Jagadevikoodi, Kalaiselvi And Rakeshmarturkar / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 3, Issue 4, Jul-Aug 2013, pp.200-206

Providing Fair Transmission Opportunity By Detecting And Penalizing Malicious Stations In IEEEE 802.11e EDCA WLAN And Analyzing The Performance Of IEEE 802.11e

Jagadevikoodi[1], Kalaiselvi[2] And Rakeshmarturkar[3]
[1]PG Student, The Oxford College of Engineering, India
[2]Asst Professor, The Oxford College of Engineering, India
[3]Asst Professor, GNDEC, Bidar, India

Abstract

IEEE 802.11e Medium Access Control (MAC) is an enhancement to the Wireless Local Area (WLAN) IEEE 802.11 standard to support QOS.IEEE 802.11e is used which enables QOS to various delay sensitive applications such as voice, video over WLAN and Streaming multimedia. In this paper we proposed a Malicious Behavior Detection Algorithm that allows identification of misbehaving wireless stations and give out punishment by not sending an Acknowledgment (ACK) packet by the malicious stations and analyze the performance of IEEE 802.11e. This algorithm is designed for an IEEE 802.11e network and is based on detecting a QOS change where a station is moved to a level which is not justified based on the parameters such as TXOPLimit, AIFS and Backoff time. Our strategy is to provide fair resource sharing between the stations which are operating from the same access point and to provide QOS by provisioning the priority to different classes of traffic and make sure that always higher prioritized traffic gets preferential access to channel than lower prioritized traffic.

Keywords – IEEE802.11, IEEE802.11e, QOS, Malicious Station, Transmission Opportunity, EDCA, MAC, WLAN

I. Introduction

IEEE 802.11 Wireless Local Area Networks (WLANs) is the most popular existing wireless technology over the world because of its low cost, easy simplicity, deployment and robustness against failures. These advantages are a result of distributed approach of Medium Access Control (MAC) protocol. Day by day the popularity of real time interactive and multimedia applications is growing rapidly. The IEEE 802.11 is a MAC sub-layer which defines two medium access coordination functions, the Distributed Coordination Function (DCF) and the optional Point Coordination Function (PCF). DCF is the basic access function for IEEE 802.11 and is based on a Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) algorithm together with a contention (back off) algorithm [1]. PCF uses a polling method cyclically where node is used to play the role of Point Coordinator (PC). The PC polls stations cyclically to give the opportunity to them to transmit. This IEEE 802.11 networks are Best-Effort networks and they do not give support to QOS. To overcome this, in year 2005, IEEE 802.11e has been introduced to replace the best effort services that guarantee QOS attributes [1]. This standard focuses on replacing the conventional Distributed Coordination Function (DCF) and the optional Point Coordination Function (PCF) of Medium Access Control (MAC) layer by a Hybrid Coordination Function (HCF) [2].The HCF defines two medium access mechanisms: a contention based channel access called as Enhanced Distributed Channel Access (EDCA), and controlled channel access called as HCF Controlled Channel Access (HCCA). For both channel access functions new concept has been introduced that is Transmission Opportunity (TXOP). During TXOP period, QOS data can be burst by a wireless station without any interruption by other wireless stations. For the contention-free period, HCCA is used with the hybrid coordinator (HC) installed at the Access Point (AP).

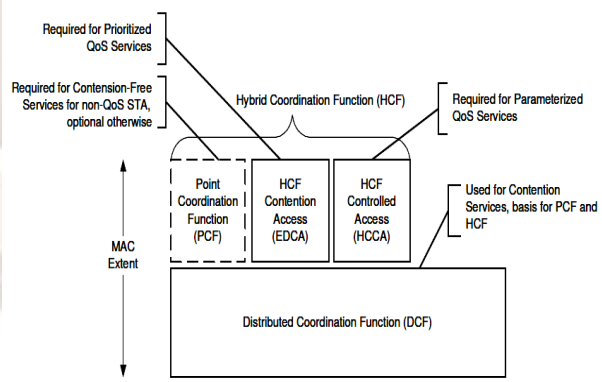

Figure 1: IEEE 802.11e MAC Architecture.

Fig.1 shows IEEE 802.11e MAC architecture where both the EDCA and HCCA are defined in order to support QOS, but with different concepts. While the HCCA supports parameterized QOS using a controlled channel access procedure, the

EDCA supports prioritized QOS in a contention-based CSMA/CA manner. These functions are not available in nQSTAs [3].The HCCA defines a traffic specification (TSPEC) frame which describes the QOS requirements for each station including maximum and minimum packet size, maximum and minimum data rate, maximum and minimum packet count, maximum jitter.Using the TSPEC frame, each wireless station negotiates with the access point for taking enough TXOP duration for transmission. Figure.2 shows the structure of the IEEE 802.11e super frame which consist of the contention-free period which is operated by HCCA and the contention period which is operated by both HCCA and EDCA. Every super frame starts with the beacon frame which is periodically broadcast by access point. The beacon frame includes network parameters which can be used for managing contention among the wireless stations.

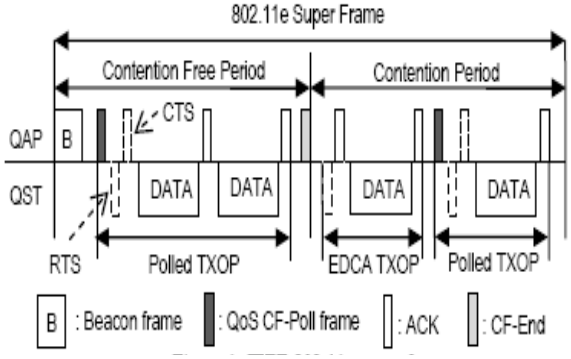

Figure 2: IEEE 802.11e super frame.

In this paper, first we consider the occurrence of the possible misbehaviors which will modify the parameter values and then propose efficient mechanism to detect the abnormal wireless stations and then do the performance analysis of the IEEE 802.11e by comparing with IEEE 802.11.This paper is organized as follows. Section II Related Work. Section III Gives a brief review of 802.11e standard EDCA scheme. Section IV Occurrence of possible misbehaviors in wireless station. Section V Proposes scheme to detect malicious stations. Section VI proposes a penalty based approach to provide fair resource sharing among the wireless stations. Section VII Performance analysis of IEEE 802.11e by comparing with IEEE 802.11 followed by Conclusions given in Section VIII.

II. Related Work

Recent years, many solutions have been proposed to efficiently detect network attacks in a network environment. Example for this is in [5]. Our concern is to focus on the schemes which are used to detect the malicious stations in wireless local area networks.

The authors investigated a case of a forged backoff value in [6] and [7] and propose a new scheme with few modifications to the DCF which is used in the IEEE 802.11 a/b/g network. In this the receiver randomly selects the backoff value based on the lower bound assigned by the sender. When the sender's backoff time is smaller than the assigned backoff value then the receiver considers that the sender is malicious because of its smaller backoff time will provide more opportunity to access the shared channel.

In [8], author used a game-theoretic approach to investigate the selfish behaviors with Nash equilibrium which is extended from Bianchi's model [9]. In this approach, specified some malicious cases where the cheater could fix its contention window. But they assumed the network is always in the saturated condition which would be infeasible in the practical condition.

In [10] , DOMINO software is developed , which is to be installed at the access point. This includes multiple modules for detecting various misbehaviors of wireless stations but they could not show the cases relevant to IEEE 802.11e EDCA networks.

III. Enhanced Distributed Channel Access (EDCA)

To provide prioritized QoS, IEEE 802.11 EDCA enhances the original IEEE 802.11 DCF by introducing user priorities (UP) and access categories (AC). When traffic arrives to the MAC layer it has a user priority value that is mapped into an access category. Table 1 shows the mapping specified in the amendment. User priority zero is mapped between two and three because of IEEE 802.1d bridge specification [IEEE802.11e]. The highest AC is the voice category and lowest is the background category.

Table 1: IEEE802.11e user priorities to access categories mappings

	User Priority	Access Category (AC)	Designation
Lowest	1	0	Background
	2	0	Background
	0	1	Best Effort
	3	1	Best Effort
	4	2	Video
	5	2	Video
	6	3	Voice
Highest	7	3	Voice

EDCA, medium access is contention-based using the same backoff algorithm as DCF and is prioritized by three configurable parameters: the contention window size (CW), the arbitration inter frame space (AIFS) and the transmission opportunity limit (TXOP). CW and AIFS determine the probability of gaining the channel access, while TXOP determines the time of occupying the channel after the channel access is obtained.

To explain the former, every time a backoff procedure is initiated, the backoff time (in number of slots) is uniformly generated in [0: CW -1]. A station has to backoff this amount of time before a transmission attempt is made.

AIFS defines the amount of time that has to be sensed idle before the backoff procedure is initialized/resumed as illustrated in Figure.3. Generally, the higher priority a class has, the smaller its CW and/or AIFS values. On the other hand, the TXOP limit enables the block acknowledgment following a normal successful DATA-ACK transmission. It determines the time of occupying the channel after the access is obtained.

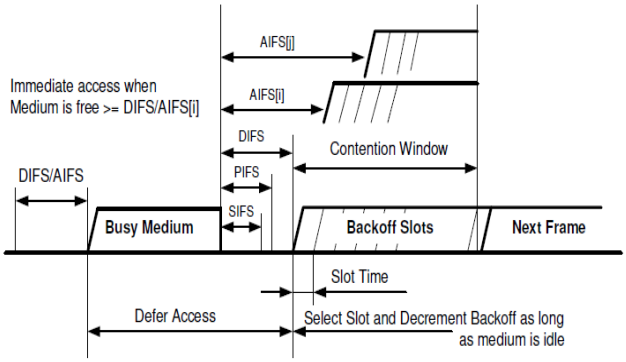

Figure 3: The relations between some inter frame spaces.

IV. Occurrence of possible misbehaviors

A. By making a shorter AIFS/Random Backoff Time

In WLAN 802.11 networks, the malicious station may copy the AIFS value to minimize the waiting time or change the AIFS/Backoff Time to transmit its next data packets with a shorter wait interval. As results, the station can increase the probability of accessing the channel by minimizing the AIFS/Backoff Time. To overcome this problem we use the approach [4] with modifications by adding the concept of the AC in EDCA.

B. By making a longer TXOPLimit

The TXOPLimit is the important concept in the IEEE 802.11e network because all QOS data should be transmitted within the assigned TXOPLimit to maintain its desirable QOS level of their voice or video applications.

The TXOP cycle consists of pair of DATA and ACK packet with Shorter Inter Frame Space(SIFS) time. Once a station acquires TXOP duration then other stations cannot interrupt during this duration. Therefore if a malicious station increases a value of the TXOPLimit then other honest station must increase their backoff window value by missing their deadline to transmit data.

Here we focus on the cases of forging the TXOPLimit by malicious QOS stations (QSTAs). There are two methods are using for determining the TXOPLimit value i.e. static and dynamic method. For the use of TXOPLimit in static method, QOSAccess Point (QAP) maintains and adjusts the value of TXOPLimit as constant value and then broadcasts that value to all connected QSTAs. In dynamic method, TXOPLimit can be considered as dynamic value which is calculated by using QOS requirements of each QSTA i.e. throughput or delay.

V. Malicious Station Detection Mechanism

The malicious station detection mechanism uses recorded values of the slot time for each QOS station. The QOS access point records statistics for several beacon indexes. In every beacon index the inter-frame space (IFS) size and the TXOP duration (TXOPdur) are recorded.

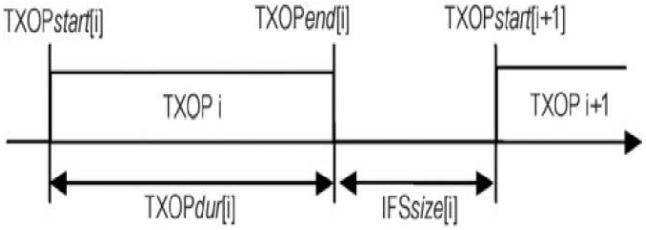

Figure 4.Time chart with variables used for the mechanism.

To calculate TXOPdur, the starting time and ending time of TXOP must be measured as showed in Figure 4. The QAP checks the destination address of the previously sent ACK packet when it receives a DATA packet. If the previous ACK's destination address and the current DATA packet's source address are same then the QAP recognizes that the TXOP has been started.

The calculated TXOPdur should not exceed the assigned TXOPLimit , otherwise the source QSTA can be considered as a malicious station.

VI. Punishment to Malicious Stations

The next step is how QAP will determine the QSTAs are the actual cheaters. For determination, use a penalty-based approach. With malicious station

detection algorithm define a flag variable which is set to true when malicious station will found. Here define four state of the potential cheater. Figure 5 shows the three states namely normal, suspicious and punish.

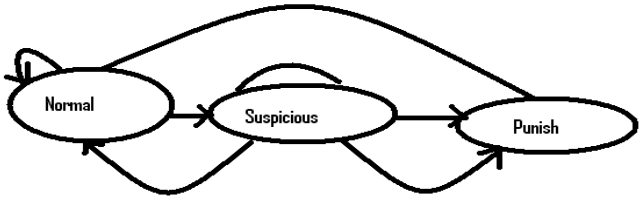

Figure 5.State transition to punish the cheater.

If the cheater reaches the punish state then QAP considers that it as the actual cheater then it does not transmit an ACK packet to it.

The goal of this project is to provide a lower bound of performance degradation for honest QSTAs with the malicious QSTAs i.e.our proposal is to allow each honest QSTA to use at least some portion of its full transmission opportunity.

VII. Performance Analysis

We have done two simulation scenarios which evaluate the performance of DCF in IEEE 802.11 standard and performance of EDCA in IEEE 802.11e scheme. These simulations were implemented using NS-2.

Table 2: Node Configuration for Simulation

PARAMETERS	VALUES
Network Simulator	NS 2.28
Channel type	Wireless channel
Radio-propagation model	Two Ray Ground
Antenna type	Omni Antenna
Routing protocol	DSDV
MAC type	802.11 & 802.11e
Traffic Type	CBR
Packet size	512
Max packet in Queue	50

Scenario for IEEE 802.11 and IEEE 802.11e technique

The simulation scenario shows the performance of IEEE 802.11 and IEEE 802.11e MAC and we obtained results for following three parameters: (i). Packet Delivery Ratio, (ii).Average Throughput, and (iii).Packet loss. The overall simulation topology of this scenario consists of 8 mobile Nodes in which are starting from Node 0 to Node 7 as shown in Fig. 5. In which topology is further assigned into four source Nodes and four destination Nodes.

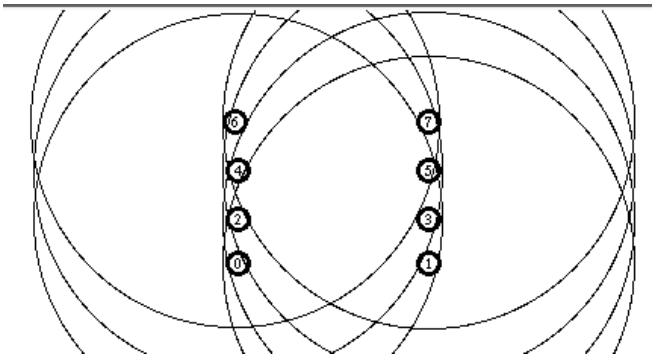

Figure 6: Node configuration scenario viewed from NAM

Here each Node will transmit packets with a different priority. Node 0 and Node 1 is given a higher priority than Node 2 and Node 3, which is also given a higher priority than Node 4 and Node 5. Node 5, in its turn, is given a higher priority than Node 6 and Node 7. To generate traffic we make sure that every source Node is a Constant Bit Rate (CBR) source over User Datagram Protocol (UDP). The total size of a transmitted packet is kept to 512 bytes and transmission rate from each Source Node to destination Node is kept to 600Kbps.The complete simulation time is limited to 80 sec.

Figure 7: Transmission of packets from Node 6 to Node 7

Table 3: Performance of IEEE 802.11

CBR Traffic (Kbps)	Packets Sent (S)	Packet Received (R)	Packet Delivery Ratio (R/S)	Packet Delivery Ratio (R/S) in %
100	6314	6314	1.0000	100
200	12628	10578	0.8377	83.77
300	18942	12109	0.6393	63.93
400	25255	12704	05030	50.30
500	31569	12753	0.4040	40.40
600	37883	12191	0.3218	32.18
700	44195	13022	0.2946	29.46
800	50509	13057	0.2585	25.85
900	56823	13295	0.2340	23.40
1000	63137	13213	0.2093	20.93

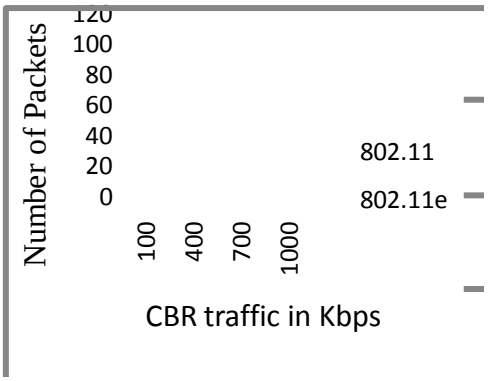

Figure 8: Packet Delivery Ratio Comparison

Table 4: Performance of IEEE 802.11e

CBR Traffic (Kbps)	Packets Sent (S)	Packet Received (R)	PDR (R/S)	PDR (R/S) in %
100	6314	6314	1.0000	100
200	12628	12628	1.0000	100
300	18942	18941	0.9999	99.99
400	25255	19827	0.7851	78.51
500	31569	22597	0.7158	71.58
600	37883	22095	0.5832	58.32
700	44195	23184	0.5246	52.46
800	50509	23944	0.4741	47.41
900	56823	23931	0.4211	42.11
1000	63137	24355	0.3857	38.57

Table 5: Average Throughput of IEEE 802.11

CBR Traffic (Kbps)	Average Throughput (Kbps)
100	329.11
200	551.27
300	631.11
400	662.07
500	664.60
600	635.34
700	678.65
800	680.47
900	692.86
1000	688.60

Table 6: Average Throughput of IEEE 802.11e

CBR Traffic (Kbps)	Average Throughput (Kbps)
100	329.14
200	658.12
300	987.10
400	1033.25
500	1177.57
600	1151.45
700	1208.17
800	1247.78
900	1247.12
1000	1269.22

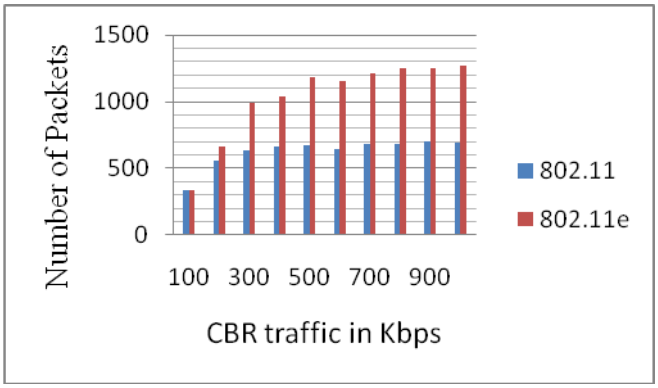

Figure 9: Average Throughput Comparison

Table 7: Number of packet loss in IEEE 802.11

CBR Traffic (Kbps)	Packet Loss
100	0
200	2050
300	6833

400	12551
500	18816
600	25692
700	31173
800	37452
900	43528
1000	49924

Table 8: Number of packet loss in IEEE 802.11e

CBR Traffic (Kbps)	Packet Loss
100	0
200	0
300	1
400	5428
500	8972
600	15788
700	21011
800	26565
900	32892
1000	38782

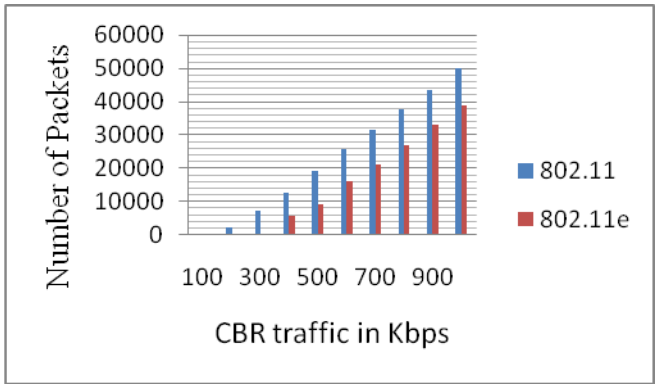

Figure 10: Packet Loss Comparison

VIII. CONCLUSION

In IEEE 802.11e Network, the malicious station avoids other honest stations for accessing channel. To detect the cheaters we proposed malicious station detection scheme which find out the malicious stations by increasing its TXOPLimit values. After finding out result the penalty function is applied to detect and block the cheaters. The QAP does not send the ACK packet to the cheater when it reaches the punish state.

In this paper, we have analyzed the performance of the IEEE 802.11e standard and compared its performance with legacy IEEE 802.11 standard. In this work it is revealed that how prioritization in IEEE 802.11e can guarantee a quality of service even when network resources are shared by different stations. The simulation results show that an EDCA may works well for a differentiated data services and prioritized access to the medium. Hence by using IEEE 802.11e EDCA mechanism we can achieve high throughput, reduced packet drop rate and higher packet delivery ratio.

References

[1] Prof. Rathnakar Acharya, Dr. V. Vityanathan, and Dr. Pethur Raj Chellaih "WLAN QoS Issues and IEEE 802.11e QoS Enhancement" International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010 1793-8201.

[2] Jose Villalon, Pedro Cuenca and Luis Orozco-Barbosa "Limitations and Capabilities of QoS Support in IEEE 802.11 WLANS"- by the Ministry of Science and Technology of Spain under project PBC-03-001.

[3] "IEEE Std 802.11™-2007" Sponsored by the LAN/MAN Standards Committee, IEEE Computer Society-2007

[4] M. Raya, J. P. Hubaux, and I. Aad, "Domino: A system to detect greedy behavior in IEEE 802.11 hotspots," in *Proc. ACM MobiSys*, Jun. 2004, pp. 84–97

[5] S. H. Kim and B.-H. Roh, "Fast detection of distributed global scale net-work attack symptoms and patterns in high-speed backbone networks," *KSII Trans. Internet Inform. Syst.*, vol. 2, no. 3, pp. 135–149, Jun. 2008.

[6] P. Kyasanur and N. Vaidya, "Detection and handling of MAC layer misbehavior in wireless networks," in *Proc. IEEE DSN*, Jun. 2003, pp. 173–182.

[7] P. Kyasanur and N. Vaidya, "Selfish MAC layer misbehavior in wireless networks," *IEEE Trans. Mobile Comput.*, vol. 4, no. 5, pp. 502–516, Sep.–Oct. 2005.

[8] M. Cagalj, S. Ganeriwal, I. Aad, and J. Hubaux, "On selfish behavior in CSMA/CA networks," in *Proc. IEEE INFOCOM*, Mar. 2005, pp.2513–2524.

[9] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," *IEEE J. Selec. Areas Commun.*, vol. 18, no. 3,pp. 535–547, Mar. 2000.

[10] M. Raya, J. P. Hubaux, and I. Aad, "Domino: A system to detect greedy behavior in IEEE 802.11 hotspots," in *Proc. ACM MobiSys*, Jun. 2004, pp.84–97.

[11] IEEE Computer Society, IEEE Std 802.11e. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2005.

[12] D. J. Deng, L. W. Chang, H. W. Wang, D. C. Huang, and Y. M. Huang, "Is RTS/CTS mechanism effective for WLAN," *J. Internet*

Technol., vol. 11, no. 7, pp. 955–964, Dec. 2010.

[13] A Comprehensive Study of the IEEE 802.11e Enhanced Distributed Control Access (EDCA) Function Technical Report No. UIUCDCS-R-2006-2711 (Engr. No. UILU-ENG-2006-1743), April 2006.

[14] Albert Banchs, Arturo Azcorra, Carlos Garcia, and Rubén Cuevas, "Applications and Challenges of the 802.11e EDCA Mechanism"- IEEE Network -2005, 0890-8044.

[15] Yang Xiao, Senior Member, IEEE "Performance Analysis of Priority Schemes for IEEE 802.11 and IEEE 802.11e Wireless LANs" IEEE Transactions on Wireless Communications, Vol. 4, no. 4, july 2005.

Authors

Miss Jagadevi Koodi received her Bachelor of Engineering in Computer Science and engineering in 2006. Currently She is a M.Tech student in Computer Networking Engineering from Visvesvaraya Technological University at The Oxford College of Engineering, Bangalore. Her research interests are wireless Local area networks, Networking, Wireless Communication.

Mrs S.Kalaiselvi received her Bachelor of Engineering in Computer Science and Engineering in 2004. She received her M.E in Computer Science Engineering with distinction from Anna University in 2009. Currently she also holds a faculty position as Assistant Professor, Department of ISE, The Oxford College of Engineering. Her main research interests are Networking, wireless sensor networks, wireless network security .

Mr. Rakesh Marturkar received his Bachelor of Engineering in Electronics and Communication Engineering in 2010. He received his M.Tech in Digitial Electronics and Communication Engineering with distinction from NMAMIT, Nitte in 2012. Currently He also holds a faculty position as Assistant Professor, Department of ECE, Guru Nanak Dev Engineering College, Bidar. His main research interests are Networking, Wireless Adhoc Networks, Wireless Communication.