlendirildi.

Değerlendirmeler sonucunda, sistemdeki olası bir saldırı durumunda, öne sürülen savunma strateji ve tekniklerinin, sistemin performansını elde edilen veri hızı açısından oldukça iyileştirdiği olduğu gözlemlendi. Ayrıca, kanal değiştirme tekniğinin, yukarıda anlatıldığı gibi, bss renk değiştirme tekniğine göre sahip olduğu dezavantajlar açık bir şekilde görülmektedir.

Gelecekte, öne sürülen savunma tekniklerinin etkili olabileceği uygun çalışma aralıkları ve mekanizmalar arası geçiş kararları kapsamlı analizler yapılarak geliştirilmesi planlanmaktadır. Bunun yanında, sistemin performans analizlerini veri hızının yanı sıra, paket gecikme ve hata oranı açılarından değerlendirip, tasarımda iyileştirilmeler öngörülmektedir. Bir sonraki aşamada ise, yeni standarda uygun çiplerin erişilebilir olması halinde, tasarlanan ve öne sürülen mekanizmaların, çiplerde uygulanması ve gerçek test ortamında test edilmeleri planlanmaktadır.



1. INTRODUCTION

Recent years have witnessed tremendous demands of users for the high speed and low delayed connections in ultra-dense networks. With the current IEEE 802.11 standards, the initial design considerations were solely focused on providing high throughput for the low number of stations (STA) regardless of environmental conditions. Following the years, as the number of active Wi-Fi capable devices across the world have reached billions, many deployments can likely be classified as a dense environment. Considering these dense deployments and predicted needs of them, the IEEE 802.11 standard committee has been started updating and evolving the standards along the years. The historical evolution of Wi-Fi standards can be listed as in order, 802.11b, 802.11g, 802.11a, 802.11n, 802.11ac. Since 2017, the 802.11 group have decided on to produce a new standard called next generation wireless local area networks (WLANs): 802.11ax.

Unlike the previous standards, which mostly consist of many extensions to the existed architects, there are significantly big differences with the new 802.11ax standard. The new standard is trying to re-design mostly the structures of physical (PHY) and media access control(MAC) layers that encounter the challenge of compatibility with the previous standards. There are two main enhancement introduced by the new amendment. The first is the transition from the orthogonal frequency division multiplexing (OFDM) architecture to orthogonal frequency multiple access (OFDMA) architect that promises to address the problems due to by channel access contentions. Thus it will also improve the user experiences considering the dense deployments. The second revolutionary feature is on improving spatial reuse techniques that promise to advance the channel capacities by simultaneous transmissions. Furthermore, this new technique will eventually turn into a solution to the problems that come up by the congestion of channels in dense networks. In this thesis, we will give some introductory information on the vital features of the new amendment, and particularly investigate the improvements by the usage of new spatial reuse (SR) techniques.

The spatial reuse improvements comprise of two techniques that work independently. These are OBSS_PD based SR and spatial reuse parameter (SRP) based SR. The "OBSS_PD SR" technique is based on identifying the basic service set (BSS) of the incoming packets, and using a secondary carrier sensing threshold for the packets that are from other BSS. By this way, while networks are allowed to transmit concurrently with adjacent BSS, it is also aimed to secure transmission of internal BSS transmissions. A detailed explanation of this SR technique will be given in Chapter 2.

In the literature, there are a few works on the evaluation of this new SR techniques. In [1], the authors propose a new algorithm in contribution to the 11 ax BSS coloring mechanism. Their motivation is different from the early introduced dynamic sensitivity control (DSC) mechanism by TGax group. The authors instead consider the interference levels and received signal strength indicator (RSSI) levels of recipients while calculating a new OBSS_PD threshold. In the evaluation of their proposed mechanism, they use Box-5 simulation scenario which is one of the reference deployment scenarios provided by TGax group, [2]. Moreover, the evaluation results show that their new scheme provides % 57 throughput gain while preserving fairness among users.

Priori of this study, the same authors had also studied on exploiting the capture effect in the 11ax standards, [3]. They evaluate the dynamic sensitivity control (DSC) and BSS color mechanisms when physical layer capture (PLC) is modeled. As a result of using PLC, the receiver can successfully switch from one packet to another when a collision occurs if the received power of the last arrived packet is greater than that of the previous. It is shown that PLC can improve the fairness and throughput for the cell edge users in some scenarios due to the fact that these users can expose more interference than the others. They also compare performances of the BSS color, DSC, PLC and combined versions. Their results demonstrate that by the combined version of DSC and PLC the network performances can be further improved rather than using only DSC mechanism.

Afaqui *et al.*, [4], had evaluated the DSC algorithm which is provided by the initial version of the new amendment. They demonstrate that the proposed DSC scheme can provide 20 % improvement over the legacy networks in very dense deployments. Furthermore, they also investigate the performance of combined DSC

with Channel Selection and Rate Control algorithms. Their results present that the initial DSC scheme could potentially improve network performances especially for dense scenarios.

Apart from these, there is another issue that is still open despite the latest amendment of Wi-Fi, which is PHY layer security. It is well-known phenomena that the traditional carrier sense multiple access with collision avoidance (CSMA-CA) mechanism of Wi-Fi has many spectral vulnerabilities on channel access. Due to the distributed nature of Wi-Fi systems, an attack can easily be produced by manipulating the carrier sensing mechanism which can eventually have effect as a jammer in WLAN networks. Furthermore, it is expected to have a severe effect on dense networks.

There are some preliminary studies that solely proposes some detection mechanism for the exposed networks [5], [6]. Although its dramatic disruptive effect, there is barely any comprehensive study on such counter-measures against these type of attacks. Given these facts, it is concluded that a comprehensive study on the evasion techniques against Wi-Fi attacks is required. Therefore, in this thesis study, we aim to touch upon the following issues,

- 1) Investigating the improvement levels of the new SR techniques.
- 2) Investigating the effects of traditional CSMA-CA carrier sensing technique and developing a new carrier sensing algorithm by accounting different needs.
- 3) Investigating the effects of misbehaving attacks destined at PHY layer and developing a counter-measuring strategy by the combined use of newly introduced features of the new amendment.

In this thesis study, the network simulator 3 (ns-3), which is a discrete event based network simulator is used for the performance evaluations. All the network layers are already updated and developed for years by its maintainers. And, it provides considerably similar performances with the real network deployments. Furthermore, due to the open-source nature of the platform, throughout the study, the related parts had been extent so as to evaluate the proposed schemes on the base of simulator framework.

The main contributions of this thesis study can be summarized as follows:

1. The challenges of traditional WLANs in dense deployments are discussed in different aspects. The core features introduced by the new amendment is explained in detail. The evaluation of the proposed SR techniques is carried out by the network simulator 3 (ns-3). To support the OBSS_PD based SR, an additional module is implemented in the ns-3.
2. The drawback of the traditional carrier sensing mechanism in dense deployments is investigated by the series of experiments in the ns-3 platform. Their results are analyzed in terms of different metrics such as airtime usages, fairness, average delay. Following the study, to improve the spatial reuses an adaptive carrier sensing scheme for legacy networks is proposed by preserving fairness levels and connectivity of STAs in any networks.
3. The disruptive effects of misbehaving nodes in dense WLAN deployments is investigated in various deployments. To support developing the countermeasure techniques, an extensive collision probability analysis is provided which mainly refer to Bianchi's model and additionally cover the case that an attacker is activated. Utilizing the newly introduced features of the new amendment, a lightweight and practical counter-measuring strategy for the 11ax networks is proposed. This strategy includes the classical channel hopping and BSS color change mechanism. In particular, the key approach is to make benefit of BSS color changing, which is not studied by any of the previous studies.
4. By considering the coordination and applicability concerns, we utilized the already existed functions of the standards, namely channel switch announcement (CSA) element and BSS Color Change element. In order to evaluate the proposed schemes, these functions and the proposed techniques are implemented to the ns-3. The advantage of utilizing the new SR techniques instead of channel hopping for the dense deployments while struggling against an attacker is clearly proved out.

In addition, this thesis study is supported by ITU-AYP 2017-3 project that is granted by the ITU BAP office.

In Chapter 2, we will provide the common issues of dense WLAN deployments and will give a detailed explanation of the new features with respect to IEEE 11ax draft V3. In addition to these, a simple comparative evaluation and discussion on the

OBSS_PD based SR technique is given. Chapter 3 includes the studies on the tuning carrier sensing mechanism considering dense legacy networks. A new carrier sensing scheme is proposed with respect to the requirements of networks. The evaluation result of this is also demonstrated in that chapter. The studies on the PHY layer security is given in Chapter 4. This chapter includes the models and the impacts of the carrier sensing attackers, and collision probability evaluations which extended for the attack circumstances. Besides these, the key study of this chapter is on designing a lightweight and efficient counter-measuring strategy and its performance evaluations. In the last chapter, an overall conclusion of the studies and future works are given.





2. INTRODUCTION TO THE NEXT GENERATION WLANS

2.1 Common Issues of the Current Wi-Fi Standards

Due to the nature of CSMA-CA of the IEEE 802.11 standards, the STAs in any multi-user environments will likely suffer from channel sharing, collisions and restriction on the spatial reuses that result in having low throughput and high delays in dense networks. These issues are briefly addressed in the next subsections.

2.1.1 Channel sharing

Sharing the same RF channel in a traditional Wi-Fi network, expose significant degradation to the networks' performances in some circumstances. Let's consider a single BSS network, where two STA is associated with the same interface of the same access point (AP), and the second STA is moving away from the AP as depicted in Figure 2.1. One of the STA is in close proximity to the AP and can use higher PHY rates, R_1 , while the second is deployed far from the AP and can only achieve lower PHY rates, R_2 (e.g., 5 mega bit per second(Mbps)). Considering a saturated traffic, the common achievable data rate for each STA_i , R_i , can be computed approximately as [7],

$$R_i = \left(\frac{1}{R_1} + \frac{1}{R_2} + \dots + \frac{1}{R_n} \right)^{-1} \quad (2.1)$$

In the given example scenario, let's assume that the R_1 and R_2 equal to 72 and 5 Mbps, respectively. According to Figure 2.1, the approximate data rate will be 4.76 mbps for each users. We have simulated the setup given in Figure 2.1, in which UDP up-link traffic is used with saturated offered load. Furthermore, the STAs are identical and have 1×1 antennas. The details of the configuration parameters for this simulation study is given in the Table 2.2.

Figure 2.2 demonstrates the throughput results versus distance of moving STA for this example scenario. It is obvious that the existence of a far STA with low transmission

speed causes a significant drop in the achievable data rates of STAs. Thus, it can be concluded that in Wi-Fi networks, the STAs with low connection rates generally degrade the performances of other STAs in the spectrum regardless of their high transmission capabilities.

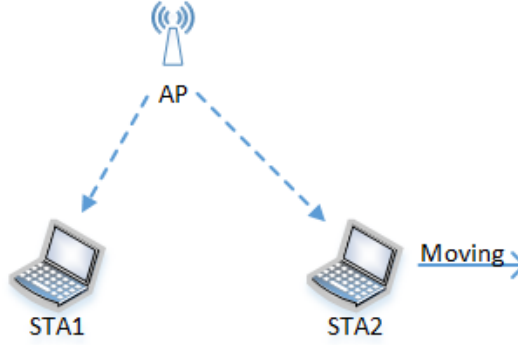


Figure 2.1 : A basic network deployment scheme, in which the STA2 is moving away.

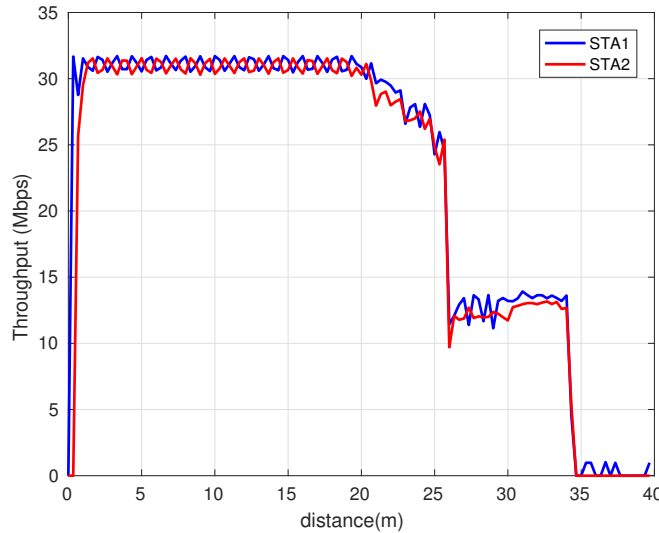


Figure 2.2 : Throughput change vs distance of STA2 for the down-link UDP traffic with saturated offered loads.

2.1.2 Collision and delay issues for the dense networks

Since the channel numbers are limited in both 2.4 GHz and 5GHz bands, most of the channels is likely to have excessive number of active traffics, which causes saturation, hence suffering from the increased packet collision rates and transmission delays.

With the DCF mechanism of the traditional CSMA-CA, as the number of contentions increase, the risk of packet collision, hence delay, packet losses are increased significantly, [8]. That is to say, beyond sharing the channel with multiple numbers

of STAs, the number of contending devices in a channel affect the total capacity of that channel, which eventually results in an additional decrease on the end users performances.

2.1.3 Spatial reuse limitations

The traditional CSMA-CA applies a protective behavior to minimize the packet collisions among the networks. On the other hand, it causes problems and limit the network performances. First, as a well-known situation, exposed node scenario as depicted in Figure 2.3, in which a transmitter node defer its transmission due by sensing transmission of the adjacent networks while the receiver node is at an interfere free area. In other words, in such a case, the transmitter unnecessarily waits the others even though the successful concurrent transmission are potentially achievable, which causes significant degradation in the network performance.

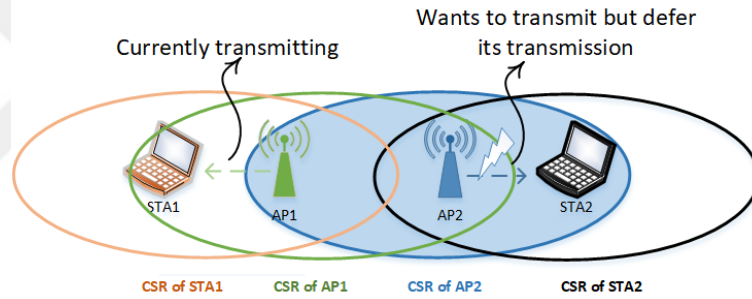


Figure 2.3 : Exposed node scheme

Another limitation is observed in some circumstances that the adjacent networks has tolerable interference to each other, in which simultaneous transmissions can be achieved. Though, the traditional CSMA-CA does not ignore these interfere signals and unnecessarily sense the channel as busy. Therefore, this protective structure of the CSMA-CA considerably limits the spatial reuse in any dense deployments.

2.2 Transition from OFDM to OFDMA

One of the most important changes in the PHY layer with the new standard is the use of OFDMA instead of OFDM. In traditional Wi-Fi, the OFDM technology allows multiple users to independently operate in different pre-defined channels or frequencies. The channel bandwidths are defined as 20, 40, 80 and 160 MHz which had been sufficient until recent years. However, simultaneous transmitting and receiving

operations by the network devices within a channel is not permitted by the nature of OFDM. Sharing the same channel with fair accessing to a channel brings some performance drop especially in dense networks which are discussed in the previous section.

With this new change, OFDMA, the problems due to channel sharing and contentions are expected to be reduced, since, in the new concept, there will be no channel sharing.

If we elaborate the OFDMA structure further, each 20 MHz channel is divided into 256 sub-carrier, which is four times of the previous amendments. Each sub-carrier is called tone and has 78.125 kHz band-width spacing. The symbol duration and cyclic prefixes are also increased four times, keeping the data rates, which provides an improvement in the robustness, especially in mixed environments. These tones are grouped into 26,52,106,242,484,996 and 2×996 which creates different Resource Units. Figure 2.4 demonstrate the RU division for the 20 MHz channels. Each RU can be allocated for a single STA at a given time. As a result of this, for a 20 MHz channel, maximum of 9 different users can be supported at a given frame transmission time.

Furthermore, although the concept of OFDMA in 11ax is similar to that of LTE, it has more challenges in terms of coordination. Since the OFDMA in 11ax standard is planned to work on top of DCF, the APs will coordinate the use of OFDMA by the help of new frame types such as trigger frame. The Tgax community provides a framework for deterministic and random access together. Each planned transmissions are negotiated between the AP and multiple STAs by the help of triggering and request messages. Afterward, the APs distribute the decided scheduling information across the network that is for a particular frame transmission slot. Each transmission opportunity, TXOP, should have equal size and duration so that synchronization for OFDMA transmissions are accomplished. In the case of insufficient packet sizes, the transmitter devices will add padding in order to fulfill the frame transmission duration or size.

2.3 Spatial Reuse Enhancements

Regarding the improvements for spatial reuse, the new standard provides three different mechanisms in MAC layer that aims to increase spatial reuse potential for dense networks. As acquiring basic understandings from the problems mentioned

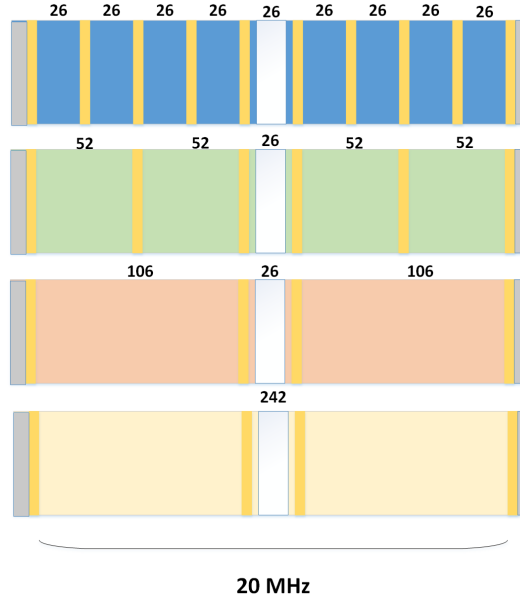


Figure 2.4 : The RU division scheme for 20 MHz channels

in 2.1.3, this newly developed features promise to improve spatial reuse while protecting the internal BSS transmissions and fairness among the networks. In the next subsections, the details of the proposed schemes will be given.

2.3.1 BSS color mechanism

The concept of BSS coloring introduced by the IEEE 11ah standard which was not aiming to use in any spatial reuse operations. As a result of innovative thinking, the TGax community decided to utilize this BSS color mechanism in spatial reusing of IEEE 11ax, [9].

Let's elaborate the BSS coloring mechanism further. Each BSS in a network is composed of an originator AP and their connected clients. The BSS color is an unsigned integer between 0-63 that will be planned to select randomly by each of different BSS in 11ax network deployments. The value of BSS color can only be decided by the originator AP and is distributed by the help of Association or Probe Response packets at the association phase, [9]. After the association is completed, the connected STAs changes their default colors with the received legitimate BSS color. These assigned BSS color values are then embedded in the related fields of header of all the physical layer convergence procedure (PLCP) protocol data unit (PPDU) packets that comprise management and data packets.

With the help of BSS color mechanism, all the received packets can be classified by only decoding the header of the packets as intra or inter BSS, which will then be used in OBSS_PD based SR. When the BSS color of a received packet is matched with the device's own BSS (the connected BSS's color) or the default color (zero), the devices will classify the packets as intra BSS, which means that the ongoing transmission is from its current BSS. On the other hand, if the color of the received packet is not matched with own color, it will be classified as inter BSS, which imply the other basic service set (OBSS) transmissions.

The new standard gives a detailed explanation on the detection and classification issues of the aforementioned BSS color mechanism for both APs and STAs.

2.3.2 OBSS_PD based SR technique

The new standard introduces a second type of clear channel assessment (CCA) threshold which is named as OBSS_PD threshold. This new threshold will be utilized to check the signal levels of received OBSS transmissions. Since the value of this threshold will likely be higher than the classical CCA threshold as depicted in Figure 2.5, the transmissions from OBSS are ignored, hence an improvement in the spatial reuse will be obtained.

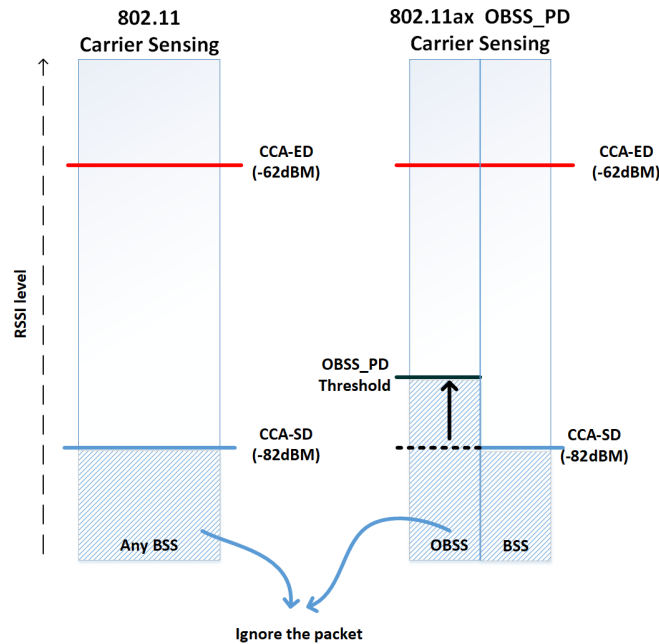


Figure 2.5 : OBSS_PD levels and Classic CCA levels comparison

The standard restricts the value of the OBSS_PD threshold with the following equation

$$OBSS_PD_{level} \leq \max(OBSS_PD_{min}, \min(OBSS_PD_{max}, OBSS_PD_{min} + (TX_PWR_{ref} - TXPWR))) \quad (2.2)$$

where, $OBSS_PD_{max}$, $OBSS_PD_{min}$, TX_PWR_{ref} are -62 dBm, -82dbm and 21 dBm, respectively. After computing and selecting the $OBSS_PD$ level, the standard also puts a restriction on the maximum allowable transmit powers of 11ax capable devices in conjunction with the $OBSS_PD_{level}$ as following [10],

$$TXPWR_{max} = \begin{cases} \text{unconstrained}, & \text{if } \Rightarrow OBSS_PD_{level} \leq OBSS_PD_{min} \\ TXPWR_{ref} - (OBSS_PD_{level} - OBSS_PD_{min}), & \text{if } \Rightarrow OBSS_PD_{max} \geq OBSS_PD_{level} > OBSS_PD_{min} \end{cases} \quad (2.3)$$

The use of $TXPWR_{max}$ constraint will only be activated in a 11ax device in the period that a OBSS signal is detected and ignored as a result of $OBSS_PD$ comparison. A basic relationship between $OBSS_PD$ level and $TXPWR$ is represented by Figure 2.6, which is given in the [10]. The essential aim of these adjustments of $OBSS_PD$ Threshold and transmit powers is to mitigate the interference levels among the OBSS so that the simultaneous transmissions are accomplished.

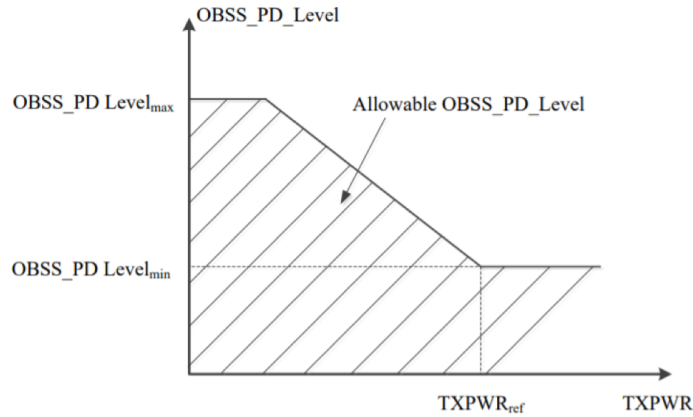


Figure 2.6 : The figure of relationship between $OBSS_PD$ level and TxPower limitations

Figure 2.7 demonstrates the change in the CSR of an AP when the $OBSS_PD$ SR is used. Since the new sensing threshold is higher than the traditional CS threshold, by the use of this mechanism, the system starts allowing simultaneous transmission between adjacent BSS networks. This is also clearly indicated in Figure 2.7.

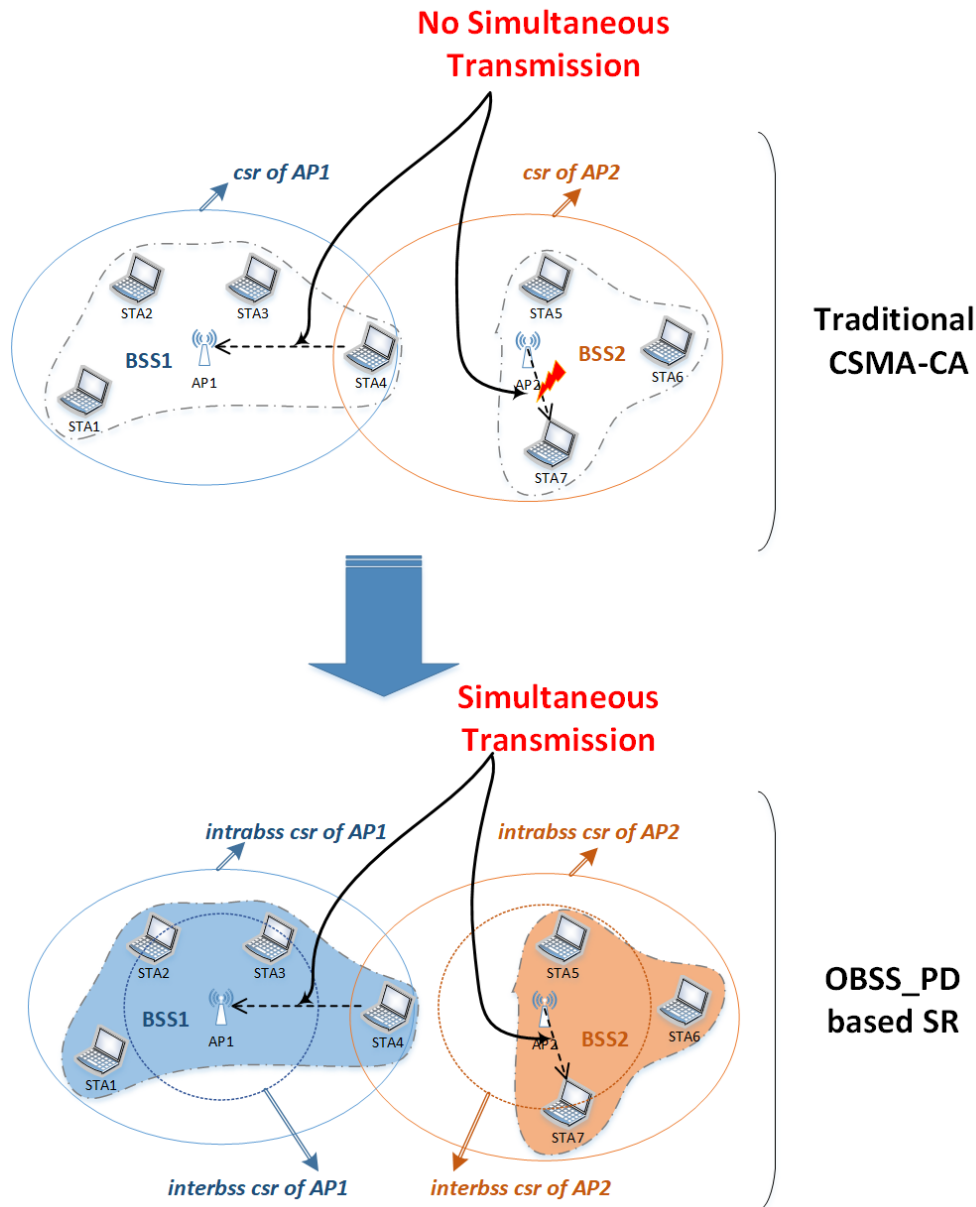


Figure 2.7 : Changes in CSR ranges and Simultaneous transmissions with the OBSS_PD and BSS coloring

A general frame reception model with the use of OBSS_PD and BSS coloring is given by the Figure 2.8. When a signal received, it is first classified to belong to whether intra or inter BSS. If the signal is coming from the own BSS (intra BSS), the normal CSMA-CA procedure is followed with the CCA threshold. Otherwise, the OBSS_PD threshold is used to compare in determination of channel availability. If the Rssi of received signal is bigger than the OBSS_PD threshold of the device, than the medium is sensed as busy, otherwise idle. This procedure is applied in all 802.11 ax capable devices.

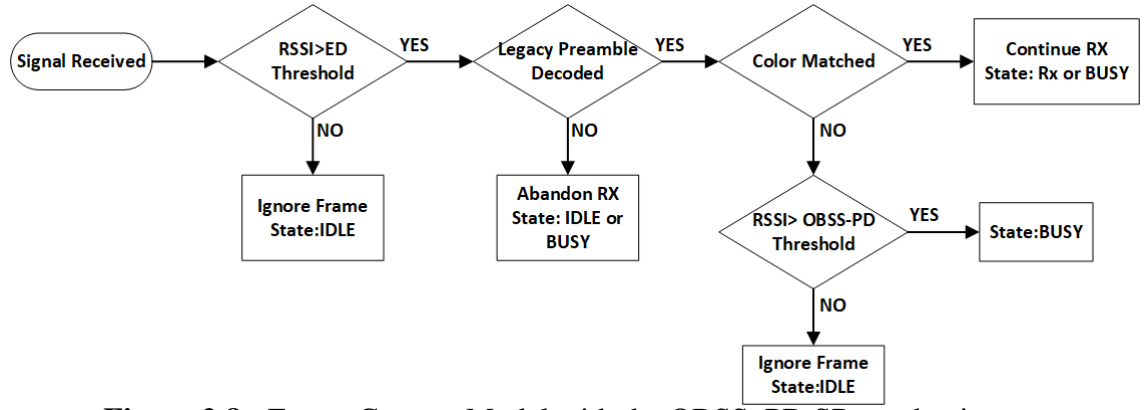


Figure 2.8 : Frame Capture Model with the OBSS_PD SR mechanism

2.3.3 SRP based SR technique

As an alternative to OBSS_PD SR, an another SR enhancement, which is named SRP based SR is proposed by the new standard. Its main idea is to give control of the potential concurrent transmissions to network devices. In the OBSS_PD, due to the distributed nature of the mechanism, the nodes can not know the potential concurrent transmissions and hence can not take actions with them. On the contrary, in the SRP based SR technique, the devices send trigger frames to the other devices in order to allow simultaneous transmissions and hence obtain a controlled SR platform in the networks. Since it is in the developing phase, there is very limited information in the last published draft. We briefly summarized the basic understandings on the sight of explanations of this feature in 802.11ax.

2.3.4 Two separate network allocation vector (NAV) mechanism

In order to adapt to some of OFDMA based new features, e.g., Mu-Mac, a two NAV based virtual carrier sensing mechanism is introduced by the new standard. These NAVs are called as Intra BSS NAV and basic NAV. When a received signal is classified as intra BSS, the corresponding NAV is set. In any other classifications, i.e., OBSS or unknown signal, the basic NAV will be set. The basic NAV working principle is the same as the single NAV in the traditional CSMA-CA. Furthermore, with these two NAV mechanisms, an 11ax capable device only sense the channel as idle, if and only if this two NAV is found zero, otherwise it senses as busy.

2.4 Evaluation of OBSS_PD Based SR

In this section, we evaluate the performance of the proposed OBSS_PD based SR technique of the IEEE 11ax standard. Currently, there are no available real hardware or driver that are capable of the 11ax features. Furthermore, in generally speaking, the Wi-Fi chip vendors, such as Broadcom or Qualcomm are planning to implement the aforementioned spatial reuse issues by the year 2020, [11]. Given these facts, we have carried out the performance evaluations on the simulation platform, [12].

2.4.1 Implementation details of the OBSS_PD based SR in simulation environment

In order to simulate the 11ax networks, PHY and mac layer classes of ns-3 are extended to support the 11ax spatial reuse features. Furthermore, the simulator is modified so as to work similarly as described in Fig 2.8. This novel 11ax implementation patch can be found in a publicly accessible GitHub repository, [13]. The implementation work mainly consists of the following steps in a sequence, 1) adding the BSS color bits on top of each PPDU packet headers 2) assigning a BSS color to each device own, 3) distributing the BSS colors by the help of associate response messages during association, 4) adapting the BSS color of each device after the association process is completed, 5) implementing the OBSS_PD threshold dependent carrier sensing technique in support with classical CSMA-CA carrier sensing.

By the implementation of OBSS_PD SR, the PPDU's that belongs to OBSS transmissions are expected to be ignored. This potentially can increase the throughput and reduce the average delay performances in dense network deployments which have saturated channels with an enormous number of active traffics.

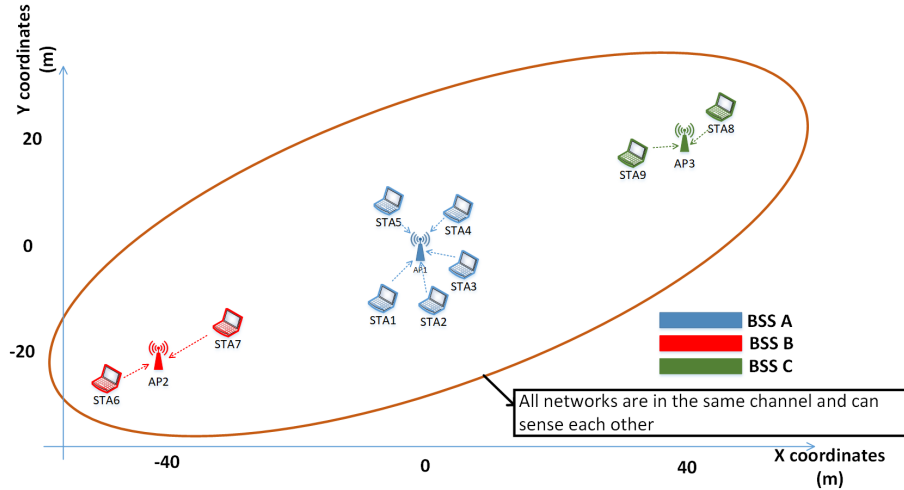
2.4.2 Experimental evaluation of OBSS_PD SR technique

Simulation of dense network deployments not only brings a giant complexity but also unexpected behaviors due to the highly probabilistic nature of Wi-Fi platform. Therefore, creating a dense network deployment is a challenging issue in the aim of clearly revealing the performance improvements. Considering these facts, we

Table 2.1 : The coordinate table of the nodes for the given deployment.

BSS A		BSS B		BSS C	
Id	Coordinates	Id	Coordinates	Id	Coordinates
AP ₁	0, 0,	AP ₂	40, 20, 0	AP ₃	-40, -20, 0
STA ₁	5, -9.5, 0	STA ₆	47.5, 10.5, 0	STA ₈	-45.5, -15.5, 0
STA ₂	3.5, 7.5, 0	STA ₇	47, 12.5, 0	STA ₉	-33, -13, 0
STA ₃	4.5, 0.5, 0				
STA ₄	-1.5, 6, 0				
STA ₅	-9, -5, 0				

have exploited the reference simulation scenarios which have been created by the Tgax community, [2]. Moreover, several evaluation results with regard to the box5 simulation scenario can be found in [14]- [15]. For this reason, to test and validate the accuracy of our initial implementations we preferred to utilize the Box-5 scenario deployment. In this study, we have used a simplified version of the Box5 scenario described in the [2]. The difference of our simplified Box5 scenario with regard to the base Box5 scenario lies in the offered load of each device. Each node generates a lower amount of traffic while located in the same coordinates with the Box5 scenario. The deployment scheme and corresponding device coordinates are given by Figure 2.9, and Table 2.1, respectively.

**Figure 2.9** : The simplified Box5 scenario deployment scheme

Along the conducted set of experiments, we have used only user datagram protocol (UDP) up-link traffic model. The data traffic is created by the use of constant bit rate (CBR) traffic generator which creates the packets with constant and regular intervals. Each STA in Figure 2.9 is associated with corresponding BSS and have active traffic along with the simulations. The offered loads of traffics are 100 Mbps which is a

Table 2.2 : Simulation parameters for OBSS_PD based SR experiments.

Simulation Parameters			
Traffic Type	UDP Uplink	Transmit Power	16 dBm
Mobility Model	Constant Position	Traffic Generator	On-Off generator
Channel Model	SpectrumWi-Fi	PHY Model	Spectrum Wi-FiPhy
Channel Num	1 (20 MHz)	Aggregation	A-MSDU enabled
Wi-Fi phy std	802.11ax	RTS-CTS	disabled
RateManager	Ideal rate control	Payloadsize	1450 Mbytes

sufficient data rate to make the channels with 20MHz bandwidth fully saturated by itself. It is a well-known paradigm for dense networks that because of the limited number of orthogonal channels in 2.4 GHz band, the congestion and saturation rates of the channels are expected to be more severe than the 5GHz band, [16]. For this reason, we applied the IEEE 802.11ax standard in the 2.4 GHz operation band. Furthermore, to examine the advantages of the new SR mechanism in several aspects, all the devices use the same channel with 20 MHz bandwidth, e.g., Channel 1, in 2.4 GHz band. The details of the simulations parameters are given in Table 2.2.

Figure 2.10 and Figure 2.11 demonstrate the throughput comparison results for each flows and aggregation of each BSS , respectively. It can be clearly observed from the results that the new applied SR technique increases throughput for both individual and cumulative aspects. Furthermore, although a reduction in the throughput of flow-7 and flow-9 is observed, the other links significantly increase their achieved data rates. Note that, these negatively effected STAs belongs to the edge BSS clusters that dominated the channel with the traditional CSMA-CA carrier sensing. By activating the new SR mechanism, all the BSS, especially the BSS A, starts ignoring the OBSS transmissions while applying a protective carrier sensing behavior for their own BSS transmissions.

On the other hand, as stated in [17], this new OBSS_PD SR technique promises to offer low delay performances in ultra-dense networks. This expectation becomes quite

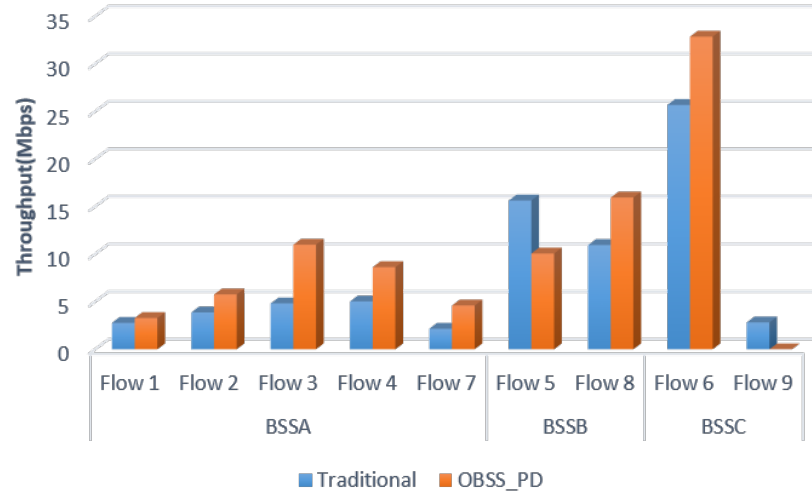


Figure 2.10 : Throughput of each flow for the CSMA-CA and OBSS_PD SR mechanisms

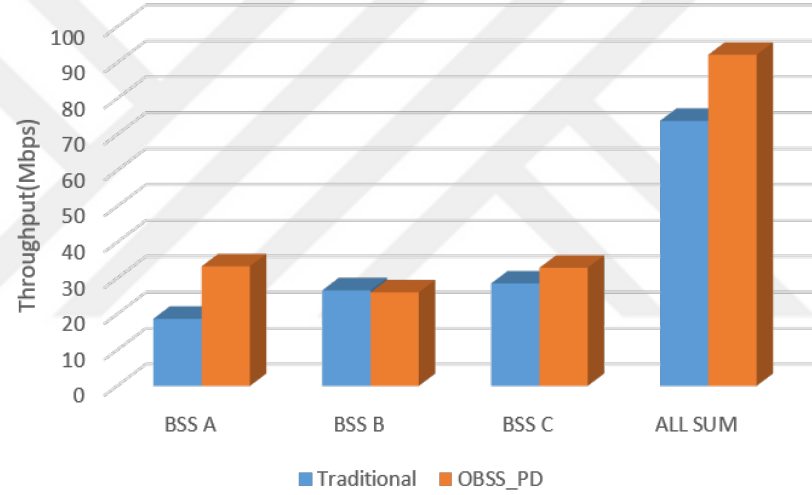


Figure 2.11 : Aggregated throughput of each BSS for the CSMA-CA and OBSS_PD SR mechanisms

consistent according to the working mechanism of the new proposed SR technique. Because, the simultaneous transmissions among OBSS networks will be allowed by the new technique instead of deferring the packets due by the traditional CSMA-CA, which potentially result in significantly reduced average packet delays for the network-wide.

The average packet delay performance results of each flow are displayed in Figure 2.12. From the figure, a significant delay reduction in the majority of traffic flow is observed. In some flow through, the delay performances go into higher values. The cumulative average delay results are demonstrated in Figure 2.13. The result indicates that a significant improvement on the packet delays can be achieved as a result of using

the proposed SR technique, which meets the above-mentioned expectations. Note that, these part of the study are planned to be published in [18].

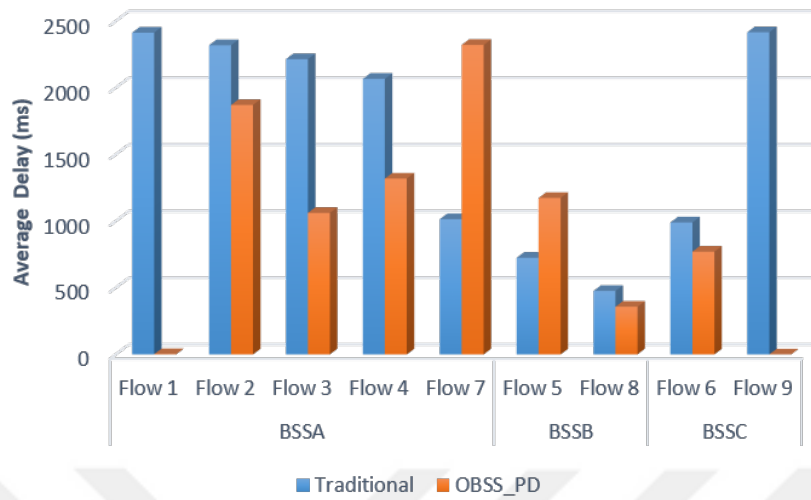


Figure 2.12 : Average delay of each traffic flow for the CSMA-CA and OBSS_PD SR mechanisms

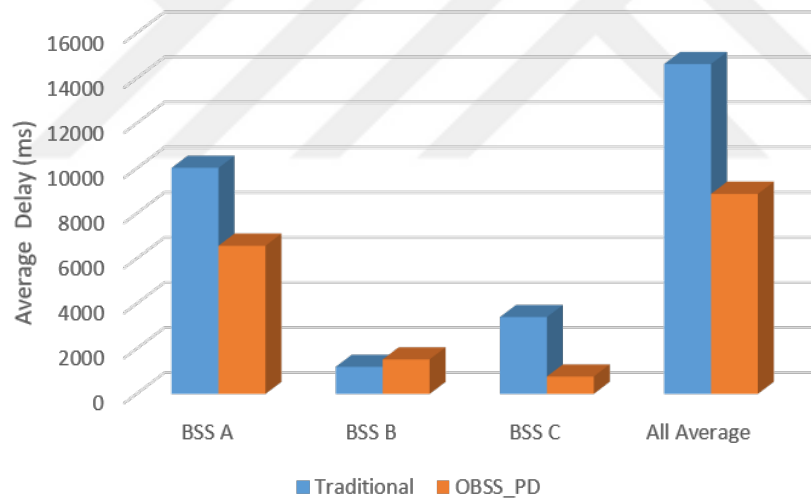


Figure 2.13 : Aggregated average delay of each BSS for the CSMA-CA and OBSS_PD SR mechanisms

3. ADAPTATION OF CARRIER SENSING THRESHOLD TO INCREASE THROUGHPUT IN DENSE 802.11AC WIRELESS NETWORKS

A dense WLAN deployment is defined as multiple WLAN's deployed in close proximity each having high number of STA's. As the available channels are limited in Wi-Fi, in such dense deployments each WLAN experiences a high amount of interference from other nearby WLANs.

In typical 802.11 WLAN, CSMA protocol uses two types of carrier sensing mechanism. The first is the virtual carrier sensing, which is optional and implemented with the request-to-send/clear-to-send (RTS-CTS) handshake. The mechanism provide a collision-protected transmission channel, which helps to avoid packet collisions.

According to standard [19], before initiating a data transmission, the transmitter-receiver device pairs can establish a collision free domain by a four way handshake signaling as depicted in Figure 3.1. When the other receivers in the network hear either RTS or CTS packets, they set their Network Allocation Vectors (NAV), which defers their transmission until the end of current transmission duration. By this way, the Wi-Fi networks forbid concurrent transmissions in any time, and therefore avoid packet collisions.

The second type of carrier sensing mechanism is the carrier sensing threshold (CST) mechanism, which is mandatory. This mechanism, frequently making use of the received signal strength (RSS) of interfering neighbors, defers transmission if the received interference signal strength is higher than the defined CST.

Both of these CS mechanisms aim to prevent collisions. However, at the same time, these mechanisms may also prevent potentially successful transmissions, which have a risk of reducing the overall system throughput. In the literature, some studies tackle with this issue and propose spatial reuse enhancements in dense networks. [20]- [21]. The design approaches of these studies can be classified according to the metrics that their models are based on, such as pairwise signal to interference noise ratios (SINR)

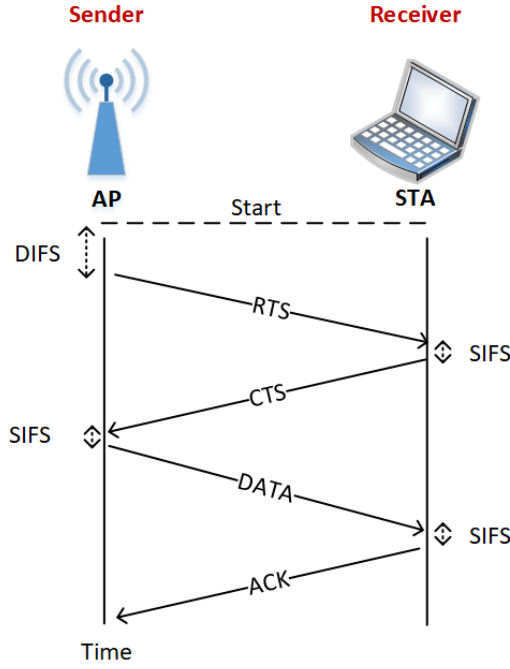


Figure 3.1 : RTS-CTS handshake mechanism

[20], [22], cumulative SINR [23], packet error rates [24] and RSS from interfere nodes [4], [25].

Hanghani *et al.* proposes an adaptive CST algorithm by evaluating busy/idle signaling at access points (APs) and current channel conditions at stations (STA) [26]. Each AP sends a busy/idle binary signal to its STAs and STAs updates their CST values. In this work, busy/idle signaling will reduce the hidden and exposed terminals and hence, increase the system's overall throughput.

Murakami *et al.* proposes an adaptive CST algorithm depending on node positions [27]. They use cameras to obtain mobile users' positions. According to the obtained positions, the system changes its CST value by using a defined positions-CST table. Although the system increases the performance by the proposed approach, it brings huge complexity in the custom network deployments.

Afaqui *et al.* proposes a dynamic carrier sensing approach which depends on the RSS levels [25]. Each AP on the system keeps track of RSS information of their associated STAs and neighbouring APs. Then, each AP adjust their CST according to their gathered RSS values. By this way, they maintain connectivity of the associated

clients in the system. Park *et al.* make derivations for the relation between the CST and system throughputs [21]. They also evaluate the differences and requirements of non-homogeneous networks where each device can have arbitrary set of parameters within carrier sensing perspective. Furthermore, the authors mention the requirement of a price penalty as a function of CST and transmit power to diminish the adverse impact of adjusting the parameters of each node to the other nodes. Pelechrus *et al.* analyses the effect of selfish manipulation of CST with the TCP and UDP traffic flows [5]. They point out the effects of using different traffic types. Additionally, the authors use a different metric to analyze the throughput degradation due to the greedy nodes.

We propose an adaptive carrier sensing algorithm based on periodic throughput gain and fairness of the system networks, which follows a different methodology from the related studies in the literature. In our work, A central controller AP gathers the throughput information from all of the networks within the system and manage CST levels of all WLANS in a dense deployment. The contribution of this part of the study is designing an algorithm by considering the fairness and connectivity issues while aiming to increase the overall network throughput.

The central controller structure proposed in this study can be realised by various systems such as a cloud based remote system, which can control WLANs without extra protocol overhead. Furthermore, the central controller logic can also be established by a software defined wireless network (SDWN) architecture as used in [28].

3.1 Channel Model and Performance Metrics

In this section we introduce the communication model and the performance metrics which form a basis for the proposed carrier sensing algorithm.

3.1.1 Communication model

In the literature, the logarithmic path loss model is widely used in the studies of 802.11 networks. According to the path-loss model, the received signal strength at a separation

distance, d is

$$P_{RX}(d) = P_{RX}(d_0) \left(\frac{d_0}{d} \right)^n [mW], \quad (3.1)$$

where n is the path loss exponent and d_0 is the reference distance (usually 1m), $P_{RX}(d_0)$ indicates the rx power at d_0 .

In densely populated networks, there are many devices, which interfere with each other. For a successful transmission, at least two criteria must be satisfied. First, the received signal strength should be higher than the receiver sensitivity or the energy detection threshold as,

$$P_{RX}(d) \geq P_0, \quad (3.2)$$

where P_0 is the receiver sensitivity. If the received signal is below this value than the signal is not captured. Second, considering cumulative interference, the ratio of the signal powers to total interference powers namely SINR should be bigger than a threshold value (S_0),

$$\frac{P_{RX}(d)}{P_N + \sum_i I_i} \geq S_0, \quad (3.3)$$

where P_N represents the total noise power and I_i denotes the received interference signal strength from interference source i . The value of S_0 depends on target data rate and modulation type. In our dense network, all devices are assumed to have the same P_0 and S_0 requirements. In dense deployments, the noise power can be neglected, since the interference power is dominant.

3.1.2 Airtime calculations

Airtime usage of each device is an important metric in densely deployed networks. The total airtime of any flow can be expressed as,

$$T_{tot} = T_{succ} + T_{col} + T_{busy} + T_{idle}, \quad (3.4)$$

in which, T_{succ} and T_{col} demonstrates the duration of successful transmissions and collisions, respectively. T_{busy} and T_{idle} give the busy duration of the channel and idle time passed before transmission. T_{busy} depends on the number of contentions within the channel.

Let the airtime duration of a transmitted packet be denoted as T_{tr} . Then, we can calculate T_{tr} as,

$$T_{tr} = T_H + T_P + T_{ACK} + SIFS + DIFS, \quad (3.5)$$

where T_H , T_P , T_{ACK} denotes the transmit duration of header, payload and ACK packets, respectively. *SIFS* and *DIFS* durations are constant and defined different for each 802.11 standard. At there, since a packet consist of headers and a payload, a transmission duration of a packet is $T_{packet} = T_H + T_P$. In other way, we can calculate a packet's transmission time by $T_{packet_n} = N_n/R_n$ where N_n and R_n demonstrates the size and transmission rate of the packet n , respectively.

After the calculation of transmission duration of the flows, we can now calculate the airtime utilization metric, which is obtained as, $AUT_i = T_{tr}/T_{tot}$. This metric provides the information on the ratio of spectrum usages among the devices within the dense networks. In a contention free network, with the full saturated traffic, its value reaches 1, since the devices use all the spectrum provided. With the traditional CSMA mechanism, for a single flow, its value becomes proportional to the number of traffic flows in the channel.

3.1.3 Fairness calculations

In densely deployed networks, one of the most challenge problems is the fair spectrum usage among the networks, During the adaptation of CST, any network between the adjacent networks can suffer from others transmissions. Having such high level of interference causes collisions and unfair channel accesses, which result in significant reduction in the data rates of the networks that are located in middle of the topology such as AP5-STA5 network pair. Thereby, it is reasonable to monitor the fairness of the system to resolve these performance degradation.

To investigate the fairness of our system, we will use a fairness metric, named as log-throughput factor [26],

$$\phi = \frac{1}{N} \sum_{i=1}^N \log(\tau_i), \quad (3.6)$$

where, N represents the total number of traffic flows in the system and τ_i demonstrates the throughput of flow i . Since it is in the logarithmic base, in any unfair spectrum sharing, the value of ϕ becomes lower.

3.2 Adaptive carrier sense threshold algorithm

We propose an adaptive carrier sensing model to increase the limited spatial reuse in dense network deployments. Our approach mainly aiming to increase the system

throughput by a series of iterative adjustments of CST, demonstrated by T_{cst} , of the system according to the change in aggregate system throughput and fairness.

We have two critical assumptions for the proper functioning of the proposed algorithm. First, we assume all the APs and STAs within the system keep their positions stable since any movement upon the time will change the network topology. Secondly, the traffic flows of the networks are assumed to be saturated in the uplink and downlink directions. In other words, each transmitter device has endless packets within their transmit queues waiting for transmission along the experiments, which ensures continuous contentions among the networks. A brief summary of used notations and the pseudo code of the proposed design are given by Table 3.1, and Algorithm 1, respectively.

The initial overall system throughput (τ_{sys}^*) and log throughput factor (ϕ_n^*) values are monitored when the initial carrier sensing threshold T_{cst}^* is applied. The connection of each associated STA must be maintained by the system while adjusting T_{cst} . Therefore, before changing T_{cst} , the system controls new T_{cst} value to not exceed the minimum received signal powers of each STA from it's associated APs, $\Gamma_{i,jmin}$.

The fairness of the system is monitored by using a fairness threshold ϕ_{pt} , which is a weighted value of the initial fairness value ϕ_n^* . The stability against the small throughput variations are controlled by a throughput change threshold $\delta_{threshold}$, determined as $0.1 \times \tau_{sys}^*$. When the above criteria are held and if the change in throughput, δ_n after applying new T_{cst} is positive and greater than the threshold, $\delta_{threshold}$, then the system increases T_{cst} by one step, ϵ_{cst} . If the change is negative, then system decreases the T_{cst} . Otherwise, T_{cst} remains unchanged.

In this study, since we are considering homogeneous networks, in which all the networks parameters are adjusted as the same, it is important to maintain the throughput of the individual networks. In densely deployed networks, increasing CST can trigger the hidden and exposed node problems, which can result in suffering of some of the networks in the system. By the usage of ϕ_{pt} , we are aiming to take the control of fair spectrum usage among networks, while increasing the number of simultaneous transmissions in the system. It's value is determined as $0.5 \times \phi_n^*$.

One another issue in the adaptation process of the CST is connectivity, which will ensure the connections of each associated client at the end of the adjustment process.

Table 3.1 : A summary of notation.

Parameter	Description
τ_i	Throughput of flow i
τ_{sys}^*	The initial cumulative throughput of the system when initial CST is applied.
τ_{sys}	The cumulative throughput of the system.
T_{cst}^*	The initial carrier sense threshold of the system.
T_{cst}	The current carrier sense threshold.
ϵ_{cst}	The step-size for carrier sensing threshold.
δ_n	The change in the throughput after applying new CST.
$\delta_{threshold}$	The threshold for throughput change
$\Gamma_{i,jmin}$	The minimum received signal power of all associated STAs from their APs.
ϕ_n	Log-throughput factor for n^{th} iteration
ϕ_n^*	Initial value of log-throughput factor when T_{cst}^* is applied.
ϕ_{pt}	Penalty threshold for log-throughput factor

Many of the related studies in the literature neglect the connectivity issue despite its critical importance in the real environments. Since our system is homogeneous and controlled by a centralized mechanism, the system should care the minimum signal power of each connected STA in each AP. After collecting of minimum received signal power $\Gamma_{i,jmin}$ among all associated STAs from all APs, the system should adjust its CST to be higher than that value.

The CST of the system should be updated periodically, η , since the system conditions can change upon the time. In the most of the currently used Wi-Fi devices, the CST values are static and set to very low values, which indeed depend on the chip vendor. Therefore, in this study, T_{cst}^* is assumed to be -99 dBm. The value of step-size change of the CST, ϵ_{cst} is set as 1 dBm, which lets the system to find the near optimum value with the adaptive process. On the other hand, the initial value of the throughput change threshold, $\delta_{threshold}$, is adjusted as 10 % of τ_{sys}^* . The aim of using such a threshold is to tolerate the vast fluctuations in aggregate throughput due to the sequential changes in the system CST.

After defining the criteria given above, we develop a heuristic search model to achieve a maximum value in aggregate system throughput while considering the system needs.

The limitations and the objective function of the search algorithm are summarized by the equation 3.7.

$$\begin{aligned}
& \underset{T_{cst}}{\text{Maximize}} && \sum_{i=1}^N \tau_i \\
& \text{subject to} && T_{cst} \leq \Gamma_{i,jmin} \\
& && \delta_{threshold} \leq \delta \\
& && \phi < \phi_{pt}
\end{aligned} \tag{3.7}$$

We have followed an iterative process since that there exist barely any available and accurate closed form equations on the calculation of throughput in particular for these type of multi variant dense networks. Therefore, the simplest way is to apply an iterative search in a heuristic manner.

The execution process of the algorithm begins with the initialization of the system parameters. Afterward, the results obtained with the selected initial parameters are used in the calculations of the parameter set. These parameters are $\delta_{threshold}$, and ϕ_{pt} . Then, the system continues with the step-wise increase of the T_{cst} in a one-minute periodic loop. In the loop, the system first controls the fairness level. When the fairness level is at a satisfying level, then the system is allowed to continue with the next steps. In the next steps, if the throughput changes with the usage of the updated CST is high enough, then the system explores whether the connectivity will be protected (steps 15-19 of the Algorithm 1). After ensuring the connectivity, the system increases the system CST. In the next section, the performance of the proposed algorithm and various dense environment analysis are evaluated and discussed.

3.3 Performance Evaluation and Simulation Results of the Adaptive Carrier Sensing Algorithm

To evaluate the performance of the proposed algorithm, we conduct simulations on the ns 3 simulator considering two basic network setups. The first network is created to observe reference throughput performance of a simple AP-STA network. The second network, on the other hand, is designed to observe the effect of CST changes on the overall system throughput. The simulation parameters are given in Table 3.2. The default transmitter power is 16 dBm for each of the network device. To apply a more realistic frequency dependent propagation and power spectral density model, the Wi-Fi SpectrumPhy and Wi-Fi Spectrum classes of the simulator are used. During the simulations, each data flow is created by a fully saturated UDP down-link traffic.

Algorithm 1 Adaptive CST algorithm

```
1: procedure
2:   Initialize  $T_{cst} = T_{cst}^*$ 
3:   Get  $\Gamma_{i,jmin}$ 
4:   Get  $\tau_{sys}^*$ 
5:    $T_{cst} \leftarrow T_{cst} + \epsilon_{cst}$ 
6:    $\delta_{threshold} \leftarrow 0.1 \times \tau_{sys}^*$ 
7:    $\phi_{pt} \leftarrow 0.5 \times \phi_n^*$ 
8:   loop  $\eta$ 
9:     Update  $\Gamma_{i,jmin}$ 
10:     $\delta_n \leftarrow \tau_{sys}^n - \tau_{sys}^{n-1}$ 
11:    if  $\phi_n < \phi_{pt}$  then
12:       $T_{cst} \leftarrow T_{cst} - \epsilon_{cst}$ 
13:    else
14:      if  $\delta_n > \delta_{threshold}$  then
15:        if  $T_{cst} + \epsilon_{cst} < \Gamma_{i,jmin}$  then
16:           $T_{cst} \leftarrow T_{cst} + \epsilon_{cst}$ 
17:        else
18:           $T_{cst} \leftarrow T_{cst}$ 
19:        end if
20:      else if  $\delta_n < -\delta_{threshold}$  then
21:         $T_{cst} \leftarrow T_{cst} - \epsilon_{cst}$ 
22:      else
23:         $T_{cst} \leftarrow T_{cst}$ 
24:      end if
25:    end if
26:    goto loop.
27: end procedure
```

Each device in these networks have a single antenna and stream. Moreover, a same 5 GHz channel with 80 MHz channel width is used by each networks. The on-off traffic model of ns-3 is utilized to generate UDP traffic flows.

3.3.1 Point to point performance of a 802.11ac network

802.11ac network throughput performance is investigated with a simple network setup as depicted in Figure 3.2 . Normally, with the usage of 802.11ac standards, it is expected to reach very high throughput values in compare with other 802.11 standards.

The throughput measurement results of the interference free network is seen in Table 3.3. Note that the modulation and coding scheme (MCS) levels are selected automatically by the algorithm you selected in NS-3. It is obtained for a single stream

Table 3.2 : Simulation parameters for the carrier sensing adaptation experiments

Simulation Parameters			
Traffic Type	UDP download	Transmit Power	16 dBm
Mobility Model	Constant Position	Traffic Generator	On-Off generator
Channel Model	SpectrumWi-Fi	Inter AP-STA distance (d1)	5m
PHY Model	Spectrum Wi-FiPhy	Inter-AP distance (d2)	108, 54, 36, 27m
Channel Num	104 (80 MHz)	Aggregation	A-MSDU enabled
Wi-Fi phy std	802.11ac	RTS-CTS	disabled
Rate Manager	Ideal rate control	Payload size	1450 Mbytes

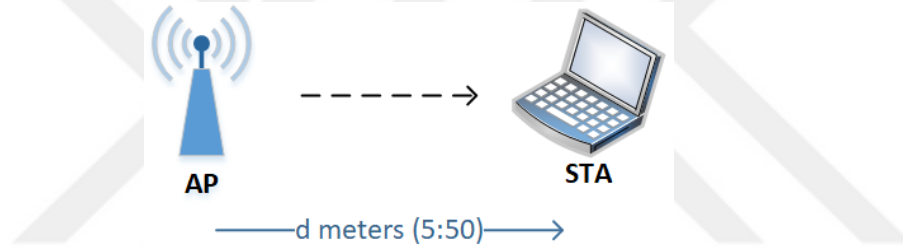


Figure 3.2 : A simple AP-STA pair network with inter distance d.

and 80 MHz bandwidth in IEEE 802.11ac standards. This table will be used as a reference for the following performance evaluations.

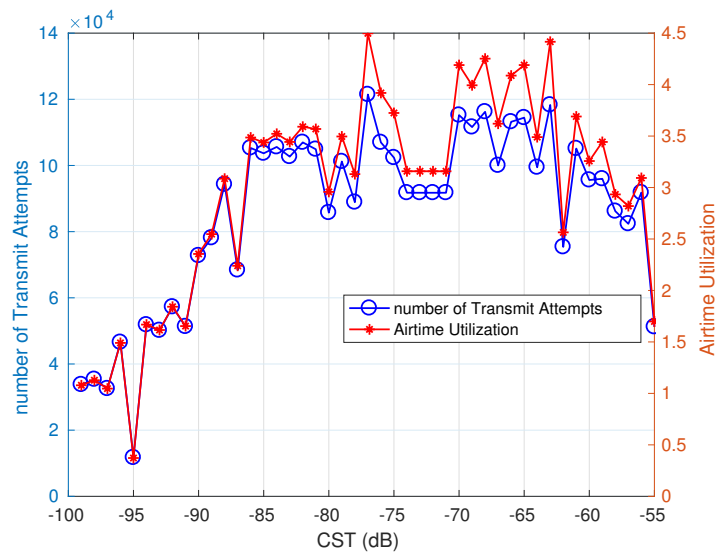


Figure 3.3 : The number of Transmission attempts and total airtime utilization rate of the channel vs CST change for network density 9

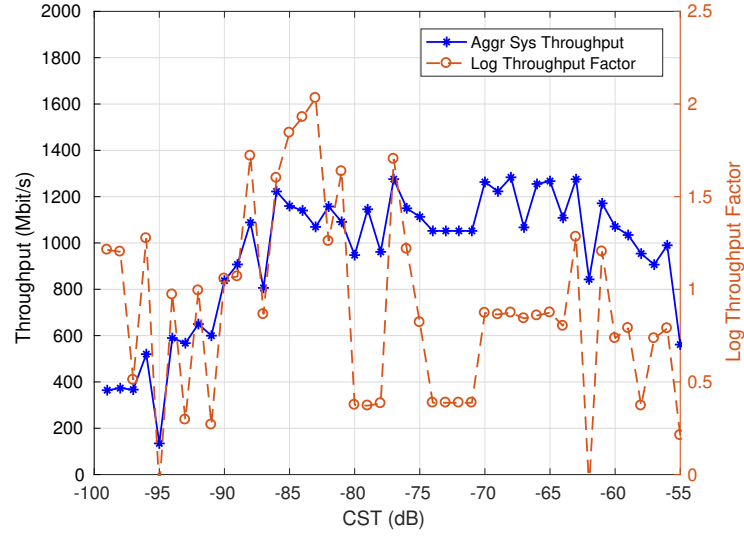


Figure 3.4 : System Throughput and Log-Throughput Factor vs CST change

3.3.2 Analysis of CST change effect on a simple grid dense network setup

In this part, we will investigate the effect of CST change from different perspectives on a simple 3×3 grid network setup. A 9 network grid topology which is depicted by Figure 3.5 is created with the inter AP-STA distance of 5 meters.

The effect of CST change on the number of total transmit attempts and total airtime utilization of the system is demonstrated in Figure 3.3. As seen from the figure, at -99 dBm of CST value, the sum of airtime utilization of the channel goes around one, which means that a single channel is in the fully usage by the devices and no simultaneous transmissions occur among the networks. On the other hand, when the CST value is increased, total airtime utilization of the channel reaches multiples of its initial value due to the simultaneous transmission among networks. Furthermore, by increasing the CST, the existence of simultaneous transmissions among networks can be deduced from the increase in the number of total transmission attempts of the devices. Figure 3.4 gives the aggregate system throughput result and log-throughput factor versus CST change for 3×3 grid topology. As shown in Figure 3.4, the aggregate

Table 3.3 : Achievable throughput values versus received signal strength (RSS).

RSS(dBm)	-55	-60	-65	-70	-75	-80	-85
Thr(Mbps)	352	271	223	166	84	56	0

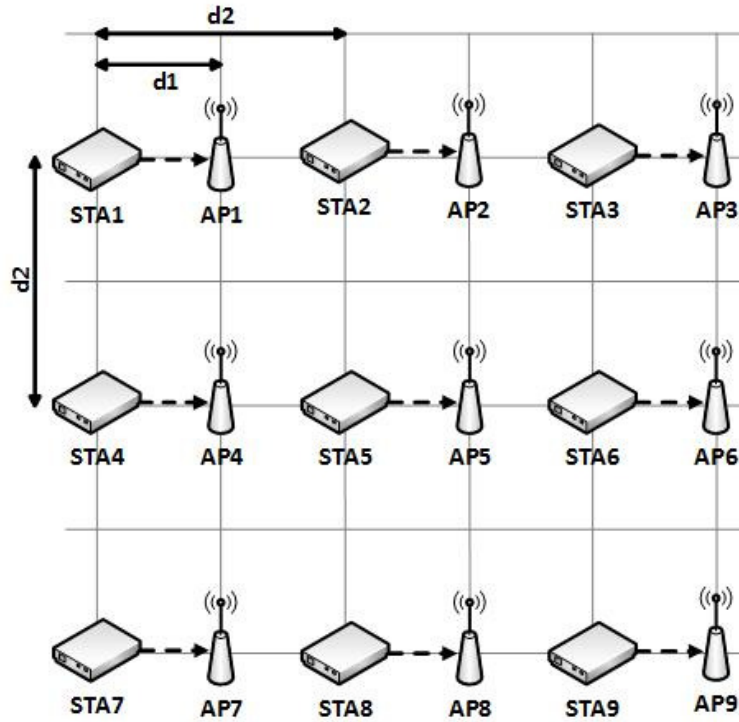


Figure 3.5 : The 3×3 simple grid dense network deployment where access points (APs) and stations (STAs) are 5m apart.

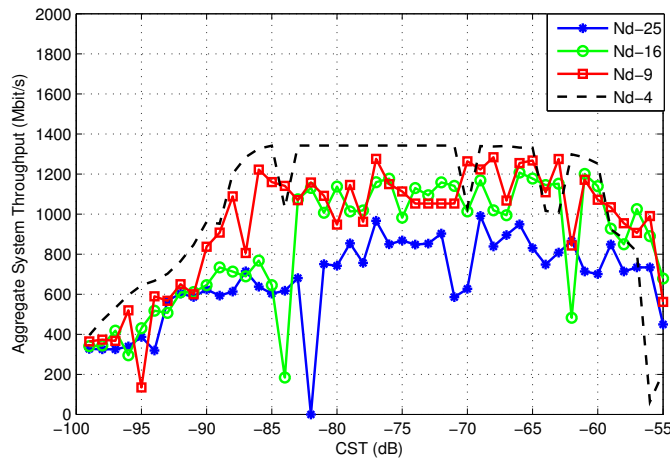


Figure 3.6 : Overall network throughput vs CST for different network densities (4-9-16-25)

throughput of the system can reach up to multiples of the default (initial low CST value) at high CST values. An oscillatin trend in fairness is observed for different values of CST. Furthermore, at some points, the value of fairness metric (0.8 in default) can dramatically fall below the tolerable level. For example, around -80 dBm of CST, although the throughput value of the overall system is around 1200 Mbps, the value of log throughput factor becomes approximately 0.3, which is a quite low value in terms of fairness. Consequently, to guarantee the fairness level among the networks, a

fairness threshold is required in any adaptive system design. For this reason, we add a fairness threshold into the proposed algorithm, which is set to 50% of the default fairness value.

We now examine the effect of CST change in different node densities. A 108 m² square box is deployed with 4, 9, 16 and 25 AP-STA pairs in a grid manner as depicted in Figure 3.7, Figure 3.8, Figure 3.9 and Figure 3.10, respectively. The simulation results for these network densities are represented by Figure 3.6, in which ‘Nd’ labels represent the network densities (i.e. ‘Nd-16’ label expresses the existence of 16 separate AP-STA pairs). It is obvious that, in presence of lower interference levels within less node density deployments, the maximum reachable throughput gains are greater than that of higher density deployments. Nevertheless, there are still significant throughput improvements for high node densities by increasing the system CST.

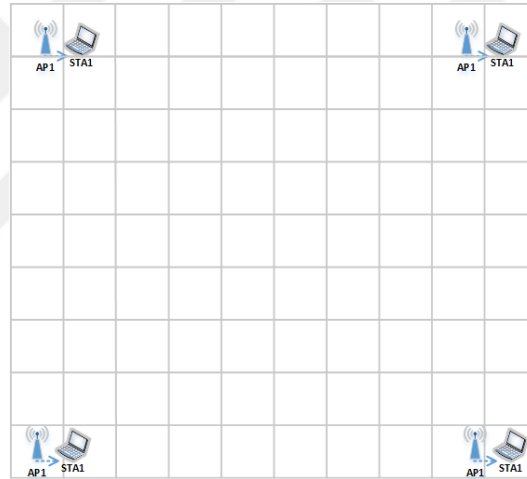


Figure 3.7 : 4 AP-STA pair grid network deployment

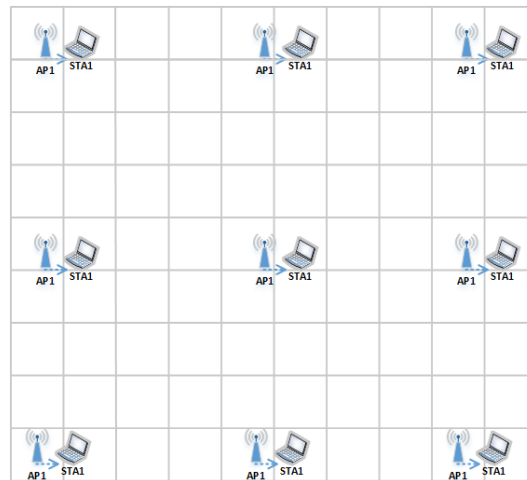


Figure 3.8 : 9 AP-STA pair grid network deployment



Figure 3.9 : 16 AP-STA pair grid network deployment

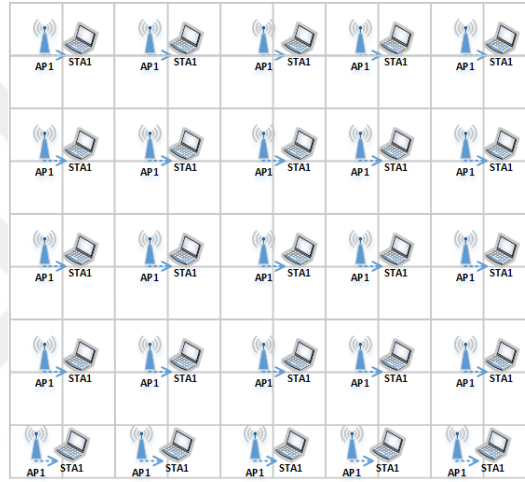


Figure 3.10 : 25 AP-STA pair grid network deployment

Moreover, some fluctuations in the throughput upon the change of CST are observed that can be correlated with the change in the interference levels, as aforementioned above. Since the mutual effect of the interference levels and simultaneous channel access plays an important role in the successful packet receptions.

3.3.3 Adaptive algorithm performance evaluations

The performance results of the proposed algorithm for different node densities are demonstrated by Figure 3.11.

The algorithm can not reach the maximum throughput values for each node density, as provided by Figure 3.6 due to the fairness and throughput variation constraints of the algorithm. However, the proposed algorithm on the average, 100 % aggregate throughput gain while guaranteeing fairness and connectivity of the networks.

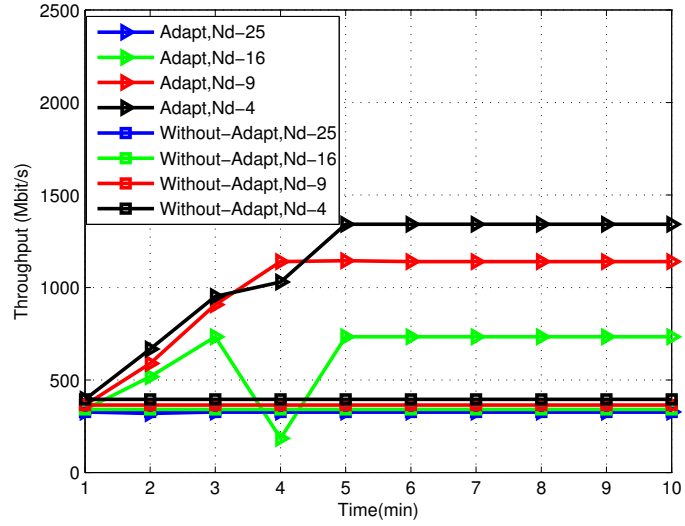


Figure 3.11 : The throughput improvement by the proposed algorithm for different network densities

It is worthwhile to note that because of the initial assumptions made. The achievable gains depend on the stability levels of the nodes in an environment. Moreover, the initial and weighted parameters should be adjusted for according to the network topology in order to reach the expected gain levels. Note that this part of the thesis is published in [29].



4. A COUNTER-MEASURE APPROACH AGAINST CARRIER SENSING ATTACKS IN WLANS

4.1 Introduction

As Wi-Fi networks become ubiquitous across the world, several challenges and limitations have arisen. In order to cater these problems, the new generation standard, namely IEEE 802.11ax, has developed many novel features in the PHY and MAC layers that will also increase the capacity of dense networks. Nevertheless, Wi-Fi networks remain vulnerable to several types of WLAN attacks. Also, there are many easy-to-use Wi-Fi attack tools such as Mad Wi-Fi driver [30], which reduce the security of WLAN networks.

In recent years, among the several types of WLAN attacks, in particular, the attacks at the PHY layer have taken more interest in the research community. Several studies tend to characterize and detect the misbehaving nodes with their novel methods and strategies, [6], [31]. These studies provide easy and applicable approaches that have high accuracy in detection of misbehaving nodes in exposed networks. However, in the literature no work has been proposed that leverages these detection mechanisms and offer a countermeasure for such misbehaving nodes at PHY layer. On the basis of these needs, in this study, we propose a two-way counter-measuring strategy by aiming avoidance of WLAN networks from the effect of greedy nodes. The new countermeasure method can be used after the detection of misbehaving nodes by one of the techniques mentioned above. This part of the study is motivated to be a complementary to the misbehaving detection studies, thus we assumed that the misbehaving node is already detected by the system. The main design consideration of this study in the fashion of applicability: 1) Without introducing a new protocol, e.g. handshaking, among the network devices, in particular for client devices: This is motivated by the practicality concerns due to closed nature of the majority of real client devices which does not permit to modify. 2) Ensuring a coordination among the legitimate nodes in order to reduce the delays, thereby minimize the destroying effects,

and stand alive the connectivity's of associated clients while struggling with jamming kind of attacks.

By the traditional CSMA-CA mechanism of Wi-Fi, the channel availability is determined by the use of Carrier Sensing Threshold (CST) which basically compares the RSSI of the incoming signals with this static CST. Its value is defined as -82 dBm by the IEEE 802.11 standards, [19]. When the RSSI level of the incoming signal exceeds this threshold, the channel is sensed as busy by the transmitter device, otherwise is idle. This mechanism helps to provide a secure environment for packet transmissions but also causes a limitation in the potential network capacity, especially in dense networks [32]. The next generation standard aims to improve these spatial reuse issues by developing some extensive structures.

One of the most attractive SR techniques in the new amendment is the OBSS_PD based SR technique in conjunction with transmit power. This technique is planned to be work on the basis of accurately identifying the bss and obss signals. A detailed explanation on the working principles of the BSS coloring and OBSS_PD based SR is given in the Chapter 2.

After exploring the new amendment, Wi-Fi systems are still open to any kind of PHY layer attacks, which will severely degrade or suppress the performance of any Wi-Fi network. In the presence of a misbehaving node pair with high CST, a channel will always be dominated by the transmissions of the attacker, since it will not sense any ongoing transmissions. Because of the nature of the CSMA-CA mechanism, the normal standard compliant nodes in any exposed network will mostly sense the channel as busy, and thereby the transmission availability check process will end up with deferral of their own packets. As a consequence, it will result in having significantly reduced data rates, a high number of packet collisions and vast delays of packets.

Even though the aforementioned attack types cannot directly be classified as traditional jamming attacks that generate continuous signals in the spectrum, because of their working principles, these selfish nodes can reasonably be evaluated as a different kind of jamming attack.

There are some studies that propose countermeasure approaches against jamming attacks in WLANs, [33], [34], [35]. Furthermore, in almost all the related studies,

the only approach that is used in the avoidance of jamming attacks is the channel hopping. However, we know that the channels in ultra-dense networks will be in full saturation by a vast number of active traffics, [16]. For this reason, a channel hopping operation in combating with jamming will not efficiently improve the legitimate network performance, but will also degrade the data rates in the new channel.

At this point, as a result of innovative thinking, a key alternative approach is proposed for 11ax networks: Changing the BSS Color. By this new approach, we are aiming to take advantage of using the BSS coloring and OBSS_PD SR techniques of the new standard. When an attacker network is located sufficiently far from the legitimate networks, it's transmission can be ignored by the usage of this new approach. As a drawback of this approach, it will not be effective in the proximity of the attacker network. Therefore, we proposed a two-way countermeasure approach which can decide on the use of channel hopping or bss color changing with respect to the conditional requirements.

Given the design goals above, in order to propose a lightweight and applicable method without introducing a handshaking protocol, the CSA and BSS color change announcement elements within beacons will be utilized. There are mainly their advantage of using these message frames: 1) They have been already introduced in the current and previous standards, as a result, every device will easily adapt itself 2) These message frames requires no handshaking in distributing a change order, which allows flexible designs 3) consists a countdown field which helps ensuring of coordinate actions among networks. The issue of coordination among the networks becomes a critic when changing color or channel because of the distributed nature of Wi-Fi architecture. Though, there is no other extensive study that provides a coordination mechanism while changing a channel. On the basis of this fact, we propose a coordinated counter-measuring scheme to reduce the delays and connectivity loss of network peripherals.

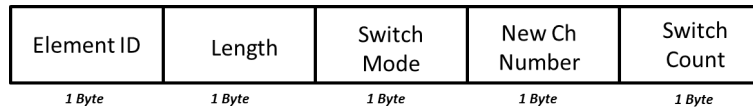


Figure 4.1 : The format of a channel switch announcement element.

4.2 Background and Related Work

4.2.1 Relevant 802.11 functions

Channel Switch Announcement (CSA) Element

In the 802.11 standards, the Channel Switch Announcement (CSA) element frame, (Fig. 4.1) is defined and be inserted in management type of packets such as beacon packets with Information Element ID equals to 37, [19]. These frames are generated and sent through only by AP devices. Since the frame type is already defined and common for all the 802.11 standard compliant devices, making use of it would brings no extra cost and difficulty to the networks. In the CSA element frame , three fields will be used in our study as Channel switch mode, New channel number, and Switch count. The channel switch mode represents whether to channel switching is enabled or not. New channel number field shows the new planned channel when the Switch Count reaches to zero.

One of the benefits of using the CSA element frames beyond the cost and implementation aspects is that it allows easy coordination of the network devices. In other words, with the help of channel switch countdown, all the devices that decodes these fields will make themselves synchronise with respect to the actions of the AP. Once the CSA mode is detected as enabled, the STA devices starts to arrange their buffers and their own traffics according to the value of CSC. Following it, when the CSC reaches zero, all the STAs across the network, will change their current channel to the planned channel. Therefore, there will only be very small amount of delay in the channel switch operation which is negligible. Thus, we can name it as coordinated channel switching.

BSS Color Change Announcement Element

Similar to the CSA element frames, the new 11ax draft v3 introduces a new frame type the Bss Color Change Announcement Frame, [10]. The working principles of

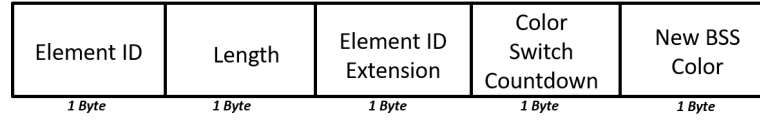


Figure 4.2 : The format of a BSS color change announcement element

this mechanism are almost the same with the CSA mechanism except the new channel. Instead of advertising a new channel, the intention of this frame type is to advertise the new planned bss color among the internal bss devices. This new frame type is allowed to be inserted in beacon packets with Extended Element Id 37. The new planned BSS color is decided only by the AP and distributed to the associated STAs by the help of these frames. The issue of establishing a coordination on the color change operations follows the same progress as the CSA element coordination, which is previously explained.

4.2.2 Related work

Misbehavior Detection of Physical Layer Attacks: Most of the misbehavior detection studies in the literature focus on a few types of WLAN attacks that are generated mostly by manipulating MAC layer parameters, especially some of back-off parameters.

Recently, attacks on the other layers, e.g., physical layers, are started to take more interest in the research communities, as the very high-density deployments become common. Furthermore, there are limited studies on the detection of attacks for the physical layers. In [5], Pelechrinis *et al.* evaluate the possible scenario of physical layer attacks and prove out the dramatic descriptive impact within a real test-bed experiment. They propose a detection methodology in which the APs send low power pings to network-wide when the system realizes an unfairness among STAs traffics. The essential assumption of this study is to have a carrier sense attacker that cannot decode low power signals and hence cannot reply to the signals from the legitimate devices. With this methodology, they have % 95 accuracy in the detection of attackers. Furthermore, this paper is the first tangible application for the view of how easy to create a physical layer attacker by the use of MAD-Wi-Fi driver tools [30].

Other studies on detecting CS attacks that exploits the asymmetry detection methodology are given in [6] and [31]. The authors use several passive sniffer devices

across the networks to estimate the interference levels and identify the asymmetry in the case of abnormal CS behavior among the node pairs. The confidence of the detecting misbehavior nodes is increased with the help of multiple witnesses- to eliminate one decision related false positives- node structure. The performance evaluation results show that the system has good detection ability in the case of CS attacks.

Considering given detection studies, a reader can be easily convinced on the detection capabilities of either method, which are pretty easy to implement as they have any requirements that could cause overheads, extra protocols or implementation difficulties.

To the best of our knowledge, there is barely any study on the counter measuring against this type of physical carrier sensing attacks, although they can cause severe degradation on the performances of the networks.

Channel and Frequency Hopping against jamming in WLANs:

It is worth noting that there is a small difference between a normal jamming and physical carrier sensing attacks. In any type of a normal jamming attack, a transmitter device sends signals out regardless of DCF, channel sensing, and acknowledgment mechanisms, in other words, the transmitter fills the spectrum without blanking. Whereas, with the CST attacks, we imply the attack that can be created by manipulating only the CST parameter of a normal WLAN device. Hence, the attacker devices follow the normal DCF procedure as the normal devices except for having high CST threshold when they attempt to access the channels.

In this context, despite that there is no straightforward study on preventing the CST attacks, some studies exist that aim to mitigate the effect of the classic jamming attacks in WLANs by the channel and frequency hopping. If we can group these hopping methods, by their working mechanisms, into two, one is the proactive hopping and the other is the reactive hopping.

With the proactive frequency or channel hopping, we are implying that the nodes periodically switch the pre-determined channels. In [36], and [37], the authors try to model the interaction between a jammer and a communication link employing frequency hopping. They make use of proactive frequency hopping scheme and

quantify its efficiency. Nevertheless, their results demonstrates that such frequency hopping mechanism is inadequate in coping with jamming attacks in current 802.11 networks.

Similarly, the authors in [33] proposes a novel proactive channel hopping scheme which provides a signal strength based channel number generation. Their results show that the probability of an agreement on the same channel without negotiation is very high. However, with such a mechanism, the detection of jamming and activating channel hopping is remained open, which potentially can cause significant delay or packet losses due to lack of coordination.

Navda *et al.* [34] uses a pseudo-random channel sequence to accomplish a proactive channel hopping against jamming attacks. They assume that the generated channel sequence is known only by the APs and legitimate clients by sharing encrypted messages. However, their mechanism is not suitable for dynamic networks such as public Wi-Fi, in which clients are changing frequently. In such networks, some clients won't have the sequence, hence will remain silent or lost in the presence of a jammer.

On the contrary, in reactive hopping, a node tries to switch to another frequency or channel when it detects the presence of a jammer. When one member of a network, e.g., a master node, decides to switch a new channel, the other nodes obey the decision and take the corresponding action after receiving an informative event message.

Hu et al [38], apply a new reactive channel changing strategy in sensor networks. The networks determine a channel to switch prior to detection of any type of jamming attacks. It can be considered as a safe zone in the case of attacks. Then, with the detection of a jamming attack, the master nodes start to switch channels without having coordination among them. The remaining network nodes are switching upon not hearing or have connection loss with the paired nodes for a long period of time. However, this strategy brings the cost of some other problems besides the evading jamming effect which are synchronization , loss of packets and latency issues.

In [35], the authors propose two reactive strategies to evade the jamming attack; channel surfing and spatial retreats. In channel surfing, they provide different algorithms for paired networks, infrastructure networks, and AdHoc networks. At first glance, their mechanism for infrastructure networks seems designed so as to cover

common circumstances such as hidden or exposed nodes in case of jamming. However, the mechanism also requires implementation in all devices within legitimate networks. And the coordination among the networks are not comprehensively considered, this may result in having a considerable loss or huge delays.

The aforementioned studies with regard to the channel hopping strategy point out a need in the coordination. One another observation is that they all require implementing the algorithms on both the APs and STAs which would make them impractical and very costly when considering hundreds of different client model to modify.

Based on these facts, in this study, we use the existed coordination frameworks and our system will require modifications only in the APs, which then will distribute the channel hopping information across the network. As a result of this, our proposed scheme is expected to reduce the cost of applicability.

4.3 Analysis of Collision Probability

In this section, we will investigate the effects on the packet collision probabilities in the case that a network is exposed to a jamming attack. In a given 802.11 network, according to Bianchi *et al.*, [8], the probability of a transmission of a device for a given slot time can be approximately computed by the following

$$\tau = \frac{2(1-p)}{(1-2p)(W_0+1) + pW_0(1-2(p)^m)}. \quad (4.1)$$

,where p represents the probability of collision, and W_0 is the maximum contention window. This model is derived by using a discrete time Markov chain model. On the basis of this model and derivation, the same authors have provided the collision probability model as,

$$p = 1 - (1 - \tau)^{N-1}. \quad (4.2)$$

where, N is the number of active STAs in the network. These models assume that all the STAs are in the carrier sense range of each other and have independent p regardless of the channel status. In the hidden node case, since the packet collisions do not have direct effects on the DCF working mechanism of the transmitters, it is stated in [39]

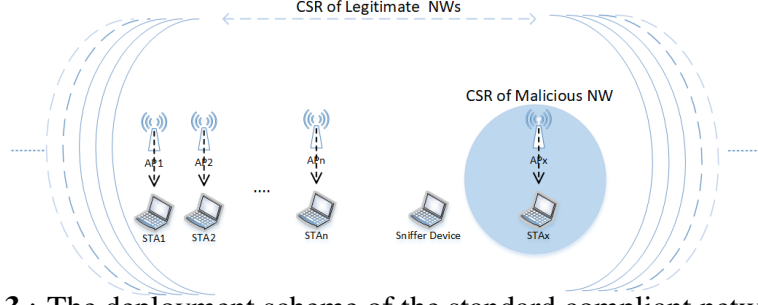


Figure 4.3 : The deployment scheme of the standard compliant networks and a misbehaving network for the analysis of collision probabilities

that the computation of transmission probabilities of STAs will be the same. Instead, the model of the packet collision calculations should be changed in order to consider the effect of hidden nodes. The authors in [40] extend the collision model for the hidden node scenarios as follows,

$$p = 1 - (1 - \tau)^{c-1} ((1 - \tau)^h)^k. \quad (4.3)$$

where, k is the average slot count decrement for the transmissions of hidden node. c and h represent the number of normal contending STAs and hidden STAs in the network, respectively. The value of k is correlated with τ and p as given by the following equation,

$$k = \frac{2 \frac{T_{succ}}{\sigma}}{1 + (1 - (1 - \tau)^n) (\frac{T_{col}}{\sigma}) + n\tau(1 - p) (\frac{T_{succ}}{\sigma} - \frac{T_{col}}{\sigma})}. \quad (4.4)$$

where, T_{succ} is the duration of a transmission is achieved and, T_{col} represents the time spent due to a collision. In addition, σ and, n demonstrate the idle slot time duration and, number of STAs, respectively.

In order to investigate the effect of a CCA attacker on packet collisions, we create a multi-user network deployment as depicted by Figure 4.3. In the setup, there are multiple numbers of standard-compliant AP-STA pairs, which have up-link saturated traffic and are deployed in the vicinity of each other. Furthermore, an attacker network is modeled just by increasing the CST of one of the AP-STA pairs which will act like an attacker. A sniffer device is located in the middle of the attacker and normal network devices in order to sense both sides in an approximate received power.

To validate the ns-3 simulator in terms of packet collisions and DCF performance, the collision probability results are compared with the mathematical model computation

provided above. In the appendix 1.1, the related code parts for both computations are given.

Figure 4.4, and Figure 4.5 represent comparative collision probability results for a high and low number of STAs, respectively. When we examine the results together for both figure, there is a small difference between Bianchi's collision model and simulator's results for the default case. Thus, it can be concluded that the simulator's DCF model performs at acceptable levels.

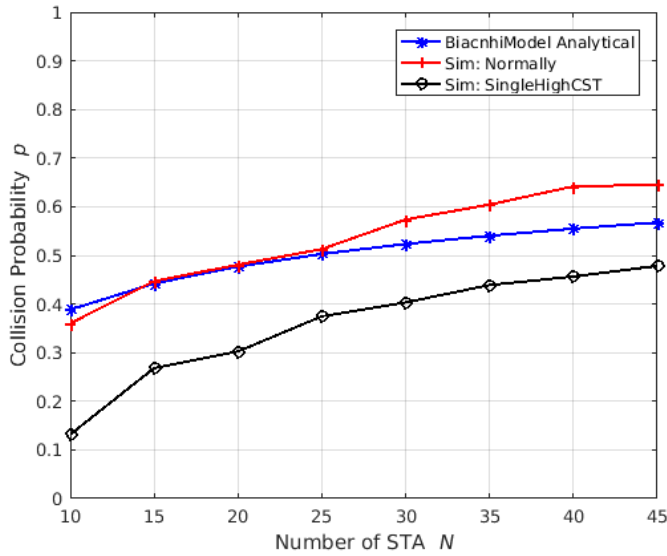


Figure 4.4 : Collision probability results for the mathematical model, simulation default and under jamming attack cases versus high number of active STAs

Let's examine the collision probabilities in the case of jamming attack. We know that in the presence of an attacker since the medium will always be filled with the attacker, all the transmissions within the network will be significantly reduced or suppressed. In addition, when a receiver device locks on an incoming PPDU at a given time, the new packets that come afterward will likely to be ignored or has no effect on the reception of current packet unless the frame capturing mechanism is not activated. A sample DCF back-off explanation scheme is depicted by Figure 4.6, which clearly indicate a packet collision situation in the presence of a jammer.

In the presence of a selfish network, since the normal STAs will sense and defer their transmissions in the majority of the time, the number of packet collisions during channel accesses are expected to be reduced. In other words, in such a case, even the collision probabilities are reduced, the throughput is significantly decreased due to

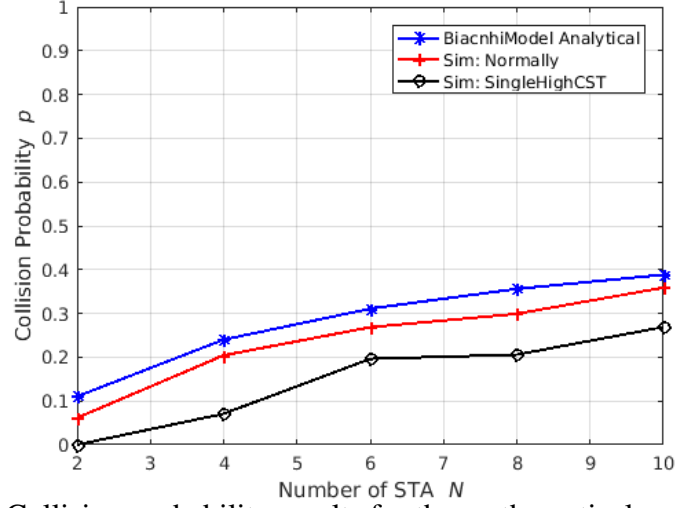


Figure 4.5 : Collision probability results for the mathematical model, simulation default and under attack versus low number of active STAs

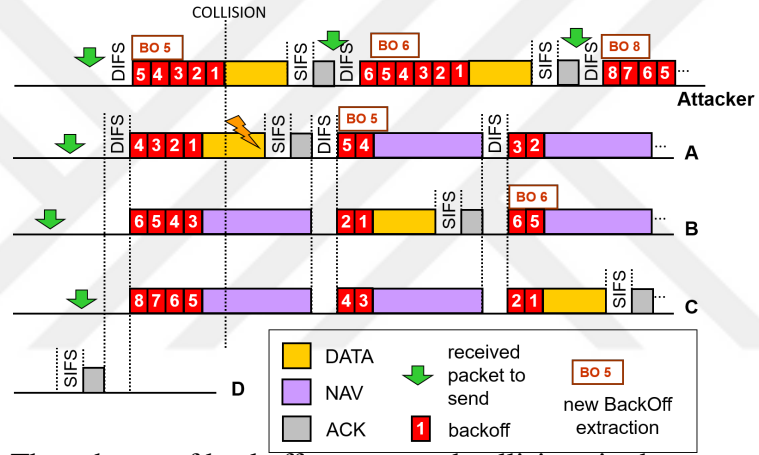


Figure 4.6 : The scheme of backoff process and collisions in the presence of a carrier sense attacker.

channel unavailability with the static carrier sensing mechanism of CSMA-CA. When we compare the collision probability results of the under jamming case with that of the normal case, which is also represented in Figure 4.4, and Figure 4.5, a decrease in the collision probability can be observed that meet with our expectations.

4.4 Impact of CCA Tuning on WLANS

In this section, we will investigate the impact of CST tuning on WLANs. The successful reception of Wi-Fi packets depends on the SINR levels for a particular modulation and coding index(MCS), S_{0m} .

The main logic behind the popular rate control algorithms, e.g., Minstrel, is to decrease or increase the MCS of the transmitter according to the packet error rates which indeed

depend on SINR, as explained in above, [41]. Therefore, by applying high CST and high interference to standard compliant STAs, we expect to observe low MCS and low throughput results besides having an enormous number of packet errors.

Let's evaluate the aforementioned interference impact within a two network setup as depicted in Figure 4.7. In the setup, the CST levels of each device are set to -65 dB which is a very high value to sense others transmissions but sufficient to sense their destined devices.

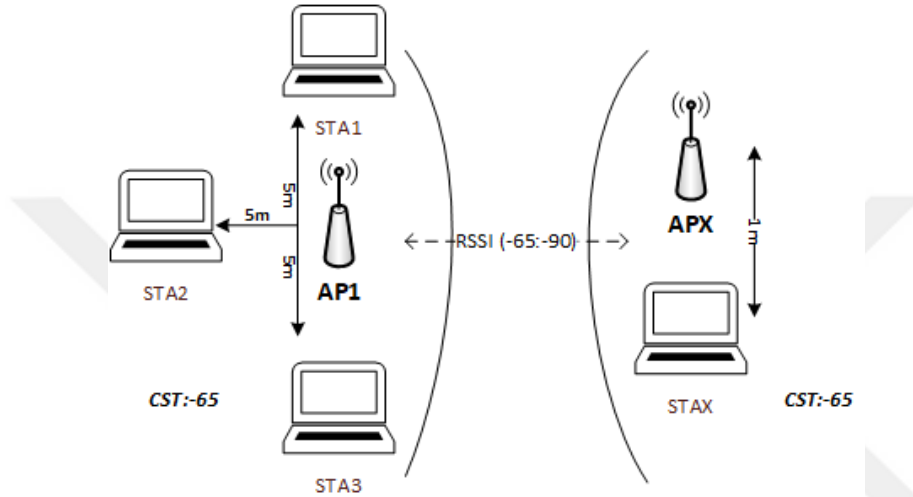


Figure 4.7 : The deployments of two high interfere networks

The two networks are clustered and located so that the reciprocal interference level to each other be changed each time. Since the networks will become blind to each other transmissions, the transmissions are neglecting the channel sensing and, hence simultaneous transmissions of adjacent networks will occur.

The important point is that since the networks can only sense their legitimate traffic, the adjacent network's transmissions will reflect as noise, which causes having a decrease in SINR levels. Furthermore, in order to evaluate the SR efficiency against attacker behavior, we deployed the APx and STAx in a close proximity. By this way, the second network will act as jammer since the SINR levels of them will be very high, which causes a little packet transmission errors and allows to use of high mcs values.

The results of CST impact evaluations are given in Figure 4.8. At first glance, the behavior of AP_x , STA_x pair seems expected, i.e., is not affected from the interference of adjacent, acting like a jammer. When the first legitimate networks' performances

examined, one can observe that the network performances are recovered as the received noise or RSSI level from the adjacent are decreased.

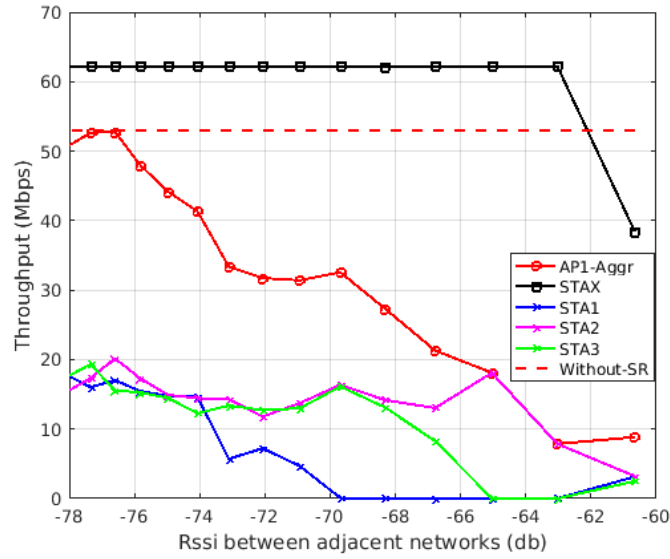


Figure 4.8 : Throughput vs adjacent network RSSI for two interfere networks when UDP uplink traffic is used.

At high interference levels, such as -60 to -70 dBm, the legitimate network has nearly half or worse throughput performance of its original capacity. In addition, it is clear that at the -76 dBm, the network can reach the original capacity. Given these observations, it can be concluded that using an SR technique in struggling with jamming attacks would be very beneficial if and only if the interference levels from the attacker are at the low levels, such as -76 dBm for this scenario.

4.5 Modelling a CCA Attacker Network and Its Effect on WLANs

Throughout the study, we propose the methods with emphasis on being easy-to-implement and practical which increases their implementation in real deployments. In this manner, we have modeled a selfish CCA tuning network which acts as a jamming attacker. In order not to make it more complicated in practice, we assume that the selfish manipulated devices will only modify a single parameter which is the CST.

In [5], the authors create an attacker device as manipulating the CCA threshold of a single device. And they also modify the ack mechanisms so that the transmitter continuously send traffic as a jammer. Modifying the mac-layer rule of working will make the system unpractical to observe in real deployments. Furthermore, since

the selfish devices are needed to associate the targeted AP, their modeling is quite vulnerable to blacklisting or de-associating by the APs upon detection.

Considering the aforementioned vulnerabilities and impracticality issues, we design a different CCA attacker network model that is composed of an AP-STA pair which have a very high CST threshold so that can sense only each other. This means that the attacker network pair can always transmit their packets in each slot regardless of the ongoing transmissions on the same channel. Moreover, since the selfish network uses normal DCF with high CST, the rule of channel access will be the same, indeed. In other words, the attacker will go into a random back-off process while transmitting their packets. The difference with the standard compliant devices is that the attacker devices will not freeze their back-offs due to not sensing which will let the attacker access the channel much more frequently than the normal standard compliant devices.

In order to cause a severe degradation, we assume that the attacker network devices selects the same BSS color with the color of the targeted network. Otherwise, the potential effect of an attacker on the targeted networks can be at negligible levels, since they will sense the attacker signals as OBSS and eventually can ignore the selfish network transmissions unless they are in very close proximity.

In addition to this, we make some essential assumptions while modeling the attacker. First, the attacker network will always have a static very high CST and saturated traffic. Secondly, the attacker network can not dynamically adapt itself or re-scan the environment. In other words, once these devices are placed, they assumed to work for long hours with the initially configured parameters. It is worth noting that, these assumptions are not far from reality, since that an easily manipulated device pair can be placed in a crowded public network for a couple of days.

Let's discuss the potential effects on the targeted networks. Since the attacker network saturates the channel by sending full buffer traffic, the target network devices will mostly sense the channel as busy and thus defer their transmissions. This deferring process will continue until they access the channel. Thus, the obtained throughput of these networks is expected to be significantly degraded in the case of a carrier sensing attack.

In terms of collisions, we know that once a receiver locks on an incoming PLCP header, the later incoming packets will be ignored at reception layer. Therefore, the probability of collision of packets will be at normal levels as mentioned in detail in the above section.

4.6 The Proposed Countermeasure Algorithm

In this section, we will provide two novel counter measuring mechanism, which will be used by the selective decision of our counter-measuring strategy. In the most of the previous jamming studies, the issue of channel saturation in ultra-dense networks are not considered or evaluated in deep.

The importance of being aware of the channel saturation over the adjacent networks in dense networks can be deduced from the upcoming and developing 11ax standard, which especially emphasizes and develops new mechanisms on the improving spatial reuses. Furthermore, one can come up from the current survey and development tendency that the channels will be more saturated in dense networks because of the explosive growth in Wi-Fi usages. Thus, we follow a conservative approach on the use of channel hopping solution in coping with jamming attacks.

On the other hand, after working through the 11ax v3 draft, we noticed that there could be a potential solution in the view of PHY layer actions, that is BSS Coloring and Spatial reuses. It is worth noting that, apart from these two mechanisms (channel hopping and Spatial reuse), there is no way to take action against PHY layer misbehaviour like jamming. The details of the BSS coloring and OBSS_PD mechanism are already given in the Chapter 2.

To the best of our knowledge, this is the first study proposing a two-way counter-measuring strategy, which additionally considers the potential challenges or inefficiencies of the ultra-dense deployments. We follow a novel strategy rather than doing only the action of channel hopping in coping with a jammer.

The selection strategy of usage of either method is designed by considering many aspects in addition to the common challenges of dense networks. In the next subsections, we will explain the working principles of the modules in detail.

4.6.1 Selection of counter-measure technique

As alluded earlier, since the channel densities in ultra-dense deployments are severe, the design approach of our counter-measuring strategy is shaped as avoiding the channel hopping as much as possible if any other methods are available and have advantages over the channel hopping.

However, as a result of spatial reuse performance investigations that is mentioned in chapter 2, the positive impact of spatial reuse can only be obtained under the condition of low interference among the networks. In other words, in the case of high interference, the use of BSS coloring and OBSS_PD will become insufficient in coping with jamming attacks. Thus, there should be a second mechanism that will rescue the network nevertheless of the interference level of the attacker. This is the main motivation behind our decision strategy.

Let's denote the cluster of STAs that are associated with the same AP and hence have the same BSS color c_i with $S_{j,ci} = \{S_{1,ci}, S_{2,ci}, \dots, S_{N,ci}\}$. And the RSSI levels of the attacker and the associated STAs at the AP side are $\mathcal{R}_A, \mathcal{R}_{S_{j,ci}}$, respectively. Then the following rules of decision on selecting the counter-measuring methodology is applied in the corresponding AP_{ci} as:

1. If the detected attacker is in the vicinity of the legitimate AP; Use Channel Switch:
In this case, there is no way to avoid the attacker's domination unless channel hopping.
2. If the detected attacker is sufficiently far from the central AP of the target BSS, and the majority of the STAs; Use BSS color change technique.

Let's further elaborate these in different aspects. Due to the nature of WLANs, we can not estimate the locations of any STA in a network without an extra protocol that communicates among STAs. Therefore, we can only follow a circular approach at the AP side. In the case of the close proximity of jammer, or $\mathcal{R}_A > \eta$, where η is the tolerable RSSI level for spatial reuse operations, the affected AP_{ci} and $S_{j,ci}$ will mostly sense the channel as busy, which means that almost any uplink or downlink traffic will barely work.

In considering the hidden or exposed node situations in the close proximity case, if we look at the AP_{ci} 's point of view, it's neither hidden nor exposed with the attacker, since the attacker is in the vicinity of AP_{ci} . On the other hand, the situations can be evaluated differently for the STAs perspective. When $\mathcal{R}_{S_{j,ci}} < \mathcal{R}_A$ or $\mathcal{R}_{S_{j,ci}} > \mathcal{R}_A$, the estimation of being in the jammer's transmission range is not possible, due to the Omni propagation of the wireless signals. Thus, we can not detect the STAs remains hidden in the presence of a jammer. This possibility of becoming hidden STA can severely affect mostly the up-link traffic since the transmitted packets will mostly collide within the AP side, which generally sense the channel busy due to the attackers' transmissions.

When the detected attacker is far from the central AP, or $\mathcal{R}_A < \eta$, two cases arise according to the location of the associated STAs. In the first case that the average normalized RSSI of STAs is bigger than the RSSI of an attacker, $\mathcal{R}_{S_{j,ci}} > \mathcal{R}_A$, the AP can decide to utilize the spatial reuse mechanism, due to the low interference impact. On the other hand, when $\mathcal{R}_{S_{j,ci}} < \mathcal{R}_A$, the risk of being exposed of the majority of STAs becomes considerable, which means that we could not benefit from the spatial reuse gains. The pseudo code of the decision logic at the AP is given in Algorithm 2.

The motivation of using spatial reuse in coping with a jammer is to provide a secure gap to heal the network performance of the targeted BSS. By means of a secure gap, we are implying that keeping the majority of associated STAs connected in the same BSS while changing BSS Color.

The value of η requires much more analysis to cover all the situations in a general deployed WLAN network. Therefore, its value will be comprehensively computed as the future work study. Nevertheless, having acquired the basic understandings as a result of the experimental studies in 4.4, we can estimate a sufficient value of η for the networks that are closely deployed and thus have relatively high SINR values. Given these observations, we can pick the value of η approximately as -77 dBm that would be sufficient to heal the network performances if the average RSSI levels of STAs are satisfactorily good.

Algorithm 2 Selection of the Counter-Measure method

```
1: procedure
2:   When an attack is detected
3:   Listen the channel 100ms
4:   Get average  $\mathcal{R}_{S_{j,ci}}, \mathcal{R}_A$ 
5:   if  $\mathcal{R}_A > \eta$  then
6:     Use Channel Hopping Mechanism
7:   else if  $\mathcal{R}_A < \eta$  &&  $\mathcal{R}_{S_{j,ci}} > \mathcal{R}_A$  then
8:     Use BSS Color Change Mechanism
9:   end if
10: end procedure
```

4.6.2 Counter-measure with coordinated channel switching

As a most common solution in dealing with a jamming type of attack, the channel hopping method can be considered not the best way in terms of performance, but the most secure way regardless of the condition. While this is true that, there are some important issues in channel hopping that can designate the level of performance improvements. These are the channel searching, channel selection, and channel hopping operations.

Channel Searching:

Channel searching can be done in either proactively or re-actively. Different from the channel hopping studies ([33]- [38]), which generally take the channel searching and channel hopping operations as a whole in defining either proactive or reactive, we will separate these, and evaluate them independently. In other words, in our proposed structure, while the channel searching is proactive, the channel hopping operation can be either proactive or reactive.

In case of the jamming attack, another important performance evaluation metric is the delays of legitimated traffic. Therefore, one of the objective with channel searching is to provide an environment with less delay while coping with the attack.

In order to reduce the delayed sum while doing channel hopping operation, in this paper, we are proposing that using a proactive channel searching in the originator AP could be more efficient than the reactive channel searching. In proactive channel searching, the AP periodically listen for t_1 milliseconds each channel and returns the

less saturated channel. The AP will do this channel searching once every t_2 minute. In our case evaluations, we take its value as 30 minutes that would be a tolerable period value to stop the traffic and listen to the other channels along with some hundred milliseconds.

In real deployments, the period of this channel searching intervals becomes very important, since there can be delay intolerant traffic types such as voice or video. If the period of channel searching interval is taken short, say 1 minute, then the active traffics will be interrupted frequently, which will result in vastly suffering from STAs. On the other hand, having a long period, say 12 hours, would cause to having wrong estimations since the channel activity conditions would change more frequently. Thus, a balance in the assigning the value of this period should be considered.

The method of founding the best available channel in terms of saturation is out of this work. However, in this work, to evaluate the proposed mechanisms, we make the system to simply decide on the channel that has minimum channel usage.

Reactive Channel Hopping operation when detecting a jammer:

After the decision on the usage of channel hopping as the counter-measuring, the system immediately fills and send the CSA field in sent beacons. As explained in section 4.2, the Channel Switch Mode is set to true and the new channel number is written. One issue that remains open with channel hopping is the coordination of channel switching. The coordination of channel switching should be considered in order not to interrupt the traffics for a long time. Some priory studies especially emphasize and address the importance of this issue, [42], [43], [44].

We simply utilize from the Channel Switch Countdown, CSC_1 , field to coordinate all the APs and STAs within negligible delays. When the system decides on using Channel Hopping mechanism, the CSC_1 value is set in the related field of beacon and is decreased one by the time that each sequential beacon messages are sent. This decrements process continues until the CSC_1 value reaches zero. Once the CSC_1 comes to zero, the AP immediately changes the channel after sending the last beacon that contains the CSC_1 value that equals to zero. The process is demonstrated by Algorithm 3.

Algorithm 3 Coordinated Chanel Hopping at AP

```
1: procedure
2:   Listen  $t_1$  ms channels every  $t_2$ 
3:   Search and Select a new channel
4: loop
5:   if Channel Hopping decision then
6:     Set the Channel Switch Mode
7:     Update the new channel
8:     Initialize the  $CSC_1$ 
9:     while  $CSC_1 \neq 0$  do
10:      Update  $CSC_1$  in the beacon
11:       $CSC_1 \leftarrow CSC_1 - 1$ 
12:    end while
13:    if  $CSC_1 = 0$  then
14:      Update  $CSC_1$  in the beacon
15:      Change the current channel
16:    end if
17:  end if
18: goto loop.
19: end procedure
```

The initial value of this counter will play a significant role when changing the channel in the absence of a jammer. A low value, as 1, would cause to have a risky channel hopping for the AP point of view, since when an AP transmits beacons to the wireless channel, there is a potential that the beacon can collide with the jammers packets. Therefore, STAs can sometimes miss beacons, which would end up with non-coordinated channel hopping. Contrarily, having a very high value, say 30, will give the system too much delay to change the channel which can increase the level of suffering in case of attack. Briefly speaking, it's valued should be in a suitable range that will provide fast and secure coordination in channel changing. Moreover, the impact and computation of its value will be studied as future work.

In this study, to the ease of performance comparison, we take its value as 7 for the rest of the experiments. By selecting its value, since the beacon interval is 100ms in general, we expect to observe the coordinated channel hopping operations across the network after approximately 700ms.

Let's look at the STAs' point of view. In the STA_{ci} , the beacon packets are received and the CSA element field is extracted from these. When the CSA mode field is detected as enabled, the corresponding STA controls the CSC_1 field of the CSA element. If the

CSC_1 is read as zero, then the STA_{ci} will immediately change their channel to the new channel that is found in the related field of CSA element. This process is given by Algorithm 4. Otherwise, it realizes the planned channel hopping operation but waits until the CSC_1 is read as zero.

Algorithm 4 Coordinated Chanel Hopping at STA

```

1: procedure
2:   Receive Beacons
3:   if CSA is enabled then
4:     Read  $CSC_1$ 
5:     Read the new Channel
6:     if  $CSC_1 = 0$  then
7:       Switch to the new channel
8:     end if
9:   end if
10: end procedure

```

4.6.3 Counter-measure with coordinated BSS color change

The decision on channel hopping as proposed in the above section is not a preferred action due to density and hence saturation of the spectrum. In other words, since the number of orthogonal channels are very limited in both 2.4 GHz and 5GHz bands, all the channels will eventually be overloaded or saturated. Moreover, this saturation problem becomes more severe especially in the 2.4GHz bands, since there are only 3 non-overlapping channels.

A break-through idea at this point would be the utilization of the upcoming 11ax features. Regarding the spatial reuse issue, as it is mentioned in Chapter 2, the new standard brings the BSS coloring mechanisms which will be used in increasing spatial reuses with the use of OBSS_PD threshold.

In this paper, we propose a BSS color change (BCC) based counter-measure as an alternative to the channel hopping. Since the nature of the BSS coloring and OBSS_PD mechanism allows simultaneous transmissions for two adjacent BSS nodes or STAs, utilizing from this will significantly heal the degraded network performance in suitable conditions.

Similar to the coordinated channel hopping mechanism, in BSS Color Change, we follow a two-step approach which is proactive color searching and reactive color changing.

Proactive Color Searching In order to reduce the delay and STA performance, the system will proactively search for the best suitable color around it. Moreover, the system logic will be almost the same as the proactive channel search. The only difference is that, since the BSS color change operation is intended for the current channel, the system will only listen to the current operating channel for a short period of time, e.g. 10ms.

There are no extensive studies on the BSS color allocation schemes for the 11ax networks. By intuitive thinking, we predict that there will be unused BSS colors across the networks since there are 64 different colors which can be used for each of different BSS clusters. Therefore, for the evaluation of the BSS color changing, the system will simply decide on one of the unused colors that are founded within the current channel.

Reactive Color Change in the presence of an interference source

When the system is decided on the usage of BSS Color change mechanism, the corresponding AP immediately places the related fields of the BCC element in the following beacon messages. In detail speaking, the color change countdown and the new color is embedded into the beacons. The decrements of the initialized countdown and update process work the same as for the channel hopping. In other words, the countdown value is decremented by one and updated while sending beacons until it reaches zero. After sending the last beacon, the AP will immediately change its current color with the new published color. The pseudo code of this explained mechanism is given in Algorithm 5.

The color change operation in the STA side is very simple and applicable. Since the standard includes the BCC functionality, all the standard compliant STAs will obey decision on the change of color when the received countdown reaches zero. This pre-defined mechanism makes the system very practical in terms of integration and application of our proposed algorithm. The explained mechanism for the compliant STAs works as given by the Algorithm 6.

Algorithm 5 Coordinated BSS Color Change at AP

```
1: procedure
2:   Listen  $t_1$  ms channels every  $t_2$ 
3:   Decide on the new BSS color
4:   loop
5:     if BSS Color Change decision then
6:       Set the New BSS Color
7:       Initialize the  $CSC_2$ 
8:       while  $CSC_2 \neq 0$  do
9:         Update  $CSC_2$  in the beacon
10:         $CSC_2 \leftarrow CSC_2 - 1$ 
11:      end while
12:      if  $CSC_2 = 0$  then
13:        Update  $CSC_2$  in the beacon
14:        Change the BSS color
15:      end if
16:    end if
17:  goto loop.
18: end procedure
```

Algorithm 6 Coordinated BSS Color Change at STA

```
1: procedure
2:   Receive Beacons
3:   if BCC is enabled then
4:     Read  $CSC_2$ 
5:     Read the new BSS color
6:     if  $CSC_2 = 0$  then
7:       Change the BSS color
8:     end if
9:   end if
10: end procedure
```

It is worth noting that, once we sending these change messages by beacons, a remarkable question arises as that what if the attacker network sense and take the corresponding action, e.g., color changing? The answer would be that since the manipulated devices are modeled so as to do not sense and decode the legitimate traffic' packets, the beacons, and thus the related change information fields will not be detected by the attacker devices. This issue is extensively addressed in [5].

4.7 Evaluation of the Proposed Counter-Measure Mechanisms

In this section, we evaluate the proposed counter measuring strategies in a comparative manner. Because of the unavailability of any 11ax capable devices that support the

current planned 11ax SR features, we used the network simulator (ns-3), [12], which is a discrete event-driven simulator thus allow simulating the behavior of dense networks. Though, the current version of simulator (ns3.29) does not support the last standard. To overcome this, we have extended the modules of the simulation platform so as to support the IEEE 11ax standard. The implementation process and working mechanism of the features are explained in detail in Chapter 2.

4.7.1 Implementation of the used functionalities

Another miscellaneous issue is the implementation of the CSA and BSS color change elements in the beacon messages. We have implemented these functionalities as defined in the standard. The patch code for ns-3.29 can be found in [13]. By the mechanisms, each AP device is capable of adding the related elements while creating beacon packets. Besides this, each STA in the system is made capable of extract and read of the related functional element information upon reception of a beacon. The notion of actions can be visible by using Wireshark [45]. Figure 4.9 shows the default mode of a CSA element frame which can be found under the tagging information section of a beacon packet. To test these newly implemented features, we have activated the CSA and BSS color with randomly selected parameters. Figure 4.10 and 4.11 show the pcap screenshot of the countdown values at the STA sides. These figures prove out that the functions work as desired. On the other hand, Wireshark does not include the corresponding packet dissector for the new BSS Color Change element. Therefore, to test the BSS Color Change element, we have used the same Element ID as that of for CSA mechanism, 35. Figure 4.12 demonstrates the duplicated tag of the CSA elements in which, the second field actually reserved for the information fields of the new added BSS color Change announcement element. In brief, all these pcap screen views prove that the new functionalities work proper.

4.7.2 Performance evaluations

In order to make visible the performance of either proposed strategy in the case of an attack, we have exploited the reference enterprise network scenario, which is immensely described in the Tgax simulation scenarios document, [2]. We create a simplified version of this reference scenario which is depicted by Figure 4.13. The

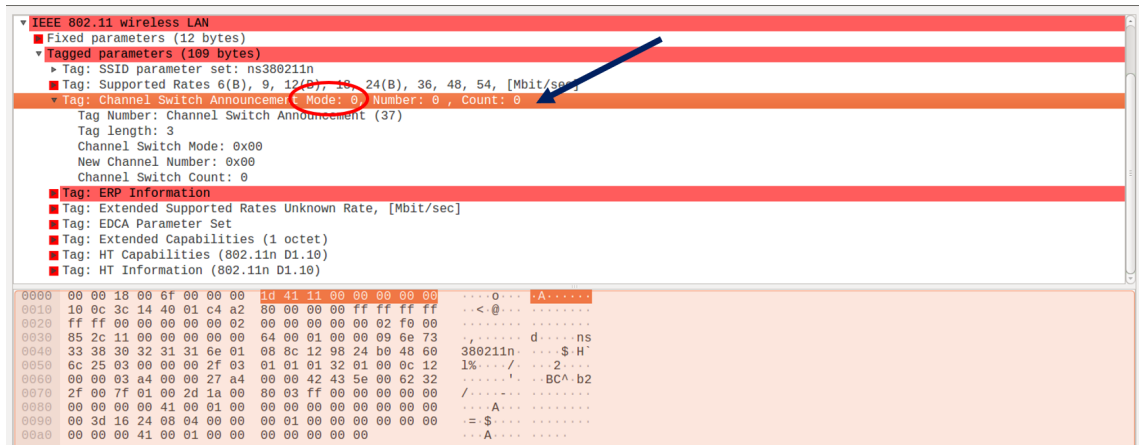


Figure 4.9 : The CSA element view in beacons, where CSA mode is disabled by default

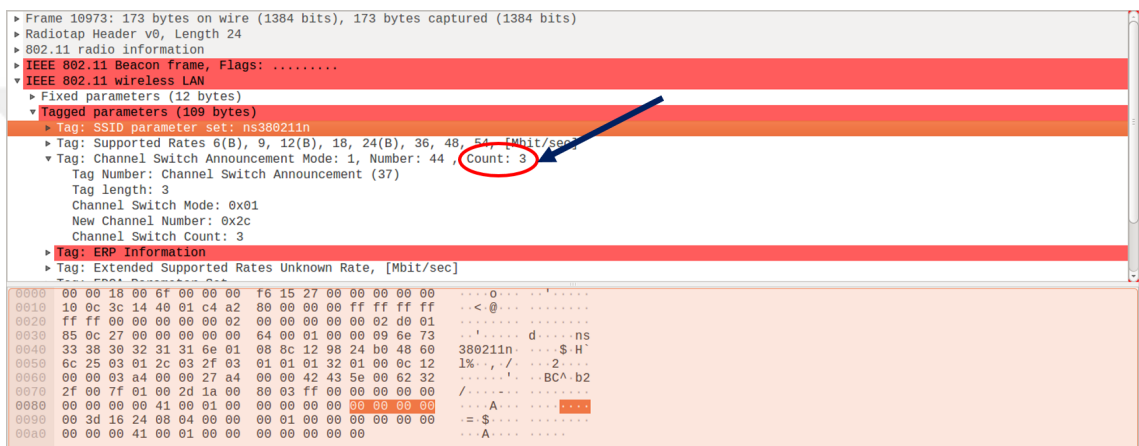


Figure 4.10 : The CSA element view in beacons, where CSC equals to 3

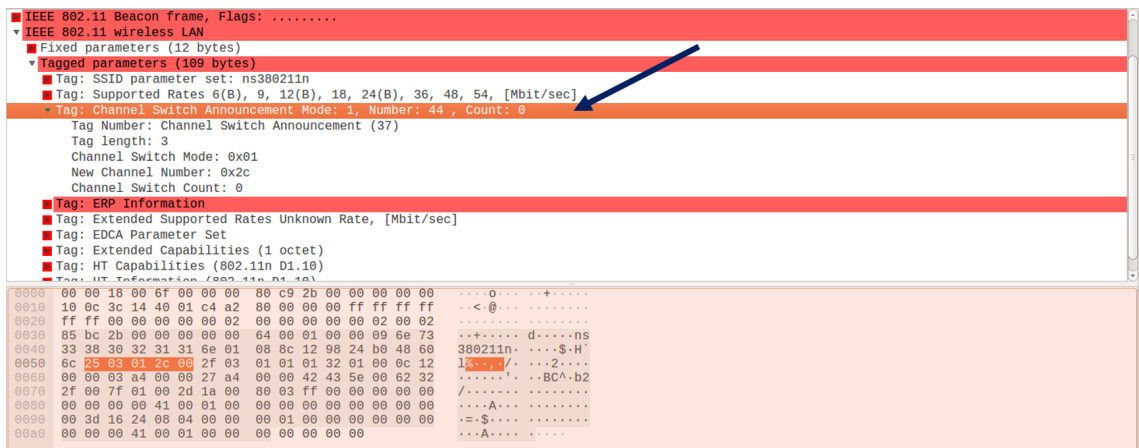


Figure 4.11 : The CSA element view in beacons, where CSC equals to zero, which imply that immediate channel switch operation

deployment consists of 4 AP and their associated clients. Each AP has 4 STA and each STA is located within different sub-square boxes that are surrounding the APs. Furthermore, we have used only UDP up-link traffic with saturated offered loads. The traffic is generated by the use of CBR that creates data packets with regular intervals. The simulation parameter details are given in Table 4.1.

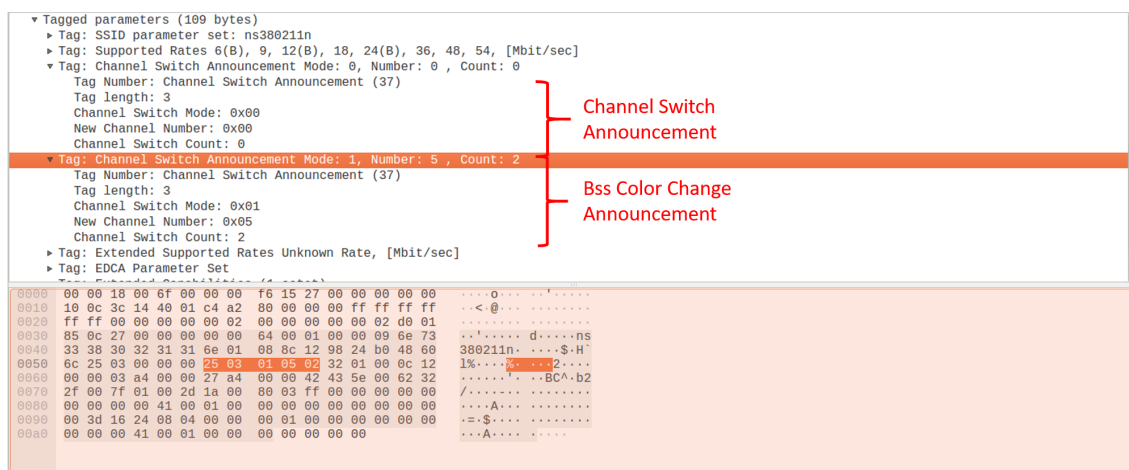
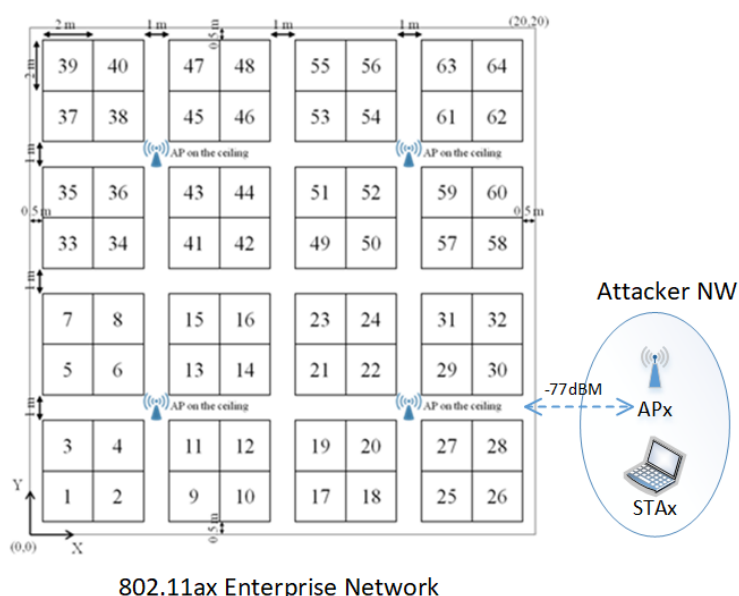


Figure 4.12 : The view of BSS Color Change elements in beacons



802.11ax Enterprise Network

Figure 4.13 : Enterprise networks deployment with the presence of an attacker

In addition to these, on the basis of reference scenario, the operation channels of the APs are assigned as 1,6,11 and 1 for the AP1, AP2, AP3 and, AP4 in 2.4 GHz bands, respectively. Besides this, the BSS colors of each BSS within the single room is differently allocated.

After creating the aforementioned setup in the simulation platform, we place an AP-STA paired attacker network in the proximity of BSS 2. The heard RSSI level of the attacker at AP2 is arranged as to be -77 dBm. This value allows the system to decide on the selection of BSS color change technique while using the proposed counter measuring strategy. Note here that, we assume that, the attacker network can initially set its BSS color to the targeted BSS' color, which is color 2 in our case.

Table 4.1 : Simulation parameters for the countermeasure performance experiments.

Simulation Parameters			
Simulator version	ns-3.29	Transmit Power	16 dBm
Mobility Model	Constant Position	Traffic Generator	On-Off generator
Channel Model	SpectrumWi-Fi	PHY Model	Spectrum Wi-FiPhy
Channel Nums	1,6,11 (20 MHz)	Aggregation	A-MSDU enabled
Wi-Fi phy std	802.11n_2.4GHz	RTS-CTS	disabled
Rate Manager	Minstrel rate control	Payload size	1450 bytes
Offered Load	100 Mbps	Traffic Type	UDP Uplink

In our example simulation case, the attacker network is activated at 2s. Since we assume that the system can already detect the misbehavior nodes, the system is directly trying to take action after the attacker is activated. By the selection of initial countdown as 7, means 700ms, the system will change its BSS color or channel at 2.7 seconds.

The selection of a new channel or BSS color is out of the scope of this study. For this reason, we assume that the system selects channel 11, in a sense that channel 11 is less crowded than channel 1. And, the new BSS color is assumed to be selected as 8 in the aim of selecting a different color while avoiding BSS color collision with the other BSS colors.

Figure 4.14 demonstrates the throughput performance of the proposed strategy in the presence of an attacker. When we deep into the figure, at the 3s, the system significantly heals the network's performance with the use of BSS color change technique. Moreover, the achieved performance gain of this technique is very greater than the use of channel hopping technique. At this point, one would argue that the performance of the proposed techniques will mostly depend on the channel conditions. While this is true that, by the fact of dense deployment natures, the channels in 2.4 GHz will be mostly saturated or even can be worse than our case study, [46].

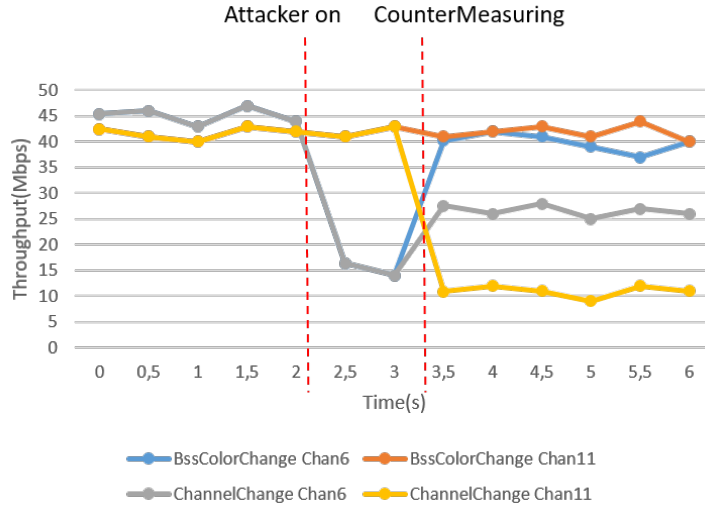


Figure 4.14 : Aggregate throughput change when the BSS color change and CSA methods are applied

The aggregate throughput results for the different cases is given by Figure 4.15. It can clearly be observed that the malicious network causes % 60 percent degradation in the throughput of the targeted BSS (BSS 2). As a result of applying the proposed countermeasures, the system can increase the throughput performance of the exposed network. The usage of BSS color change technique almost restores the throughput performance without disturbing other networks. On the other hand, despite the fact that the channel hopping technique heal the network performance a little, it degrades the destined channel's own capacity, and thus suffer the client within that channel. In other words, the technique is not suitable for dense network environments. Therefore, we can conclude that the use of BSS color change countermeasure is suggested if the interference level of the misbehaving nodes are satisfactorily low. Note that this part of the thesis is planned to be submitted in [47].

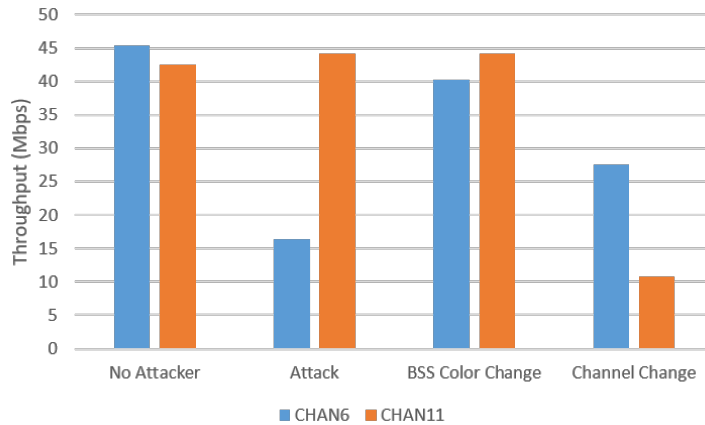


Figure 4.15 : Aggregate throughput results when the proposed countermeasure mechanisms are applied ($\mathcal{R}_A = -77dBm$).

5. CONCLUSIONS AND FUTURE WORK

In dense networks, due to the limited orthogonal channels in both 2.4 and 5GHz bands, the channels easily go into saturation, which turns into the suffering of the end users. Moreover, the classical Wi-Fi architecture is far from serving to the giant number of users that have a higher rate and low delay demands. Beyond it, the channel access mechanism of the CSMA-CA protocol causes a significant amount of packet collisions and redundant wait times with a high number of STAs. To resolve these problems and improve the end user experiences, the IEEE Tgax community have started developing the IEEE 11ax Next Generation Standard. There is two main revolutionary change by the new amendment. The first is the usage of OFDMA structure instead of OFDM. This feature promises to eliminate the overheads due to the channel contention process of the traditional Wi-Fi. The second is the new SR techniques that are developed to increase the capacity of the spectrum or spectrum reuses by allowing simultaneous transmissions among OBSS networks.

In this thesis we have worked on the followings: 1) The level of performance improvements by the new SR techniques of 11ax standards. 2) The impact of traditional carrier sensing in dense WLANs and designing an adaptive mechanism for legacy networks. 3) Developing a lightweight countermeasure scheme against the carrier sensing attackers that act as a jammer.

Note that the evaluations of all features and proposed algorithms are carried out in the ns-3 simulation tool. In this aim, the ns-3 is the extent to support the 11ax standards. Furthermore, the relevant functional elements of standards are added to the platform.

We can conclude the followings as a result of performance evaluations: 1) The new SR technique clearly brings significant performance gains in terms of throughput and average delays in dense deployments which meets with the promises of the new amendment. 2) The classical carrier sensing mechanism should be well tuned so that any of the network peripherals suffer due to unfairness problem. The proposed adaptive carrier sensing algorithm increases the aggregate throughput by as much

as 100 % while ensuring connectivity and fairness levels. 3) The new approach on the counter-measuring schemes performs very efficiently which can compensate the drawbacks of the classical channel hopping approach in struggling with the jamming kind of attacks. Moreover, by the use of existed functionalities, the system also provides coordination among the networks for the sake of operations.

As future work, we planned to conduct a comprehensive analysis of the potential effect of the new SR techniques. Moreover, the exact value of the key parameters of the PHY layer security part is planned to be determined considering general usage cases by detailed analyses. The analyses will be extended so as to include different traffic protocols and mixed flow directions which will allow us to have more accurate performance evaluations.

REFERENCES

- [1] **Selinis, I., Katsaros, K., Vahid, S. and Tafazolli, R.** (2018). Control OBSS/PD Sensitivity Threshold for IEEE 802.11 ax BSS Color, *IEEE PIMRC*, pp.1–7.
- [2] **S.Merlin,** <https://mentor.ieee.org/802.11/dcn/14/11-14-0980-16-00ax-simulation-scenarios.docx>, available on 30.04.2019.
- [3] **Selinis, I., Katsaros, K., Vahid, S. and Tafazolli, R.** (2017). Exploiting the capture effect on DSC and BSS color in dense IEEE 802.11 ax deployments, *WNS3*, pp.47–54.
- [4] **Afaqui, M.S., Garcia-Villegas, E., Lopez-Aguilera, E., Smith, G. and Camps, D.** (2015). Evaluation of dynamic sensitivity control algorithm for IEEE 802.11 ax, *IEEE WCNC*, pp.1060–1065.
- [5] **Pelechrinis, K., Yan, G., Eidenbenz, S. and Krishnamurthy, S.V.** (2012). Detection of selfish manipulation of carrier sensing in 802.11 networks, *IEEE Trans. on Mob. Comp.*, 11(7), 1086–1101.
- [6] **Paul, U., Kashyap, A., Maheshwari, R. and Das, S.R.** (2013). Passive measurement of interference in wifi networks with application in misbehavior detection, *IEEE Trans. on Mob. Comp.*, 12(3), 434–446.
- [7] **L. Hongkun, C.Y. and Chi, Z.** (2008). Multi-hop effective bandwidth based routing in multi-radio wireless mesh networks, *IEEE GLOBECOM 2008*, pp.1–5.
- [8] **Bianchi, G.** (2000). Performance analysis of the IEEE 802.11 distributed coordination function, *IEEE Journal on selected areas on comm.*, 18(3), 535–547.
- [9] **Qu, Q., Li, B., Yang, M., Yan, Z., Yang, A., Yu, J., Gan, M., Li, Y., Yang, X., Aboul-Magd, O. et al.** (2018). Survey and Performance Evaluation of the Upcoming Next Generation WLAN Standard-IEEE 802.11 ax, *arXiv preprint arXiv:1806.05908*.
- [10] **Omar, H.A., Abboud, K., Cheng, N., Malekshan, K.R., Gamage, A.T. and Zhuang, W.** (31 July 2018). IEEE Draft Standard for Information Technology – Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks – Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment Enhancements for High Efficiency WLAN, *IEEE P802.11ax/D3.0*, 1–682.

- [11] **url-1**, https://www.arubanetworks.com/assets/wp/WP_802.11AX.pdf, available on 30.04.2019.
- [12] **url-2**, https://www.arubanetworks.com/assets/wp/WP_802.11AX.pdf, available on 30.04.2019.
- [13] **url-3**, <https://github.com/omerft/ns3-11ax-SR.git>, available on 30.04.2019.
- [14] **J.Pang**, <https://mentor.ieee.org/802.11/dcn/14/11-14-1177-02-00ax-box5-calibration-discussion.pptx>, available on 30.04.2019.
- [15] **S.Kim**, <https://mentor.ieee.org/802.11/dcn/14/11-14-1392-01-00ax-simulation-results-for-box-5-calibration.pptx>, available on 30.04.2019.
- [16] **Baid, A. and Raychaudhuri, D.** (2015). Understanding channel selection dynamics in dense Wi-Fi networks, *IEEE Communications Magazine*, 53(1), 110–117.
- [17] **Afaqui, M.S., Garcia-Villegas, E. and Lopez-Aguilera, E.** (2017). IEEE 802.11ax: Challenges and requirements for future high efficiency WiFi, *IEEE Wireless Communications*, 24(3), 130–137.
- [18] **(To be submitted) Topal, O.F., Kurt, G.K. and Kuran, S.** (2019). A comprehensive evaluation on the new spatial reuse improvements of the IEEE 802.11ax standards: Does it really outperform the others?, *IEEE Vehicular Technology Magazine*.
- [19] (2016). IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, *IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012)*, 1–3534.
- [20] **Fu, L., Liew, S.C. and Huang, J.** (2013). Effective carrier sensing in CSMA networks under cumulative interference, *IEEE Trans. on Mob. Comp.*, 12(4), 748–760.
- [21] **Park, K.J., Choi, J., Hou, J.C., Hu, Y.C. and Lim, H.** (2011). Optimal physical carrier sense in wireless networks, *Elsevier Ad Hoc Networks*, 9(1), 16–27.
- [22] **Kim, S., Yoo, S., Yi, J., Son, Y. and Choi, S.** (2017). FACT: Fine-grained adaptation of carrier sense threshold in IEEE 802.11 wLANs, *IEEE Trans. on Vehic. Tech.*, 66(2), 1886–1891.
- [23] **Chau, C.K., Ho, I.W., Situ, Z., Liew, S.C. and Zhang, J.** (2017). Effective static and adaptive carrier sensing for dense wireless csma networks, *IEEE Trans. on Mob. Comp.*, 16(2), 355–366.
- [24] **Zhu, J., Guo, X., Yang, L.L. and Conner, W.S.** (2004). Leveraging spatial reuse in 802.11 mesh networks with enhanced physical carrier sensing, *IEEE Comm.*, volume 7, pp.4004–4011.

- [25] **Afaqui, M.S., Garcia-Villegas, E., Lopez-Aguilera, E. and Camps-Mur, D.** (2016). Dynamic sensitivity control of access points for IEEE 802.11 ax, *IEEE ICC*, pp.1–7.
- [26] **Haghani, E., Krishnan, M.N. and Zakhor, A.** (2010). Adaptive carrier-sensing for throughput improvement in IEEE 802.11 networks, *IEEE GLOBE-COM*, pp.1–6.
- [27] **Murakami, K., Ito, T. and Ishihara, S.** (2015). Improving the spatial reuse of IEEE 802.11 WLAN by adaptive carrier sense threshold of access points based on node positions, *IEEE ICMU*, pp.132–137.
- [28] **Saldana, J., Munilla, R., Eryigit, S., Topal, O., Ruiz-Mas, J., Fernández-Navajas, J. and Sequeira, L.** (2018). Unsticking the Wi-Fi client: Smarter decisions using a software defined wireless solution, *IEEE Access*, 6, 30917–30931.
- [29] **Topal, O.F., Kurt, G.K. and Soysal, A.** (2018). Adaptation of Carrier Sensing Threshold to Increase Throughput in Dense 802.11 ac Wireless Networks, *2018 Global Information Infrastructure and Networking Symposium (GIIS)*, IEEE, pp.1–6.
- [30] **url-4**, <http://madwifi-project.org>, available on 30.04.2019.
- [31] **Paul, U., Das, S.R. and Maheshwari, R.** (2010). Detecting selfish carrier-sense behavior in WiFi networks by passive monitoring, *IEEE DSN*, pp.11–20.
- [32] **Thorpe, C. and Murphy, L.** (2014). A survey of adaptive carrier sensing mechanisms for IEEE 802.11 wireless networks, *IEEE Communications Surveys & Tutorials*, 16(3), 1266–1293.
- [33] **D.Sirojiddin, C. Jin-Ghoo, S.K.S. and Yeob, N.** (2017). Channel hopping scheme to mitigate jamming attacks in wireless LANs, *EURASIP Journal on Wireless Comm. and Networking*, 2017(1), 11.
- [34] **N. Vishnu, B. Aniruddha, G. and Dan, R.** (2007). Using channel hopping to increase 802.11 resilience to jamming attacks, *IEEE INFOCOM 2007*, IEEE, pp.2526–2530.
- [35] **W. Xu, T. Wood, W. and Zhang, Y.** (2004). Channel surfing and spatial retreats: defenses against wireless denial of service, *Proc. 3rd ACM Wksp. Wireless Security*, ACM, pp.80–89.
- [36] **Pelechrinis, K., Koufogiannakis, C. and Krishnamurthy, S.V.** (2009). Gaming the jammer: Is frequency hopping effective?, *IEEE WIOPT*, pp.1–10.
- [37] **Pelechrinis, K., Koufogiannakis, C. and Krishnamurthy, S.V.** (2010). On the efficacy of frequency hopping in coping with jamming attacks in 802.11 networks, *IEEE Trans. on Wireless. Comm.*, 9(10), 3258–3271.
- [38] **Xu, W., Ma, K., Trappe, W. and Zhang, Y.** (2006). Jamming sensor networks: attack and defense strategies, *IEEE network*, 20(3), 41–47.

- [39] **Vu, H.L. and Sakurai, T.** (2006). Collision probability in saturated IEEE 802.11 networks, *ATNAC*.
- [40] **Ekici, O. and Yongacoglu, A.** (2008). IEEE 802.11 a throughput performance with hidden nodes, *IEEE Communications Letters*, 12(6), 465–467.
- [41] **Mohamed, M., Bahget, W. and Mohamed, S.** (2014). A performance evaluation for rate adaptation algorithms in IEEE 802.11 wireless networks, *International Journal of Computer Applications*, 99(4), 54–59.
- [42] **Shin, I., Shen, Y., Xuan, Y., Thai, M.T. and Znati, T.** (2011). A Novel Approach Against Reactive Jamming Attacks., *Ad Hoc & Sensor Wireless Networks*, 12(1-2), 125–149.
- [43] **Bhandari, V. and Vaidya, N.H.** (2007). Connectivity and capacity of multi-channel wireless networks with channel switching constraints, *IEEE INFOCOM 2007-26th IEEE International Conference on Computer Communications*, IEEE, pp.785–793.
- [44] **Skalli, H., Ghosh, S., Das, S.K., Lenzini, L. and Conti, M.** (2007). Channel assignment strategies for multiradio wireless mesh networks: Issues and solutions, *IEEE Communications Magazine*, 45(11), 86–95.
- [45] **url-5**, <https://www.wireshark.org>, available on 30.04.2019.
- [46] **den Hartog, F., Raschella, A., Bouhafs, F., Kempker, P., Boltjes, B. and Seyedebrahimi, M.** (2017). A Pathway to solving the Wi-Fi Tragedy of the Commons in apartment blocks, *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*, IEEE, pp.1–6.
- [47] **(To be submitted) Topal, O.F., Kurt, G.K. and Kuran, S.** (2019). A lightweight and practical countermeasure approach against carrier sensing attacks for the next generation WLANs, *IEEE Transactions on Industrial Informatics*.

APPENDICES

APPENDIX A.1 : The Simulation Code Parts





APPENDIX A.1

1.1 Collision Probability Simulation Codes

Listing A.1: NS-3 Simulation code to run the Single High CST case experiment

```
1  /* -*- Mode:C++; c-file-style:"gnu"; indent-tabs-mode:nil; -*- */
2  /*
3   * Copyright (c) 2005,2006 INRIA
4   *
5   * This program is free software; you can redistribute it and/or modify
6   * it under the terms of the GNU General Public License version 2 as
7   * published by the Free Software Foundation;
8   *
9   * This program is distributed in the hope that it will be useful,
10  * but WITHOUT ANY WARRANTY; without even the implied warranty of
11  * MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
12  * GNU General Public License for more details.
13  *
14  * You should have received a copy of the GNU General Public License
15  * along with this program; if not, write to the Free Software
16  * Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
17  *
18  * Authors:
19  *   -JAUME, https://groups.google.com/forum/#!searchin/ns-3-users/probability%20of%20successful%20channel%20access/ns-3-users/7byjPHGlcmo/f7UivGZKj5cJ
20  *   -Omer Topal, <omerft16@gmail.com>
21  */
22
23 #include "ns3/core-module.h"
24 #include "ns3/point-to-point-module.h"
25 #include "ns3/network-module.h"
26 #include "ns3/applications-module.h"
27 #include "ns3/wifi-module.h"
28 #include "ns3/mobility-module.h"
29 #include "ns3/csma-module.h"
30 #include "ns3/internet-module.h"
31 #include "ns3/config-store-module.h"
32 #include <stdio.h>
33 #include <stdlib.h>
34 #include <time.h>
35 #include <string>
36 #include <sstream>
37 #include <iostream>
38
39 using namespace ns3;
40
41 static bool g_verbose = true;
42
43 void
44 DevTxTrace (std::string context, Ptr<const Packet> p)
45 {
46     if (g_verbose)
47     {
48         std::cout << context << " TX p: " << *p << std::endl;
49     }
50 }
51
52 void
53 DevRxTrace (std::string context, Ptr<const Packet> p)
54 {
55     if (g_verbose)
56     {
57         std::cout << context << " RX p: " << *p << std::endl;
58     }
59 }
60
61 void
62 PhyRxOkTrace (std::string context, Ptr<const Packet> packet, double
63 snr, WifiMode mode, enum WifiPreamble preamble)
64 {
65     if (g_verbose)
66     {
67         std::cout << context << " PHYRXOK mode=" << mode << " snr=" <<
```

```

72     snr << " " << *packet << std::endl;
73 }
74 }
75 }
76
77 void
78 PhyRxErrorTrace (std::string context, Ptr<const Packet> packet, double snr)
79 {
80     if (g_verbose)
81     {
82         std::cout << context << " ERROR snr=" << snr << " " << *packet << std::endl;
83     }
84 }
85
86 void
87 PhyTxTrace (std::string context, Ptr<const Packet> packet, WifiMode
88 mode, WifiPreamble preamble, uint8_t txPower)
89 {
90     if (g_verbose)
91     {
92         std::cout << context << " PHYTX mode=" << mode << " " << *packet << std::endl;
93     }
94 }
95
96 }
97
98 void
99 PhyStateTrace (std::string context, Time start, Time duration, enum
100 WifiPhy::State state)
101 {
102     if (g_verbose)
103     {
104         std::cout << context << " state=" << state << " start=" << start <<
105 " duration=" << duration << std::endl;
106     }
107 }
108
109 int main (int argc, char *argv[])
110 {
111     uint32_t n_sta = 10; // number of stations
112     uint32_t i; // iteration index
113     uint32_t pkt_arrv_rate = 1000; // pkt/s
114     float pkt_interval; // sec
115     double simTime=50; // sec
116     bool SingleHighCST = false; // pkt/s
117
118     float randtime_1, randtime_2; // random start time
119     srand(time(NULL));
120
121     std::string controlRate ("DsssRate1Mbps");
122     std::string dataRate ("DsssRate11Mbps");
123
124     CommandLine cmd;
125     cmd.AddValue ("PacketArrivalRate", "packet arrival rate on each station (/s)", pkt_arrv_rate);
126     cmd.AddValue ("StationNumber", "the number of stations", n_sta);
127     cmd.AddValue ("simTime", "simTime", simTime);
128     cmd.AddValue ("SingleHighCST", "SingleHighCST", SingleHighCST);
129
130     cmd.Parse (argc, argv);
131
132     // Calculate packet arrival interval
133     pkt_interval = 1.00 / pkt_arrv_rate;
134
135     // Enable rts/cts all the time
136     //
137     Config::SetDefault ("ns3::WifiRemoteStationManager::RtsCtsThreshold",
138 StringValue ("99999"));
139     // Fix non-unicast data rate to be the same as that of unicast
140     Config::SetDefault ("ns3::WifiRemoteStationManager::NonUnicastMode",
141 StringValue (controlRate));
142
143     // Set the retransmission limit
144     Config::SetDefault ("ns3::WifiRemoteStationManager::MaxSrc",
145 StringValue ("7"));
146     Config::SetDefault ("ns3::WifiRemoteStationManager::MaxSsrc",
147 StringValue ("4"));
148     NodeContainer sta;
149     sta.Create (n_sta+1);
150     YansWifiChannelHelper channel = YansWifiChannelHelper::Default ();
151     YansWifiPhyHelper phy = YansWifiPhyHelper::Default ();
152     phy.SetPcapDataLinkType (WifiPhyHelper::DLT_IEEE802_11_RADIO);
153     phy.SetChannel (channel.Create ());
154
155     WifiHelper wifi;
156     // = WifiHelper::Default ();

```

```

160 // wifi.SetRemoteStationManager ("ns3::AarfWifiManager"); //rate control algorithm
161 // Set data rate as 12Mbps; control rate as 1Mbps
162 wifi.SetRemoteStationManager ("ns3::ConstantRateWifiManager",
163                                "DataMode",StringValue(dataRate),
164                                "ControlMode",StringValue(dataRate)); // controlRate
165 wifi.SetStandard(WIFI_PHY_STANDARD_80211b); // IEEE 802.11g
166 NqosWifiMacHelper mac = NqosWifiMacHelper::Default ();
167
168 // Set it to adhoc mode
169 mac.SetType ("ns3::AdhocWifiMac");
170 NetDeviceContainer devices = wifi.Install (phy, mac, sta);
171
172 /* Setting mobility model */
173 MobilityHelper mobility;
174 Ptr<ListPositionAllocator> positionAlloc = CreateObject<ListPositionAllocator> ();
175 mobility.SetMobilityModel ("ns3::ConstantPositionMobilityModel");
176
177 if(SingleHighCST){ // Increase the CST of a node pair
178     uint32_t numberOfNodes = NodeList::GetNNodes();
179     std::cout<<"numberOfNodes"<<numberOfNodes;
180     Ptr<WifiPhy> AttackerNWsPHY1 = NodeList::GetNode(numberOfNodes-2)
181         ->GetDevice(0)->GetObject<WifiNetDevice>()->GetPhy ();
182     AttackerNWsPHY1->SetCcaModelThreshold(-60);
183     AttackerNWsPHY1->SetEdThreshold(-60);
184
185     Ptr<WifiPhy> AttackerNWsPHY2 = NodeList::GetNode(numberOfNodes-3)
186         ->GetDevice(0)->GetObject<WifiNetDevice>()->GetPhy ();
187     AttackerNWsPHY2->SetCcaModelThreshold(-60);
188     AttackerNWsPHY2->SetEdThreshold(-60);
189 }
190
191 for(uint32_t i=0;i<n_sta-2;i++){
192     positionAlloc->Add (Vector (0.0, 0.0, 0.0));
193 }
194
195 positionAlloc->Add (Vector (30, 0.0, 0.0));
196 positionAlloc->Add (Vector (31, 0.0, 0.0));
197
198 positionAlloc->Add (Vector (0.0, 0.0, 0.0));
199
200 mobility.SetPositionAllocator (positionAlloc);
201 mobility.Install (sta);
202
203 // Internet and Stack
204 InternetStackHelper stack;
205 stack.Install (sta);
206 Ipv4AddressHelper address;
207 address.SetBase ("10.1.1.0", "255.255.255.0");
208 Ipv4InterfaceContainer ipadd = address.Assign (devices);
209
210 //===== Generate traffic
211 // define UDP port
212 uint16_t port_1 = 4000;
213 uint16_t port_2 = 2000;
214 // define UDP maximum packet number and packet size
215 uint32_t maxPacketCount = 400000000;
216 uint32_t MaxPacketSize = 1024;
217
218 for (i=0; i<n_sta; i+=2) {
219     std::cout<<"Here create traffic from "<< i+1 <<" to "<<i<<std::endl;
220
221     // Generate random time
222     randtime_1 = (rand()%1000+1)/1000.00; //random time 1: [0,1]sec
223     randtime_2 = (rand()%1000+1)/1000.00; //random time 2: [0,1]sec
224
225     // UDP: 10.1.1.(i) ==>>> 10.1.1.(i+1)
226     // Create one udpServer applications on 10.1.1.(i+1)
227     UdpServerHelper server_1 (port_1);
228     ApplicationContainer apps_1 = server_1.Install (sta.Get(i+1));
229     apps_1.Start (Seconds (0.0));
230     // Create one UdpClient application to send UDP datagrams from 10.1.1.(i) to 10.1.1.(i+1).
231     Time interPacketInterval = Seconds (pkt_interval);
232     UdpClientHelper client_1 (ipadd.GetAddress (i+1), port_1);
233     client_1.SetAttribute ("MaxPackets", UintegerValue (maxPacketCount));
234     client_1.SetAttribute ("Interval", TimeValue (interPacketInterval));
235     client_1.SetAttribute ("PacketSize", UintegerValue (MaxPacketSize));
236     apps_1 = client_1.Install (sta.Get (i));
237     apps_1.Start (Seconds (randtime_1));
238     // apps_1.Start (Seconds (DoubleValue(RandomVariableValue( (UniformVariable (0.0, 1.0))))));
239
240     // UDP: 10.1.1.(i+1) ==>>> 10.1.1.(i)
241     // Create one udpServer applications on 10.1.1.(i)
242     UdpServerHelper server_2 (port_2);
243     ApplicationContainer apps_2 = server_2.Install (sta.Get(i));
244     apps_2.Start (Seconds (0.0));
245     // Create one UdpClient application to send UDP datagrams from 10.1.1.(i+1) to 10.1.1.(i).
246     UdpClientHelper client_2 (ipadd.GetAddress (i), port_2);

```

```

248     client_2.SetAttribute ("MaxPackets", UIntegerValue (maxPacketCount));
249     client_2.SetAttribute ("Interval", TimeValue (interPacketInterval));
250     client_2.SetAttribute ("PacketSize", UIntegerValue (MaxPacketSize));
251     apps_2 = client_2.Install (sta.Get (i+1));
252     apps_2.Start (Seconds (randtime_2));
253 //     apps_2.Start (Seconds (RandomVariableValue (UniformVariable (0.0, 1.0))));
254 }
255
256
257 // Set simulation stop time
258 Simulator::Stop (Seconds (simTime));
259
260 //Connect the trace sources
261 Config::Connect ("/NodeList/*/DeviceList/*/Mac/MacTx", MakeCallback
262     (&DevTxTrace));
263 Config::Connect ("/NodeList/*/DeviceList/*/Mac/MacRx", MakeCallback
264     (&DevRxTrace));
265 Config::Connect ("/NodeList/*/DeviceList/*/Phy/State/RxOk", MakeCallback
266     (&PhyRxOkTrace));
267 Config::Connect ("/NodeList/*/DeviceList/*/Phy/State/RxError", MakeCallback
268     (&PhyRxErrorTrace));
269 Config::Connect ("/NodeList/*/DeviceList/*/Phy/State/Tx", MakeCallback
270     (&PhyTxTrace));
271 Config::Connect ("/NodeList/*/DeviceList/*/Phy/State/State", MakeCallback
272     (&PhyStateTrace));
273
274
275
276 // Start the simulation
277 Simulator::Run ();
278 Simulator::Destroy ();
279 return 0;
280
281 }

```

Listing A.2: NS-3 Simulation script of Collision Probability Experiments

```

1  /* -- Mode:C++; c-file-style:"gnu"; indent-tabs-mode:nil; -- */
2  /*
3   * Copyright (c) 2005,2006 INRIA
4   *
5   * This program is free software; you can redistribute it and/or modify
6   * it under the terms of the GNU General Public License version 2 as
7   * published by the Free Software Foundation;
8   *
9   * This program is distributed in the hope that it will be useful,
10  * but WITHOUT ANY WARRANTY; without even the implied warranty of
11  * MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
12  * GNU General Public License for more details.
13  *
14  * You should have received a copy of the GNU General Public License
15  * along with this program; if not, write to the Free Software
16  * Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
17  *
18  * Authors:
19  *   -JAUME , https://groups.google.com/forum/#!searchin/ns-3-users/
20  *   probability%20of%20successful%20channel%20access
21  *   /ns-3-users/7byjPHGlcmo/f7UivGZKj5cJ
22  *
23  *   -Omer Topal , <omerft16@gmail.com>
24  */
25
26 #include "ns3/core-module.h"
27 #include "ns3/point-to-point-module.h"
28 #include "ns3/network-module.h"
29 #include "ns3/applications-module.h"
30 #include "ns3/wifi-module.h"
31 #include "ns3/mobility-module.h"
32 #include "ns3/csma-module.h"
33 #include "ns3/internet-module.h"
34 #include "ns3/config-store-module.h"
35 #include <stdio.h>
36 #include <stdlib.h>
37 #include <time.h>
38 #include <string>
39 #include <sstream>
40 #include <iostream>
41
42 using namespace ns3;
43
44 static bool g_verbose = true;
45
46 void
47 DevTxTrace (std::string context, Ptr<const Packet> p)
48 {
49     if (g_verbose)
50     {

```

```

51         std::cout << context << " TX p: " << *p << std::endl;
52     }
53 }
54 }
55
56 void
57 DevRxTrace (std::string context, Ptr<const Packet> p)
58 {
59     if (g_verbose)
60     {
61         std::cout << context << " RX p: " << *p << std::endl;
62     }
63 }
64
65 void
66 PhyRxOkTrace (std::string context, Ptr<const Packet> packet, double
67 snr, WifiMode mode, enum WifiPreamble preamble)
68 {
69     if (g_verbose)
70     {
71         {
72             std::cout << context << " PHYRXOK mode=" << mode << " snr=" <<
73             snr << " " << *packet << std::endl;
74         }
75     }
76 }
77
78 void
79 PhyRxErrorTrace (std::string context, Ptr<const Packet> packet, double snr)
80 {
81     if (g_verbose)
82     {
83         std::cout << context << " ERROR snr=" << snr << " " << *packet << std::endl;
84     }
85 }
86
87 void
88 PhyTxTrace (std::string context, Ptr<const Packet> packet, WifiMode
89 mode, WifiPreamble preamble, uint8_t txPower)
90 {
91     if (g_verbose)
92     {
93         std::cout << context << " PHYTX mode=" << mode << " " << *packet << std::endl;
94     }
95 }
96
97 }
98
99 void
100 PhyStateTrace (std::string context, Time start, Time duration, enum
101 WifiPhy::State state)
102 {
103     if (g_verbose)
104     {
105         std::cout << context << " state=" << state << " start=" << start <<
106         " duration=" << duration << std::endl;
107     }
108 }
109
110
111 int main (int argc, char *argv[])
112 {
113     uint32_t n_sta = 10; // number of stations
114     uint32_t i; // iteration index
115     uint32_t pkt_arrv_rate = 1000; // pkt/s
116     float pkt_interval; // sec
117     double simTime=50; // sec
118
119
120     float randtime_1, randtime_2; // random start time
121     srand(time(NULL));
122
123     std::string controlRate ("DsssRate1Mbps");
124     std::string dataRate ("DsssRate11Mbps");
125
126     CommandLine cmd;
127     cmd.AddValue ("PacketArrivalRate", "packet arrival rate on each station(/s)", pkt_arrv_rate);
128     cmd.AddValue ("StationNumber", "the number of stations", n_sta);
129     cmd.AddValue ("simTime", "simTime", simTime);
130
131     cmd.Parse (argc, argv);
132
133     // Calcuate packet arrival interval
134     pkt_interval = 1.00 / pkt_arrv_rate;
135
136     // Disable rts/cts all the time
137     Config::SetDefault("ns3::WifiRemoteStationManager::RtsCtsThreshold",
138    StringValue ("99999"));

```

```

139 // Fix non-unicast data rate to be the same as that of unicast
140 Config::SetDefault ("ns3::WifiRemoteStationManager::NonUnicastMode",
141 StringValue (controlRate));
142
143 // Set the retransmission limit
144 Config::SetDefault ("ns3::WifiRemoteStationManager::MaxSsrc",
145 StringValue ("7"));
146 Config::SetDefault ("ns3::WifiRemoteStationManager::MaxSsrc",
147 StringValue ("4"));
148 NodeContainer sta;
149 sta.Create (n_sta+1);
150 YansWifiChannelHelper channel = YansWifiChannelHelper::Default ();
151 YansWifiPhyHelper phy = YansWifiPhyHelper::Default ();
152 phy.SetPcapDataLinkType (WifiPhyHelper::DLT_IEEE802_11_RADIO);
153 phy.SetChannel (channel.Create ());
154
155 WifiHelper wifi;
156
157 wifi.SetRemoteStationManager ("ns3::ConstantRateWifiManager",
158 "DataMode", StringValue (dataRate),
159 "ControlMode", StringValue (dataRate)); // controlRate
160 wifi.SetStandard (WIFI_PHY_STANDARD_802_11b); // IEEE 802.11g
161 NqosWifiMacHelper mac = NqosWifiMacHelper::Default ();
162
163 // Set it to adhoc mode
164 mac.SetType ("ns3::AdhocWifiMac");
165 NetDeviceContainer devices = wifi.Install (phy, mac, sta);
166
167 /* Setting mobility model */
168 MobilityHelper mobility;
169 Ptr<ListPositionAllocator> positionAlloc = CreateObject<ListPositionAllocator> ();
170 mobility.SetMobilityModel ("ns3::ConstantPositionMobilityModel");
171
172 for (uint32_t i=0; i<n_sta+1; i++)
173 {
174     positionAlloc->Add (Vector (0.0, 0.0, 0.0));
175 }
176
177 mobility.SetPositionAllocator (positionAlloc);
178 mobility.Install (sta);
179
180 // Internet and Stack
181 InternetStackHelper stack;
182 stack.Install (sta);
183 Ipv4AddressHelper address;
184 address.SetBase ("10.1.1.0", "255.255.255.0");
185 Ipv4InterfaceContainer ipadd = address.Assign (devices);
186
187 //===== Generate traffic
188 // define UDP port
189 uint16_t port_1 = 4000;
190 uint16_t port_2 = 2000;
191 // define UDP maximum packet number and packet size
192 uint32_t maxPacketCount = 400000000;
193 uint32_t MaxPacketSize = 1024;
194
195 for (i=0; i<n_sta; i+=2)
196 {
197     // Generate random time
198     randtime_1 = (rand()%(1000+1))/1000.00; //random time 1: [0,1]sec
199     randtime_2 = (rand()%(1000+1))/1000.00; //random time 2: [0,1]sec
200
201     // UDP: 10.1.1.(i) ==>>> 10.1.1.(i+1)
202     // Create one udpServer applications on 10.1.1.(i+1)
203     UdpServerHelper server_1 (port_1);
204     ApplicationContainer apps_1 = server_1.Install (sta.Get(i+1));
205     apps_1.Start (Seconds (0.0));
206     // Create one UdpClient application to send UDP datagrams from 10.1.1.(i) to 10.1.1.(i+1).
207     Time interPacketInterval = Seconds (pkt_interval);
208     UdpClientHelper client_1 (ipadd.GetAddress (i+1), port_1);
209     client_1.SetAttribute ("MaxPackets", UintegerValue (maxPacketCount));
210     client_1.SetAttribute ("Interval", TimeValue (interPacketInterval));
211     client_1.SetAttribute ("PacketSize", UintegerValue (MaxPacketSize));
212     apps_1 = client_1.Install (sta.Get (i));
213     apps_1.Start (Seconds (randtime_1));
214
215     // UDP: 10.1.1.(i+1) ==>>> 10.1.1.(i)
216     // Create one udpServer applications on 10.1.1.(i)
217     UdpServerHelper server_2 (port_2);
218     ApplicationContainer apps_2 = server_2.Install (sta.Get(i));
219     apps_2.Start (Seconds (0.0));
220     // Create one UdpClient application to send UDP datagrams from 10.1.1.(i+1) to 10.1.1.(i).
221     UdpClientHelper client_2 (ipadd.GetAddress (i), port_2);
222     client_2.SetAttribute ("MaxPackets", UintegerValue (maxPacketCount));
223     client_2.SetAttribute ("Interval", TimeValue (interPacketInterval));
224     client_2.SetAttribute ("PacketSize", UintegerValue (MaxPacketSize));
225     apps_2 = client_2.Install (sta.Get (i+1));
226     apps_2.Start (Seconds (randtime_2));

```

```

227     }
228
229
230     // Set simulation stop time
231     Simulator::Stop (Seconds (simTime));
232
233     //Connect to trace sources
234     Config::Connect ( "/NodeList/*/DeviceList/*/Mac/MacTx", MakeCallback
235         (&DevTxTrace));
236     Config::Connect ( "/NodeList/*/DeviceList/*/Mac/MacRx", MakeCallback
237         (&DevRxTrace));
238     Config::Connect ( "/NodeList/*/DeviceList/*/Phy/State/RxOk",
239         MakeCallback (&PhyRxOkTrace));
240     Config::Connect ( "/NodeList/*/DeviceList/*/Phy/State/RxError",
241         MakeCallback (&PhyRxErrorTrace));
242     Config::Connect ( "/NodeList/*/DeviceList/*/Phy/State/Tx",
243         MakeCallback (&PhyTxTrace));
244     Config::Connect ( "/NodeList/*/DeviceList/*/Phy/State/State",
245         MakeCallback (&PhyStateTrace));
246
247     // Start the simulation
248     Simulator::Run ();
249     Simulator::Destroy ();
250     return 0;
251
252 }

```

Listing A.3: Bash script code to Run Collision Experiments

```

1  #!/bin/bash
2  cd ../../..
3
4  NumberofNode='5'
5  NodeNumberArray='10 20 30 40 50 60 70 80 90'
6  FileName='CollCalcOutput-4STA-SingleHighCST'
7  FolderFileName='11bCollProb/HighNofSTA/NormalCST'
8
9  for NumberofNode in $NodeNumberArray
10 do
11     FileName="CollCalcOutput-STA$NumberofNode-Normal.txt"
12
13     ./waf --run "scratch/CollisionCalc-ns3 --PacketArrivalRate=30000
14         --StationNumber=$NumberofNode" > $FolderFileName/$FileName &
15     echo "FileName: $FileName"
16 done

```

Listing A.4: Bash Script code to gather Statistics Results

```

1
2  NumberofNode='10'
3  NodeNumberArray='10 20 30 40 50 60 70 80 90'
4  FileName='CollCalcOutput-NORMAL'
5
6
7  for NumberofNode in $NodeNumberArray
8  do
9      FileName="CollCalcOutput-STA$NumberofNode-Normal.txt"
10     RXOK=$(grep NodeList/$NumberofNode $FileName |grep PHYRXOK |wc -l)
11     RXERROR=$(grep NodeList/$NumberofNode $FileName |grep ERROR|wc -l)
12     echo "Normal N:$NumberofNode, RXOK: $RXOK RXERROR: $RXERROR"
13 done
14 echo "*****"

```

Listing A.5: Octave code of Computation of Bianchi Model

```

1  function y=f(x)
2  N=50 ;
3  CW=15;
4  m=7;
5  y(1)=(2*(1-2*x(1)))/((CW+1)*(1-2*x(1))+x(1)*CW*(1-(2*x(1))^m))-x(2);
6  y(2)=-x(1)+1-(1-x(2))^(N-1);
7  end
8
9  % To solve this non linear equation, run the following command in Octave Command Window
10 % [x,info]=fsolve("fattack",[0.06;0.06]);

```



CURRICULUM VITAE



Name Surname: Ömer Faruk TOPAL

Place and Date of Birth: Bursa 11.12.1992

E-Mail: omerft16@gmail.com

EDUCATION:

- **B.Sc.:** 2011-2016, Izmir Institute of Technology, Electronic and Communication Engineering.
- **M.Sc.:** 2016-, Istanbul Technical University, Telecommunication Engineering.

PROFESSIONAL EXPERIENCE AND REWARDS:

- 2017-, AirTies Wireless Networks, Research Engineer.
- 2018-2019, Wi-5 Horizon 2020 Project.

TRAINING:

- 2018, Methodologies and Applications of Project Management, PMI.
- 2018, Introduction to Java Programming,

PUBLICATIONS, PRESENTATIONS AND PATENTS ON THE THESIS:

- O. F. Topal, G. K. Kurt, and A. Soysal, "Adaptation of Carrier Sensing Threshold to Increase Throughput in Dense 802.11 ac Wireless Networks.", *IEEE Global Information Infrastructure and Networking Symposium 2018*, pp. 1-6, 2018.

OTHER PUBLICATIONS, PRESENTATIONS AND PATENTS:

- J. Saldana, R. Munilla, S. Eryigit, O. Topal, J. Ruiz-Mas, J. Fernández-Navajas and L. Sequeira, "Unsticking the Wi-Fi client: Smarter decisions using a software defined wireless solution.", *IEEE Access Journal*, 6, 30917-30931, 2018
- O. Topal, J. Saldana, R. Alessandro and N., Jan, "Deliverable 5.2: Integration Results", *Wi-5 H2020 Project*, 2018.