International Journal of Research (IJR) Vol-1, Issue-11 December 2014 **ISSN 2348-6848**

A Study of CSMA (Carrier Sense Multiple Access) and MACA (Multiple Access with Collision Avoidance) over AODV and DSR

Amit Kumar Kar[1], Madhulika Sharma [2]
Department of Computer Science and Engineering
Azad Institute of Engineering and Technology, Lucknow
amit.kar1983@gmail.com[1], madhulikasharma4@gmail.com[2]

ABSTRACT

Ad hoc wireless network (AWN) is a collection of mobile hosts forming a temporary network on the fly, without using any fixed infrastructure. QoS (Quality of Service) is the idea that transmission rates, error rates, and other characteristics can be measured, improved, and to some extent guaranteed in advance in ad hoc network however in particular concern for the continuous transmission of high bandwidth video and multimedia information this kind of content dependably transmitting is difficult in public networks using ordinary "best effort" protocols. 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. MACA (Multiple Accesses with Collision Avoidance) Protocol is a Contention based Sender initiated Protocol which uses Three way handshaking means that RTS—CTS—Data packet exchange. It used in network congestion avoidance to help in determining the correct sending rate by binary exponential back off (BEB) Algorithm in which if any packet transmitted by a node is lost, the node uses the binary exponential back-off (BEB) algorithm to back off a random interval of time before retrying which is also inadequate trustworthy because of data sending acknowledgement is not received.

Keywords- *AWNs, MACA, CSMA, AODV, DSR, Throughput.*

1. INTRODUCTION

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.

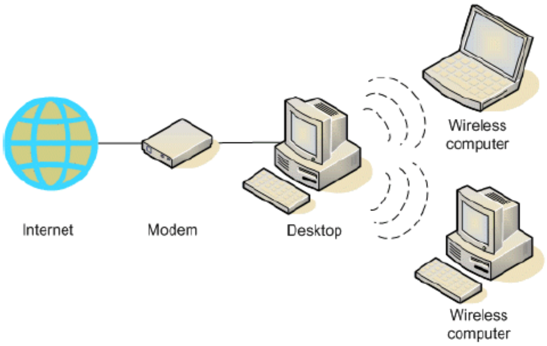

Figure 1: Mobile Ad Hoc Network

Ad hoc wireless networks (AWNs) are zero configurations, self organizing, and highly dynamic networks formed by a set of mobile hosts connected through wireless links [1], [2], [3], [4], [5], [6], [12]. As these are infrastructure less networks, each node should act also as a router. Hence they, the termed ''mobile host'', ''node'', and ''station'' and used interchangeably. As a router, the mobile host represents an intermediate node which forwards traffic on behalf of other nodes. If the destination node is not within the transmission range of the source node, the source node takes help of the intermediate nodes to communicate with the destination node. Tactical communication required on battle-fields, among a fleet of ships, or among a group of armored vehicles are some of the military applications of these networks. Civilian applications include peer-to-peer computing and file sharing, collaborated computing in a conference hall, and search and rescue operations.

Quality of service (QoS) is the performance level of a service offered by the network to the user. 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 [1], [2], [3], [4], [7], [8]. A network or a service provider can offer different kinds of services to the users. Here, 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).

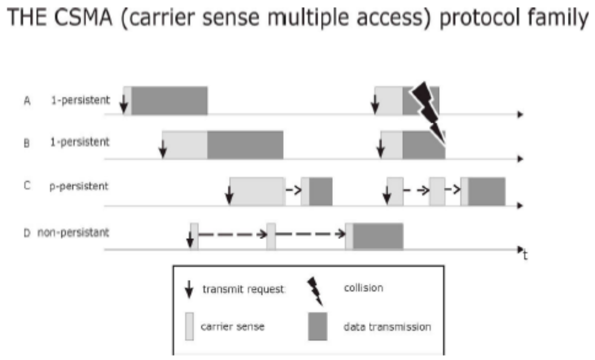

Figure 2: CSMA Protocol

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 Access 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
- Sender initiated Protocol
- Binary Exponential back off Algorithm
- RTS—CTS carrier information about the duration of time for neighbor nodes.

The basic idea of MACA is a wireless network node makes an announcement before it sends the data frame to inform other nodes to keep silent. When a node wants to transmit, it sends a signal called *Request-To-Send* (RTS) with the length of the data frame to send. If the receiver allows the transmission, it replies the sender a signal called *Clear-To- Send* (CTS) with the length of the frame that is about to receive. Meanwhile, a node that hears RTS should remain silent to avoid conflict with CTS; a node that hears CTS should keep silent until the data transmission is complete.

- When a node wants to transmit a data packet, it first transmits a RTS frame.
- The receiver node, on receiving the RTS packet, if it is ready to receive the data packet, transmits a CTS packet.
- Once the sender receives the CTS packet without any error, it starts transmitting the data packet.
- If a packet transmitted by a node is lost, the node uses the binary exponential back-off (BEB) algorithm to back off a random interval of time before retrying.

2. ROUTING PROTOCOLS FOR MANETS

In this paper we have studied two routing protocols which are as follow:

A. Ad-hoc On-Demand Distance Vector Routing (AODV):

Ad-hoc On-Demand Distance Vector Routing (AODV) [6] is essentially a combination of both DSR and DSDV. It borrows the conception of sequence numbers from DSDV, plus the use of the on-demand mechanism of route discovery and route maintenance from DSR. It is called a “pure on-demand route acquisition system”; nodes that do not lie on active paths neither maintain any routing information nor participate in any periodic routing table exchanges. It is loop-free, self-starting, and scales to a large number of mobile nodes. When a source node needs to send a packet to a destination node for which it has no routing information in its table, the Route Discovery process is initiated. The source node broadcasts a route request (RREQ) to its neighbors. Each node that forwards the RREQ packet creates a reverse route for itself back to source node. Every node maintains two separate counters: a node sequence number and a broadcast id. Broadcast id is incremented when the source issues a new RREQ. Together with the source's address, it uniquely identifies a RREQ. In addition to the source node's IP address, current sequence number and broadcast ID, the RREQ also contains the most recent sequence number for the destination which the source node is aware of.

A node receiving the RREQ may unicast a route reply (RREP) to the source if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. Otherwise, it re-broadcasts the RREQ. Each node that participates in forwarding a RREP packet back to the source of RREQ creates a forward route to the source node. Each node remembers only the next hop unlike source routing which keeps track of the entire route. Nodes keep track of the RREQ’s source IP address and broadcast ID. If they receive a RREQ packet that they have already processed, they discard the RREQ and do not forward it. As the RREP propagates back to the source, nodes set up forward pointers to the destination. Once the source node receives the RREP, it may begin to forward data packets to the destination.

At any time a node receives a RREP (for any existing destination in its routing table) containing a greater sequence number or the same sequence number with a smaller hop count, it may update its routing information for that destination and begin using the better route. Routes are maintained as follows: If an upstream node in an active route senses a break in the active route, it can reinitiate the route discovery procedure to establish a new route to the destination (local route repair) or it can propagate an unsolicited RERR with a fresh sequence number and infinity hop count to all active upstream neighbors. Those nodes subsequently relay that message to their active neighbors. This process continues until all active source nodes are notified. Upon receiving notification of a broken link, source nodes can restart the discovery process if they still require the destination. Link failure can be detected by using Hello messages or by using link-layer acknowledgements (LLACKS). The main benefit of AODV over DSR is that the source route does not need to be included with each packet, which results in a reduction of routing protocol overhead. Because the RREP is forwarded along the path established by the RREQ, AODV requires bidirectional links.

B. Dynamic Source Routing (DSR):

Dynamic Source Routing (DSR) [5], as the name suggests, is based on the concept of source routing. There are no periodic routing advertisements; instead, routes are dynamically determined based on cached information or on the result of a route discovery process. In source

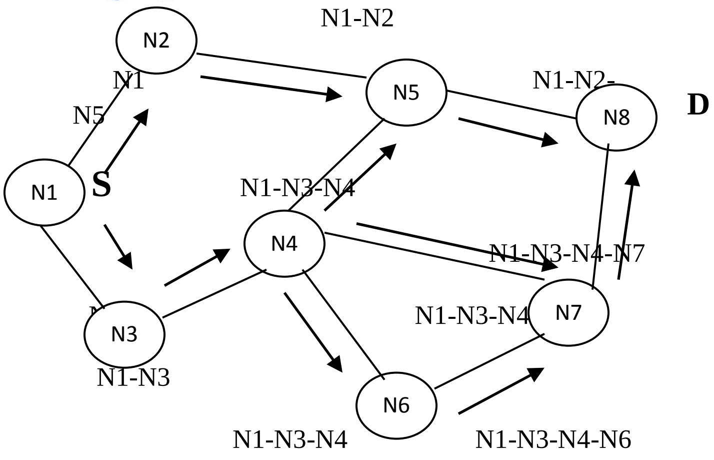

Figure 3(a): Building the Route Record during the Route Discovery

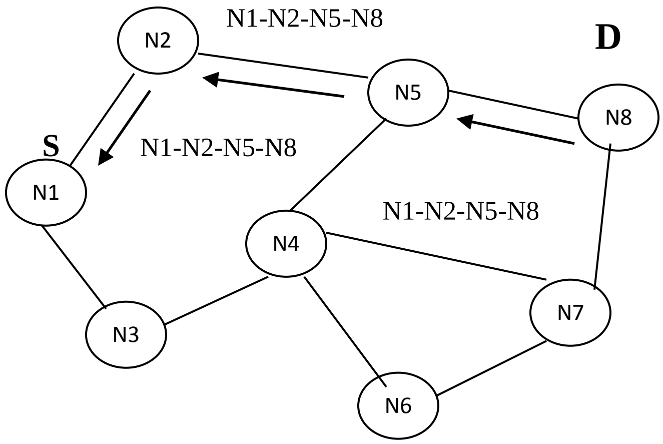

Figure 3(b): Propagation of the Route Reply with the Route Record

routing, the sender of the packet specifies the complete sequence of the nodes that the packet has to take. The sender explicitly lists this route in the packet's header, identifying each forwarding "hop" by the address of the next node to which the packet must be sent on its way to the destination host. A key advantage of source routing is that intermediate hops do not need to maintain routing information in order to route the packet they receive, since the packets themselves already contain all the necessary routing information. Unlike conventional routing protocols, the DSR protocol does not periodically transmit route advertisements, thereby reducing control overhead, particularly during periods when little or no significant host movement is taking place. The DSR protocol consists of two mechanisms: ***Route Discovery*** and ***Route Maintenance***.

When a mobile node wants to send a packet to some destination, it first consults its route cache for a non-expired route. If the node does not have such a route, it will initiate route discovery by broadcasting a route request (RREQ) packet, which contains the addresses of the source node and the destination, and a unique sequence number "request id", which is set by the source node. Each node in the network maintains a list of (source address, request id) pair that it has recently received from any host in order to detect duplicate route requests received. On receiving a RREQ, a node checks to see if it has already received a request with the same (source address, request id) pair (duplicate RREQ). In such an event, or if the node sees its own address already recorded in the request (routing loop), it discards the copy and does not process it further. Otherwise, it appends its own address to the route record in the route request packet and re-broadcasts the query to its neighbors.

When the request packet reaches the destination, the destination node then sends a route reply packet to the source with a copy of the route. If a node can complete the query from its route cache, it may unicast a route reply (RREP) packet to the source without propagating the query packet further. Furthermore, any node participating in route discovery can learn routes from passing data packets and gather this routing information into its route cache. Figure 3 (a) and 3 (b) is an example of the creation of a route record in DSR [5].

Route Maintenance is used to detect if the network topology has changed such that the route in the node's route cache is no longer valid. Each node along the route, when transmitting the packet to the next hop, is responsible for detecting if its link to the next hop has broken. Many wireless MAC protocols, such as IEEE 802.11, retransmit each packet until a link-layer acknowledgement is received, or until a maximum number of retransmission attempts have been made. Alternatively, DSR may make use of a passive acknowledgement. When the retransmission and acknowledgement mechanism detects that the link is broken, the detecting node unicast a Route Error packet (RERR) to the source of the packet. Every hop en-route to the source that received or overheard the RERR removes the broken link from any route caches and truncates all routes that contain this hop. The source can then attempt to use any other route to the destination that is already in its route cache, or can invoke Route Discovery again to find a new route.

The DSR protocol is intended for networks in which the mobile nodes move at a moderate speed with respect to packet transmission latency [5]. An advantage of DSR over some on-demand protocols is that DSR does not use periodic routing advertisements, thereby saving bandwidth and reducing power consumption. On the other hand, as the network becomes larger, control packets and data packets also become larger because they need to carry addresses for every node in the path. Also, aggressive use of route cache and the absence of any mechanism to expire stale routes will cause poor delay and throughput performance in more stressful situations.

3. PERFORMANCE METRICES

Following performance metrics are studied in this survey.

A. 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].

B. 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].

C. 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].

D. Average End to End Delay

Average packet delivery time from a source to a destination. First for each source-destination pair, an average delay for packet delivery is computed. Then the whole average delay is computed from each pair average delay.

4. CONCLUSION

The Study shows that the Efficient MAC protocols can provide significant benefits to mobile ad hoc networks, in terms of both performance and reliability. The issues associated with the design of a MAC protocol for wireless ad hoc networks are: node mobility; an error- prone, broadcast and shared channel; time-synchronization; bandwidth efficiency; QoS support. Many MAC protocols for such networks have been proposed so far but their performance in terms of Throughput, Total packet received, Average end to end delay and drop packet ratio is questionable and is not satisfactory.

The study shows that the behavior of routing protocols vary with the environments. In some condition CSMA and for some situation MACA are better. It depends where we have to use these.

In future we can implement these routing protocols with CSMA and MACA environments and check how they behave. The previous work was done with AODV routing protocols.

5. 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 CSE, IIT, Madras 600036, India, AdHoc 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 (2003) 13–64.

[3] C.K. Toh, “Ad Hoc Mobile Wireless Networks: Protocols and Systems”, Springer Prentice Hall Publishers, 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., “Performance Comparison of Wireless Mobile Ad- Hoc Network Routing Protocols”, Bangalore & Research Scholar, Dept. of CS, School of Science & Technology, Dravidian University, Kuppam- 517425, A. P., India, June 2008.

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

[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, “Comparison of QoS performance between IPv6 QoS management model and IntServ and DiffServ QoS models”, Dalhousie University, Department of Engineering Mathematics, and Halifax, 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/qualnettut1.pdf.

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

[12] C. Siva Ram Murthy and B. S. Manoj, “Ad Hoc Wireless Networks: Architectures and Protocols”, 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”, University of Oulu, Finland.