Empirical Study of CSMA, MACA and EMACA Protocols to Support QoS under Varying Conditions of Pause Time in Ad-hoc Wireless Network by Resources of DSR Routing Protocol

Prof. Neeraj Agrawal

Assistant Professor, Gwalior Engineering College, Gwalior

Dr. Sanjeev Sharma

HOD, SOIT, Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal

Prof. Arun Nahar

Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal

Dr. Ramjeevan Singh

Maulana Azad National Institute of Technology (MANIT), Bhopal

ABSTRACT

DSR routing protocol was used to evaluate the MACA and EMACA performance. Results show that the EMACA simulation performs well as compared to MACA in sense of Throughput, Total Packet Receive, Drop Packet Ratio and Average Jitter under varying conditions of Pause Time. In this paper we will try to change route selection mechanism proactively. We will also define a link stability parameter in which a stability value is assigned to each link. Given this feature, destination node can estimate stability of routes and can select the best and more stable route. Therefore we can reduce the delay and jitter of sending data packets. We have evaluated the operation of DSR through detailed simulation on a variety of movement and communication patterns, and through implementation and significant experimentation in a physical outdoor ad-hoc networking testbed we have constructed, and have demonstrated the excellent performance of the protocol.

Keywords

AWNs, QoS, MAC, CSMA, MACA, EMACA, DSR, Throughput, and Total Packet Received Drop Packet Ratio and Average Jitter.

1. INTRODUCTION

An Ad-Hoc Wireless Network is a wireless network between several devices where no one device controls the network. Each device on the network sends information directly to other devices. There is no access to wired devices or the Internet. Mobile ad-hoc network is a collection of wireless mobile nodes which dynamically form a temporary network without the use of any existing network infrastructure or centralized administration [18], [19], [20]. Since the topology of network is constantly changing, the issue of routing packets between any pair of nodes becomes a challenging task. Ad-hoc routing protocols can be classified into three main categories: Proactive, reactive and hybrid protocols. Mobile Ad-Hoc

Networks are wireless networks which do not require any infrastructure support for transferring data packet between two nodes [1], [2], [3], [4], [12]. In these networks nodes also work as a router that is they also route packet for other nodes. Nodes are free to move, independent of each other, topology of such networks keep on changing dynamically which makes routing much difficult. Therefore routing is one of the most concerns areas in these networks. Normal routing protocol which works well in fixed networks does not show same performance in Mobile Ad-Hoc Networks. In these networks routing protocols should be more dynamic so that they quickly respond to topological changes.

Figure 1: Mobile Ad Hoc Network

Quality of service (QoS) is the performance level of a service offered by the network to the user. With the increase in the Quality of service (QoS) needs in evolving application, it is also desirable to support these services in the MANETs. The resource limitation and variability further add to the need for Quality of provision in such networks. A network or a service provider can offer different kinds of services to the users. A service can be characterized by a set of measurable pre specified service requirements such as minimum bandwidth, maximum delay, maximum delay variance (jitter), and maximum packet loss rate. After accepting a service request from the user, the network has to ensure that service requirements of

the user's flow are met, as per the agreement, throughout the duration of the flow (a packet stream from the source to the destination). After receiving a service request from the user, the first task is to find a suitable loop-free path from the source to the destination that will have the necessary resources available to meet the QoS requirements of the desired service. This process is known as QoS routing. The goal of QoS provisioning is to achieve a more deterministic network behavior, so that information carried by the network can be better delivered and network resources can be better utilized [4], [7], [8].
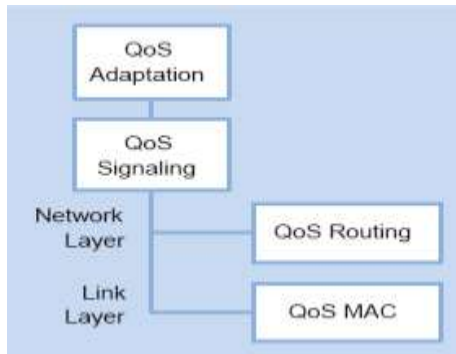

Figure 2: Quality of Service layered perspective

A network's ability to provide a specific QoS depends upon the inherent properties of the network itself which span over all the layers in the network. The physical layer should take care of changes in transmission quality, for example by adaptively increasing or decreasing the transmission power. Similarly, the link layer should react to the changes in link error rate. QoS-Routing and QoS-Signaling operate at the network layer in order to search for routes with sufficient resources or to allocate and release bandwidth respectively.

A MAC protocol in a multi-access medium is essentially a distributed scheduling algorithm that allocates the channel to requesting nodes [2], [4], [12], [13]. Two commonly used access principles in wireless networks are fixed assignment channel access and random access method. In the former method, a pair of nodes is statically allocated a certain time slot (frequency band or spread spectrum code), as is the case for most of voice-oriented wireless networks. On the other hand, in random access MAC protocols, the sender dynamically competes for a time slot with other nodes. This is a more flexible and efficient method of managing the channel in a fully distributed way, but suffers from collisions and interference.

Carrier Sense means that every Ethernet device listens to the Ethernet wire before it attempts to transmit. If the Ethernet device senses that another device is transmitting, it will wait to transmit. Multiple Access means that more than one Ethernet device can be sensing (listening and waiting to transmit) at a time. Collision Detection means that when multiple Ethernet devices accidentally transmit at the same time, they are able to detect this error. Carrier Sense

Multiple Access (CSMA) refers to a family of protocols used by stations contending for access to a shared medium like an Ethernet cable or a radio channel. There are multiple "flavors" of CSMA; each has a different way of dealing with the collisions that can occur when more than one station attempts to transmit on the shared medium at the same time.

Multiple Accesses with Collision Avoidance (MACA) is a slotted media access control protocol used in wireless LAN data transmission to avoid collisions caused by the hidden station problem and to simplify exposed station problem [2], [12], [14], [15], [16]. This MACA protocol is not fully solve the hidden node and exposed terminal problem and nothing is done regarding receiver blocked problem.

- ❖ Contention Based Protocol
- ❖ Nodes are not guaranteed periodic access to the channel.
- ❖ They cannot support real time traffic.
- ❖ Three way handshaking.
- ❖ RTS—CTS—Data packet exchange
- ❖ Binary Exponential back off Algorithm
- ❖ Sender initiated Protocol
- ❖ RTS—CTS carrier information about the duration of time for neighbor nodes.

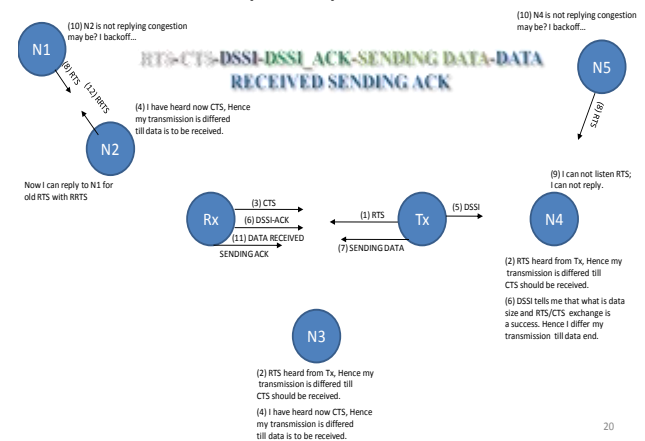### Enhancement of Multiple Access Collision Avoidance (EMACA) Protocol

Figure 3: EMACA Protocol

EMACA (Enhancement of Multiple Accesses with Collision Avoidance) Protocol is based on MACA with some modifications over it. Instead of three way handshaking in MACA, EMACA protocol has five way handshaking RTS – CTS – DSSI – DSSI_ACK – DATA Sending – ACK [26].

2. ROUTING PROTOCOL

Routing is the act of moving information from source to a destination in an internet work. During this process, at least one intermediate node within the internet work is encountered. The routing concept basically involves two

activities: firstly, determining optimal paths and secondly, transferring the information groups (called packets) through an internet work. The latter concept is called as packet switching, which is straight forward, and path determination is very complex. Routing protocol uses several matrices to calculate the best path for the routing the packet to its destination. These matrices are a standard measurement that could be number of hops, which is used by the routing algorithm to determine the optimal path for the packet to its destination [21], [22]. The process of path determination is that, routing algorithms initialize and maintain routing tables, which contain the total route information for packet. This route information varies from one routing algorithm to another. Routing tables are filled with a variety of information which is generated by routing algorithms. Most common entries in the routing table are ip-address prefix and the next hop. Routing tables Destination/next hop associations tell the router that a particular destination can be reached optimally by sending the packet to router representing the "next hop" on its way to final destination and ip-address prefix specifies a set of destinations for which the routing entry is valid for.
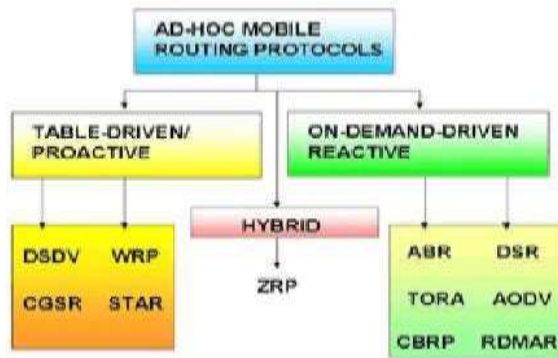

Figure 4: Routing Protocol

Dynamic Source Routing (DSR) is a reactive protocol i.e. it doesn't use periodic advertisements. It computes the routes when necessary and then maintains them. Source routing is a routing technique in which the sender of a packet determines the complete sequence of nodes through which the packet has to pass, the sender explicitly lists this route in the packet's header, identifying each forwarding "hop" by the address of the next node to which to transmit the packet on its way to the destination host. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration. The protocol is composed of the two mechanisms of Route Discovery and Route Maintenance, which work together to allow nodes to discover and maintain source routes to arbitrary destinations in the ad hoc network. The use of source routing allows packet routing to be trivially loop-free, avoids the need for up-to-date routing information in the intermediate nodes through which packets are forwarded, and allows nodes forwarding or overhearing packets to cache the routing information in them for their own future use.

Overview and Important Properties of the Protocol

The DSR protocol is composed of two mechanisms that work together to allow the discovery and maintenance of source routes in the ad hoc network:

- Route Discovery is the mechanism by which a node S wishing to send a packet to a destination node D obtains a source route to D. Route Discovery is used only when S attempts to send a packet to D and does not already know a route to D.

- Route Maintenance is the mechanism by which node S is able to detect, while using a source route to D, if the network topology has changed such that it can no longer use its route to D because a link along the route no longer works. When Route Maintenance indicates a source route is broken, S can attempt to use any other route it happens to know to D, or can invoke Route Discovery again to find a new route. Route Maintenance is used only when S is actually sending packets to D.

Basic DSR Route Discovery

When some node S originates a new packet destined to some other node D, it places in the header of the packet a source route giving the sequence of hops that the packet should follow on its way to D. Normally, S will obtain a suitable source route by searching its Route Cache of routes previously learned, but if no route is found in its cache, it will initiate the Route Discovery protocol to dynamically find a new route to D. In this case, we call S the initiator and D the target of the Route Discovery.

When another node receives a ROUTE REQUEST, if it is the target of the Route Discovery, it returns a ROUTE REPLY message to the initiator of the Route Discovery, giving a copy of the accumulated route record from the ROUTE REQUEST, when the initiator receives this ROUTE REPLY, it caches this route in its Route Cache for use in sending subsequent packets to this destination. Otherwise, if this node receiving the ROUTE REQUEST has recently seen another ROUTE REQUEST message from this initiator bearing this same request id, or if it finds that its own address is already listed in the route record in the ROUTE REQUEST message, it discards the REQUEST. Otherwise, this node appends its own address to the route record in the ROUTE REQUEST message and propagates it by transmitting it as a local broadcast packet (with the same request id).

In returning the ROUTE REPLY to the initiator of the Route Discovery, such as node E replying back to A node E will typically examine its own Route Cache for a route back to A, and if found, will use it for the source route for delivery of the packet containing the ROUTE REPLY. Otherwise, E may perform its own Route Discovery for target node A, but to avoid possible infinite recursion of Route Discoveries, it must piggyback this ROUTE REPLY on its own ROUTE REQUEST message for A. It is also possible to piggyback other small data packets, such as a TCP SYN packet, on a ROUTE REQUEST using this same mechanism. Node E could also simply reverse the sequence of hops in the route record that it trying to send in the

ROUTE REPLY, and use this as the source route on the packet carrying the ROUTE REPLY itself.
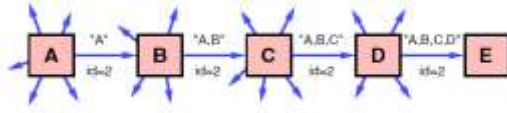

Figure 5.1: Route Discovery Example (Node A is Initiator

and Node E is the Target)

When initiating a Route Discovery, the sending node saves a copy of the original packet in a local buffer called the Send Buffer. The Send Buffer contains a copy of each packet that cannot be transmitted by this node because it does not yet have a source route to the packet's destination. Each packet in the Send Buffer is stamped with the time that it was placed into the Buffer and is discarded after residing in the Send Buffer for some timeout period; if necessary for preventing the Send Buffer from overflowing, a FIFO or other replacement strategy can also be used to evict packets before they expire.

While a packet remains in the Send Buffer, the node should occasionally initiate a new Route Discovery for the packet's destination address. However, the node must limit the rate at which such new Route Discoveries for the same address are initiated, since it is possible that the destination node is not currently reachable. In particular, due to the limited wireless transmission range and the movement of the nodes in the network, the network may at times become partitioned, meaning that there is currently no sequence of nodes through which a packet could be forwarded to reach the destination. Depending on the movement pattern and the density of nodes in the network, such network partitions may be rare or may be common.

Basic DSR Route Maintenance

When originating or forwarding a packet using a source route, each node transmitting the packet is responsible for confirming that the packet has been received by the next hop along the source route; the packet is retransmitted until this confirmation of receipt is received. For example, node A has originated a packet for E using a source route through intermediate nodes B, C, and D. In this case, node A is responsible for receipt of the packet at B, node B is responsible for receipt at C, node C is responsible for receipt at D, and node D is responsible for receipt finally at the destination E. This confirmation of receipt in many cases may be provided at no cost to DSR, either as an existing standard part of the MAC protocol in use or by a passive acknowledgement (in which, for example, B confirms receipt at C by overhearing C transmit the packet to forward it on to D). If neither of these confirmation mechanisms are available, the node transmitting the packet may set a bit in the packet's header to request a DSR-specific software acknowledgement be returned by the next hop; this software acknowledgement will normally be transmitted directly to the sending node, but if the link between these two nodes is uni-directional, this software acknowledgement may travel over a different, multi-hop path.
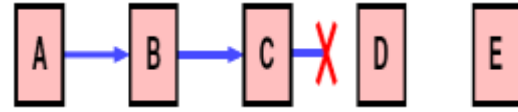

Figure 5.2: Route Maintenance Example (Node C is

unable to forward a packet from A to E over its link to Next

Hop D)

If the packet is retransmitted by some hop the maximum number of times and no receipt confirmation is received, this node returns a ROUTE ERROR message to the original sender of the packet, identifying the link over which the packet could not be forwarded.

3. PROBLEM DESCRIPTION

There are three problems, First one is Hidden terminal and Exposed terminal problems, second one is the congestion problem because more than one source sends the RTS message for transmission and third one is, MACA does not use the Acknowledgement control message, so it's not a reliable. In the pre existing MACA protocol hidden terminal and exposed terminal problems were avoided and not considered crucial. EMACA Protocol is based on MACA Protocol, so it's only the solution of the pre existing problems. Second control message DSSI (Data Sending for Synchronization Information), its uses for what is Data length and RTS/CTS exchange is a success, Hence defer transmission till data ends. With simple unidirectional transmissions the only relevant congestion is at the receiver; however, with our bidirectional RTS-CTSDATA message exchange, congestion at both ends of the transmission is relevant. The last control message is ACK. ACK uses for reliability. When TX sends the Data and Rx receive the Data then after completed transmission the Rx sends the ACK for intimation that Data received.

4. EXPERIMENT CONFIGURATION

S.No.	Parameters	Values
1	Area	1500mx1500m
2	Pause Time	10, 30, 50, 70 and 100
3	Application	CBR (Constant Bit Rate) 2 to 3 Nodes
4	Mobility Model	Random Waypoint
6	Data Packet	Constant, 512 bytes packet size
7	Simulation Time	Constant, 100 Seconds
8	Max. Speed	Constant, 10 m/s
9	MAC Protocols	CSMA, MACA and EMACA
10	Routing Protocols	DSR Routing Protocol
11	Node Placement	Random
12	Seed	1

Table 1: Parameters Value

A. **Performance Metrics**

1) Throughput (bits/s):- Throughput is the measure of the number of packets successfully transmitted to their final destination per unit time. It is the ratio between the numbers of sent packets vs. received packets [4], [10], [17].

2) Total Packets received: - Packet delivery ratio is calculated by dividing the number of packets received by the destination through the number of packets originated by the application layer of the source (i.e. CBR source). It specifies the packet loss rate, which limits the maximum throughput of the network. The better the delivery ratio, the more complete and correct is the routing protocol [4], [10], [17].

3) Drop Packet Ratio:- Packet drop ratio is calculated by subtract to the number of data packets sent to source and number of data packets received destination through the number of packets originated by the application layer of the source (i.e. CBR source) [4], [10], [17].

4) Average Jitter: - Average Jitter Effect signifies the Packets from the source will reach the destination with different delays. A packet's delay varies with its position in the queues of the routers along the path between source and destination and this position can vary unpredictably [4], [10], [17].
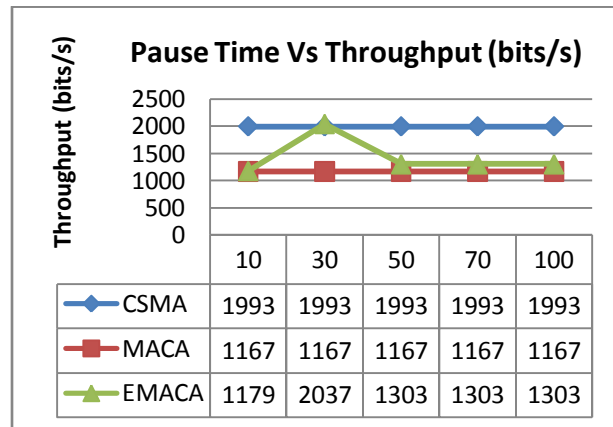
5. IMPLIMENTATION AND RESULTS

Pause Time Vs Throughput (bits/s)

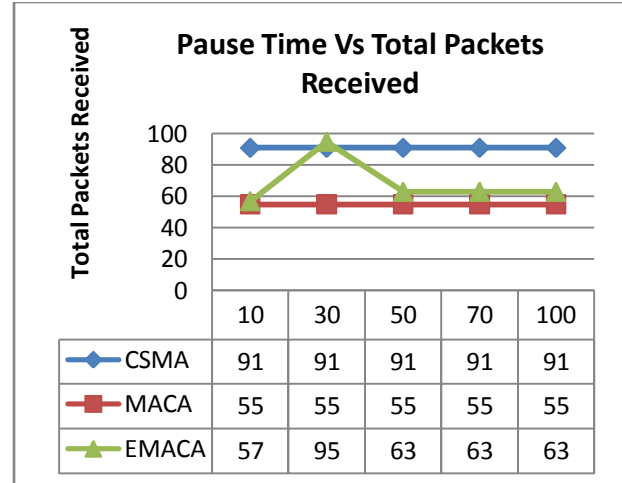|	10	30	50	70	100
CSMA	1993	1993	1993	1993	1993
MACA	1167	1167	1167	1167	1167
EMACA	1179	2037	1303	1303	1303

Figure 6.1: Pause Time Vs Throughput (bits/s)

Pause Time Vs Total Packets Received

	10	30	50	70	100
CSMA	91	91	91	91	91
MACA	55	55	55	55	55
EMACA	57	95	63	63	63

Figure 6.2: Pause Time Vs Total Packets Received

Pause Time Vs Average Jitter (Second)

	10	30	50	70	100
CSMA	0.269	0.269	0.269	0.269	0.269
MACA	0.283	0.283	0.283	0.283	0.283
EMACA	0.382	0.312	0.246	0.246	0.246
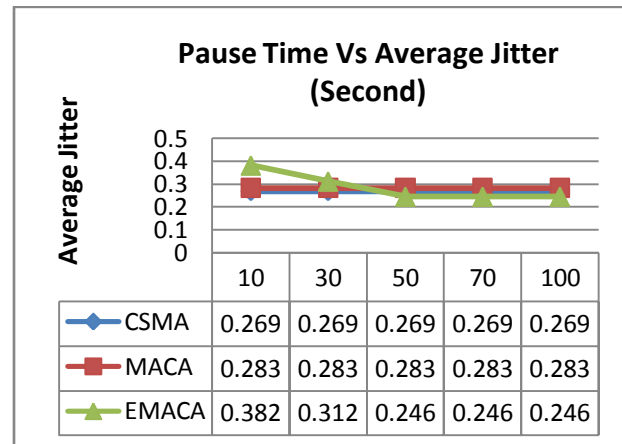
Figure 6.3: Pause Time Vs Average Jitter (Second)

Pause Time Vs Packets Drop Ratio

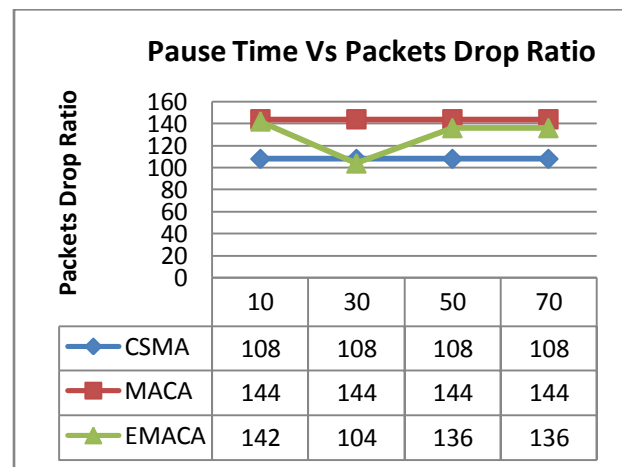|	10	30	50	70
CSMA	108	108	108	108
MACA	144	144	144	144
EMACA	142	104	136	136

Figure 6.4: Pause Time Vs Packets Drop Ratio

6. CONCLUSIONS

The Dynamic Source Routing protocol (DSR) provides excellent performance for routing in multi-hop wireless ad-hoc networks. As shown in our detailed simulation studies and in our implementation of the protocol in a real ad-hoc network of cars driving and routing among themselves, DSR has very low routing overhead and is able to correctly deliver almost all originated data packets, even with continuous, rapid motion of all nodes in the network. A key reason for this good performance is the fact that DSR operates entirely on demand, with no periodic activity of any kind required at any level within the network. This entirely on-demand behavior and lack of periodic activity allows the number of routing overhead packets caused by DSR to scale all the way down to zero, when all nodes are approximately stationary with respect to each other and all routes needed for current communication have already been discovered. As nodes begin to move more or as communication patterns change, the routing packet overhead of DSR automatically scales to only that needed to track the routes currently in use. The Dynamic Source Routing protocol (DSR) is an important component of such a system. The Efficient MAC protocols can provide significant benefits to mobile ad hoc networks, in terms of both performance and reliability. The simulation results show that the protocol EMACA has been found better in performance than MACA protocol. Preliminary simulation results presented here validate the operational correctness of EMACA and show the potential for significant throughput improvement (at least in selected topologies). So EMACA protocol is more reliable. Consequently it identified and rectified additional performance drawbacks in EMACA through the use of adaptive learning strategies and better physical layer capabilities. We used QualNet simulator, which is commercial and said to be faster than ns-2 for instance. However, the simulation speed was still slow and we were only able to perform a single run per scenario in the context of this project. Therefore, those results should be validated through multiple, additional simulation runs in a future work. Also, different initial node position patterns, more sources, additional metrics could be used.

ACKNOWLEDGMENTS

REFERENCES

[1] T. Bheemarjuna Reddy, I. Karthikeyan, B.S. Manoj, C. Siva Ram Murthy, "Quality of service provisioning in ad hoc wireless networks: a survey of issues and solutions", Department of Computer Science and Engineering, Indian Institute of Technology, Madras 600036, India, Ad Hoc Networks 4 (2006) 83–124.

[2] Imrich Chlamtac, Marco Conti, Jennifer J.N. Liu, "Mobile ad hoc networking: imperatives and challenges", University of Texas at Dallas, Dallas, TX, USA, Ad Hoc Networks 1 (2003) 13–64.

[3] C.K. Toh, "Ad Hoc Mobile Wireless Networks: Protocols and Systems", Springer Prentice Hall Publishers, ISBN 013 007 8174, 2001.

[4] Azzedine Boukerche, "Algorithms and Protocols for Wireless and Mobile Ad Hoc Networks", University of Ottawa, Ottawa, Canada, ISBN 978-0-470-38358-2 (cloth) TK5105.77.A44 2008.

[5] Arun Kumar B. R., Asst. Prof. Dept. of MCA, Sir MVIT, Bangalore & Research Scholar, Dept. of CS, School of Science & Technology, "Performance Comparison of Wireless Mobile Ad-Hoc Network Routing Protocols", Dravidian University, Kuppam-517425, A. P., India, June 2008.

[6] P Mohapatra, S Krishnamurthy, "Ad-Hoc Networks - Technologies and Protocols" Springer Publishers, 2004 (ISBN: 0-387-22689-3).

[7] Changzhou Wang, Guijun Wang, Haiqin Wang, Alice Chen, "Quality of Service (QoS) Contract Specification, Establishment, and Monitoring for Service Level Management", Rodolfo Santiago Boeing Phantom Works Seattle, WA, USA 0-7695-2743-4/06, 2006.

[8] El-Bahlul Fgee, Jason D. Kenney, William J. Phillips, William Robertson Dalhousie University, Department of Engineering Mathematics, and Halifax, "Comparison of QoS performance between IPv6 QoS management model and IntServ and DiffServ QoS models" , ISBN:0-7695 2333-1, 2005.

[9] QualNet 4.5 Programmer's Guide, Scalable Network Technologies, Inc., 6701 Center Drive West, Suite 520, Los Angeles, CA 90045.

[10] Scalable Network Technologies, "QualNet simulator 4.0 Version", tutorial on http://www.cs.binghamton.edu/~vinkolar/QualNet/qualnet-tut1.pdf.

[11] C.E. Perkins, "Ad Hoc Network", Pearson Education, ISBN: 8131720969, 2008.

[12] Ad Hoc Wireless Networks: Architectures and Protocols, C. Siva Ram Murthy and B. S. Manoj, Pearson Education, ISBN13: 9780131470231 ISBN10: 0-13-147023-X, 2008.

[13] Blerta Bishaj, "MAC protocols, contention-based with reservation and scheduling", Helsinki University of Technology.

[14] Bartlomiej Zielilski, "Contention MAC Protocols Efficiency Testing in a Small Wireless Network", Silesian Technical University, Bartlomiej.

[15] Alan Demers, Scott Shenker, Lixia Zhang, "Media Access Protocol for Wireless LAN's", University of California at Berkeley.

[16] Akhilesh Kumar Dubey Anjana Jain S.V. Charhate, "Performance Evaluation of MAC layer Protocols for Ad-hoc WLAN", 23 Park Road Indore (M.P.) INDIA DOI 10.1109/ICETET.2008.66.

[17] Jun-Zhao Sun Media Team, "Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing", Machine Vision and Media Processing Unit, University of Oulu, Finland.

[18] Mehdi Alilou, Mehdi Dehghan.t, Upgrading Performance of DSR Routing Protocol in Mobile Ad Hoc Networks, World Academy of Science, Engineering and Technology 5, March 29 2005.

[19] The MANET web page, http://www.ietf.org/html.charters/manetcharter.html.

[20] Xi J.; Bettstetter C.Wireless Multihop Internet Access: Gateway Discovery, Routing and Addressing, in Proceedings of the International Conference on Third Generation Wireless and Beyond (3Gwireless'02), San Francisco, USA, May 2002.

[21] Tom Goff, Nael B. Abu-Ghazaleh, Dhananjay S. Phatak, Ridvan Kahvecioglu ,Preemptive Routing in Ad-Hoc Networks, MobiCom 2001.

[22] David B. Johnson David A. Maltz Josh Broch, DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks, Computer Science Department Carnegie Mellon University Pittsburgh, PA 15213-3891.

[23] Neeraj Agrawal, Prof. Sanjeev Sharma, School of Information Technology, RGPV, Bhopal, " Performance and Analysis of CSMA, MACA & ALOHA to support Quality of Services (QoS) under varying conditions of no. Of nodes in Ad-Hoc wireless Networks", International Journal of Information Technology and Knowledge Management, January-June 2010, Volume-3, No.-1, PP. 19-23, ISSN: 0973-4414, INDIA. http://www.csjournals.com/IJITKM/SpecialIssue.html

[24] Neeraj Agrawal, Prof. Sanjeev Sharma, Prabhat Sharda, School of Information Technology, RGPV, Bhopal, " A Comparative Study of MAC to support Quality of Services (QoS) in Ad-Hoc wireless Networks ", Proceeding of International Conference on Mathematics and Computer Science (ICMCS) - 2010, PP. 227-231, INDIA.

[25] Neeraj Agrawal, Prof. Sanjeev Sharma, Renu Kachhoria, Sonal Chaudhary, School of Information Technology, RGPV, Bhopal, " Evaluation of CSMA, MACA & ALOHA to support Quality of Services (QoS) under varying conditions of Pause Time in Ad-Hoc wireless Networks ", National Conference on Advanced Pattern Mining and Multimedia Computing (APMMC)- 2010, Excel India Publishers, New Delhi, PP. 422-424, ISBN: 978-93-80043-83-8, INDIA.

[26] Neeraj Agrawal, Prof. Sanjeev Sharma, School of Information Technology, RGPV, Bhopal, " MAC Enhancement to support Quality of Services (QoS) in Ad-Hoc wireless Networks: EMACA (Enhancement of Multiple Accesses with Collision Avoidance) ", International Journal of Computer Applications (IJCA)-2010 (0975-8887), Volume-1, No.-2, PP. 64-70, ISBN: 978-93-80746-01-2, February 2010, Published by Foundation of Computer Science, INDIA. http://www.ijcaonline.org/archives/number2/45-152

[27] Prof. Neeraj Agrawal, Dr. Sanjeev Sharma, Prof. Arun Nahar, School of Information Technology, RGPV, Bhopal, " Analysis of CSMA, MACA & EMACA (Enhancement of Multiple Accesses with Collision Avoidance) to Support QoS under varying conditions of No. of Nodes in Ad-Hoc Wireless Networks by means of DSR Routing Protocol ", IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010, Volume-1, No.-1, PP. 1-7, ISBN: 978-93-80746-69-2, September 2010, Published by Foundation of Computer Science, INDIA. http://www.ijcaonline.org/specialissues/manets/number1/1015-57

[28] David B. Johnson Rice University Computer ScienceDepartment, MS 132 6100 Main Street Houston, TX 77005-1892, Y.Hu, University of Illinois at Urbana- Champaign UIUC D. Maltz Microsoft Research, February 2007, The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4, Request for Comments (RFC): 4728.

[29] David B. Johnson, David A. Maltz, Josh Broch, Computer Science Department, Carnegie Mellon University, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad-Hoc Networks "Pittsburgh, PA15213-3891.