Performance Model for Campus Area Network Based on MAC Protocol

Vijendra Rai[1], Arvind Kumar[2], Jaishree Rai[3], Prashant Kr. Singh[4]
[1]USIT, GGS Indraprastha University
Delhi,India
[2]YMCA Faridabad
India
[3]MNNIT Allahabad
India
[4]Shobhit University Meerut
India
{vijendrarail, arvindreamsky, raijaishree, prashant.mngr}@gmail.com

ABSTRACT: *The routing simulations over ad hoc networks indicate that network capacity is poorly utilized in terms of throughput and packet delay when the 802.11 MAC protocol is integrated with routing algorithms. Also, since wireless network access point is open to anyone, problem of security is inherent in wireless scenario. In this paper we aim to study the characteristics & performance of MAC Layer with regard to IEEE 802.11 MAC protocol and IEEE 802.3 MAC protocol from the point of view of Campus Area Network. We conducted some simulation for the same using NS-2 and concluded an adaptive performance model best suited for University Campus Area for networking in terms of throughput and fairness. We created a performance model of Wireless local area network to show what happens when large number of mobile nodes take part, move and communicate with one another in a WLAN and simulated our model taking varying slot time from 20 to 15, 12 & 10 micro sec. for getting optimum key point for such WLANs.*

Keywords: IEEE 802.3, IEEE 802.11, MAC, NS-2, WLAN

Received: 12 December 2010, Revised 19 February 2011, Accepted 2 March 2011

1. Introduction

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.

1.1 MAC (Media Access Control)

The Media Access Control (MAC) data communication protocol sub-layer, also known as the Medium Access Control, is a sub-layer of the Data Link Layer specified in the seven-layer OSI model. It acts as an interface between the Logical Link Control (LLC) sub-layer and the network's physical layer. It provides addressing and channel access control mechanisms that make it possible for several terminals or network nodes to communicate within a multi-point network.

As IEEE 802.3 standard, the MAC layer defined by IEEE 802.11 standard is the lower part of the link layer and is placed between the dependent sub-layer of the physical layer and LLC sub-layer of the link layer. The MAC architecture is composed by two basic coordination functions: Punctual Coordination Function (PCF) and Distributed Coordination (DCF).

Each of these functions defines an operation mode for the stations that want to access the wireless medium. Coordination Function is defined as the function that determines, within a Basic Services Set (BSS), when a station is enabled to transmit and/ or receive Protocol data Units at MAC level (MPDUs) through the wireless channel. DCF is a basic and compulsory mode for all stations and is located at lower part of MAC architecture. The DCF functionality is based on random techniques and is used by asynchronous traffic that does not require a severe bounded time. The IEEE 802.11 standard specifies the CSMA/CA access algorithm for this level. PCF is located over DCF and the access algorithm for this level is based on circular polling from an access point, that is, deterministic access. This mechanism allows transmission of traffic that does not tolerate random and unbounded delays or contention free asynchronous traffic. Two coordination modes operate in the same network over a structure called the superframe: during the first part of the superframe, the network operates under DCF mode allowing random access. When the contention period finishes then the access point, called central coordinator, takes the medium and a contention free period begins.

The 802.11 family uses a MAC layer known as CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) while Classic Ethernet uses CSMA/CD (Carrier Sense Multiple Access/Collision Detection).

1.2 CSMA/CD (Carrier Sense Multiple Access/ Collision Detection)

In a wired network, a network interface is able to detect collisions by sensing the carrier and ceasing transmission if a collision is detected. This results in a medium access mechanism known as carrier sense multiple access/ collision detection (CSMA/CD). Collision detection is used to improve CSMA performance by terminating transmission as soon as a collision is detected, and reducing the probability of a second collision on retry.

In this model, any station having a frame to send may attempt to do so. If two or more stations decide to transmit simultaneously, there will be a collision. Collisions can be detected by looking at the power or pulse width of the received signal and comparing it to the transmitted signal. After a station detects a collision, it aborts its transmission, waits a random period of time, and then tries again, assuming that no other station has started transmitting in the meantime. Therefore, this model for CSMA/CD will consist of alternating contention and transmission periods, with idle periods occurring when all stations are quiet.

1.3 CSMA/CA (Carrier Sense Multiple Access/ Collision Avoidance)

A wireless network station is not able to detect a collision between its transmission and the transmission from another station, since a radio transceiver is unable both to transmit and to listen for other stations transmitting at the same time. So, CSMA/CD is used in wireless networks. 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), the node waits for a randomly chosen period of time, and then checks again to see if the channel is clear. This period of time is called the backoff factor, and is counted down by a backoff counter. If the channel is clear when the backoff counter reaches zero, the node transmits the packet.

4) If the channel is not clear when the backoff counter reaches zero, the backoff factor is set again, and the process is repeated until it gets a free channel.

1.4 Slot Time

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 at which the waiting node requested to send, to reach the waiting node. If the slot time were set to a small value, it would mean that the nodes waiting to send a packet would wait for a small time before transmission and 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. Smaller slot time would mean more collisions while longer slot time would mean lesser collisions but waiting for an unnecessarily long period of time. Therefore, setting the slot time to an optimum value is important.

Time slots are divided into multiple frames, and there are several types of Inter Frame 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

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 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 "post backoff") 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.

1.5 Packet Delay

In IEEE 802.11 MAC Protocol, 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. Such packet losses may affect high layer networking schemes such as the TCP window adaptation and networking routing maintenance. The routing simulations over ad hoc networks indicate that network capacity is poorly utilized in terms of throughput and packet delay when the 802.11 MAC protocol is integrated with routing algorithms. TCP in the wireless ad hoc networks is unstable and has poor throughput due to TCP's inability to recognize the difference between a link failure and congestion. Besides, one TCP connection from one-hop neighbors will capture the entire bandwidth, leading to the one- hop unfairness problem.

1.6 Security

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 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. A wireless network access point is open to anyone within range and having proper equipment. 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 it freely. So, security is the main concern in wireless networks. 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. 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.

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 (e.g. [2]) and performance evaluation of DCF vs. EDCF has also been done (e.g. [6]) by taking into account different types of traffic such as video, voice and data. Papers on Quality of Service parameters (QoS) for IEEE 802.11 have also been published by different authors (e.g. [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 i.e. 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 by improving the MAC from IEEE 802.3 to IEEE 802.11 but, to the best of our knowledge, 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 created a Performance Model for Campus Area Network based on MAC Protocol, by varying slot time (e.g. [1]) to see the optimum point where the model performance would be the best in terms of throughput and delay.

3. Experimental Setup

The simulation experiment is carried out in LINUX (Ubuntu 9.04). The detailed simulation model, based on network simulator-2 (ver-2.33), is used in the evaluation. The NS instructions can be used to define the topology structure of the network and the motion mode of the nodes, to configure the service source and the receiver, to create the statistical data track file and so on.

4. Testing And Analysis

We created the model using Mac protocol IEEE 802.3 and IEEE 802.11 in peer to peer fashion and concluded that throughput of 802.3 Mac is always better than 802.11 MAC (Figure1).

To confirm our results, we created another model with increased number of nodes and varied packet size. The simulation time, the number of nodes, the packet size and the traffic type were same for both IEEE 802.3 MAC and IEEE 802.11 MAC. Figure 2 shows the result obtained for this scenario. It supports the conclusion drawn above where throughput for IEEE 802.3 was more as compared to that of IEEE 802.11.

In both the scenarios, IEEE 802.3 outperforms IEEE 802.11 in terms of throughput. From the above results, we can say that IEEE 802.3 MAC Protocol is more effective than IEEE 803.11 MAC Protocol for a Campus Area Network in terms of throughput.

Next, we created a Performance Model suited for University Campus Area, a typical scenario of a classroom or a conference hall, where each person is equipped with a laptop. Different parameters that were taken are as follows:

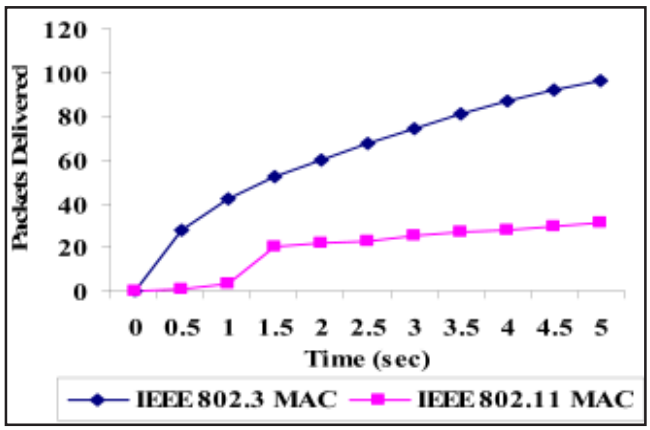

Figure 1. Throughput comparison of IEEE 802.3 & IEEE 802.11 MAC Protocols

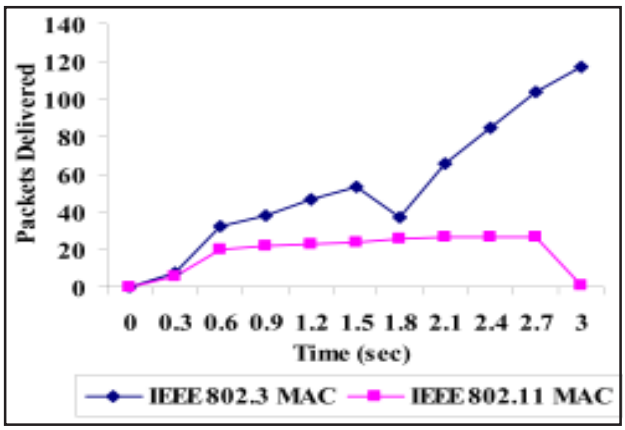

Figure 2. Throughput comparison of IEEE 802.3 & IEEE 802.11 MAC Protocols in varied scenario

We simulated our performance model by varying slot time from 20 micro sec to 15, 12 & 10 micro sec. We got the following delay for 100 nodes:

Now, we changed the scenario by decreasing the number of nodes. We found the delay for 50 nodes as follows:

Number of nodes	100-scene1, 50-scene 2
Pause Time	2 sec
Moving max. speed	10.00 m/s
Topology Boundary	Max X: 500.0, max Y: 500.0
Send Rate	0.37593984962406013
Max. connection	40
Total source/connections	25/40

Table 1. Experimental Setup for Performance Model

Micro sec.	Average(delay),
20	0.01094
15	0.010992
12	0.014026
10	0.010628

Table 2. Delay for 100 Nodes

The graph below shows the delay for two different scenarios, having 100 and 50 nodes.

Figure 3 shows that the delay at 10 micro sec is lowest for both the scenarios but this conclusion is not of any use until and

unless we compare our result with average throughput.

Throughput values corresponding to different delay for both the scenario, viz. 50 nodes and 100 nodes, gave almost same results. The following graph shows the combine result of throughput and average delay with varied slot time:

Micro sec.	average(delay), Less No. of Nodes
20	0.01051
15	0.01122
12	0.01123
10	0.01043

Table 4. Delay for 50 Nodes

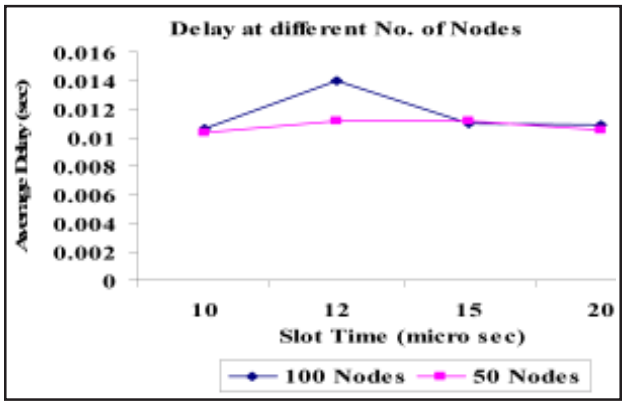

Figure 3. Delay at different NN

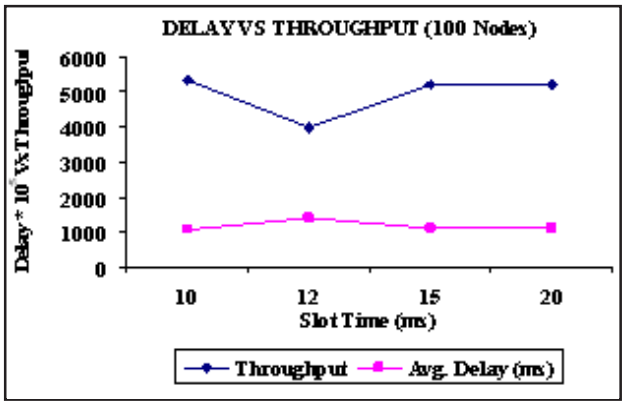

Figure 4. Throughputs vs. end to end delays for 100 nodes

The result shows that average delay at 12 micro sec. is highest and throughput is lowest. That means slot time can not be considered altogether at that time. At 20 & 15 Micro sec. there is close competition where the difference of both delay and throughput is very less .The lowest delay in our result is at 10 micro sec. but throughput is not highest. It has low throughput than throughput at 20 as well as at 15 micro sec. Highest throughput is at 15 micro sec. It seems that the optimum point is at either 20 or 15 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.

Same comparison was also performed for 50 nodes. The optimum point obtained in this case is also 10 micro sec, where average delay is lowest.

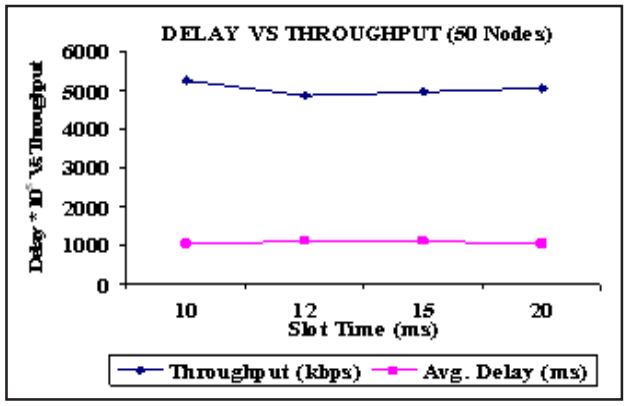

Figure 5. Throughputs vs. end to end delays for 50 nodes

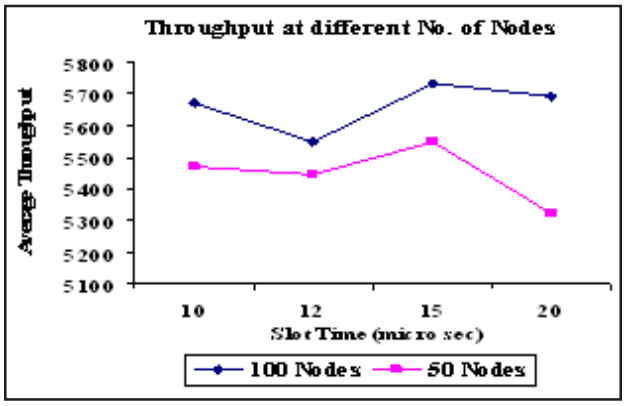

Figure 6. Throughput at different NN

Figure 5 confirms the results obtained from the scenario where we used 100 nodes.

Average throughput values for the two different scenarios shows the same result in both the cases. Throughput for IEEE 802.3 is always more as compared to IEEE 802.11. Comparison in figure 6 shows that IEEE 802.3 gives better performance than IEEE 802.11in terms of throughput.

5. Conclusion

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 that has been standardized for wireless LAN. We conducted simulation keeping in the mind the Campus Area Network and concluded that IEEE 802.3 Mac Protocol can be more effective than 802.11. 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 or 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 better than the wireless one. So, if we ignore the one time heavy investment in setting up fiber optic wired network at University Campus, on one hand, we would be able to solve the problem of security which is inherent in the wireless scenario and on the other hand, we would also get higher throughput.

6. Future Work

There are other points of consideration which make 802.11 more effective than 802.3. To make the Mac Protocol more effective, IEEE standardizes 802.11e on November 2003, which differentiates traffic such voice, video and data. The voice, video are delay sensitive and data is understood delay tolerant while IEEE 802.11 MAC provides equal access of channels for 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 poor utilization of n/w capacity. So IEEE 802.11e may also be evaluated and examined comprising with IEEE 802.11 in near future. That is Why IEEE 802.11e has been kept in third Category, a lot of work on which has been done that deals with the Quality of Service. A lot of work can be done using it.

7. Acknowledgment

We wish to acknowledge the technical and administrative support we received at the NIC (HQ) that was imperative in the completion of this paper. We would also like to express our gratitude to the friends and family who were supportive in the entire process.

References

[1] Rahman, M.M., Abu Layek, Md. (2007). Tunable Protocol for Mobile Ad hoc Network, National Conference on Communication and Information Security, NCCIS 2007 Daffodil International University, Dhaka, Bangladesh, 24 November.
[2] Zhai, H., Fang,Y. (2003). Performance of Wireless LANs based on IEEE 802.11 MAC Protocol, IEEE PIMRC.
[3] IEEE std. 802.11, 802.11a, 802.11b-1999, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE.
[4] Sarkar, S.K., Basavaraju, T.G., Puttomadappa, C. (2007) Ad-hoc Mobile wireless Networks, Principles, Protocols and Application, Auerbach Publications Oct.
[5] The Network Simulator-ns-2, (2007).http://www.isi.edu/nsnam/ns, March 28.
[6] Puschita, E., Palade, T., Chira, L. (2005). Performance Evaluation of DCF vs. EDCF Data Link Layer Access Mechanisms for Wireless LAN Scenarios:QoS Perspective, *In*: 7th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services – TELSIKS'05, September 28-30, Niš, Serbia and Montenegro, Volume 2/2, p. 356-359.
[7] He, D., Shen, C.Q. (2004). Simulation study of IEEE 802.11e EDCF, European IST Moby Dist Project.
[8] Greis, M(1998). Tutorial for the Network Simulator ns, p. 151-160, June.
[9] Pequeño, G. A., Rivera, J.R. (2006). Extension to MAC 802.11 for performance improvement in MANET, Serial Number: D2007:06 December 21.