Study and investigate adaptation of iEEE 802.11e specific parameters in EDCA

Dissertation

Submitted to the

Central Department of Computer Science and Information Technology
Tribhuvan University
in partial fulfillment of the requirements for the degree of

Masters Degree in Computer Science and Information Technology

By

Rajiv Nakarmi

August, 2008

CERTIFICATE

This is to certify that the dissertation work entitled **"Study and investigate adaptation of iEEE 802.11e specific parameters in EDCA"**, submitted by **Rajiv Nakarmi** has carried out under my supervision and guidance. In my best knowledge this is an original work in computer science and no part of this dissertation has been published or submitted for the award of any degree else where in the past.

Asst. Prof. Sharad Ghimire
Dept. of Electronics and Computer Engineering
Institute of Engineering
Pulchowk Campus
(Supervisor)

Tribhuvan University

Institute of Science and Technology

Central Department of Computer Science and Information Technology

Kirtipur, Kathmandu

Nepal

LETTER OF APPROVAL

We certify that we have read this dissertation and in our opinion it is satisfactory in the scope and quality as a dissertation in the partial fulfillment for the requirement of Masters Degree in Computer Science and Information Technology.

Evaluation Committee

Head, Central Department of Computer Science and Information Technology Tribhuvan University	**Asst. Prof. Sharad Ghimire** Dept. of Electronics and Computer Engineering Institute of Engineering Pulchowk Campus (Supervisor)
Internal Examiner	**External Examiner**

ACKNOWLEDGEMENTS

It is a great pleasure for me to acknowledge the contributions of a large number of individuals to this work. First of all, I would like to thank my supervisor Asst. **Prof. Sharad Ghimire** for giving me an opportunity to work under his supervision, and providing guidance and support through out this work. I would like to thank **Asst. Prof. Deepesh Shrestha (KU, Dhulikhel)** for his valuable comments and suggestions during my work.

I would like to extend my sincere gratitude to **Prof. Dr. Devi Dutta Paudyal** (Former Head, Central Department of Computer Science and Information Technology) for his inspiration and encouragement during two years study of my Master Degree.

I would like to express my gratefulness to the respected teachers **Prof. Dr. Shashidhar Ram Joshi**, **Prof. Sudarshan Karanjeet**, **Asst. Prof. Arun Timilsina, Dr. Tanka Dhamala** (Head, CDCSIT), **Prof. Dr. Laxmi P. Gewali** (University of Nevada, Las Vegas, USA), **Asst. Prof. Min B. Khati**, **Mr. Hemanta B. G.C.** and all other teachers who have taught me during my Master Degree.

Finally, I am thankful to my friend **Anil Awale** for his fruitful discussions. Last but not least, I would like to thank my family members for their constant support and encouragement.

Rajiv Nakarmi

ABSTRACT

In this thesis, study and analysis of one of the parameters i.e. the transmission opportunity (TXOP) mechanism described in the IEEE 802.11e supplement has been done. The constant value of TXOP is replaced by dynamic value which is derived from the formula consisting of total number of packets transferred and total collided packets till that instance. In this thesis the performance of the wireless LAN using proposed dynamic value of TXOP is evaluated in NS2 simulator. The results are compared in graphs which are calculated in terms of throughput, latency and packet loss under different network scenarios.

Table of Contents

List of Figures

List of Tables

Chapter 1: Introduction

1.1 Background

IEEE 802.11 wireless LAN (WLAN) [1] is gaining its popularity and is being largely used all over the world. Due to its many characteristics like, simplicity, flexibility and low cost Wireless technology plays a major role in the next generation wireless communication networks. This technology provides ubiquitous (available everywhere) communication and computing environment in offices, hospitals, campuses, factories, airports etc. Now a day people demand for wireless high speed data communication like VOIP, multimedia communications, High Definition Television (HDTV) even when they are moving around the areas. To fulfill these demands, multimedia applications require some quality of service (QoS) support such as guaranteed bandwidth, delay, jitter and error rate. It is a great challenge for WLAN to provide these qualities of services due to QoS unaware functions of its medium access control (MAC) layer and noisy and variable physical (PHY) layer characteristics.

Lots of research has been going on to provide the better QoS support in 802.11. IEEE 802.11 Working Group is currently focusing on enhancement of QoS support which is known as 802.11e [2]. IEEE 802.11e is in its standardization process and its final draft has been released. IEEE 802.11e has defined two medium access mechanisms which are basically the improved version of DCF and PCF. The basic MAC (Medium Access Control) mechanism of 802.11 known as Distributed Coordination Function (DCF) is based on distributed channel access and employs CDMA/CA (Carrier Sense Multiple Access / Collision Avoidance) protocol for the medium access. Another access mechanism is centralized Point Coordination Function (PCF) which requires the AP as a point coordinator (PC). Today most of the wireless installations use DCF, whereas PCF is hardly implemented because of its complexity in design and inefficiency in access mechanism. Though IEEE 802.11 has become more popular, widely deployed and cost effective, it lacks to provide quality of service (QoS) support. Here, the different

applications demand different QoS guarantees, for example Voice over IP, or audio/video conferencing and Internet telephony require specified bandwidth, delay and jitter, but can tolerate some losses whereas text data can tolerate some delay but no packet loss. Here, all types of data traffic are treated equally in both DCF and PCF, regardless of the QoS requirements of the traffic so it cannot provide quality of service support. As different applications require different traffic specification, some mechanism must be provided for service differentiation to give higher priority data traffic a better service. Due to these problems 802.11 MAC mechanisms face a big hurdle in adaptation of multimedia data transmission in wireless.

IEEE 802.11 task group has been working to provide quality of service, which is known as IEEE 802.11e. It provides a distributed access mechanism to support Quality of Service by introducing service differentiation. Here, different types of traffic are assigned with different priorities based on their requirements and service differentiation is introduced by using a different set of medium access parameters for each priority.

Chapter 2: Introduction to IEEE 802.11

2.1 Introduction

From the extensive use of mobile cell phones and PDA's over the past ten years it is clear that people are more interested in wireless communications. It is because of its simplicity, flexibility and cost effective. This technology provides people with an ever-present communication and computing environment in offices, hospitals, campuses, factories, airports, stock markets, etc. As a result, traditional ways of networking the world have proven inadequate to meet the new challenges posed by wireless. If users has to be connected to a network by physical cables, their movement would be dramatically reduced to limited area. Wireless connectivity, however, poses no such restrictions and allows a great deal of free movement on the part of the network user. The low-cost and high-speed WLANs can be integrated within the cellular coverage to provide hotspot coverage for high-speed data services, thus becoming an integral part of next generation wireless communication networks.

In 1997, IEEE (Institute of Electrical and Electronics Engineers) released the 802.11 Wireless Local Area Network (WLAN) standards [3]. As the name suggests, it belongs to the group of popular IEEE 802.x standards, e.g., IEEE 802.3 Ethernet [4] and IEEE 802.5 Token Ring [5]. IEEE 802.11 defines Media Access Control (MAC) and Physical (PHY) layers specifications for wireless LANs. Three different Physical layer specifications were defined, namely, Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS) and Infrared (IR), with the maximum data transmission rate of up to 2 Mbps. The DSSS and FHSS Physical layers operated in the license free 2.4 GHz ISM (Industrial, Scientific and Medical) band. With the passage of time, while the original MAC remained intact, the technology continued evolving with the new Physical layer specifications. In 1999, IEEE introduced two enhanced Physical layer specifications 802.11b [6] and 802.11a [7] with data transmission rates of up to 11 and 54 Mbps, respectively. 802.11b is also based on DSSS and operates in the 2.4 GHz band and

802.11a is based on OFDM (Orthogonal Frequency Division Multiplexing) and operates in the 5 GHz band.

In 2003, IEEE released 802.11g [8] that extended 802.11b Physical layer to support data transmission rates of up to 54 Mbps in the 2.4 GHz band. IEEE 802.11 gained immense popularity due to its cost effectiveness and easy deployment.

802.11 standards comparison table			
IEEE Standard	**Speed (Mbps)**	**Frequency Band (GHz)**	**Notes**
802.11	1 to 2	2.4	First Standard (1997). Featured both frequency hopping and direct-sequence modulation techniques.
802.11 a	up to 54	5	Second standard (1999), but products not released until late 2000
802.11b	5.5 to 11	2.4	Third standard, but second wave of products.
802.11 g	up to 54	2.4	Not yet standardized

Table 2. 1: 802.11 standards comparison table

These days wireless network technologies are mostly deployed in the communication world. IEEE 802.11 hotspots are available at home, offices, campuses, airports and public transport stations. IEEE 802.11 defines two different architectures, one is called BSS (Basic Service Set) and other is IBSS (Independent BSS). In a BSS, all the wireless stations are associated with a particular AP (Access Point). AP acts as a coordinator and all the communication take place through the AP. In IBSS stations can directly communicate with each other without associating with any AP just like ad-hoc. In this case if two stations are under the range of other then they can communicate with each other. This form of architecture is facilitated to form a wireless ad-hoc network in the absence of any network infrastructure. Several BSS can be connected together via a Distributed System (DS) to form an external network, called Extended Service Set (ESS).

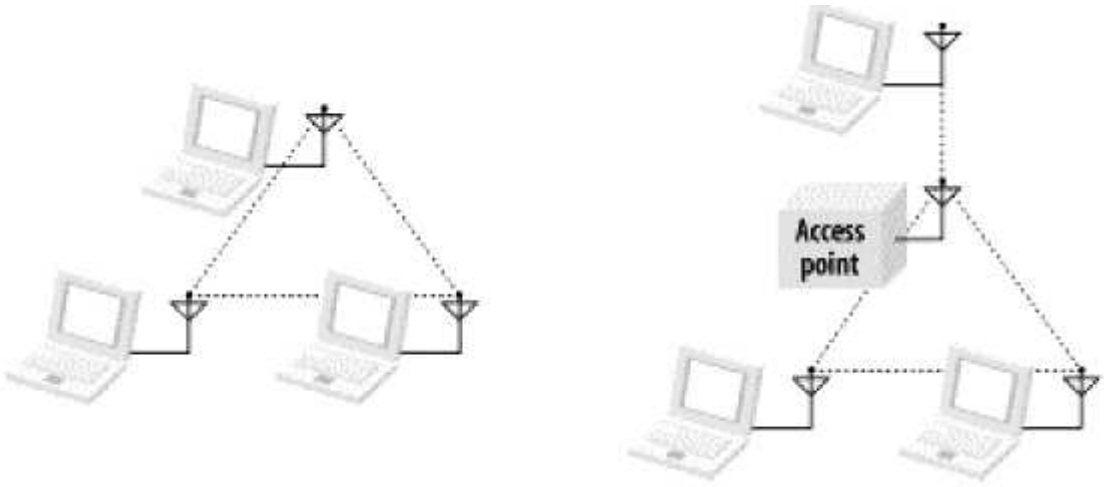

Figure 2. 1:Independent and dependent infrastructure BSSs

The fundamental access mechanism of IEEE 802.11 MAC is the Distributed Coordination Function (DCF) and optional Point Coordination Function (PCF). The DCF is a carrier sense multiple access protocol with collision avoidance (CSMA/CA) and PCF use a central coordinator for assigning the transmission right to stations, thus guaranteeing a collision free access to the shared wireless medium. While DCF has gained enormous popularity and been widely deployed, the use of PCF has been rather limited. Though, IEEE 802.11 standard was targeted at best efforts services for data transfer, but in future it is expected that WLANs will need to adapt to provide service differentiation for multimedia and interactive data transfer. Thus, A new standard, namely IEEE 802.11e, has been proposed to support QoS-sensitive data transmission. IEEE 802.11e again defines two access mechanisms namely EDCA (Enhanced DCF) and HCF (Hybrid coordination Function). Among these EDCA appears to be gaining earlier acceptance.

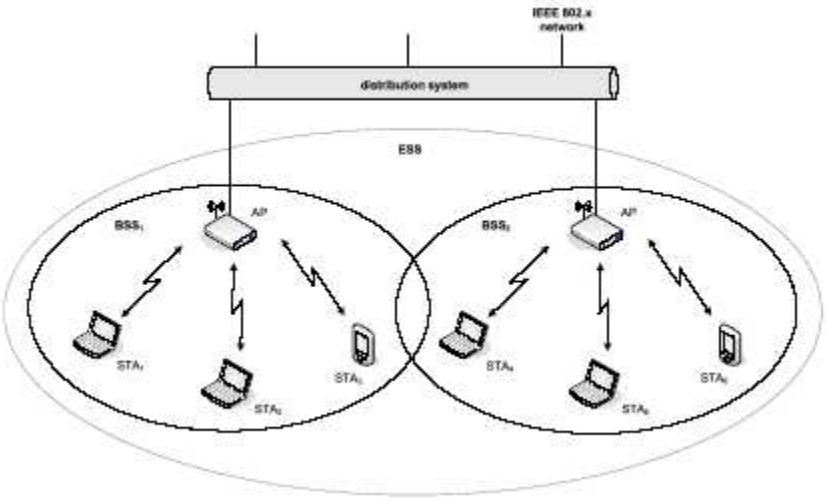

Figure 2. 2: Architecture of IEEE 802.11 Network

The Internet Engineering Task Force (IETF) has defined two different frameworks, Integrated Services (IntServ) [21] and Differentiated Services (DiffServ) [22], to support QoS for the traffic over Internet.

IntServ: IntServ can provide very high QoS to IP packets. Essentially, applications signal to the network that they will require special QoS for a period of time and that bandwidth is reserved. With IntServ, packet delivery is guaranteed. However, the use of IntServ can severely limit the scalability of a network.

Some applications, such as high-resolution video, require consistent, dedicated bandwidth to provide sufficient quality for viewers. IntServ was introduced to guarantee predictable network behavior for these applications. Because IntServ reserves bandwidth throughout a network, no other traffic can use the reserved bandwidth. Bandwidth that is unused, but reserved, is wasted.

IntServ is similar to a concept known as “hard QoS” With hard QoS, traffic characteristics such as bandwidth, delay, and packet-loss rates are guaranteed end to end. This guarantee ensures both predictable and guaranteed service levels for mission-critical applications. There will be no impact on traffic when guarantees are made, regardless of additional network traffic. Hard QoS is accomplished by negotiating specific QoS

requirements upon establishment of a connection and by using Call Admission Controls (CACs) to ensure that no new traffic will violate the guarantee. Such guarantees require an end-to-end QoS approach with both complexity and scalability limitations. Large network environments that contain heavy traffic loads will be extremely challenged to track QoS guarantees for hundreds of thousands of signaled flows. Using IntServ is like having a private courier airplane or truck dedicated to the delivery of your traffic. This model ensures quality and delivery, is expensive, and is not scalable.

IntServ is a multiple-service model that can accommodate multiple QoS requirements. IntServ inherits the connection-oriented approach from telephony network design. Every individual communication must explicitly specify its traffic descriptor and requested resources to the network.

In the IntServ model, the application requests a specific kind of service from the network before sending data. The application informs the network of its traffic profile and requests a particular kind of service that can encompass its bandwidth and delay requirements. The application is expected to send data only after it gets a confirmation from the network. The application is also expected to send data that lies within its described traffic profile.

DiffServ: DiffServ provides the greatest scalability and flexibility in implementing QoS in a network. Network devices recognize traffic classes and provide different levels of QoS to different traffic classes.

The Internet was designed for best-effort, no-guarantee delivery of packets. This behavior is still predominant on the Internet today. If QoS policies are not implemented, traffic is forwarded using the Best-Effort model. All network packets are treated exactly the same—an emergency voice message is treated exactly like a digital photograph attached to an e-mail. Without the implementation of QoS, the network cannot tell the difference between packets and, as a result, cannot treat packets preferentially. When a letter is posted in standard postal mail, it uses a Best-Effort model. The letter will be treated exactly the same as every other letter; it will get there when it gets there. With the Best-

Effort model, the letter may actually never arrive and, unless it has a separate notification arrangement with the letter recipient, It may never know if the letter does not arrive.

DiffServ was designed to overcome the limitations of IntServ models. DiffServ can provide an "almost guaranteed" QoS, while still being cost-effective and scalable. DiffServ is similar to a concept known as "soft QoS." With soft QoS, QoS mechanisms are used without prior signaling. In addition, QoS characteristics (bandwidth and delay, for example), are managed on a hop-by-hop basis by policies that are established independently at each intermediate device in the network. The soft QoS approach is not considered an end-to-end QoS strategy because end-to-end guarantees cannot be enforced. However, soft QoS is a more scalable approach to implementing QoS than hard QoS, because many (hundreds or potentially thousands) of applications can be mapped into a small set of classes upon which similar sets of QoS behaviors are implemented. Although QoS mechanisms in this approach are enforced and applied on a hop-by-hop basis, uniformly applying global meaning to each traffic class provides both flexibility and scalability. With DiffServ, network traffic is divided into classes based on business requirements. Each of the classes can then be assigned a different level of service. As the packets traverse a network, each of the network devices identifies the packet class and services the packet according to that class. In this model packet can choose many levels of service. For example, voice traffic from IP Phones is usually given preferential treatment over all other application traffic. E-mail is generally given Best-Effort service. And non business traffic can either be given very poor service or blocked entirely.

2.2 Carrier-Sensing Functions and the Network Allocation Vector

Carrier-Sensing is used to check if the wireless link is free to use. Two types of carrier sensing functions are used to manage the link. First one is physical carrier sensing and other one is virtual carrier-sensing functions. Physical carrier-sensing function is provided by physical layer and depends on the medium and modulation used. It is difficult and expensive to build physical carrier-sensing hardware for RF-based media, because transceivers can transmit and receive simultaneously only if they incorporate

expensive electronics. Also, physical carrier-sensing cannot provide all the necessary information for solving hidden node problem. Virtual carrier-sensing is provided by the Network Allocation Vector (NAV). NAV is a duration during which station can use the medium, including any frames necessary to complete the current (or atomic) operations. NAV is a timer that indicates the amount of time the medium will be reserved. Other stations that are trying to access the medium count down from NAV to 0. When the NAV is nonzero, the virtual carrier-sensing function indicates that the medium is busy; when the NAV reaches 0, the virtual carrier-sensing function indicates medium is idle. NAV helps to guarantee the transmission of atomic operation are not interrupted.

For example, the RTS/CTS sequence in Figure 2-3 is atomic. Figure 2-3 shows how the sequence of interruption is protected by NAV. Shaded bars are used to show the activity on the medium by stations. Here, each bar is labeled with the frame type. Interframe spacing is depicted by the lack of any activity. At the bottom the NAV timer is represented by the bars on the NAV line. The NAV is carried in the frame headers on the RTS and CTS frames; it is shown on different line how the NAV relates to actual transmissions in the air. When ever there is a NAV bar is present on the NAV line, stations should defer access to the medium because the virtual carrier-sensing mechanism will indicate a busy medium.

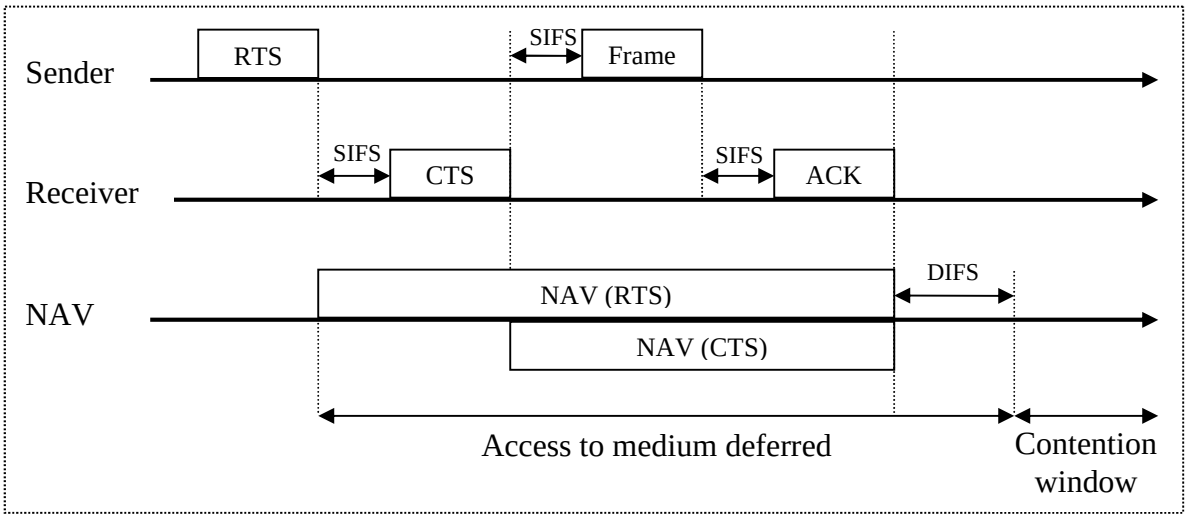

Figure 2. 3: Using the NAV for virtual carrier sensing

Here, so as to confirm the sequence of transmission is not interrupted, node 1 sets NAV in its RTS to block other station from accessing the medium. All stations that hear the RTS defer access to medium until NAV reaches to zero. Though, RTS frame is transmitted to all only the intended station responds and sends back CTS frame which also include a shorter NAV (CTS). This NAV prevents other stations from accessing the medium until the transmission is over. When DIFS has elapsed then other stations can access the medium during contention window. RTS/CTS mechanism is useful in crowded areas with multiple overlapping networks where hidden node problem may exist. Even other stations are in different networks they receive NAV frame and defers access appropriately.

2.3 Interframe Spacing

Interframe spacing plays a significant role in coordinating access to the transmission medium. In 802.11 there are four different Interframe spaces which are described below:

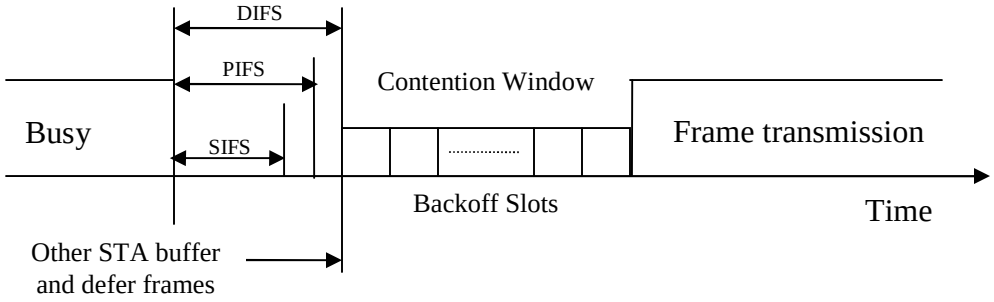

Figure 2. 4: Interframe spacing relationships

In 802.11 MAC, station delay transmission until the medium becomes idle and this is carried out by using varying interframing spacing. Different interframing spacing creates different levels of priority for different types of traffic. The different levels of priority facilitate so that high-priority traffic doesn't have to wait as long after the medium has become idle thus gets earlier chance to access the medium then lower priority traffic. To be interoperable between different data rates, the interframe space is a fixed amount of

time, independent of the transmission speed. Different physical layers, however, can specify different interframe space times.

Short interframe space (SIFS)

Short interframe space is the shortest interframe so it is used for the highest-priority transmissions, such as RTS/CTS frames and positive acknowledgements. As soon as SIFS time elapses, high-priority transmissions can begin. And once high-priority transmission start, the medium becomes busy, so frames transmitted after the SIFS has elapsed have priority over frames that can be transmitted only after longer intervals.

PCF interframe space (PIFS)

It is also called priority interframe space. It is used by PCF during contention free operations. Stations that has data to transmit in the contention free period can transmit after the PIFS elapsed and prevent any contention based traffic.

DCF interframe space (DIFS)

It is minimum medium idle time for contention based services. Station has to wait for DCF interframe time to get access to medium. After that it may have immediate access to the medium once the medium is free for a period more than DIFS period.

Extended interframe space (EIFS)

Extended interframe space is not fixed interval. It is used only when there is an error in frame transmission. It is not used to control access onto the radio link.

2.4 DCF (Distributed Coordination Function)

DCF is the basis for the standard CSMA/CA access mechanism. CSMA works as listen before talk. Like Ethernet, it first checks to see whether radio link is clear or not. If the medium is found clear for DIFS time period, then transmission starts if not then waits for medium to be clear. When destination receives frame it acknowledges by sending back

ACK frame after SIFS time period. Collision is avoided by assigning different backoff values for each station contending to access medium once the medium is seized by any other station. Backoff value is a random value which is drawn between (contention window) CWmin and CWmax. CTS/RTS mechanism is also used to further reduce the possibility of collisions.

SIFS is the shortest of the three Inter frame spaces defined in IEEE 802.11 to control the access to the medium. IFS relationship is shown in figure 2.5. Succeeding frame transmissions are separated by these inter frame spaces depending on the priority of the frame exchange sequence, so, higher the priority of the frame sequence, shorter the interframe space used between the frames. In the above figure 2.3, the SIFS between the data and acknowledgement frame is used to prevent other stations from accessing medium at the same time and to reduce transmission failure. As other station has to wait for DIFS time period which is longer than SIFS, this reduces the collision. Thus, ACK transmission is given high priority over station transmitting data frames.

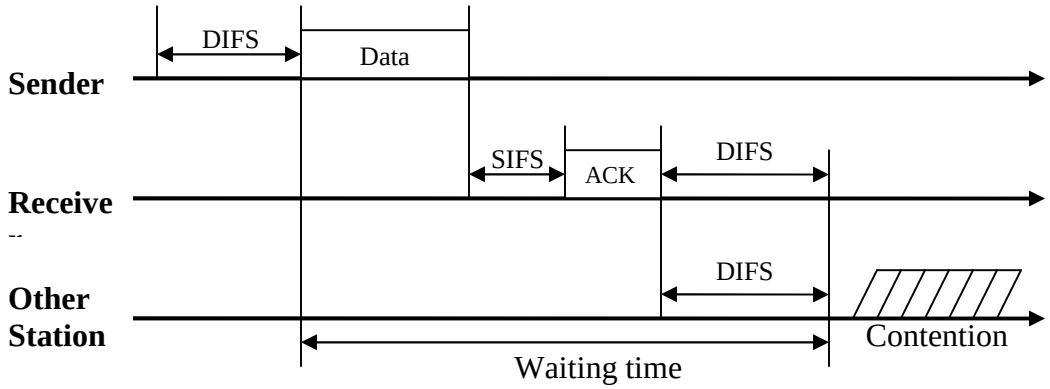

Figure 2. 5: DCF basic access mechanism.

The second shortest interframe space is PIFS which is used by access point in PCF (the optional access mechanism of IEEE 802.11). In PCF Point Coordinator (PC) or Access Point (AP) centrally controls the access to the medium by polling each station one after another. In PCF PC has priority over other stations so PC has to wait for PIFS time period (which is shorter than DIFS) after the medium is freed. The value of interframe space is

dependent on the underlying physical layer (PHY) and defined in relation to a slot time. PIFS consists of a SIFS plus one slot time and DIFS consists of SIFS plus two slot times.

Two types of carrier sensing are used to determine whether the medium is free or busy. One is Physical Carrier Sensing in which wireless channel is sensed itself at Physical Layer. And another is Virtual Carrier Sensing which is used at MAC layer. In the MAC layer when station receives a frame that is not send to it, what it does is it examines the duration field on the frame header, this header tells time required to transmit the frame to the destination station plus time to send ACK to the source in response, from this time all other stations defers the access to the medium for that particular period of time.

2.4.1 Collision Avoidance and Backoff Procedure

Considering the above scenario if two or more stations sense the medium busy and try to access at the same time after medium is freed then collision will occur. In order to avoid such situation, station has to wait an additional time which is called backoff period again after waiting for DIFS time period. Here, if even two or more stations sense the medium busy, the stations defer access until the medium becomes idle, and draws a random backoff value which specifies the time period measured in time slots. Now, all the stations that are waiting for channel access has to wait for backoff period in addition to DIFS. Since, backoff for each station is drawn randomly, different stations will get different value and wait time differs as a result no collision will occur. If this was not case all the stations will try to access the medium at a same time. This mechanism is called Collision Avoidance (CA), and thus the process is called CSMA/CA.

Actually, in wireless medium, there is no collision detection mechanism to determine whether collision has occurred as in the case of IEEE 802.3 Ethernet [4]. In Ethernet transceiver can communicate in full duplex mode i. e, two stations can receive and transmit at a same time and therefore able to detect collisions. In wireless networks two stations cannot receive and transmit simultaneously. Even if the station has the ability of

receiving and transmitting at a same time, the fundamental characteristics of wireless communication do not allow it to detect other signals. In wireless medium the strength of the signal decreases proportionally to square of the distance between sender and receiver. Also due to various types of interferences, fading and noises it attenuates the signal strength making impossible to sense the others signal in the presence of its own signal. It is because the strength of own signal is several times higher than the strength of others signal [9]. Thus, in wireless collision detection is not possible as in the case of Ethernet where signal strength doesn't drop below an acceptable level and it is possible to detect the colliding signal. The station starts decrementing its backoff time as soon as the medium is sensed idle for atleast DIFS time period. In case if the medium is accessed by other station then this backoff process is halted. When the medium is freed and sensed idle for DIFS time period the station resumes its paused backoff timer again. When the timer reaches to zero the station starts transmission. Here, to allow the station which has waited longer or tried to access the medium first will get priority over other station as it has to decrement only the remaining backoff time. And the random backoff value is chosen from the interval CWmin and CWmax. CWmin is used during first transmission. After each unsuccessful transmission the contention window is doubled until it reaches CWmax and it remains there for further retransmissions. The CW is increases exponentially by (2 x (CW + 1) -1) until it reaches the CWmax. The value of CWmin and CWmax are dependent on the underlying physical layer. For example DSSS PHY uses 31 and 1023 values as CWmin and CWmax. Here, for each unsuccessful transmission it increases in the form of 31, 63, 127, 255, 511 and 1023. For further retransmission it will remain at 1023 and after once successful transmission the value is set to minimum i.e. CWmin.

Collision is detected when sender does not receive any ACK frame within a specified time. After ACK timeout period has elapsed the station assumes that collision has occurred and the station enters into the backoff period again after waiting for the medium to be idle for DIFS. Now, new backoff value will be drawn from the interval CWmin and (2 x (CWmin + 1) -1). With the new CW which is the double of previous CW it reduces

the probability of collision as large number of distinct numbers can be drawn from doubled CW.

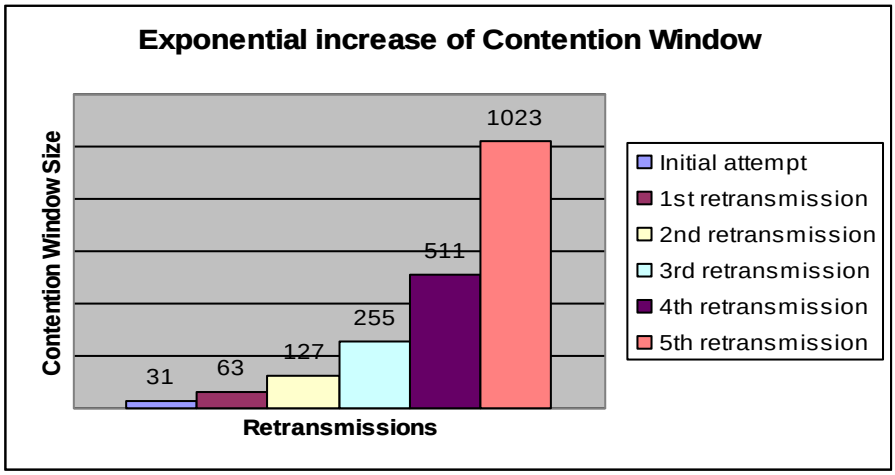

Figure 2. 6: Exponential increase of Contention Window.

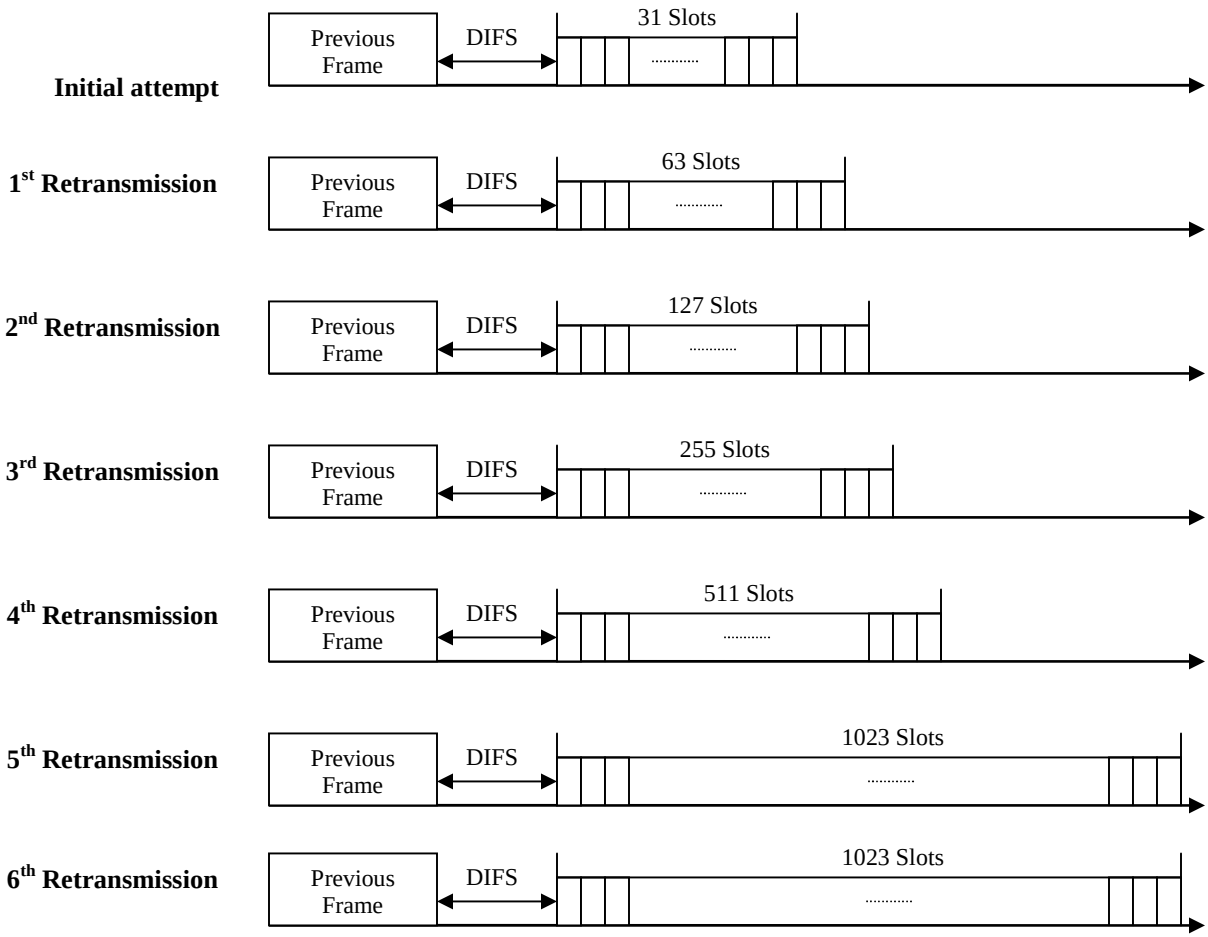

Figure 2. 7: DSSS contention window size

DCF specified a retransmit limit or retry limit which is the number of times the frame can be retransmitted. Once the retransmit limit is reached and if unsuccessful transmission is detected then that frame will be dropped. After first successful transmission the CW is reset to CWmin. The backoff mechanism is also used after successful transmission before sending the next frame. When sender station has to send another frame, it has to wait the medium to be idle for the DIFS time and chooses a new backoff value. This is called post backoff which ensures that there is at least one backoff interval between two consecutive transmissions. This provides other stations to decrement their backoff value and opportunity to access the medium sooner.

Some times the last post backoff time may have already been elapsed i.e. the queue is empty, and then in that case the station can immediately access the medium just after DIFS time period. The frame immediately after this frame has to be transmitted after backoff, until the transmission queue is empty.

Though, all these mechanisms are used for collision avoidance, it doesn't remove the total risk of collisions. Collision may occur if two or more stations reach its backoff timers to zero at the same time. This may also happen if two or more stations draw same random backoff value. Here, the probability of collision is high when Contention Window size is small as there is more chances to get same number from small CW. On the contrary larger CW value may result in longer delay and inefficient bandwidth utilization. In the following example I have further explained about backoff procedure and collision. Also, the important role of DIFS and CWmin and CWmax parameters in the access mechanism process has been described.

2.4.2 Example of DCF Operation

In the following figure 2.8, station 3 tries to access, since the medium is free there is no backoff process, the station starts its transmission immediately after sensing the medium idle for the DIFS time period. This period is indicated by busy in the time line. In the mean time station 1 and 2 arrive and try to sense the medium idle for DIFS time period, as the medium is busy with station 3, they defer the access. After the transmission of station 3 finishes and the medium becomes idle for DIFS time period, a random backoff is drawn for each station from contention window. Lets suppose that each get backoff of slot time 6, 14 and 19 respectively. The backoff performed by station 3 is called post backoff since it is done after the successful transmission of first frame. After getting backoff period each station starts to decrement the backoff counter till the medium is free, once the medium is accessed by any station remaining stations will defer the countdown until the medium becomes free again. Here in the example station 1 get

backoff value 6 it will get first chance to access the medium while other stations 2 and 3 have deferred counter at 8 and 13 respectively.

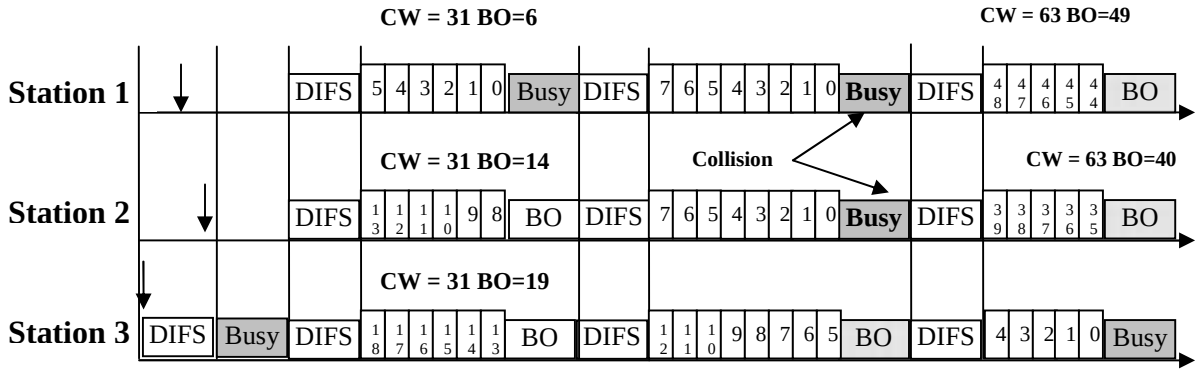

Figure 2. 8: DCF access mechanism with backoff procedure.

After the medium becomes idle and DIFS time period has elapsed again, station 1 draws a new backoff value of 8, while station 2 and 3 resumes their backoff timers. Here, remaining backoff of station 2 and new backoff of station 1 are same, both will try to access the medium at the same time when the counter reaches 0. And station 3 senses the medium busy and defers its countdown at 5. Due to lack of collision detection, both the stations 1 and 2 won't know about the collision, so both stations will wait for ACK frame from destination stations. As no ACK frame will receive within ACK timeout period, both stations assumes that a collision has occurred, and thus try to resend the same frame with new backoff value which is drawn from double the contention window size than before. Once the medium is freed for DIFS time period, station 1 and 2 will draw new backoff value as 49 and 40 respectively. At this time backoff value of station 3 is 5, so after 5 slot time station 3 will access the medium while stations 1 and 2 will defer their respective counter until the medium is free and DIFS time period has elapsed.

2.4.3 RTS/CTS Mechanism

RTS/CTS mechanism is used to avoid hidden node problem found in wireless networks that use CSMA. In RTS/CTS mechanism sender and receiver exchange RTS and CTS control frames by performing handshake mechanism as shown in the figure 2.9 below.

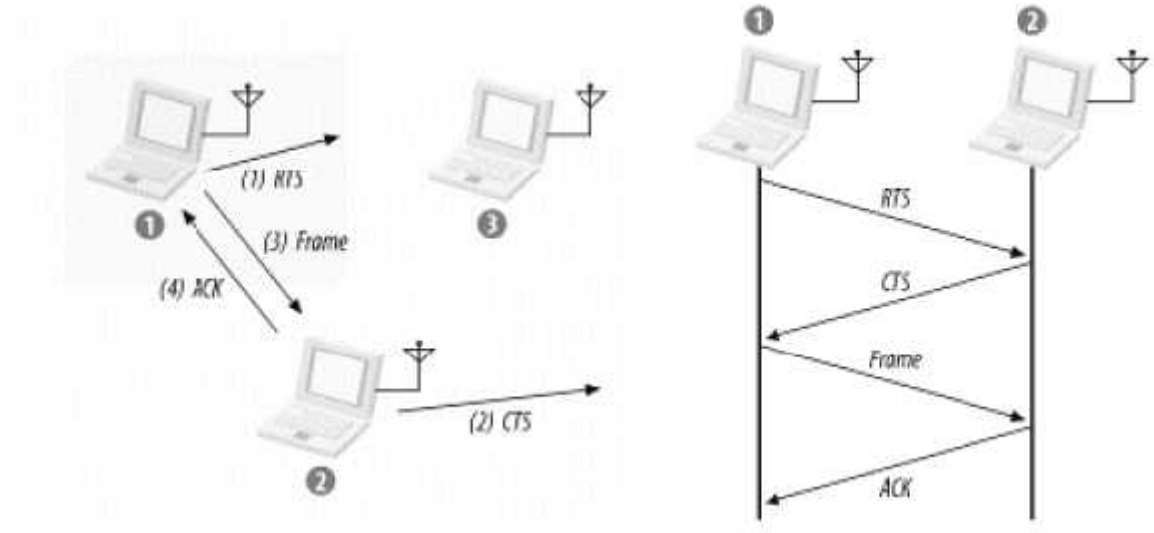

Figure 2. 9: RTS/CTS clearing

After DIFS has elapsed the sender first transmit RTS frame to receiver, and receiver in response sends back CTS frame after SIFS time period. The CTS frame indicates that handshake is successful and confirms that the medium can be used by sender and receiver for transmission.

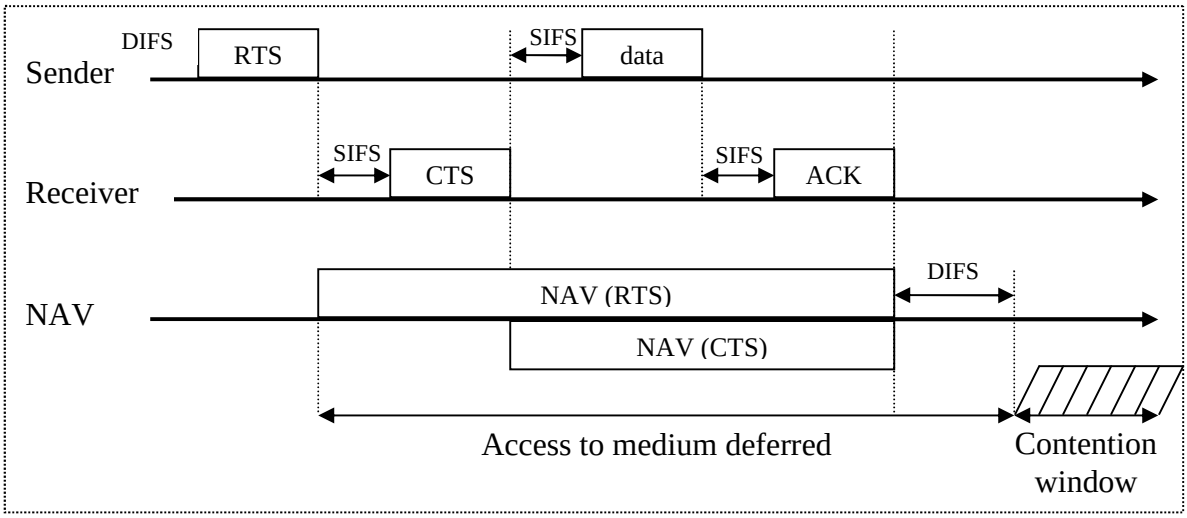

Figure 2. 10: Frame exchange sequence with RTS/CTS mechanism

RTS/CTS mechanism uses Virtual Carrier Sensing i. e, NAV is used to ensure the complete exchange of RTS and CTS frames including SIFS and ACK. Here, the stations within the range of receiving and sender stations sets the NAV after receiving the RTS and CTS frames, so that other stations know they have to wait until RTS/CTS transmission is completed. NAV is same like backoff timer which is decremented in each slot time and once it reaches to zero then only other stations can access the medium.
RTS/CTS mechanism doesn't totally eliminate collision. At the beginning two or more stations may start transmitting at a same time resulting in a collision. Here, if the RTS frame sender doesn't receive CTS frame within a specified time sender transmit the RTS frame again. As the size of RTS frame is smaller compared to data frame, even though there is a collision, RTS/CTS mechanism provides a fast recovery from collisions, as sender becomes aware of failure and retransmit more quickly. Also, SIFS interval between RTS, CTS and data frames prevents other stations to transmit and thereby interrupting the transmission. RTS/CTS mechanism requires extra burden of transmitting RTS and CTS exchange between each frame transmission so this results in inefficient bandwidth utilization, overhead and higher delays when used with smaller data frames, so it is best suited for transmission of larger frames only.

In the above figure 2.10, node 1 initiates transmission by sending RTS frame. If the target station receives this frame it will send the CTS frame to begin the transmission of data. All other stations receiving RTS or CTS frame which are not intended to them silences and waits. Once the RTS/CTS frame exchange is completed, node 1 can begin transmission of frames. In transmission of each frame sender waits for ACK from receiver for confirmation. The RTS/CTS procedure may be controlled by setting the RTS threshold so that RTS/CTS mechanism is used for frames larger than the threshold.

2.4.4 Fragmentation

In order to minimize the Bit Error Rates (BER) in WLAN occurred by interference, frames are fragmented which exceeds the threshold value. Each fragment is transmitted

and acknowledge is received in return and then only another transmission starts. Frames are fragmented as smaller frames have higher probability of being transmitted without any errors. Once, a station reserves the medium, it can send multiple fragments of the frame i. e, in each fragment burst period multiple fragments can be transmitted which are separated by SIFS as shown in figure 2.11. During fragmentation burst no other station is able contend for the medium thus preventing disturbances of multiple fragment transmission.

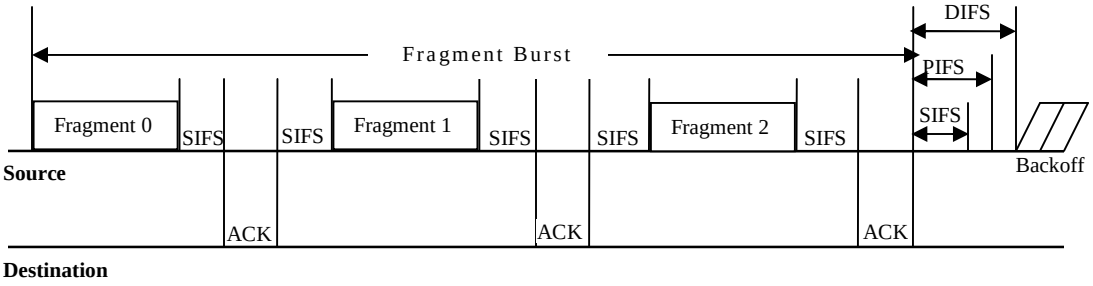

Figure 2. 11: Frame Fragmentation

Chapter 3: Quality of Service and Limitations of IEEE 802.11

3.1 Introduction

The quality of data traffic over a network is described by set of qualitative and quantitative characteristics, such as throughput, delay, jitter and packet loss. The application has certain QoS requirements, and the network or application point of view. The application has certain QoS requirements, and networks that provide these requirements is said to support QoS. QoS requirements vary from application to application and can be classified as bandwidth, delay, jitter and data loss [10].

3.1.1. Bandwidth:

Bandwidth is an important parameter and refers to the amount of data that can be transfer during a given period of time. Bandwidth is often measured with respect to throughput, which is the data transfer rate, measured as the number of bits transmitted per second. Greater the bandwidth, lager the application receives data packets and vice versa. Several other terms are used for bandwidth such as data rate, transmission rate, bit rate and capacity. Some applications are bandwidth sensitive which requires data transfer at constant rate, such application in the absence of bandwidth results in undesirable delays and data loss. For example, multimedia applications, internet telephony (VoIP) and videoconferencing require dedicated bandwidth. On the other hand some applications like email, file sharing, web and instant messaging does not require bandwidth constraints but require delivery guarantee. To eradicate the bandwidth problem one simply solution is increasing the link capacity to accommodate all applications and user, with some extra bandwidth to spare. Though this solution is simple, but increasing bandwidth is expensive and takes time to implement. Also, there are technological limitations in upgrading the existing system. One another solution can be classifying the traffic into QoS classes and

prioritize traffic according to its importance. Thus, voice and video traffic should get higher priority where as background and best effort traffics will get remaining bandwidth. Another solution can be, optimizing link usage by compressing the payload of frames which increases the link bandwidth. Compression, on the other hand, also increases delay because of the complexity of compressions algorithms. Hardware compressions can be used to accelerate the packet compression. Also, for the small data frames, header compression can be used where payload to header ratio is small.

3.1.2. End to end delay:

End to end delay is the total delay from the time packet is generated at sender side to the time application at the receiver side receives it. It includes all types of delay such as processing delay, queuing delay, propagation delay etc. It consists of two parts:
Fixed network delay: Two types of fixed delays are serialization and propagation delays. Serialization is the process of placing bits on the circuit. So, if the link is higher speed the delay will be less. Where as propagation delay is the time it takes frames through physical media.

Variable network delay: Processing delay is a type of variable delay, and is the required by networking devices to look up the actual route, change the header, and complete other switching tasks. In some case the packet also must be manipulated, as for example, when the encapsulation type or the hop count must be changed. Each of these steps can contribute to the processing delay.

In summary, there are four types of delay, as follows:

i. Processing delay: the time a networking device takes the packet from input interface and put the packet into the output queue of the output interface. The processing delay depends upon CPU speed, CPU utilization etc.

ii. Queuing delay: The time a packet resides in the output queue before it is transmitted. Queuing delay depends upon number of packets, size of each packet in the queue, bandwidth of the interface and the queuing mechanism. End to end delay highly affects voice applications, and packets that is delayed only few milliseconds are useless.

iii. Serialization delay: The time to place frame on the physical medium for transport.

iv. Propagation delay: Time to travel packet on the physical media interface. Propagation delay depends upon the velocity of the propagation of the signal across the transmission media [12], which in the care of free space is equal to the speed of the light i. e, 3×10^8 m/s.

3.1.3. Jitter:

Jitter is variation of delay. Jitter becomes significant in constant bit rate multimedia data transmission. Jitter is difference in the end to end delay values of two voice or video packets. For such data transmission, decoder application at the receiver application is used which decode the received data according to the bit rate it was encoded at the sender station. Here, high variation in delay results problems in decoding, so, most of the multimedia applications use buffer to store the received data before decoding. The mechanism to control the frames in buffer is controlled according to the maximum expected jitter and the bit rate of the data it was sent [12].

3.1.4. Packet loss:

Loss of packet is caused by collision of packets and congestion in the link. Lost of packets result in speech dropouts or a stutter effect. Most of the multimedia applications are loss tolerant but are sensitive to bandwidth and delay. i. e, they require strict

bandwidth and delay guarantees but can tolerate certain amount of data losses. Jerks in videos and drop out voices are cause of data loss which reduces the voice and video quality. The effects of such losses on the quality and the amount of tolerable losses depend upon the application and technology used for coding [11]. Whereas data oriented applications such as email, file transfer, instant messaging, web documents can tolerate delay for some amount but require reliable transfer of data.

3.2 QoS Limitation of IEEE 802.11 DCF

IEEE 802.11 DCF supports only best-effort services and does not guarantee Quality of Services. Voice over IP (VoIP), or multimedia communications are time sensitive data and require specified bandwidth, delay and jitter but can tolerate some level of losses. Since priority is not defined in DCF, all the stations in one BSS contend for the resources and channel with same priority. There is no differentiation mechanism to guarantee bandwidth, delay, jitter and loss for high priority stations. It serves all stations with same priority without considering QoS requirements. Thus, all the stations and applications suffer from same amount of delays, losses, and variations in bandwidth as network becomes congested. There is no provision to serve high priority data with special care.

In wireless medium there are more challenges than in wired networks since it has limited bandwidth, higher bit error rate due to propagation loss, link noise, interference, multipath, shadowing, fading and weather etc. Now a days modern packet oriented telecommunication networks are also employing QoS mechanisms. GPRS(General Packet Radio Service) enables users to specify a QoS profile, which determines the priority of service the user is acquiring. Here, three priorities are defined, high, normal and low. Also, three classes are defined reliability class, delay class and throughput constraints [9]. Thus, with the evolving need of QoS enabled networks, a large amount of research has been going on to enhance the QoS in 802.11.

For last four, five year, parallel to the activities in the research community, the IEEE 802.11 Working Group has also been working on a new version of 802.11, called 802.11e

[2], to introduce QoS support in 802.11 networks. 802.11e has been available in draft forms, and recently the final version of the draft, draft 13th, has been released.

Chapter 4

4.1 Introduction to IEEE 802.11e

In order to support QoS in the legacy IEEE 802.11 MAC, IEEE is working on new standard called IEEE 802.11e. In this standard, there is a provision for service differentiation so that higher priority traffic gets better services which are not possible in legacy 802.11. To support service differentiation, it assigns different priorities for each data traffic. Furthermore, four different Access Categories (AC) queues are used with different priority. Access to the medium is then granted based on the priority of the data by mapping the data traffic to specific Access Category.

In IEEE 802.11e, the AP and STA that provides QoS services are referred to as QAP (QoS Access Point) and QSTA (QoS Station) respectively, and the BSS they are operating in is called QBSS (QoS Basic Service Set). IEEE 802.11e introduces a new coordination function, called Hybrid Coordination Function (HCF), to provide QoS support. Following sections describe HCF together with the detailed description of its service differentiation mechanism.

4.2 HCF (Hybrid Coordination Function)

Hybrid Coordination Function (HCF) is a new mechanism to provide service differentiation to the different traffic profiles. In order to support both IntServ and DiffServ QoS approach HCF multiplexes between two access modes: contention-based channel access (EDCA) and controlled channel access mechanism (HCCA).

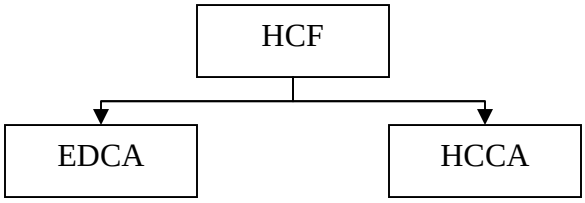

Figure 4. 1: Hybrid Coordination Function

In HCF four access categories (AC) queues are used in addition to eight traffic stream (TS) queues at MAC layer. When a data frame arrives at MAC layer, it is marked with a traffic priority identifier (TID) according to the QoS requirement, whose value ranges from 0 to 15. The frames having TID 0 to 7 are mapped into for access categories using EDCF access rule whereas frames with TID 8 to 15 are mapped into eight traffic streams(TS) queues using HCF controlled channel access rule. AC is used to support strict prioritized QoS while TS is used to support parameterized QoS.

4.3 EDCA (Enhanced Distributed Channel Access)

EDCA provides differentiated, distributed access to the medium using different priorities for different types of data traffic. The detailed description of the components and operations of EDCA are as follows:

4.3.1 Access Categories (ACs)

Four Access Categories (ACs) are defined in EDCA for different types of data traffic. Service differentiation is introduced such that for each AC, a different set of parameters are used to contend for the medium. These parameters are referred to as EDCA parameters. Here, data frames from different application profiles are mapped into different ACs in MAC depending on its QoS requirements. The four Access Categories are named AC_BK, AC_BE, AC_VI AND AC_VO, for background, best effort, video

and voice data traffic respectively. Here, AC_BK has the lowest priority and AC_VO has highest priority. So, each frame from the higher layer arrives at the MAC layer along with a priority. This priority value is called User Priority (UP) and is assigned according to its service requirement. There are eight different priorities values ranging from 0 to 7.

Priority	User Priority (UP)	Access Category (AC)	Designation
Lowest	1	AC_BK	Background
.	2	AC_BK	Background
.	0	AC_BE	Best Effort
.	3	AC_BE	Best Effort
.	4	AC_VI	Video
.	5	AC_VI	Video
.	6	AC_VO	Voice
Highest	7	AC_VO	Voice

Table 4. 1: User Priority (UP) to Access Category (AC) mappings.

The draft does not specify about how such a priority is assigned, it is left as higher layer implementation issue. It can be assigned by application generating the traffic or by the user itself. If the priority is adaptively assigned at the application layer, based on the traffic type such as data rate, packet size etc. then it is certain that some modifications must be done to higher layers. If it is assigned by user itself then every application has to be updated in order to be compatible with 802.11e. At MAC layer, each frame with a particular UP is further mapped to an AC. ACs are derived from the UPs as shown in figure 4.2.

4.3.2 EDCAF (Enhanced Distributed Channel Access Function)

EDCAF is an enhanced version of DCF, which contends for the medium as in DCF i. e, CSMA/CA mechanism. The EDCF is designed for the contention based prioritized QoS

support. Here, each QoS enhanced station (QSTA) has 4 queues called Access Categories (AC) to support 8 user priorities (UPs) as defined in IEEE 802.1D [20]. Since, there are 8 user priorities and only 4 priority queues, so more than one UPs are mapped to the same AC queue as shown in table 4.1. This is because usually eight different applications do not transmit frames simultaneously, and using less ACs than Ups reduces the MAC layer overheads. Here, each AC queue acts as an independent DCF station and uses its own backoff parameters.

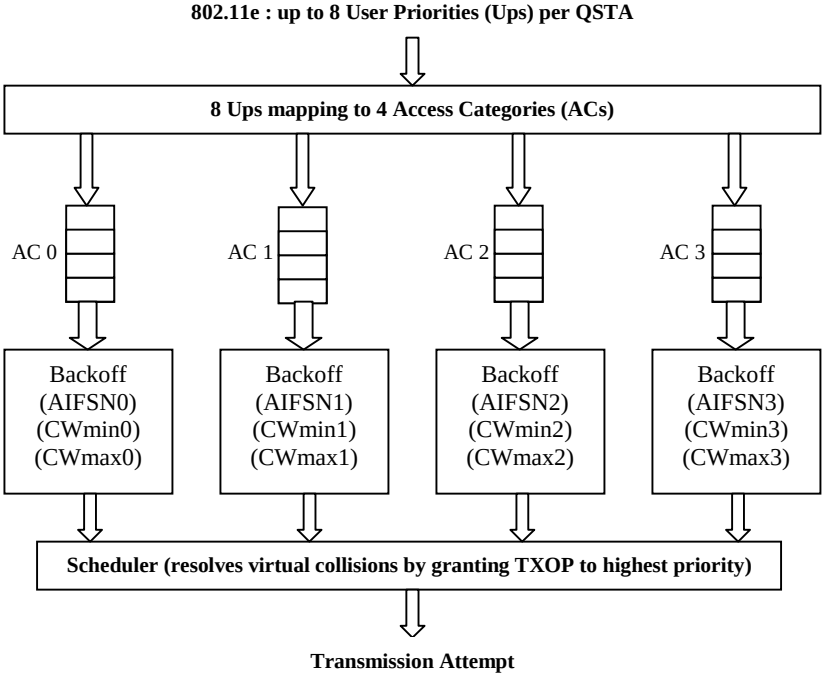

Figure 4. 2: Enhanced Distributed Coordinated Function (EDCF)

In EDCF, two methods are introduced to support service differentiation; the fist one is to use different InterFrame Space (IFS) sizes for different ACs. Second one is allocating different CW sizes for different ACs. High priority AC is assign less CW size so that it gets opportunity to use the medium earlier. If two or more stations have backoff counter zero at the same time, a scheduler inside the station will avoid the virtual collision by granting the EDCF-TXOP to the highest priority AC. And other colliding AC will double its CW and starts backoff as if external collision has happened.

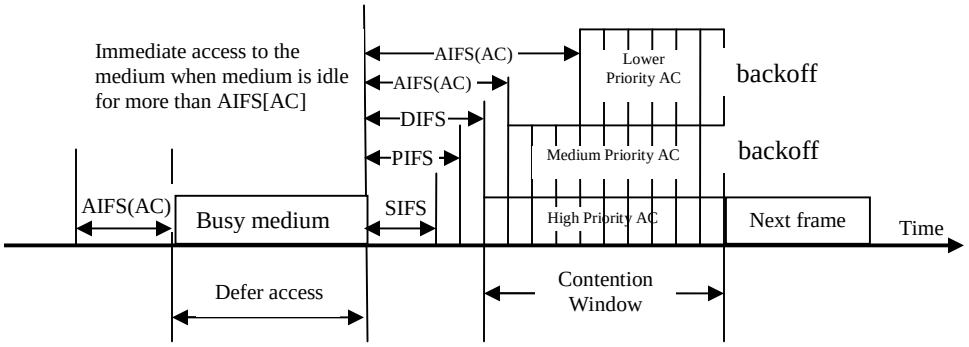

Figure 4. 3: EDCA channel access prioritization

4.3.2.1 EDCA Parameters

Following are the parameters associated to Access Category (AC) which are used for EDCF contention.

- AIFS – Time period the medium has to be idle before the transmission start.
- CWmin, CWmax – Minimum and maximum size of Contention Window used for backoff.
- TXOP Limit – The maximum time, during which two stations can use the medium after they have acquired it.

EDCA parameters are specified different for different Access Categories. As shown in figure 4.3, the higher priority AC has to wait less time i. e, AISF time period than lower priority before accessing the medium. Also, the size of Contention window varies for different ACs, i. e. size of contention window is small for higher priority traffic while larger for lower priority traffic since backoff values are drawn from this contention window. On the other hand TXOP limit also varies; it is larger for higher priority so that it can use the medium for longer period of time and shorter for lower priority traffic. In summary we can say that for higher priority ACs, AIFS and contention window will be

small while TXOP will be larger. Since, the EDCA parameters are AC specific, so they are referred as AIFS[AC], CWmin[AC], CWmax[AC] and TXOP limit[AC]. Thus, the main difference between DCF and EDCF is EDCF uses AC specific parameters AIFS[AC], CWmin[AC], CWmax[AC] instead of only one DIFS, CWmin and CWmax. QAP is scheduled to advertise the EDCA parameters periodically. QAP determines these parameters dynamically by considering the present network condition.

Following are the EDCA parameters i. e. AIFS, CW and TXOP, used for service differentiation:

AC	CWmin	CWmax	AIFSN	TXOP Limit	
				FHSS	DSSS
AC_BK	CWmin	CWmax	7	0	0
AC_BE	CWmin	CWmax	3	0	0
AC_VI	(CWmin+1)/2 - 1	CWmin	2	6.016ms	3.008ms
AC_VO	(CWmin+1)/4 - 1	(CWmin+1)/2 - 1	2	3.264ms	1.504ms

Table 4. 2: Default EDCA parameter values.

AIFS (Arbitration Inter-Frame Space)

It is the time the medium should be idle before acquiring the medium or backoff is started. The AIFS[AC] is calculated as

$$AIFS[AC] = AIFSN[AC] * SlotTime + SIFS$$

The default values of AIFSN is shown in the above table 4.2. AIFSN specifies the number of slot time plus SIFS time period. The minimum value of AIFSN is 2 as the DIFS is equal to 2 * SlotTime + SIFS, it shows that the minimum length of AIFS is equal to DIFS. But in the case of HCCA, the minimum value of AIFSN is 1 as 1 * SlotTime + SIFS equals to PIFS. AIFSN value is directly proportional to delay. So, higher priority traffic is assign low AIFSN value that is 2 as shown in above table so that higher priority traffic will get larger share of bandwidth. Though higher priority data are given preference, low priority may suffer from longer delays but since, these low priority data

are delay tolerable, certain amount of delay do not degrade the performance beyond the acceptable level.

CWmin, CWmax

As in the DCF in EDCF the size of CW is also not constant and varies according to AC. Contention Window (CW) is also directly proportional to delay. So, higher priority traffics (AC) are assigned low value of CW so that it is able to access the medium ahead of lower priority traffic (AC). If two ACs try to access the medium at the same time then internal collision will occur. In that case the scheduler inside the QSTA selects higher priority AC to access the medium and other lower priority traffic enter a backoff process with doubling the CW[AC] size as in case of external collision.

	FHSS	DSSS
CW_{min}	15	31
CW_{max}	1023	1023

Table 4. 3: Contention window parameters for different physical layers.

The CWmin and CWmax values of AC_BK and AC_BE are same as in the legacy 802.11 DCF, but priority is given to AC_BE over AC_BK by assigning it AIFSN value 3 which is less than AIFSN 7 of AC_BK. The values of AC_VI and AC_VO are different and smaller as one half or quarter compare to lower priority ACs. This is to provide smaller backoff values for higher priority ACs and thereby shorter medium access delays. Here, one drawback of smaller contention window value is that, there is more probability that two or more ACs get same random backoff value leading to an internal collision. To minimize this internal collisions CWmax value is set such that it is always less than CWmin of lower priority traffic ACs. So, even though there is collision and CW is doubled, its value never exceeds the CWmin of the lower priority traffic thus it avoids overlapping values facilitating to get different CW value. So, it is confirmed that higher

priority traffic ACs get greater share of the bandwidth even in the congested network condition. However, this may lead the lower priority ACs to starvation.

The transmissions is said to be failed or collision is said to occur when two or more ACs or STA tries to access the medium at a same time. For each collision, the value of Contention Window is doubled by following equation:

$$CWmin = 2^m * (CWmin +1) -1,$$

Where m is the maximum backoff stage.

$$CW = 2^i * (CWmin + 1) – 1, \text{ if } 0<i<m,$$
$$\text{and } CW = CWmax, \text{ if } m<=i,$$

where, i is the number of unsuccessful attempts. Once it reaches CWmax, its value remains constant i. e. CWmax, after first successful transmission its value will be reset to CWmin.

TXOP Limit

Transmission Opportunity limit is the maximum time duration during which multiple packets can be exchanged between two stations acquiring the medium without interferences of other stations. The multiple packets also includes ACKs frames, RTS/CTS frames which are separated by SIFS within the TXOP period.

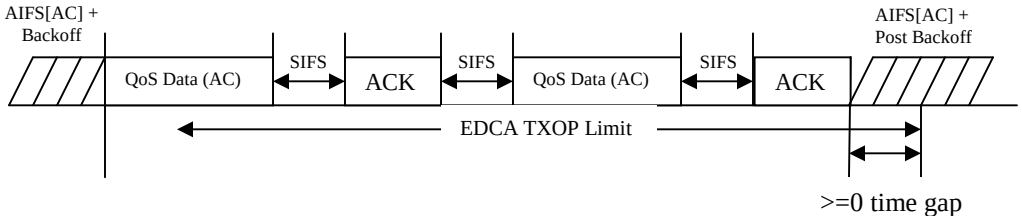

Figure 4. 4 Contention Free Brusting (CFB)

The maximum value of TXOP is called TXOP Limit and it is determined by QoS AP. The default value of TXOP is shown in the above table 4.2. The zero value of TXOP for AC_BK and AC_BE indicates that CFB is disabled and only one frame can be exchanged during TXOP. If RTS/CTS is enabled then RTS/CTS frame is also included in the transmission. If the time to transfer first frame exceeds TXOP Limit then the frame should be fragmented. But the TXOP Limit value of AC_VO and AC_VI are 3.264 ms and 6.016 ms in FHSS respectively, so, these AC can transmit multiple frames in TXOP Limit duration provided that the frames belong to the same AC. This period is known as contention free bursting period. In this period the frames are separated by SIFS time period. The multiple frames of same AC are only allowed to transfer for which the TXOP was obtained during this time. If RTS/CTS mechanism is employ in CFB, then the RTS and CTS frames are exchanged only once during the first time, and later frames can transfer with the gap of SIFS till the TXOP Limit. In the above table, the default values of TXOP limits for the low priority ACs, AC_BK and AC_BE are set to zero indicating that CFB is disabled. But for high priority AC_VO and AC_VI, the CFB allows to access the medium for large duration this provide service differentiation for high priority AC. But this may lead lower priority AC suffer from starvation. When CFB is applied, to let the other stations aware of it, virtual carrier sensing is applied such that the duration field in the frame header is set to remaining duration of the whole TXOP which is transmitted.

4.3.3 EDCA Operation

EDCA works similar to DCF, only difference is that, it has different AIFS, CWmin, CWmax and TXOP Limit for different ACs. When the medium is sensed free for AIFS time period, ACs draws a random backoff value from contention window interval. This backoff value is decreamented at each slot time and once its value reaches zero, it can start the transmission acquiring the medium.

Considering the following figure, here all the four ACs have frames to transmit so are contending for the medium.

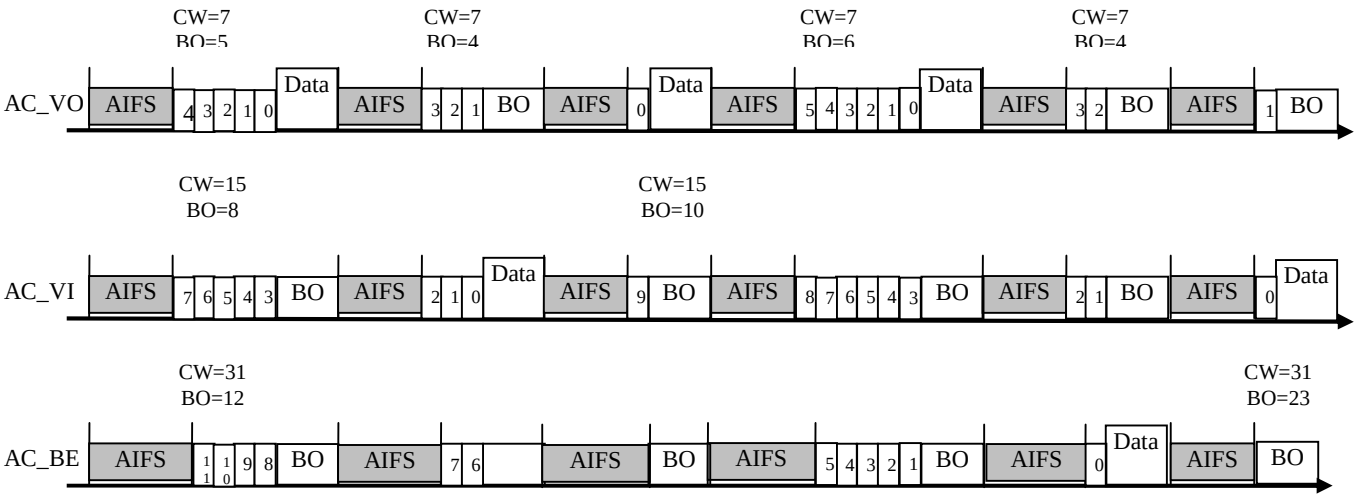

Figure 4. 5: EDCA access mechanism

From the table 4.2, the AIFSN values of AC_VO and AC_VI are 2 and that of AC_BE and AC_BK are 3 and 7 respectively. So, AC_BE and AC_BK have to wait for some additional slot time to access the medium. As high priority AC has smaller minimum and maximum contention window limits, it gets smaller backoff values and so has to wait less time contending the medium. Here, the highest priority AC gets access to the medium and other ACs pause their backoff timer until the medium is idle for AIFS time period. Thus at a certain time, lower priority AC has smaller backoff value when higher priority AC chooses a new backoff value for every next frame. Lower priorities ACs just decrement its paused backoff value. This helps to avoid starvation of low priority ACs. In this way higher priority ACs gets larger share of the bandwidth transmitting the frame more frequently then low priority ACs. In the above figure it is clearly seen that AC_VO send 3 frames, AC_VI send 2 frames, and AC_BE send 1 frame. While AC_BK which is the lowest priority AC could not send single frame till that time since it has to sense the medium to be idle for longest AIFS time period. Actually, it is unable to decrement its backoff value because another AC acquires the medium before its AIFS is finished.

When two of more ACs tries to access the medium at a same time then collision is said to occur. This happens when backoff timer of two or more ACs decrement to zero at a same time. Such collision is called internal collision. To handle such situation, the internal scheduler selects the highest priority ACs and grant access to the medium, while other

ACs doubles its CW and draws new backoff value after the medium becomes idle for AIFS time period. The situation is shown in the following figure 4.6.

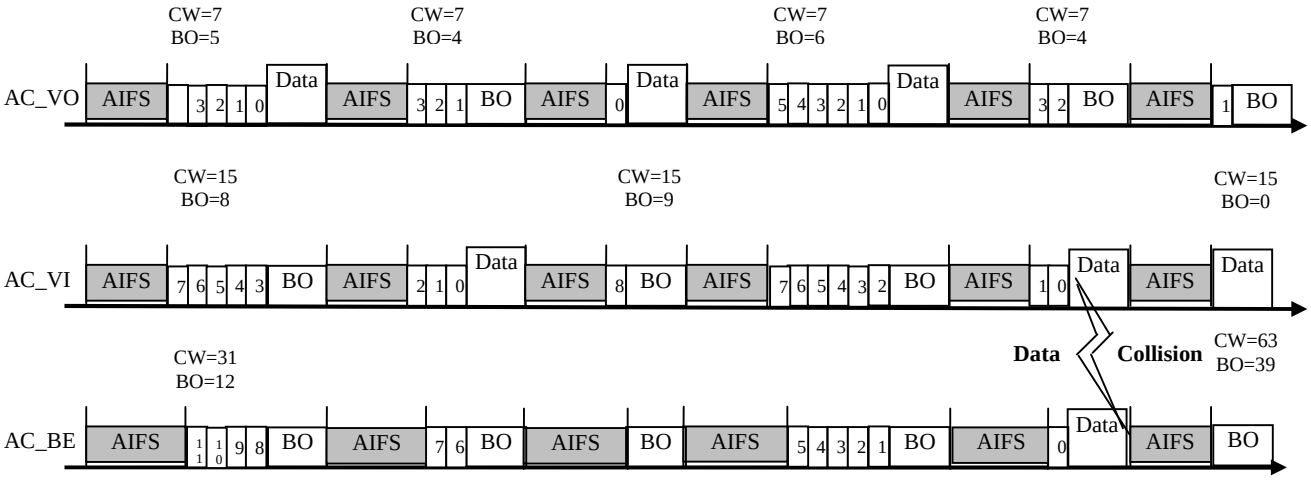

Figure 4. 6: EDCA access mechanism and internal collision.

In the above case, the only drawback is low priority AC has to wait for longer time. The case gets even worse when EDCF for low priority collides, and the backoff value is drawn from double the last CW size.

When two or more stations tries to access the medium at a same time, then the collision is said to occur. This collision is called external collision and occurs when backoff value of two or more STAs countdowns to zero at a same time. The recovery process is somehow similar to internal collision, only difference is, here station is considered instead of particular AC. Here for external collision, the al the colliding EDCAFs increases their contention window to double and new backoff value is drawn while other stations starts countdown from their last value. In the figure below, Two EDCAFs for AC_VO and AC_VI in two different stations contends for the medium and their backoff timer countdowns to zero at a same time. Both stations try to access the medium and transfer their data. When no ACK frame is received then the stations realize that collision has occurred. Now both colliding EDCAFs double their contention window. Other stations continue decrementing their paused backoff values while colliding stations start from new backoff.

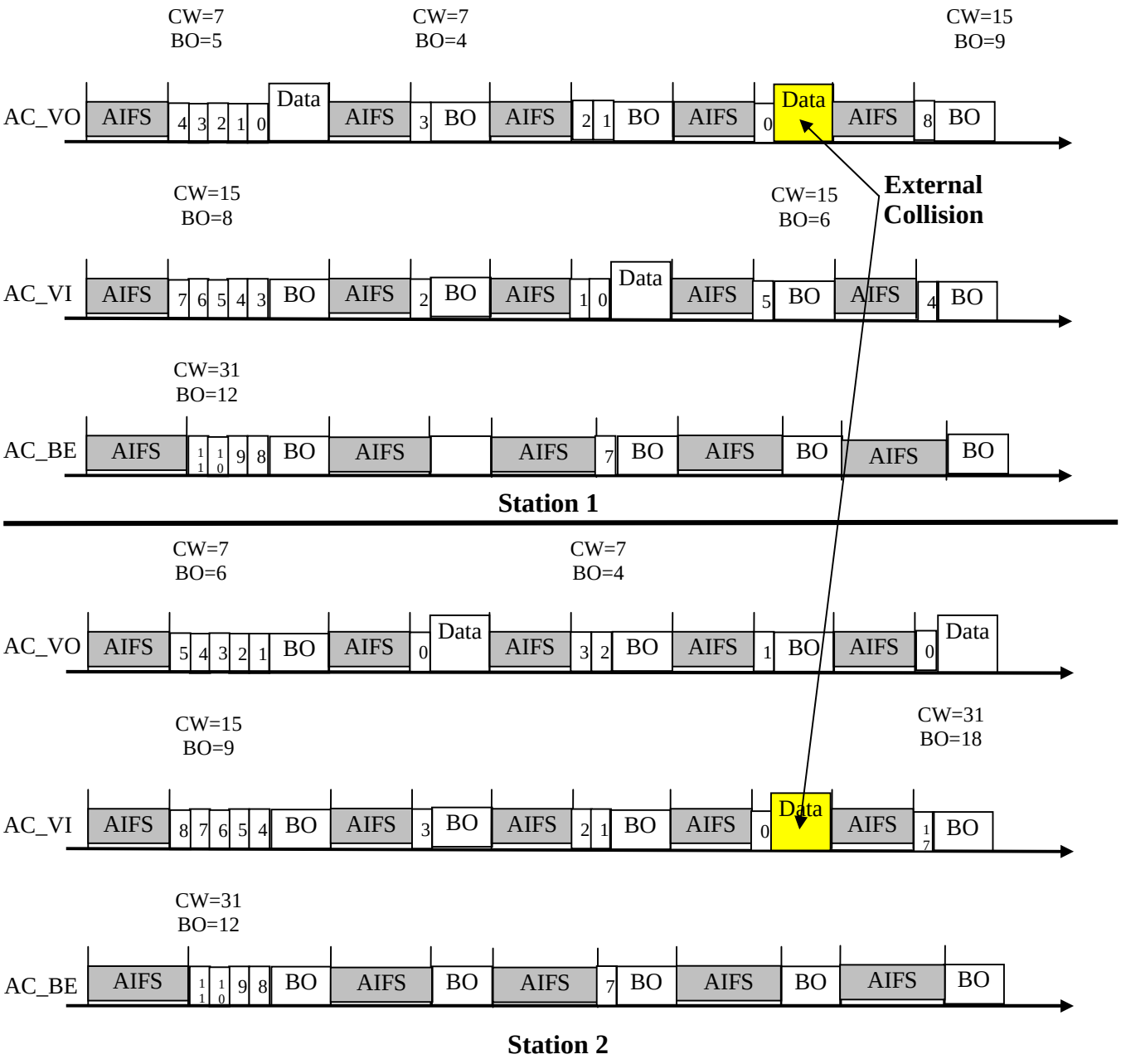

Figure 4. 7: EDCA access mechanism and external collision.

4.4 Architecture and Important Frame Formats

In order to provide backward compatibility, 802.11e also includes two old coordination functions they are, DCF and PCF of 802.11 so that non-QoS STA can associate with QAP in a QBSS. In such case QBSS operates just like in ordinary 802.11 and do not use frame formats specific for QoS services. Besides that QSTA can also operate in a non-QoS BSS by associating itself to a non-QoS AP in the absence of QAP.

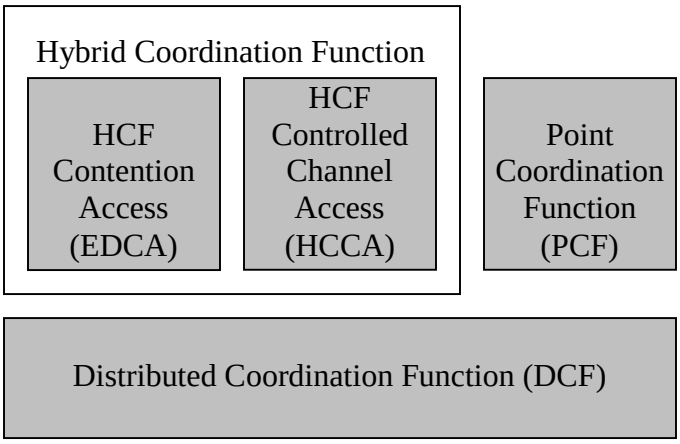

Figure 4. 8: IEEE 802.11e MAC architecture.

HCF controlled channel access is a centrally controlled channel access mechanism. It is designed for the parameterized QoS support, combining the advantages of both PCF and DCF of 802.11. EDCA operates in CP where as HC operates in both CP and CFP.

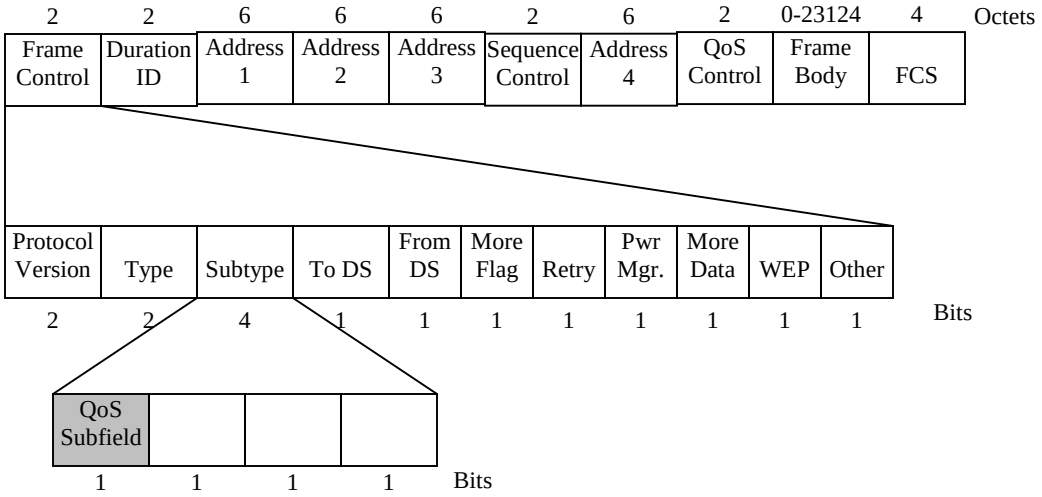

Figure 4. 9: MAC data frame header and QoS subfield

Protocol Version field - Version of 802.11 frame in use.

Type and Subtype fields - Identifies one of three functions and sub functions of the frame: control, data, and management.

To DS field - Set to 1 in data frames destined for the distribution system (devices in the wireless structure).

From DS field - Set to 1 in data frames exiting the distribution system.

More Fragments field - Set to 1 for frames that have another fragment .

Retry field - Set to 1 if the frame is a retransmission of an earlier frame.

Power Management field - Set to 1 to indicate that a node will be in power-save mode.

More Data field - Set to 1 to indicate to a node in power-save mode that more frames are buffered for that node.

Wired Equivalent Privacy (WEP) field - Set to 1 if the frame contains WEP encrypted information for security.

Order field - Set to 1 in a data type frame that uses Strictly Ordered service class (does not need reordering).

Duration/ID field - Depending on the type of frame, represents either the time, in microseconds, required to transmit the frame or an association identity (AID) for the station that transmitted the frame.

Destination Address (DA) field - MAC address of the final destination node in the network.

Source Address (SA) field - MAC address of the node that initiated the frame.

Receiver Address (RA) field - MAC address that identifies the wireless device that is the immediate recipient of the frame.

Transmitter Address (TA) field - MAC address that identifies the wireless device that transmitted the frame.

Sequence Number field - Indicates the sequence number assigned to the frame; retransmitted frames are identified by duplicate sequence numbers.

Fragment Number field - Indicates the number for each fragment of a frame.

Frame Body field - Contains the information being transported; for data frames, typically an IP packet.

FCS field - Contains a 32-bit cyclic redundancy check (CRC) of the frame.

In the above figure, QoS subfield is specified in the frame control field of the MAC header. This value specifies whether the station is communicating as QSTA or nQSTA, here 1 specifies the station to be QSTA and 0 specifies nQSTA.

Here, each frame is assign a priority as traffic identifier (TID). TID specifies the user priority (UP) which ranges from 0 to 7. This TID field is supported only if the station has its QoS subfield with value 1 in its Frame Control field i. e. the station is working as QSTA with QAP. The TID is meaningless if QSTA is associated with nQAP. This is specified by QoS subfield value equal to zero. If nQSTA is associated with QAP then the frames from nQSTA is treated with priority zero.The queue size field in QoS Control field of the frame header specifies the total number of frames of the particular priority in the AC transmit queue excluding the current frame. TXOP duration requested/queue size is shown in the figure below.

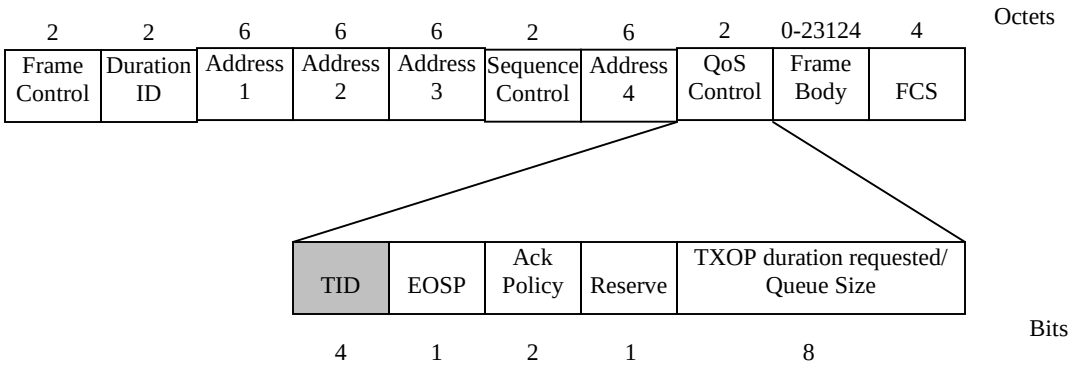

Figure 4. 10: TID field in QoS Control field.

TXOP can be obtained in both EDCA and HCCA access modes which are called EDCA TXOP and HCCA TXOP (polled TXOP) respectively. In EDCA mode, EDCA TXOP is obtained as soon as QSTA accesses the medium. On the other hand HCCA TXOP is granted by HC in HCCA. HCCA polls all the STAs one by one to grant HCCA TXOPs based on their requirements. QSTA set the duration/ID field in the frame header to specify about the multiple frames. During operating in HCCA, a QSTA requests the TXOP of specific duration by setting TXOP duration subfield of QoS control field. TID field is used to specify the AC for which the TXOP is being requested. The Hybrid Coordinator or QAP then assign a TXOP of the requested size or minimum size which ever is possible. EDCA parameters are defined in EDCA Parameter Set Element, and are periodically advertised by the QAP in selected frame (becaons), figure 4.10. QAP then adapt these parameters dynamically, depanding on the network condition. The values of EDCA parameters are specified in the subfields AIFSN, ECWmin, ECWmax, and TXOP Limit, in the EDCA Parameter Set element. All QSTAs that receive the EDCA Parameter Set element from QAP, update their EDCA parameter values and use new values to contend for the medium. The draft standard specifies the default values of EDCA parameters if not advertised by the QAP, as presented in Table 4.2.

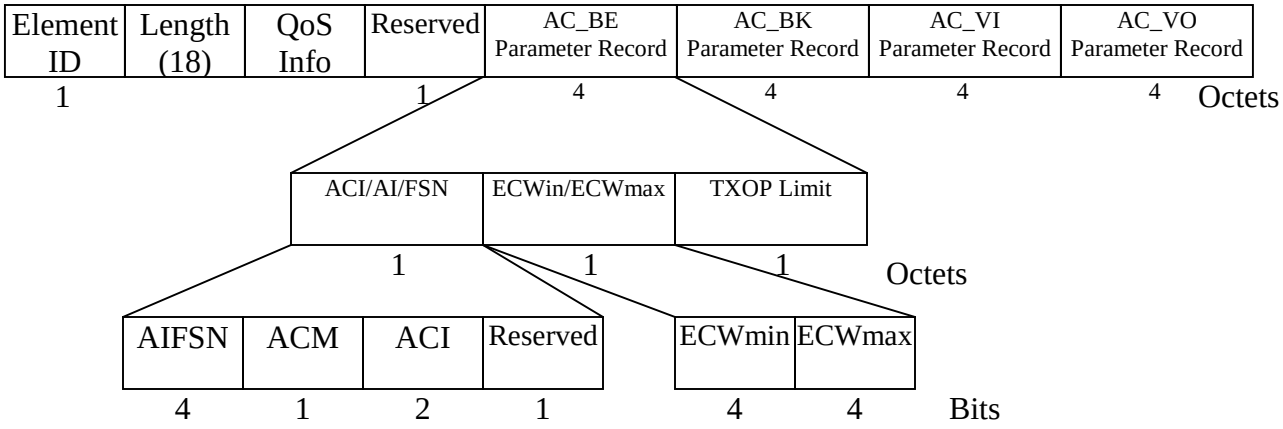

Figure 4. 11: EDCA Parameter Set element.

Every time QAP updates the EDCA parameters, it increments the value of EDCA Parameter Set Update Count field in QoS Info field in the QoS Capability element sent in selected frames. The QSTAs use this information to confirm that they are using the latest set of EDCA parameters. The structure of QoS Capability element is illustrated in Figure 4.12.

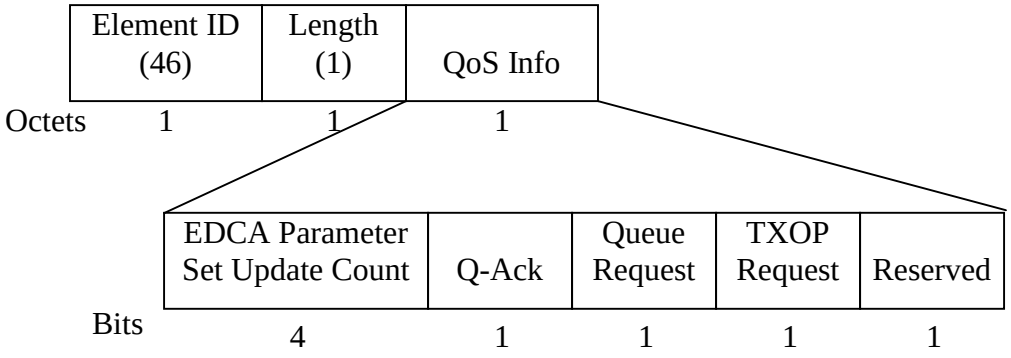

Figure 4. 12: QoS Capability element and QoS Info field.

Chapter 5: Implementation

In this thesis, implementation of 802.11e is done in Network Simulator 2. To implement 802.11e four queues has been maintained for different priority data. These four queues act as four different virtual stations inside each station. Each queue has different AIFSN[i] value where i=0 to 3, and the queue that reaches AIFSN value zero will get opportunity to transmit the data first. So, in this way, quality of service is maintained, thus higher priority data gets more opportunity to transmit than lower one maintaining the lower priority data not to get starved waiting for long time to transmit. The EDCA parameters that are responsible to provide quality of service are Arbitration InterFrame Space (AIFS), Contention Window (CW) and Transmission Opportunity (TXOP) which are described in chapter 4. In this thesis only transmission opportunity has been considered. Since, a reasonable amount of work has been done in Contention Window such as Adaptive Fair Channel Allocation for QoS Enhancement in IEEE 802.11 Wireless LANs [13], Adaptive QoS Management for IEEE 802.11 Future Wireless ISPs [14] and Adaptive EDCF: Enhanced Service Differentiation for IEEE 802.11 wireless Ad-Hoc Networks [15]. In the earlier version of 802.11e the value of transmission opportunity is constant which is described in prioriy.tcl file in NS2.

```
#Default values set in 802.11e
# 802.11b parameters (default EDCA parameter set), a CWmin=31, a CWmax=1023
proc priority { ifq_name } {
  upvar $ifq_name ifq

   # parameters for Queue 0
   $ifq Prio 0 PF 2
   $ifq Prio 0 AIFS 2
   $ifq Prio 0 CW_MIN 7
   $ifq Prio 0 CW_MAX 15
   $ifq Prio 0 TXOPLimit 0.003264          #Default value

   #parameters for Queue 1
   $ifq Prio 1 PF 2
   $ifq Prio 1 AIFS 2
   $ifq Prio 1 CW_MIN 15
   $ifq Prio 1 CW_MAX 31
   $ifq Prio 1 TXOPLimit 0.006016          #Default value

   #parameters for Queue 2
   $ifq Prio 2 PF 2
   $ifq Prio 2 AIFS 3
   $ifq Prio 2 CW_MIN 31
   $ifq Prio 2 CW_MAX 1023
   $ifq Prio 2 TXOPLimit 0                 #Default value

   #parameters for Queue 3
   $ifq Prio 3 PF 2
   $ifq Prio 3 AIFS 7
   $ifq Prio 3 CW_MIN 31
   $ifq Prio 3 CW_MAX 1023
   $ifq Prio 3 TXOPLimit 0                 #Default value
```

In this implementation the transmission opportunity limit value has been varied according to the network condition. This function is named as myTXOP which computes new value each time a node has to transfer data. Two new variables for counting number of collision and total data transferred has been used. The ratio of data transfer is to total number of collision times the previous TXOP value gives the new value of myTXOP.

i. e. nowtxoplimit = (rec_count / colcount) * prevtxoplimit

nowtxoplimit is the new value calculated according to the present condition of network.

Initially, the number of collision will be zero, so myTXOP will give divide by zero error, to resolve that a condition has been used so that the new value will be calculated only when collision count is greater than zero, other wise its default value will be used. Later on during the transmission a new value of myTXOP is used. The simulation is done under congested network where every station has some packets of data to transfer.

```
double Mac802_11e::myTXOP(int i) //Implimentation of the myTXOP
{
  double prevtxoplimit;
  double nowtxoplimit;
  double collisioncount;
  double receivecount;
  collisioncount = col_count[i];
  recreceivecount = recv_count[i];
  prevtxoplimit = prevTXOP[i];
        if (collisioncount > 0) {                    // if any packet collided
                nowtxoplimit = (receivecount / collisioncount) * prevtxoplimit;
        }
        else {
                return -1;
        }
        col_count[i] =0;
        recv_count[i] =0;
   prevTXOP[i] = nowtxoplimit;       //assigning for later calculation
   return nowtxoplimit;
}
```

The files that are updated in the Network Simulator are **mac-802_11e.cc and mac-802_11e.h** which resides in 802_11e folder. These files contain the configuration of how quality of service is maintained in MAC layer. These files have been changed to support my dynamic transmission opportunity (myTXOP) adding above C++ function.

A topology is designed in TCL (.tcl) scripts for different number of stations. This file is run in NS2 simulator and the result in redirected into a trace file (.tr). This trace file contains raw data of simulation values in column format. Using Perl scripts taking these trace file as input file, throughput, latency and packet loss is calculated. And finally, these values are plotted in graph using xGraph of NS2.

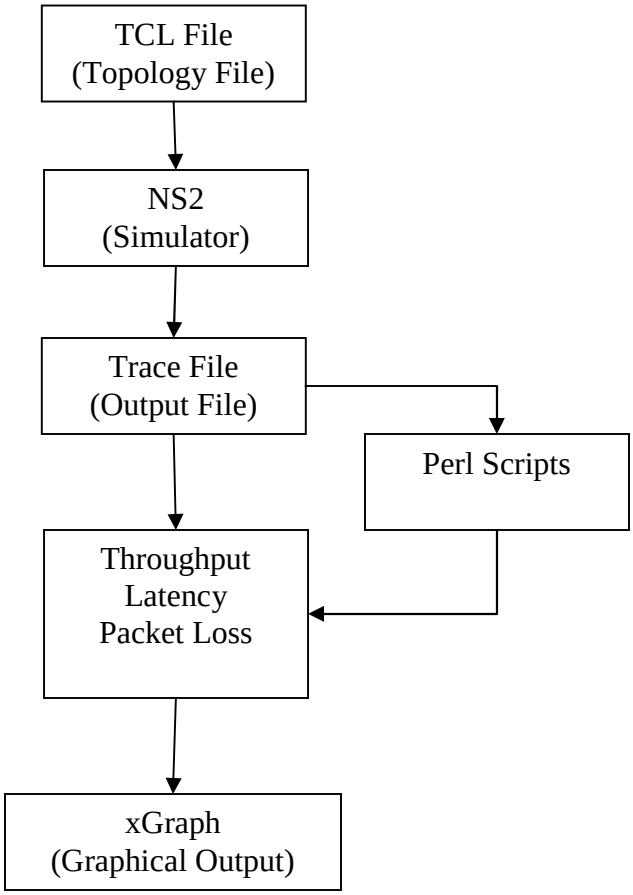

Figure 5. 1: Implementation Steps

Description of the Perl scripts to generate throughput, latency and packet loss.

Throughput:

Throughput is calculated as the ratio of sum of all the received packets is to the total time of the simulation and average throughput is calculated by dividing the throughput by total number of stations:

Throughput = size of total data received / total time of simulation

Average Throughput = throughput / total number of stations

Latency:

The latency of the packet is calculated by subtracting sending time from receiving time. The average latency is calculated by dividing total latency by total number of packet transferred.

Latency = receiving time – sending time

Average latency = sum of latency / total no. of packets transferred (received)

Packet loss:

The dropped packets are packet loss. The dropped packets are calculated by counting all the dropped packets. To calculate the average packet loss, the dropped packets is divided by total number of packet sent.

Packet loss in percent = (sum of dropped packets / sum of sent packets) * 100

Chapter 6: Simulation and Output

The simulations under different scenarios are carried out with default values of TXOP and the proposed dynamic value of TXOP. The following results are found during simulation:

Normal TXOP (Default)			
No. of Stations	**Throughput (Bytes/s)**	**Latency (Sec.)**	**Packet Drop (%)**
5	44652.7949374102	0.00205090938749955	0.00%
10	27047.7342529175	0.09034247888314310	40.94%
15	18463.0520792620	0.22912355998490900	59.95%
20	13600.6223316437	0.29260202387778000	70.44%
25	10767.9302314958	0.29304692686557900	76.74%
30	9085.2161175651	0.29942973903868100	80.29%

Dynamic TXOP			
No. of Stations	**Throughput (Bytes/s)**	**Latency (Sec.)**	**Packet Drop (%)**
5	44652.7949374102	0.00205090938749955	0.00%
10	27219.9459315213	0.06864365334842990	40.74%
15	18867.6795192337	0.17683276969954000	59.30%
20	13741.3318739176	0.21923981901344900	69.79%
25	10840.1751308126	0.22320749969567600	76.24%
30	8741.4928078313	0.24829948705910200	80.16%

Table 6. 1: Simulation Output

The above result shows that the dynamic value of TXOP gives better performance of the network. These results can be analyzed in the following graphs:

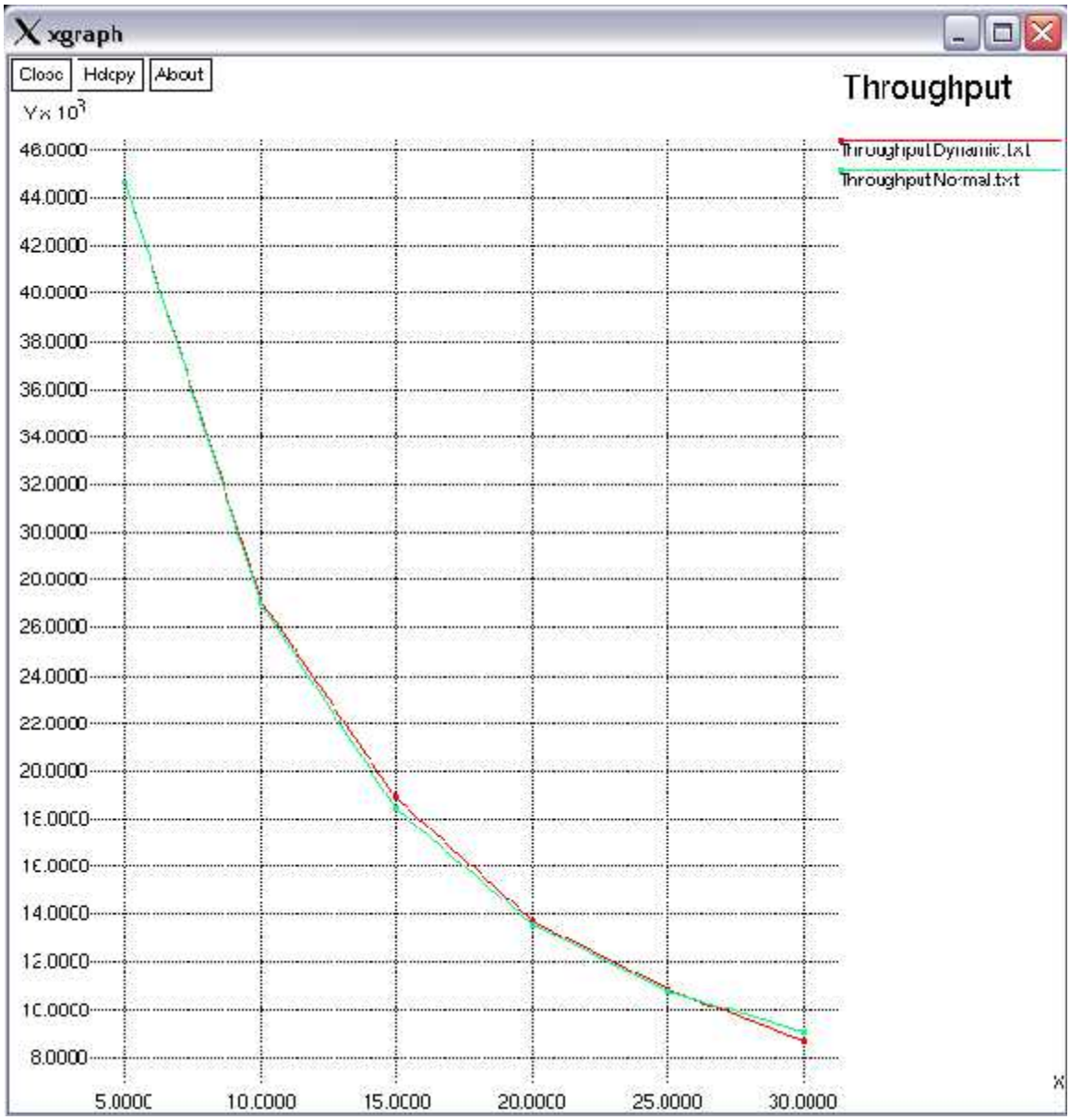

Figure 6. 1: Throughput Comparisons (No. of stations vs. KB/s)

In the above graph we see that up to simulation of 10 stations, the dynamic value of TXOP does not change throughput significantly. From 10 stations up to 25 stations the simulation showed that the dynamic TXOP contributed in throughput increment, but from 25 to 30 stations the throughput decreased which is due to increased in number of stations.

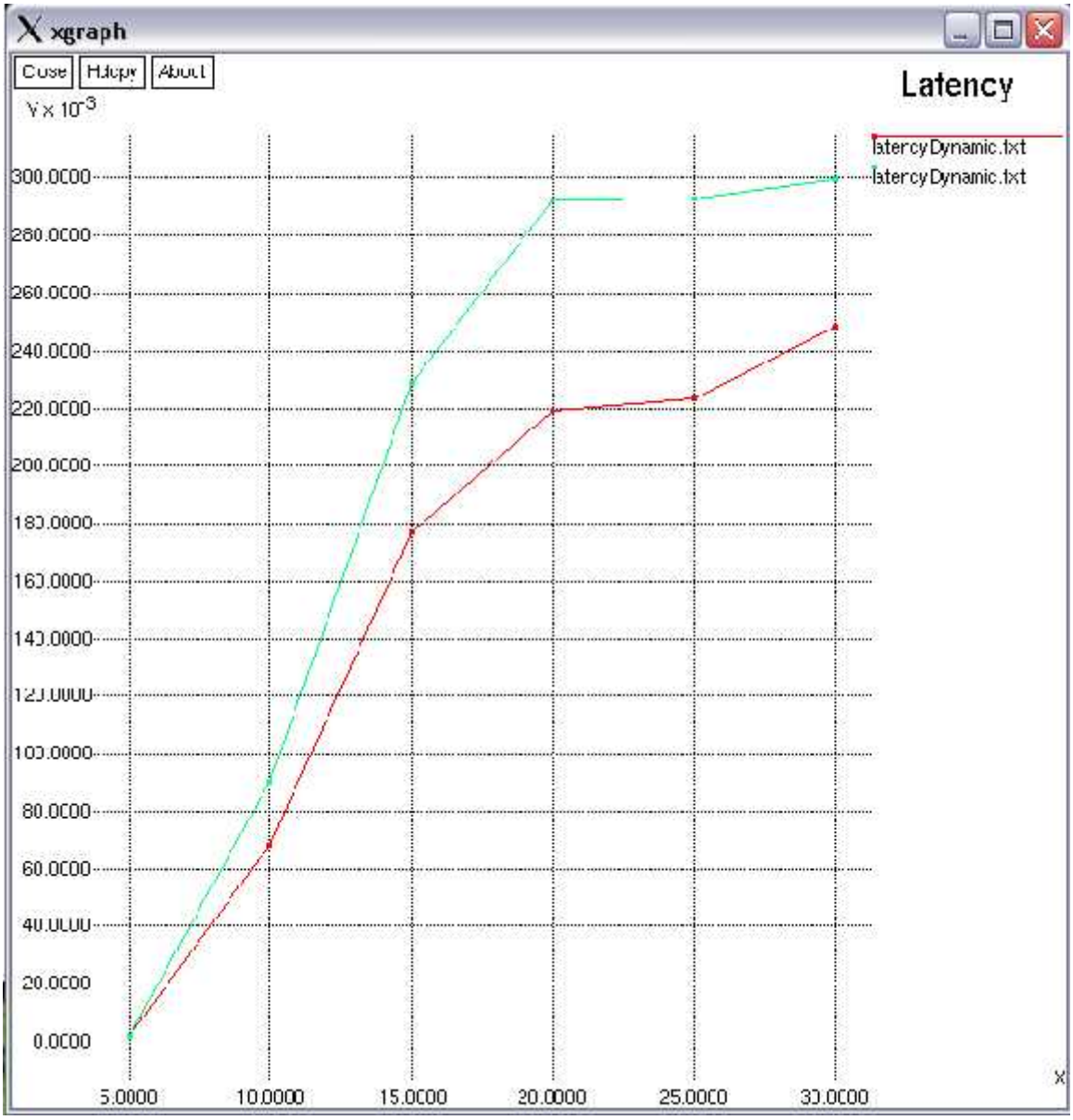

Figure 6. 2: Latency Comparisons (No. of Stations vs. Latency (msec.))

In the above graph the new dynamic TXOP value significantly contributed in decreasing latency. In the simulation of 20 stations, the latency is decreased drastically. Thus, we can infer that the new dynamic TXOP value considerably decrease the latency and increased network performance.

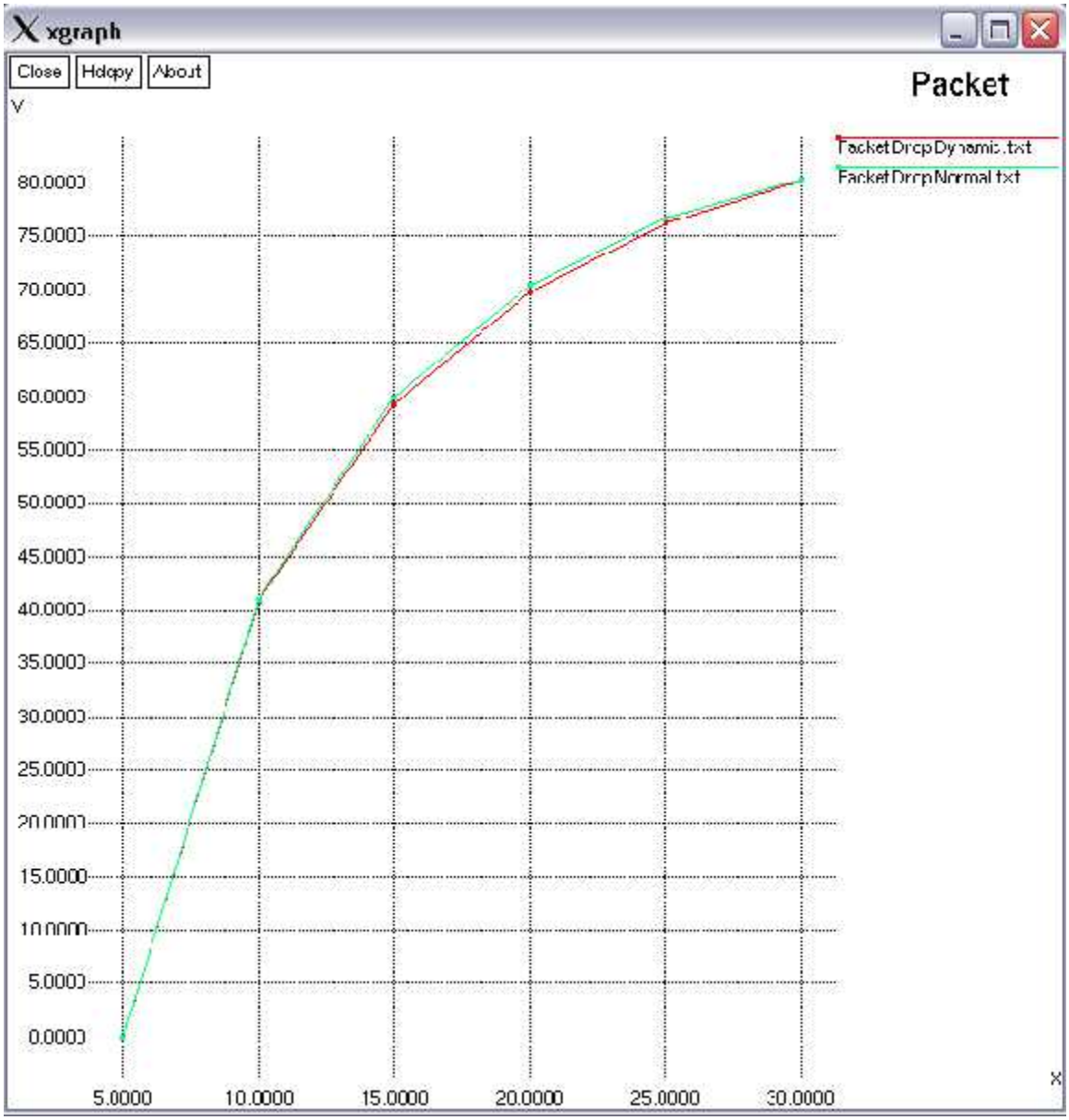

Figure 6. 3 Packet Loss Comparisons (No. of Stations vs. No. of Packet Loss (%))

In the above graph though the new dynamic TXOP value doesn't show considerable decrease in packet loss, however, the network performance has been improved slightly. Thus, it can be inferred that the new dynamic TXOP value definitely contributed in increasing network performance.

Chapter 7: Conclusion and Future work:

7.1. Conclusion

The primary objective of this thesis is to analyze of one of the quality of service parameter i.e. TXOP. A new dynamic value of TXOP is used which is calculated during each transmission rather than the default constant value. The simulation is done in NS2 under different network scenarios having different number of stations. The output results proved that the implemented dynamic TXOP improved the network performance.

7.2. Future work

The performance of the network is evaluated as a whole network; performance of each application can be done in future work. Analyzing the dynamic TXOP on each traffic type is not done in this thesis which can be done later. The more complex formula can be used to get the better dynamic value of TXOP. Some artificial intelligence algorithm which can better evaluate the present network condition can be implemented to get the optimized value of not only TXOP but also AIFSN and CW which will contribute in calculating better value of dynamic TXOP.

References:

[1] IEEE 802.11 WG, Reference number ISO/IEC 8802-11:1999(E) IEEE Std 802.11, 1999 edition. International 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, 1999.

[2] IEEE 802.11e/D13.0, Draft Supplement to Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Access Control (MAC) Quality of Service (QoS) Enhancements. January 2005.

[3] IEEE Std. 802.11, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. 1997.

[4] IEEE Std. 802.3, Part 3: Carrier Sense Multiple Access with Collision Detection(CSMA/CD) Access Method and Physical Layer Specifications. 1985.

[5] IEEE Std. 802.5, Token Ring Access Method and Physical Layer Specificationss. 1985.

[6] IEEE Std. 802.11b, Supplement to Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band. 1999.

[7] IEEE Std. 802.11a, Supplement to Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher-Speed Physical Layer Extension in the 5GHz Band. 1999.

[8] IEEE Std. 802.11g, Supplement to Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications: Further Higher-Speed Physical Layer Extensionin the 2.4 GHz Band. 2003.

[9] J. Schiller. Mobile Communications. Addison-Wesley, second edition, 2003.

[10] Q. Ni, L. Romdhani, T. Turletti “A Survey of QoS Enhancements for IEEE 802.11 Wireless LAN” Planete Group, INRIA, 2004 route des Lucioles BP93, 06902 Sophia Antipolis, France
http://www.hamilton.ie/Qiang_Ni/papers/JWCMC_Qiang.pdf

[11] J. F. Kurose and K. W. Ross. Computer networking: a top-down approach featuring the Internet. Addison-Wesley, third edition, 2003.

[12] F. Halsall. Multimedia Communications, Applications, Networks, Protocols and Standards. Addison-Wesley, 2001.

[13] M. Malli, Q. Ni. et. Al. “Adaptive Fair Channel Allocation for QoS Enhancement in IEEE802.11 Wireless LANs”, 2004

[14] H. Chaouchi, A. Munaretto "Adaptive QoS Management for IEEE 802.11 Future Wireless ISPs", 2004.

[15] L. Romdhani, Q. Ni et. al. “Adaptive EDCF: Enhanced Service Differentiaion for IEEE 802.11 Wireless ad-hoc networks” 2003.

[16] N. Ramos, D Panigrahi et. al. “Quality of Service Provisioning in 802.11e Networks: Channenges, Approaches and Future Direction”, 2005.

[17] J. Majkowski, F. Casadevall “Admission control in IEEE 802.11e EDCA” International wireless Summit 2005.

[18] S. Mangold, S. Choi et. al. “IEEE 802.11e Wireless LAN for Quality of Service”, 2001.

[19] S. Wang, A. Helmy “Performance Limits and Analysis of Contention-based IEEE 802.11 MAC”, 2005.

[20] P. Ansel, Q. Ni et. al. “An Efficient Scheduling Scheme for IEEE 802.11e”, 2004

[21] R. Braden, D. Clark, and S. Shenker. Integrated services in the Internet architecture: An overview. RFC 1633, June 1994.

[22] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss. An architecture for differentiated service. RFC 2475, December 1998.

[23] Kiran K, Nitin R et. al. “QoS Assurance in Unreliable Networks”, 2002.

[24] N. Ramos, D. Panigrahi et. al. “Dynamic Adaptation Policies to Improve Quality of Service of Multimedia Applications in WLAN Networks”, 2003.

[25] S. Selvakennedy, “The Impact of Transmit Buffer on EDCF with Frame-Bursting Option for Wireless Networks”, the Annual IEEE Int. Conf. on Local Computer Networks, 29 Tampa, Florida, USA Nov. 2004

[26] N. Ramos, D. Panigrahi et. al. “ChaPLeT: Channel-dependent Packet Level Tuning for Service Differentiation in IEEE 802.11e”, 2003

[27] D. Yasir “ A Survey of QoS Techniques in 802.11” Department of Computer Science, Kent State University, 2002.

[28] S. Choi, J. Prado, S Shankar, S. Mangold “IEEE 802.11e Contention-Based Channel Access (EDCF) Performance Evaluation (2003).

[29] S. Mangold, S. Choi, P. May, O. Klien, G, Hiertz, L. Stibor “IEEE 802.11e Wireless LAN for Quality of Service”.

[30] IEEE 802.1D-1998, part3: Media Access Control (MAC) Bridges, ANSI/IEEE Std. 802.1D, 1998 edition, 1998.

[31] H. Zhu and I. Chlamtac, “An Analytical Model for IEEE 802.11e EDCF Differential Services”, 2003.

[32] N. Dhanakoti, S. Gopalan et. al. “Perfectly Periodic Scheduling for Fault Avoidance in IEEE 802.11e in Context of Home Networks”, 2003

[33] A. Denmark Sep. 2005. W. Stallings. High-Speed Networks and Internets: Performance and Quality of Service. Prentice-Hall, second edition, 2002.

Appendix A

List of Abbreviations

AC	Access Category
ACK	Acknowledgement
AIFS	Arbitration Inter-Frame Spacing
AP	Access Point
CA	Collision Avoidance
CBR	Constant Bit Rate
CFB	Contention Free Bursting
CFP	Contention Free Period
CP	Contention Period
CSMA	Carrier Sense Multiple Access
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access / Collision Detection
CW	Contention Window
CWmax	Contention Window Maximum
CWmin	Contention Window Minimum
DCF	Distributed Coordination Function
DS	Distribution System
DSSS	Direct Sequence Spread Spectrum
EDCA	Enhanced Distributed Channel Access
EDCAF	Enhanced Distributed Channel Access Function
ESS	Extended Service Set
FEC	Forward Error Correction
FHSS	Frequency Hopping Spread Spectrum
HC	Hybrid Coordinator
HCCA	HCF Controlled Channel Access
HCF	Hybrid Coordination Function
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IR	Infrared
ISM	Industrial, Scientific and Medical
MAC	Medium Access Control
NAV	Network Allocation Vector
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open Systems Interconnection
PC	Point Coordinator
PCF	Point Coordination Function
PIFS	PCF Inter-Frame Spacing
QAP	Quality of Service Access Point
QSTA	Quality of Service Station
QBSS	Quality of Service Basic Service Set

QIBSS	Quality of Service Independent Basic Service Set
QoS	Quality of Service
RTS/CTS	Request To Send / Clear To Send
SIFS	Short Inter-Frame Spacing
TCP	Transmission Control Protocol
TID	Traffic Identifier
TXOP	Transmission Opportunity
UDP	User Datagram Protocol
UP	User Priority
VoIP	Voice over IP
WLAN	Wireless Local Area Network