DESIGN & MODELING OF MANET USING DIFFERENT SLOT TIME SIMULATED BY NS-2

MOHD. IZHAR & MOHD. SHAHID

P.hd. Scholars of Mewar University,Chittorgarh, Rajasthan,

DR. V.R.SINGH,

Director, PDM College Of Engineering, Bahadurgarh, Haryana

Abstract— Abstract— IEEE 802.11 MAC protocol has been the standard for Wireless LANs, and also adopted in many network simulation packages for wireless multi-hop ad hoc networks.MAC is defined to proper access to the channel and that is also responsible for throughput and fairness in the network. IEEE 802.11 MAC protocol has been the standard for Wireless LANs, and also adopted in many network simulation packages for wireless multi-hop ad hoc networks. While IEEE 802.3 MAC Protocol had been standardized for Wired LAN.

in this paper we worked on assessment and evaluation of wireless MAC aiming at College Campus Area. We simulated using ns2 and concluded a performance model best suited for College Campus Area for networking in terms of throughput and delay. We created performance measurement model of Wireless local area network for large number of mobile nodes that take part, move and communicate one another in a WLAN i.e. in a typical scenario of a College Classroom or College's conference hall where each person is equipped with a Lap Top or other walkie-talkie instruments and simulate our models taking varying time slot from 30 to 20, 15 & 10 micro sec. for getting optimum key point for such WLANs.

Keywords: ad hoc network, wired, wireless LAN, mobility, radio frequency, Slot time, throughput, delay

I. INTRODUCTION

The needs of accessing information while moving around make mobile technologies very demanding and preferred by a lot of users. In fact, when we talk about mobility, the closest term that comes to our mind is "Wireless Network" which is any network system that provides users with both mobility and flexibility in accessing information. Because of the needs for mobile communication, wireless network has become very popular. Unlike the wired Local Area Network, IEEE 802.11, one of the most popular WLAN does not require a physical connection from the client to be connected to the network because the data is transmitted and received over the air [1]. In ad hoc networks, communications are done over wireless media between stations directly in a peer to peer fashion

Without the help of wired base stations or access points. The nodes are self-organizing, autonomous and mobile and act as hosts, routers, transmitters, receivers or intermediate hops The scope of MANETs is tremendous; it is one of the emerging fields, which will prove to be very useful in the near future [2]. However, there are many problems encountered in the upper protocol layers in IEEE 802.11 wireless networks. The packet delay greatly increases when there are serious collisions due to the heavy traffic. Packets may be dropped either by the buffer overflow or by the MAC layer contentions.

Besides in infrastructure network in wireless Technologies there is access points where there Security is main Concern. By default, a wireless network access point is open to anyone within in range with the proper equipment and if the router or access point is configured to distribute IP addresses via DHCP (Dynamic host configuration protocol), anyone equipped with a wireless enabled laptop or PDA can use that one freely. Older wireless routers/access points have two basic security methods: **MAC address** filtering and Wired Equivalent Privacy **(WEP)**. Both MAC and WEP offer only very basic security, and the risks are associated with them. Even Newer versions of wireless routers/access points make use of 2 additional security methods. The first is the Wireless Application Protocol **(WAP),** of which there are several variations. A router/access point may also support the Remote Authentication Dial In User Service **(RADIUS),** a protocol that works in conjunction with Network Operating Systems such as Windows, UNIX or Linux servers and is used for larger networks. But yet a lot of security measures are required to be done.

In this paper we study the characteristics & performance of Mac Layer with regard to IEEE 802.11 MAC protocol and 802.3 MAC protocol [3-4] from the point of view of **COLLEGE AREA NETWORK**. That means our Area includes no hilly region or such where lying of fiber optic cable is altogether unrealistic. On the basis of that we concluded that if we ignore the one time heavy investment in setting up fiber optic wired network at University Campus, we on the one hand would be able to solve the problem of security which are inherent in the wireless scenario and would get also higher throughput, fair delay and less packet losses as we already discussed the problems of TCP which was actually meant for wired network. To Support our vision we conducted our simulation using ns2. We simulated & evaluated MAC that means old legacy and new Protocol with TCP and checked throughput, fairness & Performance restricting to the environment of College Campus Area. We created Performance model for noting down better throughput and less delay if one chose to select WLAN for CAN.

2. Related Work

Many Papers have been published relating to performance of wireless Lan based on Mac Protocol In which probability distribution of the MAC layer packet service time (i.e., the time interval between the time instant a packet starts for transmission and the time instant that the packet either is acknowledged for correct reception by the intended receiver or is dropped) has been characterized[2]. Different types of traffic such as video, voice and data has been taken into account that means performance evaluation DCF vs. EDCF has been done[6]. Paper on QoS that is IEEE 802.11e has also been published by different authors.[2,6 7]. From the network perspective, QoS refers to the service quality or service level that the network offers to applications or users in terms of network QoS parameters, including: latency or delay of packets traveling across the network, reliability of packet transmission, and throughput. From the application/user perspective QoS generally refers to the application quality as perceived by the user. That is, the presentation quality of the video, the responsiveness of interactive voice, and the sound quality of streaming audio.

However improved Performance of wireless LAN has been thought and simulated from by improving the MAC from old legacy to IEEE 802.11e but to the best of our knowledge and belief no one thought to create a Model particularly for University Campus Area or Area which comes in between the Wired Local Area Network and Wide Area Network. So we Create Performance Model for Campus Area Network based on MAC Protocol, we change slot time[1] to see the optimum point where the model performance would be the best in terms of throughput and delay.

3. BACKGROUND

MAC (Media Access Control)

The 802.11 family uses a MAC layer known as **CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)** while Classic Ethernet uses CSMA/CD - collision detection). CSMA/CA is, like all Ethernet protocols, peer-to-peer (there is no requirement for a master station).

As any 802.x protocol, the 802.11 protocol covers the MAC and Physical Layer, the Standard currently defines a single MAC which interacts with three PHYs (all of them running at 1 and 2 Mbit/s) :

- Frequency Hopping Spread Spectrum in the 2.4 GHz Band
- Direct Sequence Spread Spectrum in the 2.4 GHz Band,
- Infra Red

<table>
<tr><td colspan="3">802.11</td><td rowspan="2">DATA LINK LAYAER</td></tr>
<tr><td colspan="3">802.11 MAC</td></tr>
<tr><td>Frequency Hopping</td><td>Direct Sequence Spread Spectrum</td><td>Infra Red</td><td>PHYSICAL LAYER</td></tr>
</table>

The MAC Layer defines two different access methods,

1. Distributed Coordination Function and
2. Point Coordination Function

The Basic Access Method: CSMA/CA

The basic access mechanism, called Distributed Coordination Function, is basically a Carrier Sense Multiple Access with Collision Avoidance mechanism (usually known as CSMA/CA). CSMA protocols are well known in the industry, where the most popular is the Ethernet, which is a CSMA/CD protocol (CD standing for

Collision Detection).
A CSMA protocol works as follows:
A Wireless node that wants to transmit performs the following sequence:

1. Listen on the desired channel.
2. If channel is idle (no active transmitters) it sends a packet.
3. If channel is busy (an active transmitter) node waits until transmission stops then a further **CONTENTION** period. (The Contention period is a random period after every transmit on every node and statistically allows every node equal access to the media. To allow tx to rx turn around the contention time is **slotted** 50 micro sec for FH and 20 micro sec for DS systems).

If the channel is still idle at the end of the **CONTENTION** period the node transmits its packet otherwise it repeats the process defined in 3 above until it gets a free channel.

These kind of protocols are very effective when the medium is not heavily loaded, since it allows stations to transmit with minimum delay, but there is always a chance of stations transmitting at the same time (collision), caused by the fact that the stations sensed the medium free and decided to transmit at once. These collision situations must be identified, so the MAC layer can retransmit the packet by itself and not by upper layers, which would cause significant delay. In the Ethernet case this collision is recognized by the transmitting stations which go to a retransmission phase based on an exponential random backoff algorithm.

While these Collision Detection mechanisms are a good idea on a wired LAN, they cannot be used on a Wireless LAN environment, because of two main reasons:

1. Implementing a Collision Detection Mechanism would require the implementation of a Full Duplex radio, capable of transmitting and receiving at once, an approach that would increase the price significantly.
2. On a Wireless environment we cannot assume that all stations hear each other (which is the basic assumption of the Collision Detection scheme), and the fact that a station willing to transmit and senses the medium free, doesn't necessarily mean that the medium is free around the receiver area in order to overcome these problems, the 802.11 uses a Collision Avoidance mechanism together with a Positive Acknowledge scheme, as follows:

A station willing to transmit senses the medium, if the medium is busy then it defers. If the medium is free for a specified time (called DIFS, Distributed Inter Frame Space, in the standard) then the station is allowed to transmit, the receiving station will check the CRC of the received packet and send an acknowledgment packet (ACK). Receipt of the acknowledgment will indicate the transmitter that no collision occurred. If the sender does not receive the acknowledgment then it will retransmit the fragment until it gets acknowledged or thrown away after a given number of retransmissions.

Slot time is the time it takes for a packet to travel the maximum theoretical distance between two nodes in a network. Collision detection protocols always wait for a minimum of slot time before transmitting; allowing any packet that was being sent over the channel at the same time to which(channel) the waiting node requested to send, to reach the waiting node.If the slot time were less it would mean that the nodes waiting to send a packet would wait for a small time before transmission. If the slot time were set to a large value, it would mean that they would have to wait for a longer period of time. From this we can conclude that smaller slot time would mean more collisions and longer slot time would mean lesser collisions. Setting the slot time to an optimum value is important. While we would not want to set it to a value too small, we would also not want to set it to a value bigger than necessary. That would mean that the nodes would have to wait for an unnecessarily long period of time[1]. Time slots are divided into multiple frames, and there are several types of InterFrame Spacing (IFS) slots. In increasing order of length, they are the Short IFS (SIFS), Point Coordination Function IFS (PIFS), DCF IFS (DIFS), and Extended IFS (EIFS). The node waits for the medium to be free for a combination of these different times before it actually transmits. Different types of packets can require the medium to be free for a different number or type of IFS. For instance, in ad hoc mode, if the medium is free after a node has waited for DIFS, it can transmit a queued packet. Otherwise, if the medium is still busy, a backoff timer is initiated. The initial backoff "10" value of the timer is chosen randomly from between 0 and CW-1, where CW is the width of the contention window, in terms of time slots. After an unsuccessful transmission attempt, another backoff is performed with a doubled size of CW as decided by a Binary Exponential Backoff (BEB) algorithm. Each time the medium is idle after DIFS, the timer is decremented. When the timer expires, the packet is transmitted. After each successful transmission, another random backoff (known as "postbackoff") is performed by the transmission-completing node. A control packet such as RTS, CTS, or ACK is transmitted after the medium has been free for SIFS.

4. Simulation Results

We create the model using mac protocol IEEE 802.3 and IEEE 802.11 in peer to peer fashion and concluded that throughput of old legacy mac is always more far than the new mac Protcol (figure1)

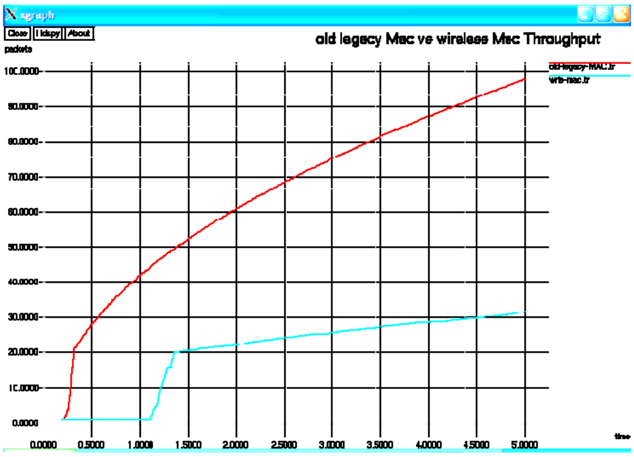

Figure 1: Throughput of old legacy MAC and New MAC in P2P fashion

Then we create another model now this time no. of nodes are increased, we varied the packet size. The Simulation Time, the no. of nodes, the packet size, traffic type were the same for both ieee 802.3 old legacy mac and ieee 802.11 new mac. and got the same result that old legacy mac gives rise to throughput if compared to new mac.

Now we create a performance Model in which different parameters were taken as follows: We create a separate file for movement of nodes. The different parameters chosen were as follows : No. of nodes: 100, pause time : 2.00 sec., moving max speed: 10.00 m/s, Topology boundary max x: 500.00, max y: 500.00 and initial position were as follows

```
$node_(0) set X_ 130.438757275991
$node_(0) set Y_ 139.623985169872
$node_(0) set Z_ 0.000000000000
$node_(1) set X_ 428.221660566075
$node_(1) set Y_ 7.964065916959
$node_(1) set Z_ 0.000000000000
…
$node_(99) set X_ 353.582387567762
$node_(99) set Y_ 124.185311452147
$node_(99) set Z_ 0.000000000000
$ns_ at 2.000000000000 "$node_(0) setdest 349.538592902019 119.186864535061 0.051098892146"
…
$ns_ at 2.000000000000 "$node_(99) setdest 208.687573649691 175.900926135339 3.203277244764"
```

For Communication we choose the following parameters :

nodes: 100, max conn: 40, send rate: 0.37593984962406013, seed: 1.0 e.g.

```
# 1 connecting to 2 at time 2.5568388786897245
set udp_(0) [new Agent/UDP]
$ns_ attach-agent $node_(1) $udp_(0)
set null_(0) [new Agent/Null]
$ns_ attach-agent $node_(2) $null_(0)
set cbr_(0) [new Application/Traffic/CBR]
$cbr_(0) set packetSize_ 512
$cbr_(0) set interval_ 0.37593984962406013
$cbr_(0) set random_ 1
$cbr_(0) set maxpkts_ 10000
$cbr_(0) attach-agent $udp_(0)
$ns_ connect $udp_(0) $null_(0)
$ns_ at 2.5568388786897245 "$cbr_(0) start"
…
# 44 connecting to 45 at time 141.0795085137149
set udp_(39) [new Agent/UDP]
$ns_ attach-agent $node_(44) $udp_(39)
set null_(39) [new Agent/Null]
```

```
$ns_ attach-agent $node_(45) $null_(39)
set cbr_(39) [new Application/Traffic/CBR]
$cbr_(39) set packetSize_ 512
$cbr_(39) set interval_ 0.37593984962406013
$cbr_(39) set random_ 1
$cbr_(39) set maxpkts_ 10000
$cbr_(39) attach-agent $udp_(39)
$ns_ connect $udp_(39) $null_(39)
$ns_ at 141.0795085137149 "$cbr_(39) start"
Total sources/connections: 25/40
```

Micro sec.	average(delay),
10	0.176715
15	0.18272
20	0.175573
30	0.165745

Table 1: Delay at 75 Nodes

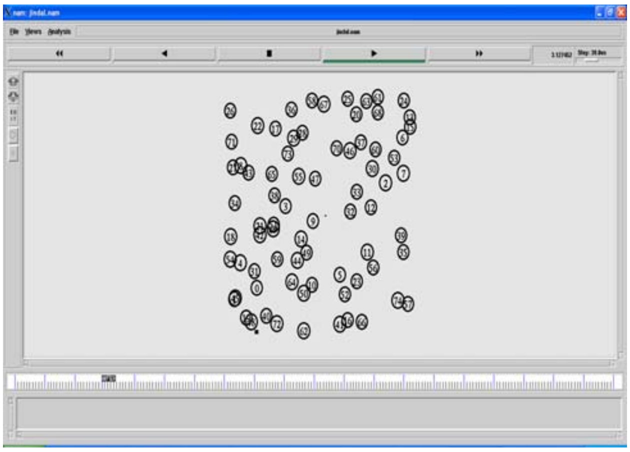

Figure 2: Scattered 75 nodes within a CAN (College Area Network)

We simulate our performance model by varying slot time from 20 micro sec. to 15, 12 & 10. We got the following delay.

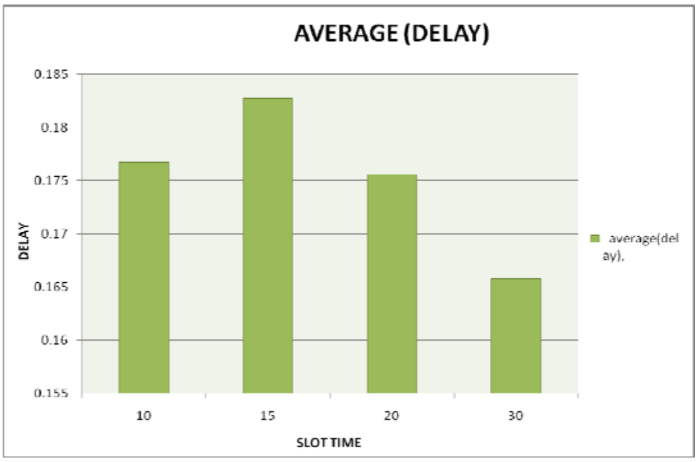

Figure 3: Average end to end delay

We conclude that the delay at 30 micro sec is lowest but this conclusion is not of any use until and unless we compare our result with average throughput. That is comparing result with delay only & taking varied slot time for performance is not enough.

The following table shows the combine result of throughput and average delay with varied slot time.

Slot time(micro sec)	Average (delay)	Average (throughput)	Result Per 1000 (Throughput)
30	1657.45	3644.1112	2198.62515
20	1755.73	4510.5842	2569.06486
15	1827.2	5112.4264	2797.95665
10	1767.15	5071.0332	2869.61109

Table 2: Throughput & Delay at 75 Nodes

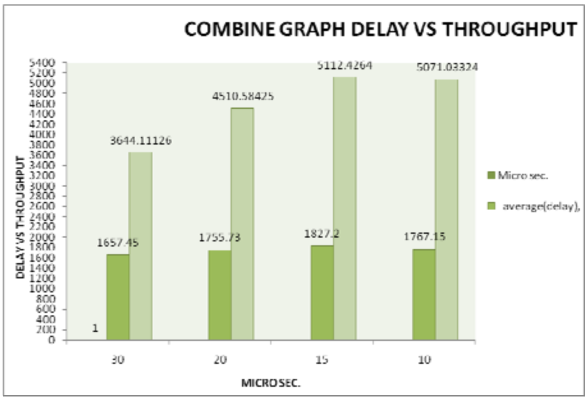

Figure 4: Throughputs Vs end to end delays

Micro sec.	average(delay), Less No. of Nodes(20)
30	0.011242
20	0.016797
15	0.024545
10	0.005916

Table 3: Average Delay at Less No. of Nodes

The Graph also shows the same result as expected

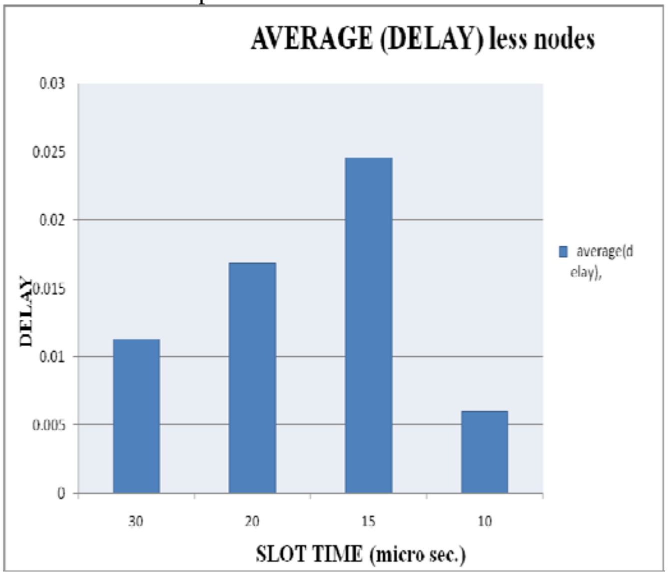

Figure 5: Average delay with less no. of nodes

Again we conclude that the delay at 10 micro sec is lowest but again this conclusion is not of any use until and unless we compare our result with average throughput. That means again comparing result with delay only; taking varied slot time for performance is not enough.

The following table & Graph shows the combine result of throughput and average delay with varied slot time

Slot time Micro sec	**Average (delay)**	**average (throughput)**	**Result Per 1000 (Throughput)**
30	**1124.2**	**4783.1977**	**4254.757**
20	**1679.7**	**3757.91**	**2237.251**
15	**2454.5**	**2861.3609**	**1165.761**
10	**591.6**	**2047.6992**	**3461.29**

Table 4: Throughput at 20 Nodes

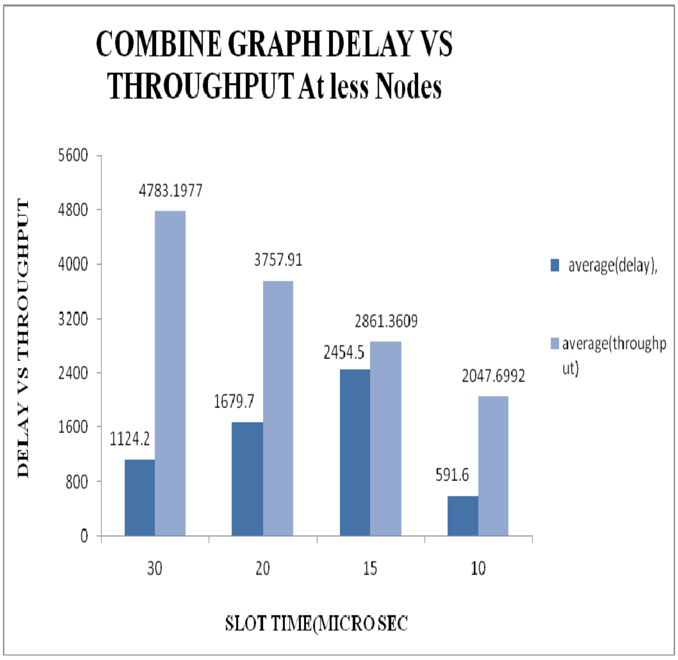

Figure 6 : Combine graph with less nodes

This time we take average throughput with more nodes and lesser no. of nodes for simulation and conclude that the graph created from values of both types of scenario gives almost same result.

Slot time	Average(throughput) 75 nodes	Average(throughput) 40 nodes
30	3644.11126	4643.8824
20	4510.58425	4287.821
15	5112.4264	3020.2468
10	5071.03324	2101.607

Table 5 : Average Throughput at75 & 40 Nodes

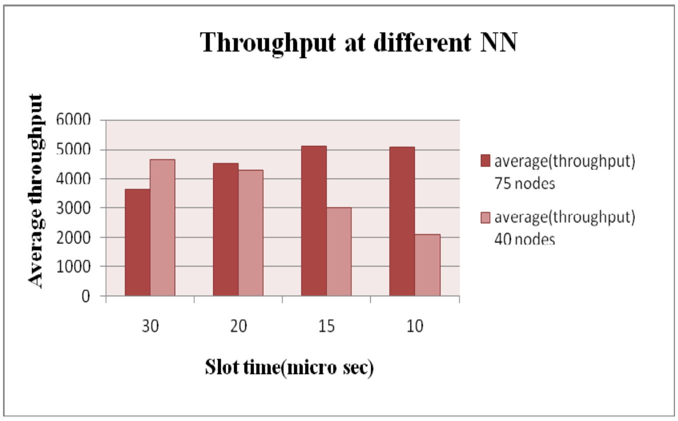

Figure 7: Throughput at Different NN

We also show our result by taking the delay also at the scenario of different no. of nodes through following table & Graph and conclude that the graph is moving similar way in both scenarios

Slot time	average(Delay) 75 nodes	average(delay) 40 nodes
20	1657.45	895.6
15	1755.73	1012
12	1827.2	1094.6
10	1767.15	593.2

Table 6: Average Delay at75 & 40 Nodes

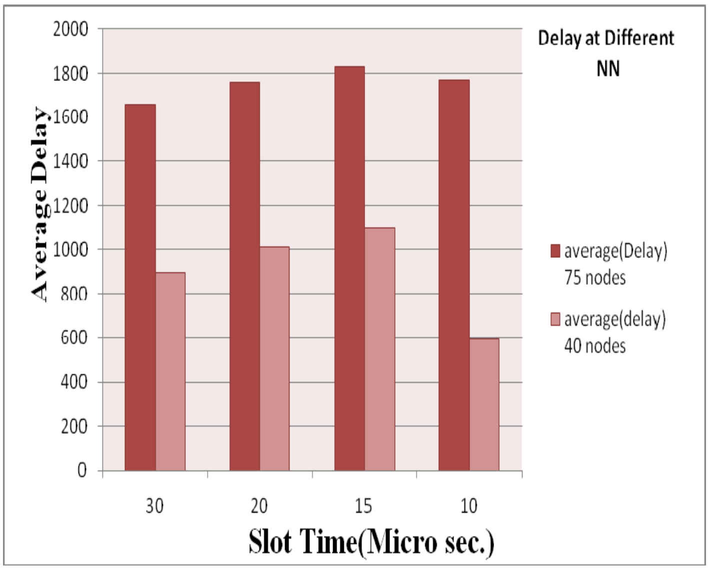

Figure 8: Delay at Different NN

Now we again take less no. of nodes from 50 nodes to 25 nodes thinking a small class room in University and find out that this time the simulation results of delay and throughput was similar to previous one except some variation. We Combine the delay and Throughput and calculated throughput taking the delay fixed as per 1000 to get the exact answer. The following tables and graph shows the same.

Slot time	Throughput vs. Delay(Per1000) at 75 nodes	Throughput vs. Delay (Per1000) at 40 nodes	Throughput vs. Delay (Per1000) At 20 nodes
30	2198.625153	4159.437	4254.757
20	2569.064862	4339.275	2237.251
15	2797.956655	3305.962	1165.761
10	2869.611091	1246.673	3461.29

Table 7: Throughput vs. Delay at 75, 40 & 20 Nodes

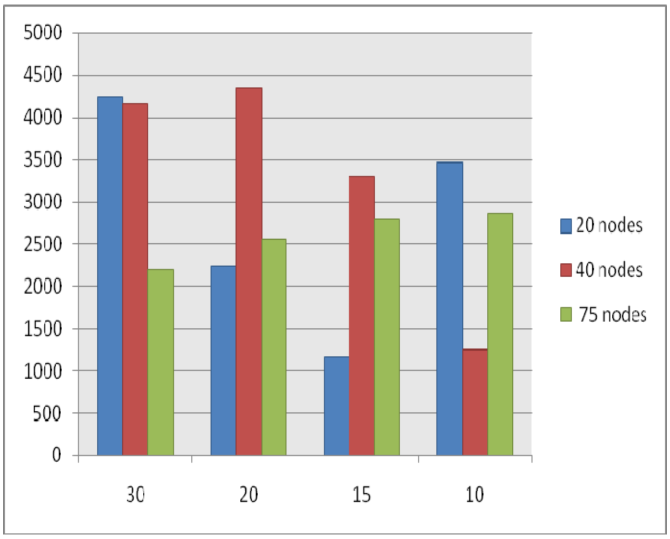

Figure 9: Throughput Vs Delay (Per 1000) at different NN

On the basis of this final graph one can conclude that the throughput of 75 nodes & 40 nodes, keeping the delay fixed as 1000 for all the no. of nodes, is best at the slot time of 10 ms while the throughput of 40 nodes vary and it is better at 10 m/s but the best slot time is 12 m/s.

5. CONCLUSION AND FUTURE WORK

The result shows that average delay at 15 micro sec. is highest and throughput is highest. & average delay at 30 micro sec. is lowest and throughput is also lowest. That means slot time can be considered altogether at that time. At 20 & 10 Micro sec. there is close competition where the difference of both delay and throughput is medium. The lowest delay in our result is at 30 micro sec. but throughput is not highest. It has low throughput than throughput at 20 as well as at 10 micro sec. The Highest throughput is at 15 micro sec. It seems that the optimum point is at either 20 or 10 micro sec. But when we compare the result by taking the delay equal to all in per thousand, the picture becomes clear and we get the optimum point which is 10 micro sec. for our performance model.

Through this paper we aimed to know the **performance of Mac Protocol** in three different aspects keeping in mind the three different versions of Mac Protocols, standardized and specified by the IEEE. Firstly we evaluated and examined the IEEE 802.3 MAC Protocol. Secondly we took for examination IEEE 802.11 MAC Protocol standardized for wireless LAN. We Compared it with it legacy one. IEEE 802.11e has been kept in third Category, a lot of work on which has been done. IEEE 802.11 deals with the Quality of Service.

We conducted simulation and Conclude that IEEE 802.3 Mac Protocol can be effective than 802.11 but limited to our Campus Area Network. The reason is clearly drawn theoretically that wired nodes which are taking parts in the network are stationeries. The network is therefore static in nature. While wireless nodes are mobile moving as well as stationery and the topography of wireless network keep on changing that means they are dynamic in nature. That is why throughput of wired network is always good than the wireless one. Also there are other points of consideration which mac 802.11 more effective than old legacy.

To make the Mac Protocol more effective, IEEE standardizes 802.11e on Nov 2003. Which differentiate traffic such voice, video and data The Voice, video are delay sensitive while data is understood delay tolerant while 802.11 Mac provides equal access of channels to all types of traffic. Besides there are other problems of 802.11 Mac protocol such as packet delay and packet drops when traffic goes up resulting in poorly utilization of n/w capacity. So IEEE 802.11e may also be evaluated and examined comprising with IEEE 802.11 in near future.

References:

[1] M Mahbubur Rahman "Tunable Protocol for Mobile Ad Hoc Network" Daffodil International university", Bangladesh, 2007.
[2] Zhai, H. Fang. Y, "Performance of Wireless LANs based on IEEE 802.11 MAC Protocol"
[3] Emanuel Puschita, Tudor Palade, L.Chira "Performance Evaluation of DCF vs EDCF data link layer access Mechanism for WLAN "
[4] Puthal "Quality of Service Provisioning with modified IEEE 802.11 MAC Protocol" NIT, Rourkela,2008.
[5] TommiLarsson "A Study of EDCA and DCF in Multihop Ad-Hoc Networks" Master Thesis, CTU,2008.
[6] Jianping Li "Time Slot Assignment for Maximum Bandwidth in a Mobile Ad-Hoc Network" International Symposium on Wireless, USA, 2007.
[7] Mohd Izhar & Amit Prkash Singh "Effectively implementing CSMA/CA (IEEE 802.11) Protocol", 2009.
[8] Sam De Silva, "Using TCP Effectively in Mobile Ad-hoc Wireless Networks with Rate Adaptation" Report, 2007.
[9] IsmahansiBinti Ismail, "Study of Enhanced DCF(EDCF) in Multimedia Application."Master thesis. Malaysia, 2005.

[10] Guillermo Alonso Pequeno Javier Rocha Rivera, "Extension to MAC 802.11 for performance improvement in MANET". Master Thesis,2007.
[11] Pasupuleti "Throughput and Delay Evaluation of a Proposed-DCF MAC Protocol for WLAN" IIIT, Bangalore.
[12] P. Ellich "Fingerprinting 802.11Devices"California.
[13] Mohd Izuan, MohdSaad "Performance Analysis of Random-Based Mobility Models in MANET Routing Protocol "Journal of Scientific Research,2009. Page(s):444-454.
[14] Changhua He "Security Analysis and Improvements for IEEE 802.11i" Stanford.
[15] IEEE std. 802.11, 802.11a, 802.11b-1999, Part 11 Wireless LAN MAC and PHY Layer Specification.
[16] "The network simulator – ns," in, http:/www.isi.edu/nsnam/ns.