www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-2, Issue-2, Apr- 2014
Research Paper

Int. J. Sci. Res. in
Network Security
and Communication
ISSN: 2321-3256

A Scheme to Eliminate Redundant Rebroadcast and Reduce Transmission Delay Using Binary Exponential Algorithm in Ad-Hoc Wireless Networks

Deepesh Tamrakar[1*], Sreshtha Bhattacharya[2] and Shitanshu Jain[3]

[1*,2,3] *Dept. of Computer Science & Engineering, R.G.P.V.Bhopal (M.P.), India, deepesh.tamrakar@gmail.com*

Received: 16 Apr 2014 Revised: 08 Apr 2014 Accepted: 25 Apr 2014 Published: 30 Apr 2014

Abstract— Ad-hoc wireless network is a Collection of wireless mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration**.** Neighbor discovery is an important part of many protocols for wireless adhoc networks, including localization and routing. When neighbor discovery fails, communications and protocols performance deteriorate. Broadcasting is a common operation in a network to resolve many issues. In a mobile ad hoc network (MANET) in particular, due to host mobility, such operations are expected to be executed more frequently such as finding a route to a particular host, paging a particular host. Probabilistic broadcasting is best suited in terms of ad hoc network which is well known for its decentralized network nature and Binary exponential Back off (BEB) algorithm stated in the 802.11 standard plays an important role in the distributed coordinate function (DCF), which is provided at the medium access control (MAC) layer of the IEEE 802.11 standard. BEB might introduce long transmission delays without any significant benefit in respect of contention resolution due to node mobility. In fact, contending mobiles are likely to move to a different location during a large waiting time for retransmission after a packet collision and might get involved into another independent collision process elsewhere. Thus, the large growth rate in waiting time might not be appropriate in a mobile scenario as in a WLAN. Bearing this in mind, we propose certain modifications to BEB algorithm suitable for WLANs.

Keywords— DCF, MAC, CSMA/CA, BEB, MANET, Broadcast Redundancy, Flooding, Probability Based Scheme

I. INTRODUCTION

During the last few years, we have all witnessed a continuously increasing growth in the deployment of wireless and mobile communication networks. The growth in the use of wireless communications over the last few years is quite substantial and as compared to other technologies, it's huge. The primary advantage of a wireless network is the ability of the wireless node to communicate with the rest of the world while being mobile. Two basic system models have been developed for the wireless network paradigm. The fixed backbone wireless system model consists of a large number of mobile nodes and relatively fewer, but more powerful, fixed nodes. These fixed nodes are hard wired using landlines. The communication between a fixed node and a mobile node within its range occurs via the wireless medium. However, this requires a fixed permanent infrastructure, another system model, the mobile ad hoc network [1,3].

1.1 A mobile ad hoc network (MANET)

A mobile ad hoc network (MANET) is a collection of wireless nodes dynamically forming a temporary network with optional use of fixed network infrastructure such as an access point (AP) or a base station (BS). To transmit packets to a node outside its range, the network uses multi-hop store-and-forward routing. MANETs have great potential for both military and commercial applications.

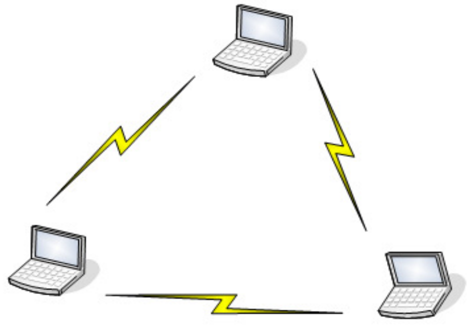
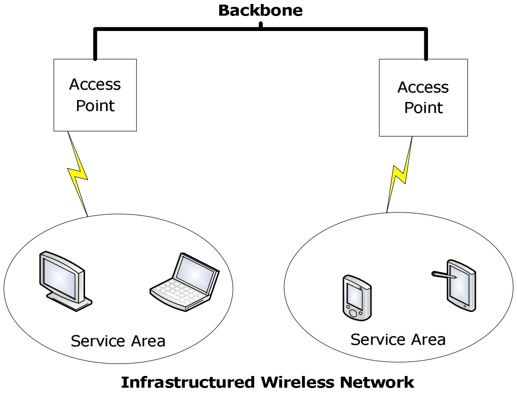


Figure 1: Overview of Mobile Ad-hoc Network

Generally there are two distinct approaches for enabling wireless mobile units to communicate with each other:



Corresponding Author: Deepesh Tamrakar[1]*
Dept. of Computer Science & Engineering, R.G.P.V.Bhopal (M.P.), India, deepesh.tamrakar@gmail.com

Infrastructure: Wireless mobile networks have traditionally been based on the cellular concept and relied on good infrastructure support, in which mobile devices communicate with access points like base stations connected to the fixed network infrastructure. Typical examples of this kind of wireless networks are GSM, UMTS, WLL, WLAN, etc.

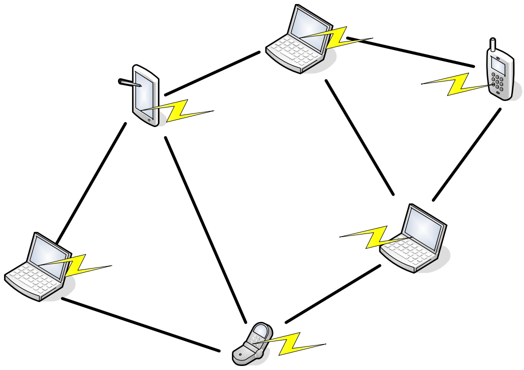


Figure 1.2: Infrastructure less Wireless Network

Infrastructure less: As to infrastructure less approach, the mobile wireless network is commonly known as a mobile ad hoc network (MANET). A MANET is a collection of wireless nodes that can dynamically form a network to exchange information without using any pre-existing fixed network infrastructure. This is a very important part of communication technology that supports truly pervasive computing, because in many contexts information exchange between mobile units cannot rely on any fixed network infrastructure, but on rapid configuration of a wireless connections on-the-fly. Wireless ad hoc networks themselves are an independent, wide area of research and applications, instead of being only just a complement of the cellular system.

An ad hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any established infrastructure or centralized administration [1,3]. We are focusing on the redundant rebroadcast, optimal broadcasting schedule and security of the Ad-hoc mobile network. Broadcasting in a MANET: **-** A MANET consists of a set of mobile hosts that may communicate with one another from time to time. No base stations are supported. Each host is equipped with a CSMAICA (carrier sense multiple access with collision avoidance) transceiver. The broadcast problem refers to the sending of a message to other hosts in the network. The problem considered here has the following characteristics. The broadcast is spontaneous:-Any mobile host can issue a broadcast operation at any time. For reasons such as the host mobility and the lack of synchronization, preparing any kind of global topology knowledge is prohibitive [1,3].

1.2 Broadcast Redundancy

The broadcast is unreliable: - No acknowledgement mechanism will be used. However, attempt should be made to distribute a broadcast message to as many hosts as possible without paying too much effort. The motivations to make such an assumption are (a) A host may miss a broadcast message because it is off-line, it is temporarily isolated from the network, or it experiences repetitive collisions. (b) Acknowledgements may cause serious medium contention (and thus another "storm") surrounding the sender (c) in many applications (e.g., the route discovery, a 100% reliable broadcast is unnecessary [1].

Broadcast Storm Caused by Flooding: **-** A straight-forward approach to perform broadcast is by flooding. A host, on receiving a broadcast message for the first time, has the obligation to rebroadcast the message. Clearly, this costs 'n' transmissions in a network of it hosts. In a CSMA/CA network, drawbacks of flooding include.

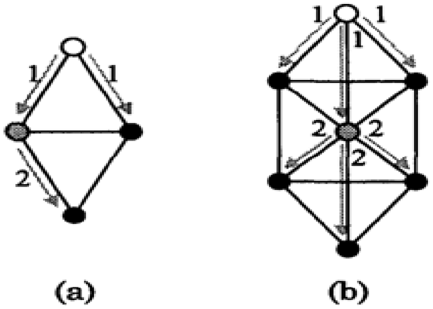
Redundant rebroadcasts: - When a mobile host decides to rebroadcast a broadcast message to its neighbors, all its neighbors already have the message.

Contention: - After a mobile host broadcasts a message, if many of its neighbors decide to rebroadcast the message, these transmissions (which are all from nearby hosts) may severely contend with each other.

Collision: - Because of the deficiency of mechanism, the lack of RTS/CTS dialogue, and the absence of CD, call back off mechanism is more likely to occur and cause more damage[1].

1.3 Redundant rebroadcast

A node resends a broadcast message even if all its neighbors have already received the message from some other neighbors [1].



Following schemes to overcome the broadcast problem

Probabilistic scheme: When each node rebroadcasts a message with a specific probability [4].

Counter-based scheme: When a node re transmits a message if it was received less than a threshold number of times over a fixed interval.

Distance-based scheme: When a message is resent only if it is received from neighbors farther away than a specific threshold distance.

Location-based scheme: When a node retransmits a message only if the additional area covered is larger than a specific threshold area.

To cover the whole network using few numbers of nodes and avoiding redundant transmissions of message.

Advances us to the following condition –
A node is to be selected as forward if the node has maximum number of neighbors.

Region of nodes to be covered by a node should be provided. It refers to the records of uncovered nodes in the network.

II. PROBABILITY BASED ALGORITHM

A Probability based algorithm is proposed in which a node is selected as forward node on the basis of its probability value. This "Probability" is the probability of disheartening related source to cover an area. If a node has minimum probability value then it assures the related source to cover maximum region expected by the source. Based on probability value a node is selected by the related source if its value is minimum. Thus such "Probability" based algorithm depends upon several calculations and make decisions based on the calculations [2].

2.1 Probability calculation

In probability based algorithm, initially the probabilities of all nodes are initialized to zero. Whenever a node is to transmit a message that is acting as source, it then calculates the probability of each of its neighbors. The process of calculating probability may be expressed in the following form:

$$Pi = 1/\,ni \qquad (1)$$

Here, Pi = Probability of node i and $i\ n$ = Number of nodes that may be covered by node i. ni = (Neighbors of node i – Neighbors of relative source) ∩ U (2)

2.2 Probabilistic Algorithm

Step 1: Initialize source.
Step 2: Set U = all the nodes in the network Neighbor of Source // Initialization phase
Set Pi = 0.0 for each node i // initializing Probability value
/*this is the phase in which forward nodes are selected*/

Step 3:
i) Source 1:=Source.
ii) Source 1 calculates the probability of all its neighbors.
iii) Source 1 selects the node with smallest probability as forward node. If no node is available to be selected as forward then go to step vii.
iv) Source 1 sends uncovered list to the selected forward node.
v) Source 1 adds the forward node into its forward list.
vi) Source 1 updates its uncovered list with covered-list available from forward node. Go to stepii.
vii) Forward pointer is incremented to show the next forward node of source 1. Swap the value of source 1 along with the current forward node available in its list. Go to step ii [2].

III. 802.11 MEDIUM ACCESS CONTROL LAYER

In a MANET, nodes transmit packets in an unsynchronized fashion. The protocol employed in the medium access control (MAC) layer is responsible for coordinating access to the shared channel while minimizing conflicts. The IEEE 802.11 WLAN MAC/PHY specification [2] is one of the standards for WLANs that defines detailed functions for both MAC and physical layers. The IEEE 802.11 distributed coordination function (DCF) MAC protocol is being widely used in test beds simulations of MANETs, as it does not require a central controller such as an AP or a BS for coordination. In DCF mode, nodes contend for the channel in a distributed manner using carrier sense multiple access scheme with collision avoidance (CSMA/CA). The CSMA/CA scheme uses both physical and virtual carrier sensing with the help of optional request-to-send/clear-to-send (RTS/CTS) control packets. The RTS/CTS control handshake is incorporated to mitigate the problems due to hidden terminals. DCF adopts binary exponential backoff (BEB) algorithm for contention resolution. At each transmission (including the first attempt as well), the backoff time is uniformly chosen in the range (0, CW - 1), where CW is the contention window. At the first transmission attempt, CW is set to a minimum backoff window (CWmin). After each unsuccessful transmission, CW is doubled starting from CWmin, until a maximum value (CWmax) is reached. If a node is successful in transmitting a packet, CW is reset to the minimum value (CWmin). If the packet fails to get through even after CW reaches CWmax, CW is refreshed back to CWmin. Thus, the operation of the BEB algorithm can be summarized as follows:

CW = min [2*CW, CWmax], upon collision (1)
CW = CWmin, upon success (2) where CWmin and CWmax are the lower and upper bounds for the backoff interval. The values of CWmin and CWmax are predetermined based on the number of active nodes and offered load of a network. WLANs have great potential for both military and commercial applications. In a WLAN, nodes transmit packets in an unsynchronized fashion. The protocol employed in the medium access control (MAC) layer is responsible for coordinating access to the shared channel while minimizing conflicts. Hence it is important to design an efficient and effective MAC protocol. In the 802.11 protocol, the fundamental mechanism to access the medium is called distributed coordination function (DCF). This is a random access scheme, based on the carrier sense multiple access with collision avoidance (CSMA/CA) protocol. Retransmission of collided packets is managed according to binary exponential backoff rules. The standard also defines an optional point coordination function (PCF), which is a centralized MAC protocol able to support collision free and time bounded services.

The MAC layer has to fulfill several tasks. It has to control roaming, authentication, and power conservation. The basic services provided by the MAC layer are the mandatory asynchronous data service and an optional time bounded service. The following three basic access mechanisms have been defined for IEEE 802.11: the mandatory basic access

method based on CSMA/CA, an optional method avoiding hidden terminal problem, and finally a contention-free polling method for time bounded services. The first two methods are also summarized as Distributed Coordination Function (DCF), the third method is called Point Coordination Function (PCF). Nodes in the wireless network share a common broadcast radio channel. Since the radio spectrum is limited, the bandwidth available for communication in such networks is also limited. Access to this shared medium should be controlled in such manner that all nodes receive a fair share of the available bandwidth, and the bandwidth is utilized efficiently [3].
Following figure depicts the architecture of 802.11 MAC layer –

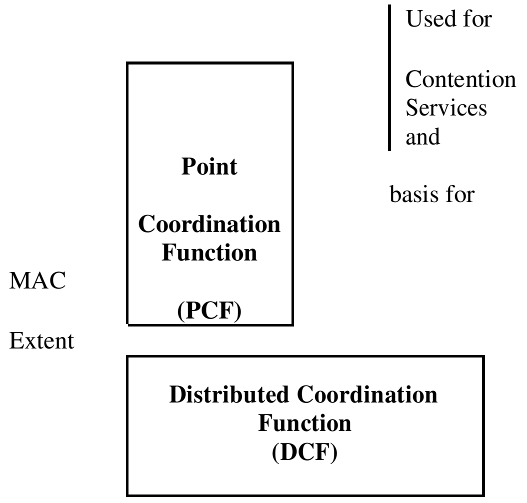


Figure 2: MAC Architecture

IV. DISTRIBUTED COORDINATION FUNCTION

The fundamental access method of the IEEE 802.11 MAC is a DCF known as carrier sense multiple accesses with collision avoidance (CSMA/CA). The DCF must be implemented in all stations, for use within both ad-hoc and infrastructure network configurations. For a station to transmit, it shall sense the medium to determine if another station is transmitting. If the medium is not determined to be busy, the transmission may proceed.

4.1 Carrier Sense Mechanism

Both physical and virtual carrier sense mechanisms are used in determining the condition of the medium (busy or idle). The medium is idle only when both mechanisms indicate such a condition. The physical layer performs a physical carrier sensing and forwards the information to the MAC. The MAC layer uses the network allocation vector (NAV) to implement the virtual carrier sense mechanism, which reserves the medium for transmitting a data frame and its acknowledgment. The NAV values tell other stations how long the current transmission might take after which those stations can try to access the medium again Reserving the medium is accomplished in two ways: by using a Duration/ID field in the request-to-send (RTS) and clear-to-send (CTS) frames, or using the Duration/ID field in directed frames[3].

4.2 MAC-Level Acknowledgments

A positive acknowledgment requires that a station receiving certain kinds of frames must respond by sending an acknowledgment back to the transmitting station. If the transmitting station does not receive the acknowledgment, it will assume that an error has occurred and will automatically retransmit the frame. An error can occur in transmitting either the data frame or the acknowledgment frame.

4.3 Interframe Space (IFS)

After sensing that the medium is idle, a station must wait for a certain interval of time, called an interframe space (IFS), before attempting to transmit. There are four different types of IFS, which prioritize a station in accessing the medium. The first type is a short interframe space (SIFS), used in sending an acknowledgement, CTS, and the second or subsequent frames of a fragment burst. During the contention-free period (CFP), a station also uses a SIFS when it responds to a poll while a point coordinator (PC) may use a SIFS for any type of frame. A SIFS is the shortest interframe space; consequently, it gives a particular station the highest priority in gaining access to the medium. The second type is a PCF interframe space (PIFS). Except when responding to the poll, a station will use PIFS during the CFP. The third type is a DCF interframe space (DIFS), which is used under the DCF. DIFS is the longest interframe space. Hence, a station waiting a DIFS period has the lowest priority. A point coordinator is guaranteed to gain and maintain control of the medium to start the CFP by employing PIFS instead of DIFS. The fourth type of IFS is an extended interframe space (EIFS), used when the first attempt to transmit a frame has failed. Since the EIFS is shorter than DIFS, a retransmission has higher priority than a normal transmission.

4.3.1Basic Access

Basic access is a core mechanism in accessing the medium. The backoff time counter is decremented as long as the channel is sensed idle, "frozen" when a transmission is detected on the channel, and reactivated when the channel is sensed idle again for duration larger than DIFS. The station transmits when the backoff time reaches zero Figure 2.5 illustrates this operation. Two stations A and B share the same wireless channel. At the end of the packet transmission, station B waits for a DIFS and then chooses a backoff time equal to 8 (uniformly chosen between 0 and CW_{min}), before transmitting the next packet. Assume that the first packet of station A arrives at the time indicated with an arrow in the figure. After a DIFS, the packet is transmitted. At the transmission time of the station A, the station B is in the middle of the Slot Time corresponding to a backoff value, equal to 5. As a consequence of the channel sensed busy, the backoff time is frozen to its value 5, and the backoff counter decrements again only when the channel is sensed idle for a DIFS

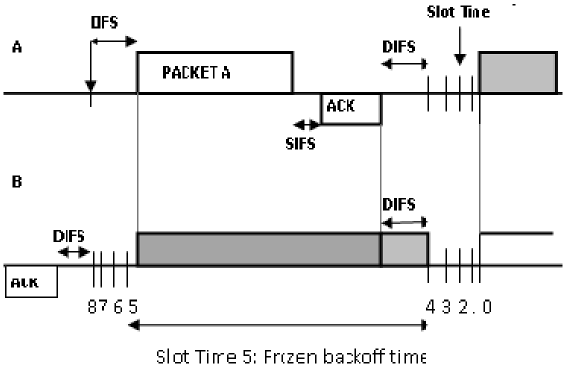


Figure 3: Protocol with Basic Access Method

The CSMA/CA does not rely on the capability of the stations to detect a collision by hearing their own transmission. For that reason, an ACK is transmitted by the destination station to signal the successful packet reception. The ACK is transmitted immediately at the end of the packet, after a period of time called short interframe space (SIFS). As the SIFS (and the propagation delay in total) is shorter than a DIFS, no other station is able to detect the channel idle for a DIFS until the end of the ACK. If the transmitting station does not receive the ACK within a specified ACK Timeout or it detects the transmission of a different packet on the channel, it reschedules the packet transmission according to the given backoff rules.

V BACKOFF PROCEDURE

The backoff procedure shall be invoked for a STA to transfer a frame when finding the medium busy as indicated by either the physical or virtual carrier-sense mechanism (see Figure). The backoff procedure shall also be invoked when a transmitting STA infers a failed transmission. To begin the backoff procedure, the STA shall set its Backoff Timer to a random backoff time. All backoff slots occur following a DIFS period during which the medium is determined to be idle for the duration of the DIFS period, or following an EIFS period during which the medium is determined to be idle for the duration of the EIFS period following detection of a frame that was not received correctly. A STA performing the backoff procedure shall use the carrier-sense mechanism to determine whether there is activity during each backoff slot. If no medium activity is indicated for the duration of a particular backoff slot, then the backoff procedure shall decrement its backoff time by slot Time. If the medium is determined to be busy at any time during a backoff slot, then the backoff procedure is suspended; that is, the backoff timer shall not decrement for that slot. The medium shall be determined to be idle for the duration of a DIFS period or EIFS, before the backoff procedure is allowed to resume. Transmission shall commence whenever the Backoff Timer reaches zero. A backoff procedure shall be performed immediately after the end of every transmission. In the case of successful acknowledged transmissions, this backoff procedure shall begin at the end of the received ACK frame. In the case of unsuccessful transmissions requiring acknowledgment, this backoff procedure shall begin at the end of the ACK timeout interval. If the transmission is successful, the CW value reverts to a CWmin before the random backoff interval is chosen, and the STA short retry count and/or STA long retry count are updated. This assures that transmitted frames from a STA are always separated by at least one backoff interval the effect of this procedure is that when multiple STAs are deferring and go into random backoff, and then the STA selecting the smallest backoff time using the random function will win the contention.

VII CONCLUSION

The objective of this paper was to introduce a new technique for broadcasting in ad hoc wireless network. The technique which was named as "Probabilistic algorithm", it is observed that the probability based algorithm obtains better solutions and works more efficiently. We also observe that The BEB algorithm causes a fast build-up (i.e., growth-rate) of waiting times spreading the backlog traffic over a larger time frame. However, this fast build-up of waiting time with increasing number of occurrence of collisions might not be appropriate for a MANET, wherein the contending nodes might leave the geographical location of contention itself after a short while due to their mobility. In view of this, we conjecture that it may not be necessary to make a node wait for a duration that builds up exponentially with a binary base.

REFERENCES

[1]. Sze-Yao Ni, Yu-Chee Tseng, Yuh-Shyan Chen, and Jang-Ping Sheu," The Broadcast Storm Problem in a Mobile Ad Hoc Network", MobiCom '99 Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking, ISBN: 1-58113-142-9, Page No (**151-162**), August **1999**.

[2]. Md. Nazrul Islam, M.M.A. Hashem and A. M. Moshiur Rahman, "A Probabilistic Algorithm for Reducing Broadcast Redundancy in Ad Hoc Wireless Networks", 8th International Conference on Computer & Information Technology (ICCIT), Page No (**752-757**), December **2005.**

[3]. Sakshi Suhane, Dr. Sanjeev Sharma and Prof. Varsha Sharma,"Performance Analysis of Backoff Algorithm in IEEE 802.11 Networks", International Journal of Scientific and Engineering Research, Volume **2**, Issue **6**, June **2011**.

[4]. Tasneem Bano and Jyoti Singhai, "Probabilistic Broadcasting Protocol In AD HOC Network And Its Advancement: A Review", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.**1**, November 2010**.**

[5]. Radu Stoleru, Haijie Wu and Harsha Chenji, "Secure neighbor discovery and wormhole localization in mobile ad hoc networks", Journal Ad Hoc Networks, Volume **10** Issue **7**, Pages No (**1179-1190**), September, **2012.**

[6]. Karan Singh and Rama Shankar Yadav, "Dynamic Security Scheme for Multicast Source Authentication", International Journal on Computer Science and Engineering, ISSN 0975-3397, **2010**.

[7]. Justin Lipman, Hai Liu, and Ivan Stojmenovic, "Broadcast in Ad Hoc Networks", FUZZ-IEEE Pages No (**1639-1644**), Feb **2009.**

[8]. Radu Stoleru, Haijie Wu and Harsha Chenji,"Secure neighbor discovery and wormhole localization in mobile ad hoc networks", Journal Ad Hoc Networks, Volume **4**, **2006**.

[9]. Shu-jen Chang and Morris Dworkin, "Workshop Report, The First Cryptographic Hash Workshop", NIST, October **2005**.

[10]. S.Vaudenay "A Classical Introduction to Cryptography Applications for Communications Security" Springer, ISBN 978-0-387-25880-5, **2006**.

[11]. E. Biham, R. Chen, A. Joux, P. Carribault, W. Jalby and C. Lemuet. "Collisions in SHA-0 and Reduced SHA-1- In Advances in Cryptology" – Eurocrypt'05, Springer-Verlag, **2005**.

[12]. IEEE 802.11 standard, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE Std, June **1999**.

[13]. C. Rama Krishna, Saswat Chakrabarti, and Debasish Dutta, "A modified backoff algorithm for IEEE 802.11 DCF based MAC protocol in a Mobile Ad-Hoc Network", TENCON, Pages No (**664-667**), November **2004.**

[14]. Yunli Chen, Qing-An Zeng and Dharma P. Agrawal, "Performance analysis and enhancement for IEEE 802.11 MAC protocol", 10th International Conference on Telecommunications, Volume **1**, March **2003.**