Department of Computer Science and Engineering (CSE)
Islamic University of Technology

An Improved Channel Access Mechanism For IEEE 802.11 WLAN

Author

Imamul Ahsan - 144433
Sabbir Ahmed Sristy- 144436

Supervisor

Md. Ashraful Alam Khan
Assistant Professor
Department of CSE
Islamic university of Technology

A thesis submitted to the Department of CSE in partial fulllment of the requirements for the degree of B.Sc. Engineering in CSE.
Engineering in CSE
Academic Year:2017-18
November-2018

Author's declaration

This is to certify that the work presented in this thesis is the outcome of the analysis and experiments carried out by Imamul Ahsan and Sabbir Ahmed Sristy under the supervision of Md. Ashraful Alam Khan, Assistant Professor, Department of Computer Science and Engineering (CSE), Islamic University of Technology (IUT), Dhaka, Bangladesh. It is also declared that neither of this thesis nor any part of this thesis has been submitted anywhere else for any degree or diploma. Information derived from the published and unpublished work of others has been acknowledged in the text and a list of references is given.

Author 1:

Name: Imamul Ahsan Student ID: 144433 Signature:..........................

Author 2:

Name: Sabbir Ahmed Sristy Student ID: 144436 Signature:..........................

Supervisor:

Signature:..
Md. Ashraful Alam Khan
Assistant Professor
Department of Computer Science & Engineering (C.S.E.)
Islamic University of Technology (I.U.T.)

Dedication and acknowledgements

We would like to express our grateful appreciation for **Md. Ashraful Alam Khan**, Assistant Professor, Department of Computer Science Engineering, IUT for being our advisor and mentor. His motivation, suggestions and insights for this thesis have been invaluable. Without his support and proper guidance this research would not have been possible. His valuable opinion, time and input provided throughout the thesis work, from first phase of thesis topics introduction, subject selection, proposing algorithm, modification till the project implementation and finalization which helped us to do our thesis work in proper way. We are really grateful to him.

Abstract

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) has been used for so many years in 802.11 WLANs for its simplistic nature. A Binary Exponential Backoff (BEB) is used here so that each contending station in a network is chosen randomly. However the overall throughput of the network degrades drastically due to random nature of backoff mechanism. Therefore an alternate contention mechanism is required to overcome this problem. To overcome this problem of MAC inefficiency, we propose a modified backoff mechanism for MAC which can order the contending station by predictive backoff values of others stations. We use a hash based backoff mechanism to resolve the initial contention of the contending stations and after each successful transmission a fixed slot is assigned to each individual station. Therefore, our proposed approach contain the combination of backoff mechanism which is predictive hash based backoff for initial contention and modified deterministic backoff after successful transmission. In this way, a collision free schedule can be created and can support a large number of contenders. The simulation study show that the proposed scheme reduces the contention overhead and can gain high efficiency compared to standard channel access mechanism.

Table of Contents

List of Tables

LIST OF FIGURES

FIGURE **Page**

CHAPTER 1

INTRODUCTION

1.1 Overview

The physical layer data rate (PHY) in wireless network has been advanced steadily. To cope with the demand of multimedia applications recent 802.11a support physical (PHY) rate upto 600 [14] Mbps and the future standards like 802.11 ac/ad aims to support PHY layer rate more than Gbps [6, 18] range. This increase in the PHY data rate does not come up useful as the MAC data rate is not also increased. Although the transmission rate increases significantly, one does not see a commensurate increase in user throughput because the MAC efficiency of IEEE 802.11 rapidly decreases as the PHY rate increases [5, 15]. Even though increasing PHY rate leads to faster transmission of MAC frame payloads, overhead such as PHY headers and contention time typically do not decrease at the same rate. In fact, in transmitting a frame, the proportion attributed to overhead becomes larger as the PHY rate increases. According to the study conducted by Li et al. [4], the MAC efficiency decreases from 42% to 10% as the PHY rate increases from 54 Mbps to 432 Mbps.

Therefore the overall throughput of the netowrk degrades as the daa rate in the MAC layer acts as the bottleneck of the whole network. The lower data rate in the MAC layer is caused by some overhead such as the PHY header and contention time, and existence of idle slots. For this reason some modification needed in the current CSMA/CA to improve MAC efficiently.

1.2 Problem Statement

Conventional WiFi networks perform channel contention in time domain. This is known to be wasteful because the channel is forced to remain idle while all contending nodes are backing off for multiple time slots. Access control strategies are designed to arbitrate how multiple entities access a shared resource. Several distributed protocols embrace randomization to achieve arbitration. In WiFi networks, for example, each participating node picks a random number from a specified range and begins counting down. The node that finishes first, say N1 , wins channel contention and begins transmission. The other nodes freeze their countdown temporarily, and revive it only after N1's transmission is complete. Since every node counts down at the same pace, this scheme produces an implicit ordering among nodes. Put differently, the node that picks the smallest random number transmits first, the one that picks the second smallest number transmits second, and so on. The overall operation is often termed as "backoff".

Two types of problems are found in the traditional MAC protocol due to its randomness. They are – idle slot and collision. While backoff arbitrates channel contention, it incurs a performance cost. Specifically, when multiple nodes are simultaneously backing off, the channel must remain idle, naturally leading to under-utilization. Thus the shared channel has to remain idle for multiple slot times while contending stations carryout their time domain backoff. The figure 01 shows that two stations under utilizing the channel time by waiting for random slots count back to zero. So, station A and B in the figure 01 has to wait 9 and 7 time slots respectively to transmit a frame.

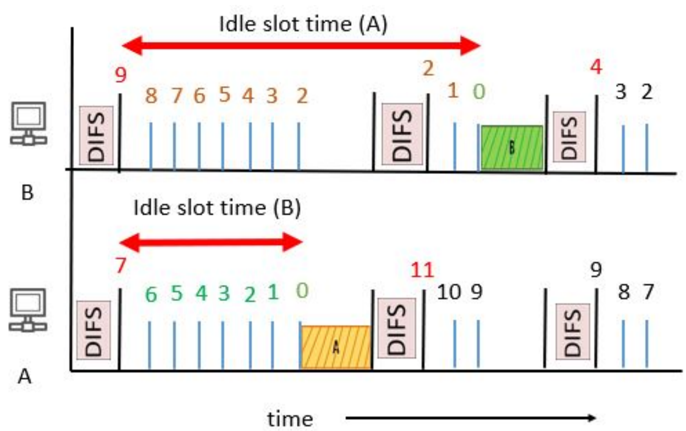

Figure 1.1: Channel under utilization due to random nature of channel access mechanism.

The proportion of such channel wastage is huge, which leads to significantly decreased MAC sublayer efficiency. To send 1500-byte data packet in a 300 Mbps network, only 40 micro seconds time is necessary. But the combined overhead of DIFS, Contention Window and ACK result in another 120 micro seconds. Thus, in this scenario, MAC layer efficiency is only 25% [5].

Moreover, network congestion prompts an exponential increase in the backoff range, introducing the possibility of greater channel wastage. Authors in [3] show more than 30% reduction in throughput due to backing off; [1] shows the severity at higher data rates. According to experiment conducted in [5], the IEEE 802.11 MAC efficiency falls from 42% to 10% when the PHY rate increase from 54 Mbps to 432Mbps. The efficiency of IEEE 802.11 network deteriorates from over 80% at 1 Mbps to under 10% at 1 Gbps. The figure 02 shows the collision problem in the traditional CSMA/CA where three stations contend for the channel access but due to picking up same random number collision occurs which ultimately reduces the network throughput.

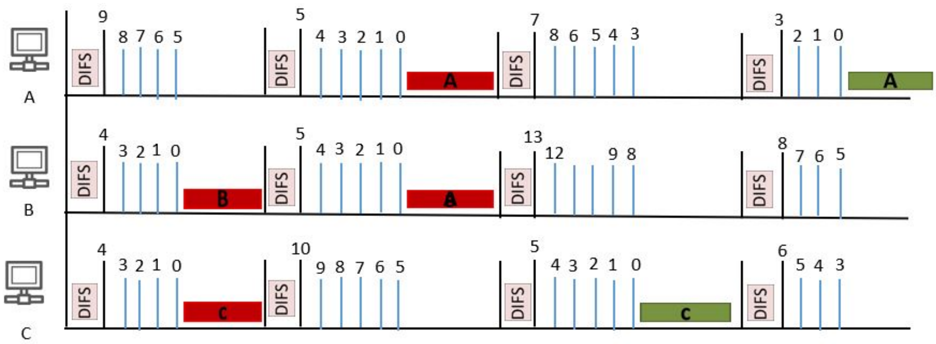

Figure 1.2: Channel access mechanism cannot avoid collision between the contending stations.

1.3 Research Challenges

Several alternate approaches have been proposed in the recent years to reduce the number of collision and idle slot in the MAC layer. Existing medium access control protocols (MACs) for collision avoidance in wireless networks can be classified into four categories, i.e., coordination-based schemes, multi-frequency assisted schemes, slot-assignment schemes and backoff-tuning schemes.

The coordination-based schemes utilize a central coordination for resource allocation [7, 13], while multi-frequency assisted schemes either use out-of-band signaling to avoid colliding transmission or use multiple frequency bands for concurrent transmission [10, 11]. Because these two schemes requires extra infrastructure, i.e., a central coordination (CC) or extra frequency bands (EFB), which limits their scalability for general distributed networks. Although many works has been done involving the limitations of traditional MAC but there remains a need of huge improvement.

In our approach, we use Time Domain Solution and provide a little modification to the traditional CSMA/CA so that both type of stations can co-exist in the same network. In traditional CSMA/CA, when a station has a new frame transmit it has to wait Distributed Inter Frame Space (DIFS) time and then start transmitting if the channel is found idle. otherwise, if the channel is busy the backoff process starts after DIFS interval. The initial backoff counter is chosen from a predefined range [0,CW]. For the first transmission the contention window (CW) is set to minimum value, CWmin. The backoff counter is decremented on slot time as long as the channel is sensed idle. When the backoff counter reaches zero the frame is transmitted. A transmission becomes successful when an acknowledgement (ACK) is recieved by the transmitting station. Our proposed MAC scheme differ in the initial backoff counter than traditional MAC. In our approach, all the contending stations set their initial backoff from a seed value. Given a seed value, a station can calculate their own backoff value and also estimate the backoff value of other stations. In this way, the stations can order themselves in transmission of frames. Now in this ordering, if the frame transmission is successful the backoff counter of the station remains the same for the next cycle i.e. modified deterministic backoff is used. In this way, a collision free schedule can be created in the next cycles. So, using this approach we tried to improve the MAC channel access efficiency.

1.4 Thesis Objective & Contribution

The objective of this thesis is to develop an efficient channel access mechanism for IEEE 802.11 WLAN. Our approach is able to find and overcome the following gaps of traditional MAC protocol:

- Reduce The collision of frames of the contending stations and therefore reducing the contention time of frame transmission.
- Reduce the idle slot while randomly contending for the channel.
- Try to obtain a higher throughput by a very fast convergence of the network.
- Utilization of beacon frame and achieve a collision free schedule in a decentralized manner i.e. using any central coordination system.

1.5 Organization of thesis

In Chapter 1 we have discussed our study in a precise and concise manner. Chapter 2 deals with the necessary literature review for our study and there development so far. In Chapter 3 we have stated our proposed method, proposed algorithm and also the a detail insight of the working procedure of our proposed MAC protocol for IEEE 802.11 WLAN to improve channel efficiency. Chapter 4 shows the results and comparative analysis of successful implementation of our proposed method. The final segment of this study contains all the references and credits used. We conclude our thesis and show the future prospects and research scopes of our proposed method.

Chapter 2

Related Works

The recent advancement of PHY layer data rate has led researchers to re-think about the current MAC protocol. Several MAC scheme are proposed which can outperform the current MAC protocol in certain conditions.

A. Zero Collision MAC

Zero collision MAC (ZC-MAC) [4]| is a distributed MAC protocol that can achieve a zero collision schedule without any control message or synchronization. The principle of ZC-MAC is to create a predefined virtual schedule of M-slot length. The contending station reserve each slot when there is a frame to transmit. If two contending stations pick the same slot then it would ultimately end up in collision. Therefore it would force the contenders to randomly pick up another slot and free the collided slot. Finally, a collision free schedule can be created when N number of station reserve different slots.

ZC-MAC will be able to provide a collsion free schedule if and only if the number of contending station is less than the predefined virtual slot i.e. $N < M$. Again, if the predefined virtual slot is over-estimated i.e. $M \geq N$ then the number of idle slot is increased which degrades the overall throughput.

B. CSMA/ECA

Carreir Sense Multiple Access with Enhanced Collision Avoidance (CSMA/ECA) [9] can create a collision free schedule by simply modifying the contention mechanism of CSMA/CA. In CSMA/ECA, the stations transmit with deterministic backoff after each successful transmission/ Therefore the stations follow random backoff until a frame is transmitted successfully. So, a collision free schedule is created when all the station follow deterministic backoff.

The problem with CSMA/ECA is that the collision free schedule can never be created when the number of node is greater than the number of slots. To solve this problem the writer introduced Hysteris in which the contention window will be increased if there is still collision after deterministic schedule. They also introduced Fairshare which takes the advantage of frame aggregation for the stations that have very large contention window.

C. BCCA

BCCA [12] is also a distributed MAC scheme takes the advantages of CSMA/CA and TDMA. It is heavily dependent on the beacon frame which is one of the managemen frames of 802.11 WLAN. In BCCA, every station transmit with a deterministic backoff v(d) after successful transmission.

This scheme can dramatically improve the channel efficiency by rearranging the reserved slot utilizing the information from the beacon frame. This rearrangement reduces the idle slot. However the collision free state cease o exist when the number of stations is greater than v(d). This can be solved by updating the v(d) after beacon interval.

D. E-MAC

Collision during transmission is the ultimate cause of the degradation of throughput and non-deterministic latency in wireless networks. The existing mechanism for avoiding collision in a distributed wireless networks are basically based on random backoff. But the existing mechanism doesn't provide the assurance of collision-free channel access. In this paper, a simple collision-avoidance MAC (E-MAC) [17] was designed for distributed wireless networks that can achieve collision free access iteratively. In E-MAC, each transmitter will adjust its next transmission time according to which part of its packets suffering from the collision. The iteration of this adjustment will lead to a group of nodes converging to a collision-free network. Here no central coordinator is required. It is scalable to new entries to the network and length of packets. It is also robust to system errors, such as inaccurate timing.

In distributed wireless networks, the collision occurs due to the overlapping of more than two interfering nodes' transmission.Transmission collision is classified into two categories: the synchronized collision and the hidden node collision. When no less than two nodes start to transmit simultaneously synchronized collision occurs. This usually happens in single-hop wireless networks, where more than two nodes are to select the same backoff counter to transmit after detecting that the wireless medium is idle. But in hidden-node collision, the packets that are collided can be overlapped at any stages. And in hidden-node collision is the dominating collision scenario in multi-hop networks, where there exist hidden nodes.

E-MAC uses elaborate, instead of random backoff mechanism to iteratively achieve collision-free access. The main idea is that every node can transmit at most once in a given cycle and if one node experiences a collision, the node will adjust its transmission time in the next cycle according to which part of its packets suffering from the collision. If the front part of the packet is collided it will transmit latter in the next cycle and if the back part is collided then it will transmit earlier in the next cycle.

E. I-DCF

Improved DCF (I-DCF) [8] for IEEE 802.11 regulates the sharing of the radio channel assigning differentiated and unique initial backoff values to each station. The backoff values are dynamically adapted according to the network load. The IEEE 802.11 WLAN provides flexible access to the internet and it is being researched for many years.

Wireless medium sharing in WLANs is handled by the medium access control (MAC) protocol using the the coordination mechanism to provide channel access. Here DCF is used as primary medium access method based on Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). With the evolution of new 802.111 standards, new enhancements are proposed at MAC layer. However, DCF still remains the backbone of the new standards and new propositions are made over this random access technique. Moreover, another access scheme named Time Division Multiple Access (TDMA) has significantly gained popularity. In TDMA, channel is shared by allocating conflict free transmission slots to different stations in such a way that stations within interfering range can transmit at different times. TDMA can prevent collision but it suffers with overhead issues that are needed to maintain detailed topology information for assigning slots and to be in synchronization.

In DCF, the main algorithm is based on the random technique of CSMA/CA. This can't provide gurantee of collision-free channel access and significantly suffers collision with increasing network load. Thus, efficiency is reduced and performance is degraded of the whole system. I-DCF is a new scheme that enhances backoff process to avoid collisions. The basic idea of I-DCF is similar to 802.11 DCF as some features of CSMA/CA are to adopt to avoid collisions.

F. Learning Perfect Coordination With Minimal Feedback

Whenever stations share resources across a network, coordination becomes a central problem. In the absence of coordination, there will be collision,congestion or interference thus reducing the performance of network. Perfect Coordination (PC) [16] protocols are fully distributed (neither require central control nor the exchange of any control messages), fast(with speeds comparable to those of any existing protocols), fully efficient(achieving perfect coordination,with no collision and no gaps) and require minimal feedback. PC protocols rely heavily in learning, exploiting the possibility to use both actions and silence as messages and the ability of stations to learn from their own histories while simultaneously enabling the learning of other stations.

In perfect coordination protocol, the protocol is designed regarding two settings: one the number of stations is known and another the number of stations is unknown(but an upper bound is known). These protocols are perfectly distributed and require no central control,no exchange of control messages between stations and minimal feedback. Stations that transmit learn whether or not their transmission successful and stations that are idle can not sense the channel and hence learn nothing. The protocols that are introduced converge as rapidly and with higher probability and achieve perfect coordination, not merely zero collision, hence greater throughput and smaller delay.

These protocols lead stations to learn about the evolving state of the system, to condition their pattern of actions on what is learned, and to enable the learning of other stations. Stations learn more and use more of what they have learned, especially about the pattern of actions of other stations.

CHAPTER 3

PROTOCOL DESCRIPTION

3.1 Distributed Coordination Function

Distributed Coordination Function (DCF) is known as the fundamental MAC channel access technique of IEEE 802.11 based WLAN standard. The DCF procedurueof a station is described as follows.

When a station has to transmit a frame the channel is monitored by the station. A station starts to transmit if the channel is idle for a period of time equal to Distributed Inter-Frame Space (DIFS). Otherwise, if the channel is sensed busy, it continues to monitoring the channel until the channel is measured idle for a DIFS interval. After the DIFS interval, random backoff process starts for the stations. Initially the backoff counter has a predefined range [0,CW]. All the stations initialize its backoff counter within this range. Contention Window (CW) for a station depends on the number of transmissions failed for a frame. CW is set equal to CW_{min} at first transmission attempt. The backoff counter is decremented once per slot time as long as the channel is sensed idle. Whenever a transmission is sensed on the channel, the backoff counter is frozen and restarts the counter again after the channel is sensed idle for a DIFS interval.

The station transmits its frame in the next slot time, when the backoff counter reaches to zero. An acknowledgement (ACK) is sent to notify the transmitting station, whenever the frame is received successfully. If the acknowledgement is not received within a given timeout, the station reschedules its transmission by re-entering backoff process. CW

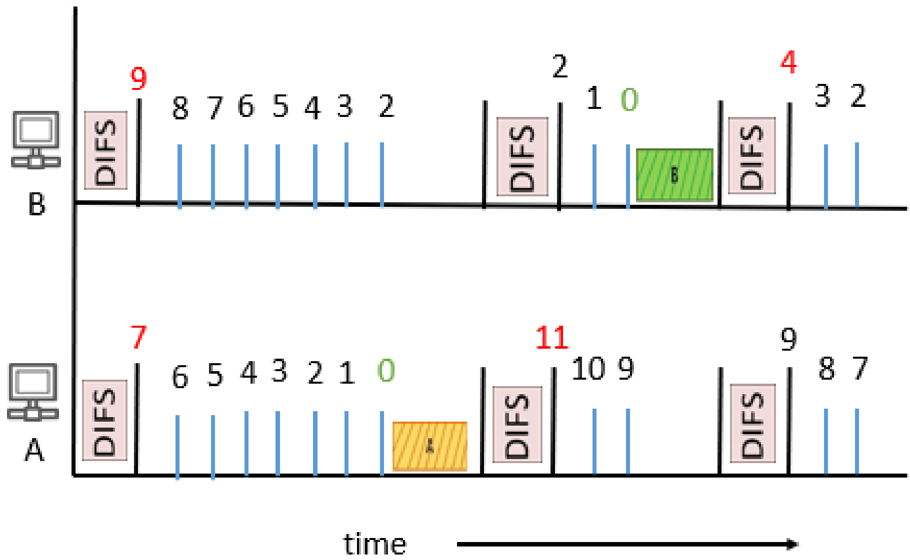

Figure 3.1: Process of Distributed Coordination Function (DCF).

is doubled for each unsuccessful transmission until it reaches CW_{max}. Figure 1 and Algorithm 1 provides the summary of IEEE 802.11 MAC access mechanism and the Binary Exponential Backoff (BEB) procedure, respectively.

Algorithm 1: BEB (Binary Exponential Backoff)		
1:	**if** (R_c == 0) **then**	// First transmission
2:	$CW = CW_{min}$	
3:	**else**	//Re-transmission
4:	$CW = 2^k(CW+1)-1$	
5:	$CW = min(CW, CW_{max})$	
6:	Backoff = rand(1, CW) x (slot)	

R_c is the re-transmission count. Initially it is set to 0 at the first transmission and incremented by one per re-transmission. min (CW, CW_{max} returns the smaller number. rand (1, CW) returns an integer value chosen randomly between 1 and CW.

3.2 Beacon Frame

Beacon frame is one of the management frame in IEEE 802.11 based WLAN standard. It contains all the information about the network and enables stations to establish and maintain communications in an orderly fashion. In an infrastructure BSS, beacon frames are transmitted by the access point (AP) periodically to announce the presence of a wireless LAN. A typical beacon frame carries the following information in the frame body:

- **Beacon interval:** This is the time interval between beacon transmission. Typically configured as 100ms in the AP.
- **Timestamp:** After receiving a beacon, a station uses the timestamp value to update its local clock. This process enables synchronization among all stations in the AP.
- **Service Set Identifier (SSID):** The SSID identifies a specific wireless LAN. Before associating with a particular WLAN, a station must have the same SSID as the AP.
- **Supported rates:** Each beacon carries information that describes the rates that the particular WLAN supports. With this information, stations can use the performance metrics to decide which AP to associate with.
- **Other information carried by beacon frames:** Parameter Sets, Capability Information, Traffic Indication MAP (TIM) and etc.

Beacon frames are sent using the 802.11 CSMA/CA protocol. If a station is transmitting a frame when the beacon is to be sent, then the AP delays its beacon transmission.

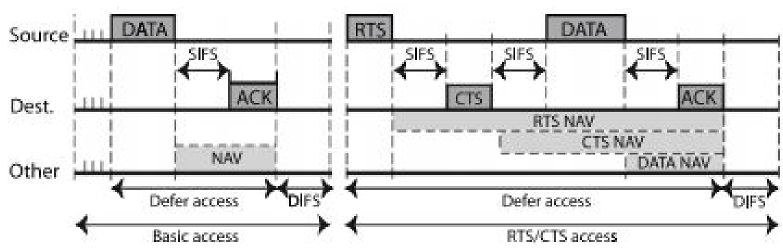

Figure 3.2: IEEE 802.11 MAC access mechanisms

Therefore, the actual time between beacons frames may be longer than the beacon interval. However, if one of the beacon frames is delayed, then the next beacon is sent according to the original schedule, not 100 ms after the delayed beacon frame is sent.

3.3 Improved Channel Access Mechanism For MAC 802.11 WLANs

The proposed scheme that we called Improved Channel Access Mechanism for MAC WLAN 802.11 is the combination of hashed backoff and deterministic backoff. Our approach is fully decentralized and differs from traditional CSMA/CA in choosing the backoff values. The initial channel access mechanism is done by hash based predictive backoff and the remaining channel access uses modified deterministic backoff. Each cycle is maintained by a beacon frame as shown in figure 3.3.

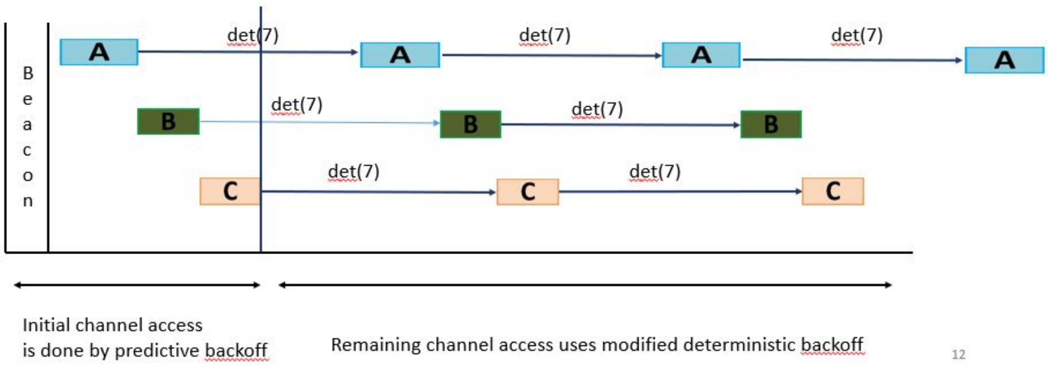

Figure 3.3: Proposed channel access mechanism for three contending stations

Collisions are handled as in CSMA/CA, which is described in Algorithm 1. In Algorithm 1, the station selects a random value from the Contention Window (CW_{min}). The typical value of the Contention Window, (CW_{min}) = 16. Therefore, the stations can choose random value from the range[0,15]. Upon collision, the involved stations will double their Contention Window by incrementing their backoff stage in one and use a random backoff from Contention Window [0, $2^k CW_{min} - 1$] as shown in Algorithm 1. The proposed approach consists of two backoff procedures which are described in the following subsections.

3.3.1 Predtictive Backoff

The only difference between the traditional CSMA/CA and our approach is the change of the random value generation technique. We know that in a collision domain every station can overhear the address of each other. We use the IP address of each station as a hash value and random backoff as a hash key. In this way all the station can predictively know the backoff values of each other.

In this case for generating random backoff values for each stations we are using a double hash function. We are using the IP address of each station and current time. The IP address and current time are added and the added result is mod by the size of the hash table. If no station is assigned on particular mod value the station takes that mod value. If a station gets the mod value where already a station is assigned collision occurs. So to avoid collision we use double hash function so that the stations that is colliding can get another random backoff.

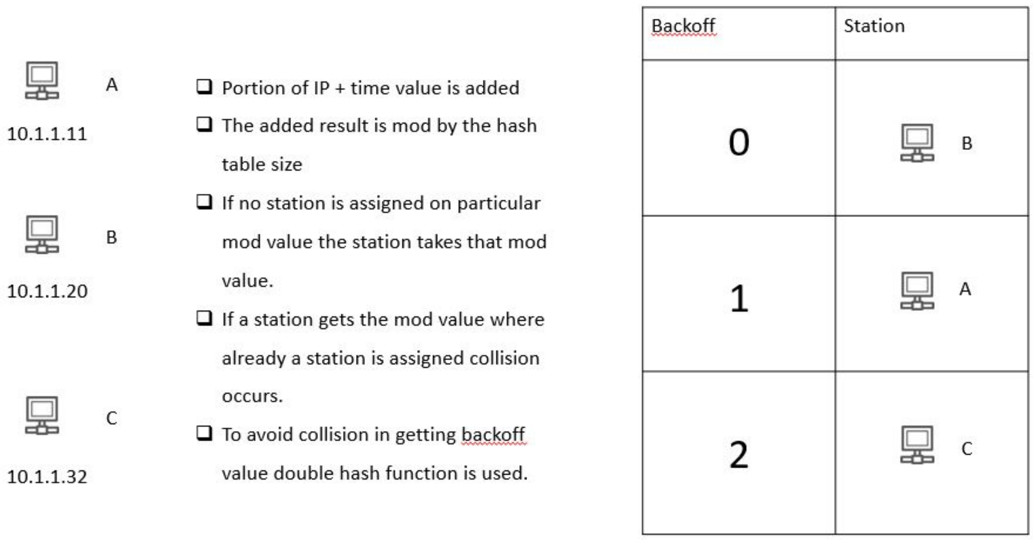

Figure 3.4: Determining Hash Backoff

For example, for the convenience to understand we are assuming that there are three stations in a network (Figure 3.4). Stations A, B and C whose IP addresses are respectively 10.1.1.11, 10.1.1.20 and 10.1.1.32 and we are assuming that in the network the current time is 1352 ms. Now, Station A's IP address's last portion 11 and current time is added which results 1363. As there are three stations in the network so the size of the hash table is 3. So, for choosing the hash based backoff for Station A, 1363 is mod by 3 which gives 1. As no station has choosen that backoff so, Station A will get the hash backoff 1. Now, we come for Station B. The last portion of IP address of Station B is 20 and in the network current time is 1352 ms. The last portion of IP address and the current time is added which results 1372. Now, added result 1372 is mod by 3 which gives 1. But Station B can't get the hash backoff 1, becuase Sation A has already authorized it. So, Station B has to choose another backoff. For choosing another backoff we use the double hash function or second hash function. In double hash function we take a value which is an immediate prime number, m less than the hash table size. So, in this case that m is 2. To find random backoff for station B 1372 is mod by 2 which results 0 and and it will be minus from m which results 2. But this is not the hash backoff for station B. At the first hash function we got the backoff value 1 for Station B and at the second hash function the value is 2. So, ultimately the hash backoff for station B will be shifted 2 key from the hash backoff 1. So, the new hash backoff is 0. Now eventually, Station C gets the hash backoff 2. The formula regarding determining the hash backoff is given below:

First Hash Function:

hash backoff = (IP + Current Time) mod hash table size

Second Hash Function:

shifing value= m - (IP + Current Time) mod m

here m = immediate prime number which is less than the size of the hash table.

3.3.2 Modified Deterministic Backoff

Initial contention mechanism is resoloved by hashed backoff. After each successful transmission the stations will go through a modified determinisic backoff i.e. the backoff value will be same for the rest of the cycle until a beacon frame appears. The following algorithm shows how the deterministic backoff is used. Our approach is a fully decentralised and collision-free MAC for WLANs. It differs from CSMA/CA in that it uses a deterministic backoff, $B_d = \lceil CW_{min}/2 \rceil - 1$ after successful transmissions, where CW_{min} is the minimum contention window of typical value CW_{min} = 16. By doing so, contenders that successfully transmitted on schedule n, will transmit without colliding with other successful nodes in future cycles.

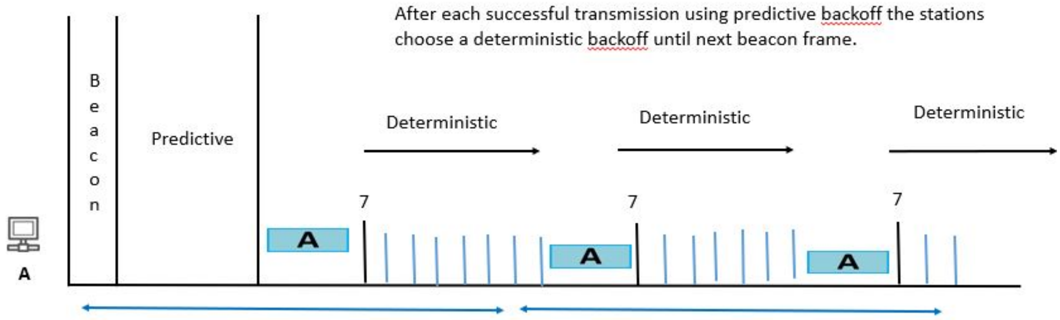

Figure 3.5: Modified Deterministic Backoff

Algorithm 2 provides an explanation of modified deterministic backoff procedure of our proposed approach in which the main difference from CSMA/CA is the assignment of fixed backoff after successful transmission and table 3.1 provides a short list of notations used throughout the text.

Algorithm 2: Deterministic Backoff
while the device is on **do**
r = 0 ; k = 0;
B = $\mu[0,\ 2^k CW_{min} - 1]$;
while there is a packet to transmit **do**
repeat
while B > 0 **do**
wait 1 slot;
B = B - 1;
Attempt transmission of 1 packet;
if collision **then**
r = r + 1;
k = min (k+1, m);
B = $\mu[0,\ 2^k CW_{min} - 1]$;
until (r = R) or (access);
r = 0;
k = 0;
if success **then**
$B_d = \lceil 2^k CW_{min}/2 \rceil - 1$;
B = B_d;
else
Discard packet;
B = $\mu[0, 2^k CW_{min} - 1]$;
Wait until there is a packet to transmit;

Table 3.1: Notation of Our Proposed Approach

Notation	**Description**
k	Backoff stage
m	Maximum backoff stage
B	Random backoff
B_d	Deterministic backoff
CW_{min}	Minimum contention window

3.3.3 Overall Protocol

The proposed scheme assumes that all stations on the medium are bounded by a deterministic backoff period, B_d. Certain number of time slots constitutes the deterministic backoff period. The timeline diagram as in figure 3.6 shows that three stations A, B, C are contending for the channel access. The horizontal lines represents a time axis with each number indicating the amount of empty slots left for the backoff to expire. Stations willing to transmit begin the contention for the channel by waiting a random backoff, B. The initial contention is resolved by using hashed backoff, so all the stations are sorted according to their backoff values and collision occurs. After each successful transmission all the stations will use modified deterministic backoff, B_d = 7.

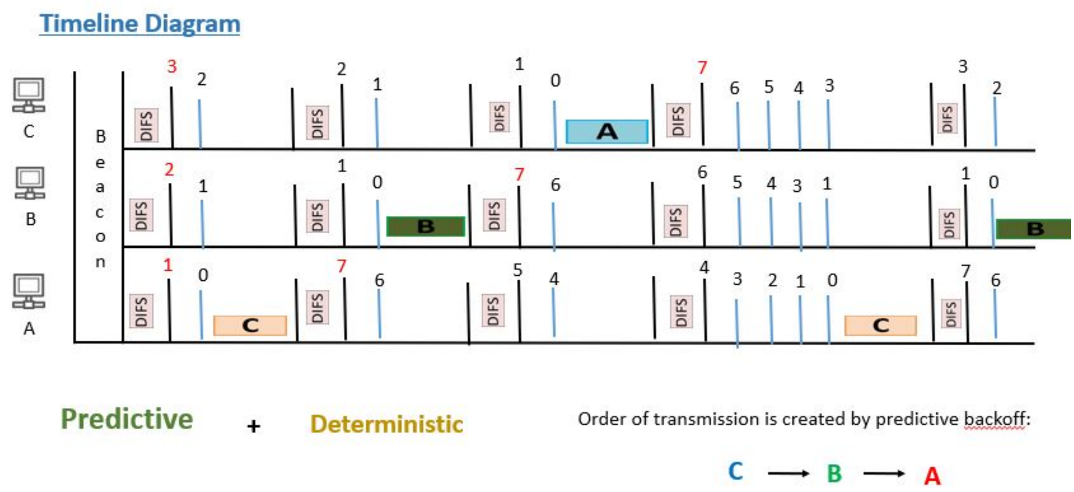

Figure 3.6: Overall approach for our protocol.

The reason we choose two kinds of backoff because of the complexity of using hash backoff and the simplicity of deterministic backoff. In initial channel access the stations has to calculate the backoff values of other stations which can be costly. Therefore, for the next transmission we have to use deterministic backoff for its simplicity as shown in figure 3.7

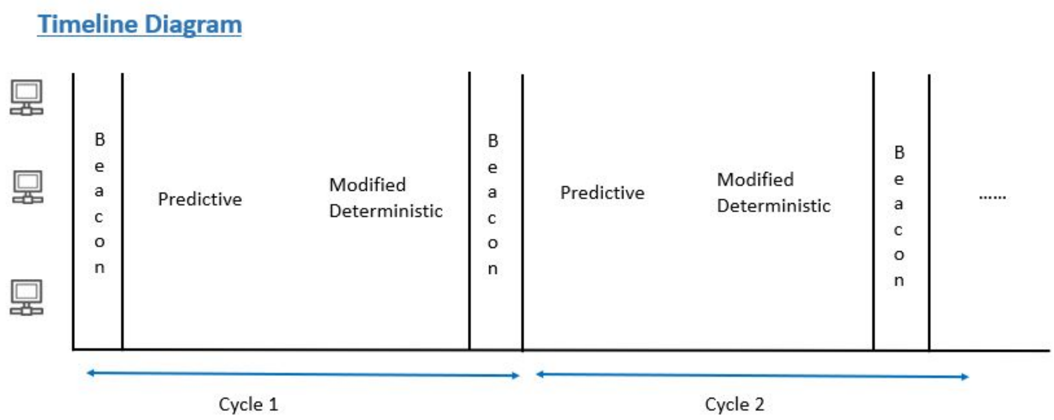

Figure 3.7: Use of two backoff in each beacon transmission.

3.3.4 Critical Operation

In our approach, a new station assoiciated with a network, waits for one learning cycle (approximately backoff period of at least two neighbouring stations) before its first transmission attempt. The backoff values of the new stations will be within the deterministic backoff values. In this way, a new station can enter into a collision free schedule easily. The modified backoff value of a new station is $DB_{new} = DB_{old} + DB_{old}/2$. As shown in the figure 3.8, a new station D enters the network after the three stations A, B, C initializes their network status. So there is no way station D can know the running deterministic backoff value of the network. So the station D waits for a learning cycle to know the running deterministic value of the network. In the figure 3.8, the running deterministic value was B_d = 7, so a new station D can pick up the backoff value from the range $[0, B_d]$. Here for station D, we use deterministic backoff $DB_{new} = DB_{old} + DB_{old}/2$ in this scenario.

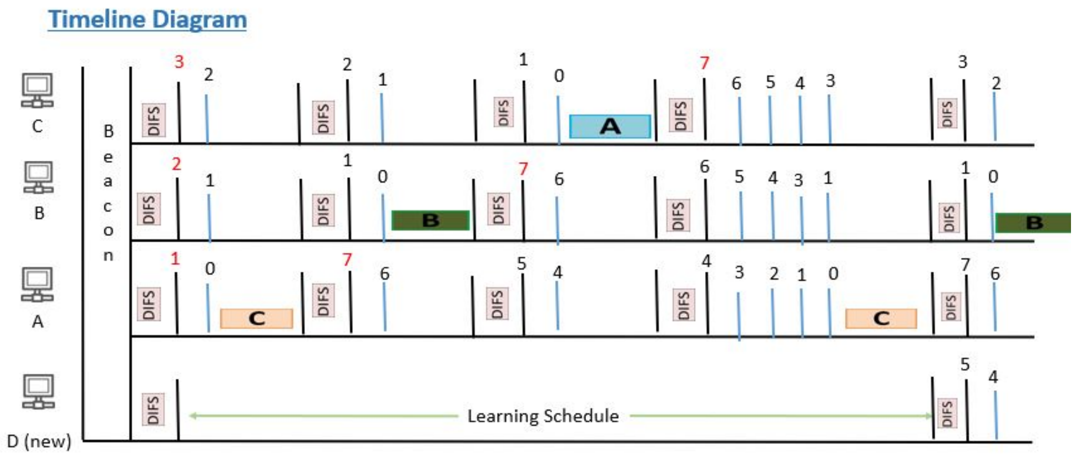

Figure 3.8: Critical operation of a new node association.

3.3.5 Backward Compatibility & Co-existence

Our approach springs from a modification to CSMA/CA's backoff mechanism. It keeps the range of values CSMA/CA nodes use to draw a random backoff (i.e. use the same CW_{min} and CW_{max}, allowing the contenders of our protocol to co-exist with CSMA/CA nodes in the same nework.

Chapter 4

Simulation & Results

This sections provides the simulation parameters for testing our protocol in different graphic conditions. We also provide details on channel errors and its effects on transmissions. The results are obtained by running multiple simulations over a simulation software called ns3 [2]. PHY and MAC parameters are detailed in table 4.1. Some assumptions were made in order to test the performance at the MAC layer:

- Unspecified parameters follow the IEEE 802.11n (2.4 GHz) amendment.
- All nodes are in communicaion range.
- No Request-to-Send (RTS) or Clear-to-Send (CTS) messages are used.
- Collisions take as much channel time as successful transmission.

Table 4.1: PHY and MAC parameters for the simulations

PHY	
Parameter	**Value**
PHY rate	65 Mbps
Empty Slots	9
DIFS	28
SIFS	10
MAC	
Parameter	**Value**
Maximum backoff stage (m)	5
Minimum Contention Window CW_{min}	16
Maximum retransmission attempts	6
Data payload (Bytes)	1024
MAC queue size (Packets)	1000

The aforementioned assumptions ensure that the simulation results are just effects of the MAC behaviour. If not mentioned otherwise, results are derived from 20 simulations of 100 seconds in length, each one with a different seed. Figure 4.1 also show the standard deviation.

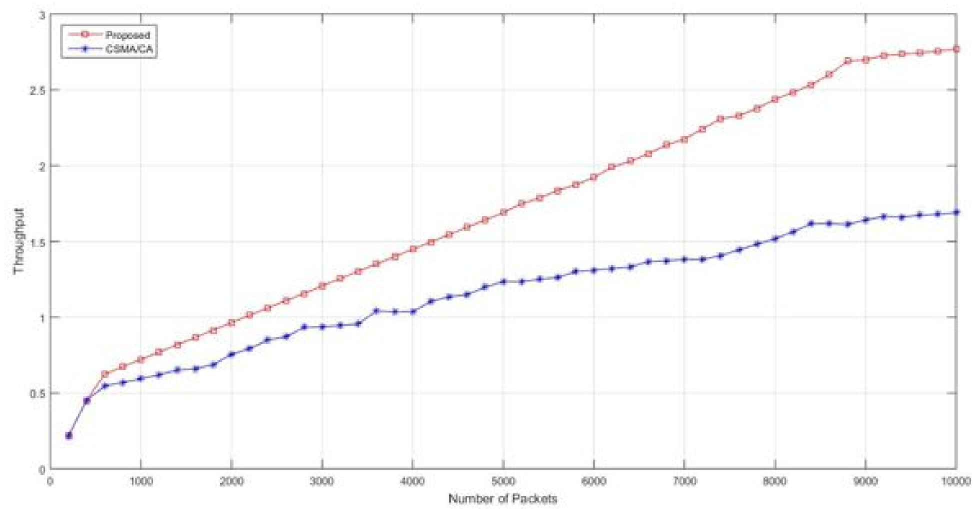

Figure 4.1: Simulation outcome.

The analytical study also shows that the predictive backoff reduces the idle listening and deterministic backoff reduces the collision as show in the figures 4.2 and 4.3.

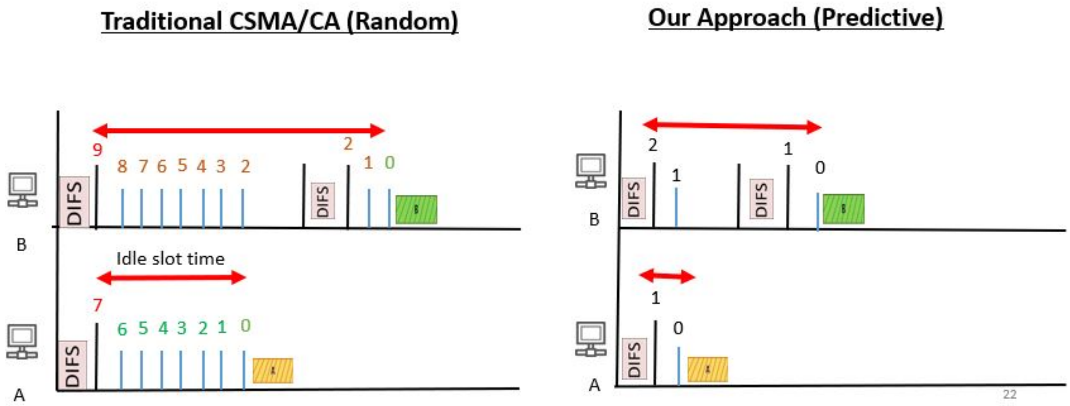

Figure 4.2: Simulation outcome.

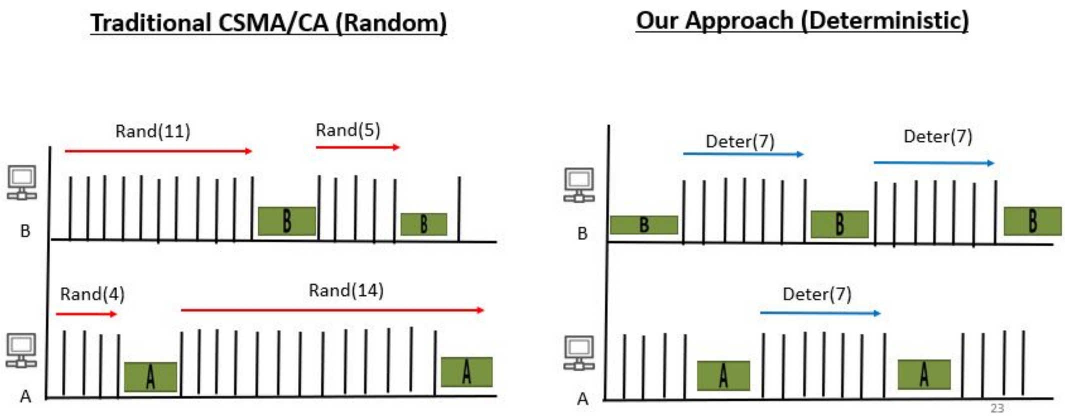

Figure 4.3: Simulation outcome.

Chapter 5

Conclusion

This article introduces an approach for channel access mechanism for IEEE 802.11 WLANs using predictive backoff and modified deterministic backoff. Combining the both approaches we came to realise that the traditional CSMA/CA requires much more improvement. Our approach is able to consruct a collision free schedule with many contenders. Taking the advantage of this condition, the cumulative throughput experienced by the nodes of our protocol goes beyond the achievable by CSMA/CA for any number of nodes.

APPENDIX A

APPENDIX A

Bibliography

[1] Y. He, J. Sun, X. Ma, A. V. Vasilakos, R. Yuan, and W. Gong, *Semi-random backoff: towards resource reservation for channel access in wireless lans*, IEEE/ACM Transactions on Networking (TON), 21 (2013), pp. 204–217.

[2] https://www.nsnam.org/.

[3] A. P. Jardosh, K. N. Ramachandran, K. C. Almeroth, and E. M. Belding-Royer, *Understanding congestion in ieee 802.11 b wireless networks*, in Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement, USENIX Association, 2005, pp. 25–25.

[4] J. Lee and J. C. Walrand, *Design and analysis of an asynchronous zero collision mac protocol*, arXiv preprint arXiv:0806.3542, (2008).

[5] T. Li, Q. Ni, D. Malone, D. Leith, Y. Xiao, and T. Turletti, *Aggregation with fragment retransmission for very high-speed wlans*, IEEE/ACM Transactions on Networking (ToN), 17 (2009), pp. 591–604.

[6] E. H. Ong, J. Kneckt, O. Alanen, Z. Chang, T. Huovinen, and T. Nihtilä, *Ieee 802.11 ac: Enhancements for very high throughput wlans*, in Personal indoor and mobile radio communications (PIMRC), 2011 IEEE 22nd international symposium on, IEEE, 2011, pp. 849–853.

[7] D. Panigrahi and B. Raman, *Tdma scheduling in long-distance wifi networks*, in INFOCOM 2009, IEEE, IEEE, 2009, pp. 2931–2935.

[8] I. Paudel and B. Jouaber, *I-dcf: Improved dcf for channel access in ieee 802.11 wireless networks*, in Vehicular Technology Conference (VTC Spring), 2014 IEEE 79th, IEEE, 2014, pp. 1–5.

[9] L. Sanabria-Russo, J. Barcelo, B. Bellalta, and F. Gringoli, *A high efficiency mac protocol for wlans: Providing fairness in dense scenarios*, IEEE/ACM Transactions on Networking, 25 (2017), pp. 492–505.

[10] S. SEN, R. ROY CHOUDHURY, AND S. NELAKUDITI, *No time to countdown: Migrating backoff to the frequency domain*, in Proceedings of the 17th annual international conference on Mobile computing and networking, ACM, 2011, pp. 241–252.

[11] K. TAN, J. FANG, Y. ZHANG, S. CHEN, L. SHI, J. ZHANG, AND Y. ZHANG, *Fine-grained channel access in wireless lan*, ACM SIGCOMM Computer Communication Review, 41 (2011), pp. 147–158.

[12] M. TUYSUZ AND H. A. MANTAR, *A beacon-based collision-free channel access scheme for ieee 802.11 wlans*, Wireless personal communications, 75 (2014), pp. 155–177.

[13] P. WANG AND W. ZHUANG, *A collision-free mac scheme for multimedia wireless mesh backbone*, IEEE Transactions on Wireless Communications, 8 (2009).

[14] Y. XIAO, *Ieee 802.11 n: enhancements for higher throughput in wireless lans*, IEEE Wireless Communications, 12 (2005), pp. 82–91.

[15] Y. XIAO AND J. ROSDAHL, *Performance analysis and enhancement for the current and future ieee 802.11 mac protocols*, ACM SIGMOBILE Mobile Computing and Communications Review, 7 (2003), pp. 6–19.

[16] W. ZAME, J. XU, AND M. VAN DER SCHAAR, *Learning perfect coordination with minimal feedback in wireless multi-access communications*, in Global Communications Conference (GLOBECOM), 2013 IEEE, IEEE, 2013, pp. 3861–3866.

[17] H. ZHAO, J. WEI, N. I. SARKAR, AND S. HUANG, *E-mac: An evolutionary solution for collision avoidance in wireless ad hoc networks*, Journal of Network and Computer Applications, 65 (2016), pp. 1–11.

[18] L. ZHENDONG, *802.11 ac/ad: The next generation wlan technology standard*, Modern Science & Technology of Telecommunications, 12 (2010), p. 004.