

Supporting MAC Layer Multicast in IEEE 802.11 based MANETs: Issues and Solutions

Hrishikesh Gossain, Nagesh Nandiraju, Kumar Anand, Dharma P. Agrawal
OBR Center for Distributed and Mobile Computing
Department of ECECS, University of Cincinnati – Cincinnati, OH 45221-0030
(hgossain, nandirns, anandk, dpa)@ececs.uc.edu

Abstract

In an IEEE 802.11 based Mobile Ad Hoc Networks (MANETs) multicast packets are generally forwarded as one hop broadcast; mainly to reach all the multicast members in the neighborhood in a single transmission. Because of the broadcast property of the forwarding, packets suffer from increased instances of hidden terminal problem. Mobility of nodes makes things more difficult, and unlike unicast transmissions where MAC can detect the movement of a nexthop by making several retries, it is not possible in case of multicast forwarding. To address these issues, we propose a multicast aware MAC protocol (MMP) for MANETs. The basic objective of MMP is to provide a MAC layer support for multicast traffic. This is done by attaching an Extended Multicast Header (EMH) by the multicast agent, which provides the address of the nexthop nodes that are supposed to receive the multicast packet. The MAC layer in MMP uses the EMH field to support an ACK based data delivery. After sending the data packet, the transmitter waits for the ACK from each of its destinations in a strictly sequential order. A retransmission of the multicast packet is performed only if the ACK from any of the nodes in EMH is missing. We compare MMP with IEEE 802.11 and results show that MMP substantially improves the performance of multicast packet delivery in MANETs without creating much MAC overhead. In addition, MMP provides a better mechanism to detect the movement of its nexthop members.

I. INTRODUCTION

Multicasting [1, 2] is the transmission of datagrams to a group of hosts identified by a single destination address and hence is intended for group-oriented computing. In MANETs, multicasting can efficiently support a variety of applications that are characterized by close collaborative efforts. Existing approaches to support multicast in mobile ad hoc networks try to capitalize on the broadcast property of ad hoc networks, wherein a single one hop broadcast packet is sent for all the members in the neighborhood. However the basic carrier-sense multiple access with collision avoidance (CSMA/CA) in IEEE 802.11 [3] does not provide any protection against the hidden terminal problem for such one hop broadcasts. As a result system performance degrades drastically due to collisions. These one hop broadcasts are not ACKed, hence a transmitter can neither determine if its nexthops have received the packet nor if they have moved out of range. Existing work in the area of multicasting in mobile ad hoc networks [4, 5] has outlined the seriousness of this problem, wherein the collision of one multicast packet, at any of the forwarding node may results into loss of packet in its complete downstream tree. This effect becomes more severe

if such collision happens near the source. Hence we argue that it is necessary to differentiate between a multicast from a general broadcast traffic in the MAC layer, and either provide some kind of protection against the hidden terminal problem or provide some retransmission strategy in case collision occurs.

Keeping this objective in mind we have designed a Multicast aware MAC Protocol (MMP) for mobile ad hoc networks. The design of MMP is directly motivated by our work in the area of Explicit Multicast (Xcast) [5], where we show the seriousness of hidden terminal problem, and node movement, in overall packet delivery. Xcast is also known as Stateless Multicast, since none of the intermediate routers need to maintain any state information related to any ongoing session. We have explained MMP assuming an Xcast way of multicast packet delivery, mainly because of its simplicity. However it should be noted that MMP is transparent to any multicast scheme, as long as the multicast layer can attach an Extended Multicast Header (EMH) before sending the packet to the MAC. A brief overview of Xcast scheme is given in Section 3.1. For a complete description of Xcast mechanism in MANETs please refer to [4, 5].

MMP is built on top of IEEE 802.11. We propose to use the *type* field in IEEE 802.11 *frame control* to uniquely identify a multicast packet. For that purpose, we have used the *subtype* value 1000 (one of the reserved subtypes in the standard) to identify a MAC layer multicast packet.

The basic working principle of MMP is as follows. Before sending a data packet to MAC, with the help of routing layer, the multicast agent creates an EMH and adds it to packet header. The EMH contains the information about the nexthop who are supposed to receive the multicast packet. The presence of EMH header triggers MAC to initiate an ACK based multicast data delivery. Before forwarding this packet, MAC sets the *type* field to “1000”, to inform the nexthops that it is a multicast packet and they have to reply with an ACK. However to prevent a collision of ACK packet at the transmitter, ACKs from the destination nodes are sent in a strictly sequential order. In case the transmitter misses ACKs from any of the next hops, it does a backoff mechanism similar to unicast packet and tries to retransmit the Xcast packet again, this time with multicast RTS (MRTS)/CTS (discussed in later sections), and only to those nexthops, from which the transmitter did not receive any ACK.

The outline of rest of the paper is as follows. We first give a brief overview of IEEE 802.11 and its multicast support in Section 2. Section 3 describes the proposed MMP protocol, followed by a simulation analysis of MMP with basic IEEE 802.11 schemes in Section 4. Section 5 describes the related work in this area, outlining their limitations. Finally, Section 6 concludes the paper highlighting some open problems and future research directions.

II. MULTICAST SUPPORT IN IEEE 802.11

In the IEEE 802.11 [3], the Distributed Coordination Function (DCF) coordinates medium access in ad hoc networks. In DCF, an optional RTS and CTS handshake generally precedes DATA communication and the following ACK. DCF in IEEE 802.11 conducts two forms of carrier sensing: physical (by listening to the wireless shared medium) and virtual. Virtual carrier sensing uses the duration field which is included in the header of RTS and CTS frames. The duration included in each of these frames can be used to determine the time when the source node would receive an ACK frame from the destination node. This duration field is utilized to set a station's Network Allocation Vector (NAV), which indicates the remaining time the medium will be busy with the ongoing transmission. Using the duration information, nodes update their NAVs whenever they receive a packet that is not destined to them. The channel is considered to be busy if either physical or virtual carrier sensing (by the NAV) so indicates. Whenever NAV is zero, a station may transmit if the physical sensing allows.

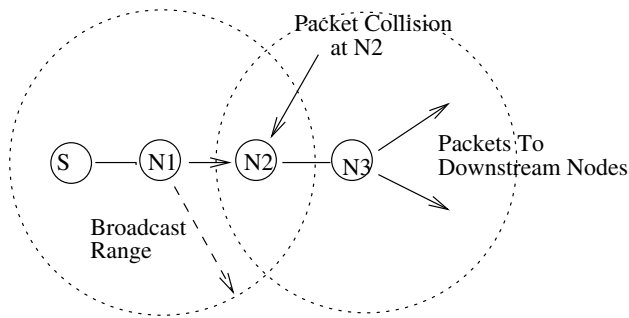


Figure 1 – Hidden Terminal

The present implementation of IEEE 802.11 DCF does not provide any support for multicast traffic. They are transmitted as a simple broadcast without any RTS, CTS and ACK. So, there is no mechanism employed by the MAC layer to tackle the “hidden terminal” problem. For example, in Figure 1, if the transmission time of nodes N1 and N3 overlap there will be a collision at N2, and hence packets will be lost. One way to minimize this effect is to introduce a jitter while forwarding a multicast packet, but as found in our simulation study, it has only a minimal effect in reducing the packet collisions.

The packet loss due to MAC layer collision has a cascading effect on the efficiency of multicast packet delivery. First of all, by adapting a one hop broadcast approach for multicast packet forwarding, a node (say N1) has no way to know if a particular nexthop (say N2) has correctly received the packet. In addition, if N2 moves out, the multicast agent (either at N1 or at source S) may not be aware of such movement till the next MEMBER_UPDATE or through neighbor discovery in some routing protocols (as in AODV). This is because the multicast packets are neither sent with RTS/CTS nor are they ACKed, as a result Short Retry Limit (SRL), the threshold maintained by IEEE 802.11 that controls the maximum number of packet (RTS or DATA) transmission attempts before a send failure is reported to the routing layer, is never incremented. Hence there is no “broken link” trigger from link layer to routing layers and there is always a potential problem of packet loss during this vulnerable period of nexthop movement detection.

III. MULTICAST AWARE MAC PROTOCOL (MMP)

The MMP protocol aims to overcome the limitations in the existing multicast support in IEEE 802.11 MAC by utilizing a new combination of adaptive mechanisms. The MMP protocol uses the same mechanism of data exchange as in the case of basic unicast packet forwarding, i.e. through DATA/ACK. We have elaborated our MMP in four phases: *generation of EMH header* by multicast agent, *MMP packet forwarding* using EMH, *MMP local recovery* if needed and finally *MMP Route recovery*. In following sections we provide a description for each of these phases.

3.1 Extended Multicast Header (EMH) Generation

We will now elaborate on the creation of EMH header through an Xcast example. Xcast is a source-based multicast scheme wherein the multicast source explicitly puts the list of destination addresses in an Xcast header, and assumes that the underlying routing protocol will deliver the packet to all of its destinations. There are schemes which extend this idea of Xcast to MANETs. For example, DDM [4] uses an extended header to include the list of destinations and their nexthops and broadcasts the Xcast packet to all of its neighbors. When a nexthop node receives such packet, it first checks if it is present in the nexthop list, and if so it extracts the destination list meant for it and employs a similar approach as the source to forward the packet. Figure 2 illustrates the basic Xcast scheme. Here, node A is the source of an Xcast session and nodes B, C, D, E, F and G are the prospective recipients. Thus, the Xcast header at the source node A will have {N1: B, C, D, E, F, G} where N1 modifies the Xcast header to {N2: B, C, D, E, F, G} and forwards the packet in its neighborhood. When the Xcast agent in node N2 receives this packet, it regroups the list of destinations based on its next hops, namely, nodes N3 and N4 and modifies the Xcast header to {N3: B, C; N4: D, E, F, G}, where N3 and

N4 are the nexthops which are supposed to receive the Xcast packet. Subsequent nodes follow similar steps until the packet reaches all the destinations. Figure 3 outlines the Xcast header used at nodes A, N2, and N6 for the topology shown in Figure 2.

The concept of EMH is similar to Xcast header, only difference being the inclusion of IDs of the nexthops only. Hence in case of Xcast forwarding there is no need to

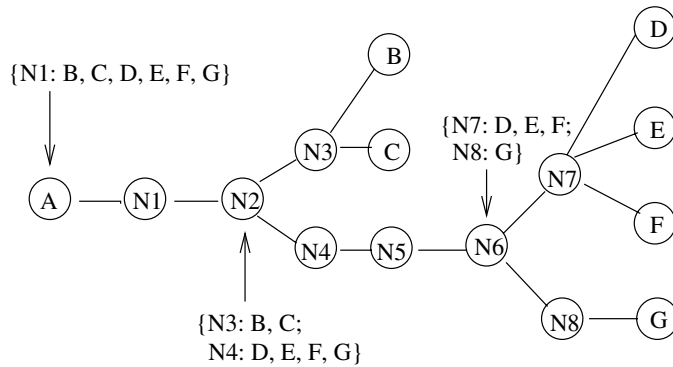


Figure 2 - Xcast packet delivery Tree, A is the source and (B, C, D, E, F, G) are destinations

Given this basic description of EMH generation, we will now assume that the packet sent to the MAC contains the EMH. In the following section, we will describe how MMP uses the EMH to forward multicast packets.

3.2 MMP Packet Forwarding

The packet forwarding algorithm in MMP is based on IEEE 802.11 DCF access mechanism. The presence of the EMH signals the MAC that it is a multicast packet and needs special treatment. Based on the EMH, MAC layer first calculates the number of nexthops it has to forward the packet. It then modifies the duration field in MAC header to include the duration of the future ACKs packets which it is expecting to receive from each of its nexthops. For example, if node N2 has only two nexthops N3 and N4 (Figure 2) which are supposed to receive the multicast packet, the duration field in the MAC header would be set to $SIFS + T_{ACK} + SIFS + T_{ACK}$, where T_{ACK} represents the duration of ACK transfer, and $SIFS$ represents the short inter frame spacing. This allows each of the nexthops to send ACK packet back to the transmitter.

However to prevent a collision of ACK packets at the transmitter node, ACKs from the nexthops are sent in a strict sequential order, beginning from the node whose index is first in the EMH, followed by second and so on. A timing diagram of MMP MAC DATA delivery (corresponding to Node N2 in Figure 2) is shown in Figure 4. In this case the content of EMH is {N3, N4}, hence N3 is the first node to send an ACK

separately attach an EMH header, rather a part of Xcast extended header (Figure 3) can serve as an EMH. However for other tree based multicast forwarding schemes (MAODV), the multicast agent needs to create a separate EMH mentioning the names of the nexthops which are supposed to receive the multicast packet and attach it to packet header.

Xcast Header		
EMH		
Node	NextHop	List of Destinations
A	N1	B, C, D, E, F, G
N2	N3	B, C
	N4	D, E, F, G
N6	N7	D, E, F
	N8	G

Figure 3 – EMH at Node A, N2, and N6 corresponding to topology in Figure 2

after waiting for $SIFS$ period followed by N4, who sends its ACK after waiting $SIFS + T_{ACK} + SIFS$ period.

This way the transmitter can detect if all of its possible nexthops have received the packet. Once the transmitter receives an ACK from a specific nexthop, it removes the row corresponding to that nexthop from the EMH. For example, if node N2 (in figure 4) receives an ACK from N3, it modifies its EMH to {N4} and waits for ACK from N4. In case N2 also receives an ACK from N4, it removes N4 from the EMH. Since the content of EMH is now empty, MAC layer in N2 decides that its packet forwarding is successful and simply drops the packet.

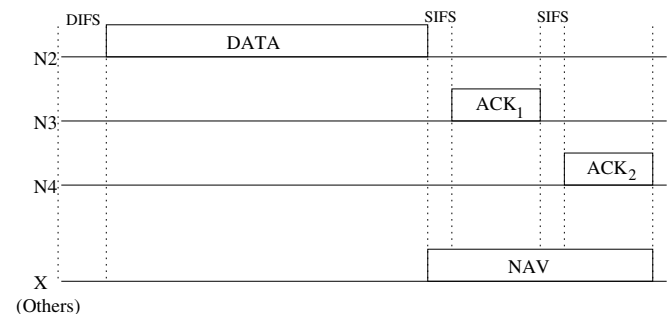


Figure 4 – Timing Diagram of N2 DATA delivery for Figure 2

On the other hand, the absence of ACK from any of the nexthops may be contributed by several factors. Among them, the two main reasons are presence of hidden terminal problem and movement of the nexthop out of the range.

MMP first employs a local recovery to tackle the hidden terminal problem. If several such attempts fail, MMP decides that the node has moved out of the range, and generates a “broken link error” message to the higher layers. In the following section we will describe the local recovery process employed in MMP.

3.3 MMP Local Recovery

Depending on the traffic condition and network load, more than one nexthops may miss the multicast packet. To



D₁, D₂, ...D_n : List of Next Hop Destinations
 TA: Transmitter Address
 FCS: Frame Check Sequence

Figure 5 – MRTS Packet Format

Interestingly, by using the basic DATA/ACK mechanism in first transmission attempt, we can reasonably assume that most of the nexthops have received the multicast packet and only few of them might have missed due to hidden terminal problem or node movement. To handle these nodes, we propose to use a mechanism similar to RTS/CTS. However, to send a single RTS for more than one nexthop (as in the case of multicast), we needed to modify the format of RTS and define a new MAC layer control packet called Multicast RTS (MRTS). The format of CTS in MMP is similar to IEEE 802.11.

The packet format of MRTS is shown in Figure 5 and is similar to RTS, except it also has a variable length destination ID field. For example, if there are two nexthops (D1 and D2) which have not responded with an ACK, the MRTS header contains the IDs of D1 and D2. The duration field in the MRTS header is modified to receive CTS and ACK from all the nexthops mentioned in MRTS header. For example, the duration in this case is set to $2*(SIFS + T_{CTS}) + T_{DATA} + 2*(SIFS + T_{ACK})$. It is to be noted that a more efficient strategy to set the duration field in MRTS header would be to set it for the duration $2*(SIFS + T_{CTS}) + \delta$, where “delta” represents a very small duration to allow the start of transfer of DATA packet [6]. It eliminates the chances of unwanted channel reservation in case none of the intended nexthops reply with CTS. However in present implementation of MMP we have employed the former approach. Also to uniquely identify a MRTS, we propose to set the *type* field in

retransmit the DATA packet we basically have two options, we can employ our basic scheme (DATA with ACK). However if any of the node has moved out of the range it will result into excessive overhead due to unnecessary retransmission of large size DATA packets. The other option is to retransmit the packet through RTS/CTS. This strategy is ideal if intended number of nexthops for retransmission is small. If this number is large, handling RTS and CTS for each such nodes becomes a tough task.

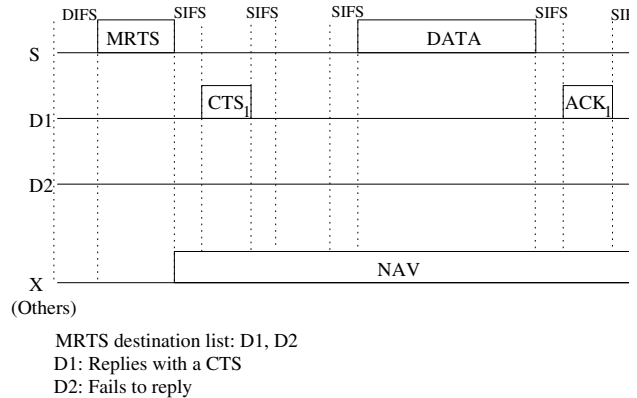


Figure 6 – Retransmission DATA Flow

IEEE 802.11 *frame control* to 1001 (one of the reserved subtypes in IEEE 802.11).

Nodes which are not in EMH header, after receiving an MRTS, set their NAV for the duration field in MRTS. However if the node is in EMH header, it does not set its NAV to allow the transmission of its CTS. Also, after successful reception of a MRTS, if a node is waiting for its turn for CTS, and if it receives CTS from any of the neighboring nodes, meant for the same destination, it ignores the CTS. It allows the node to send its CTS, which otherwise might have been prevented due to setting of NAV due to the neighboring CTS.

The CTS transmission by the nexthops (in this case D1, and D2) is done in the order of their destination IDs mentioned in MRTS header (similar to MMP DATA/ACK strategy). Figure 6 outlines a MRTS based retransmission strategy where node S tries to resend the multicast packet to nexthops D1 and D2. If the sender receives CTS from any of the nexthops (D1, D2), it sends the DATA packet, and removes the destination from the EMH. Otherwise it follows the back off mechanism similar to unicast scheme, and tries to retransmit again after a random backoff, till SRL limit is reached (generally set to 7) or it has successfully delivered the packet to all of its nexthops in EMH.

We think that SRL limit is sufficient to handle the hidden terminal problem. If the transmitter does not receive any CTS from a given node/nodes, it assumes that this is due to a

broken link and the next hop has moved out of its range. Hence once the SRL limit is reached, the transmitter's MAC layer passes the broken link information for all the remaining nexthops in EMH header to the routing layer accordingly.

3.4 MMP Route Recovery

Once the routing layer receives a "broken link" indication from the MAC, it tries to find alternate route. In general, it results into a "route error" (in DSR) message generated by the routing layer and sent to all the source nodes currently using that particular route. In our case, the source of the multicast session will receive such error message. This way MMP scheme facilitates a fast detection of neighbor movement for multicast delivery, which otherwise may take MEMBER_UPDATE period.

IV. SIMULATION ENVIRONMENT AND RESULTS

We have implemented MMP in NSv2 (version 2.26) [12] and have compared the performance of basic Xcast scheme running over MMP and CSMA/CA based IEEE 802.11 with no multicast support. The following metrics are used to compare the performance of different schemes:

- **Data Packet Delivery Ratio:** Ratio of the number of data packets actually received by group members to the number of data packets which should have been received.
- **Average Packet Delay:** It refers to the difference of time data is generated at the application and time it is correctly received at a member.
- **Forwarding Efficiency:** This is a measure of the number of MAC data bytes transmitted per data byte successfully delivered.

Table I: Simulation Parameters

	Parameters	Value
Simulation	Number of Nodes (Random Scenario)	50
	Packet Size	512 bytes
	Simulation Time	900s
	X-dimension of Motion	1000m
	Y-dimension of Motion	1000m
	Transmission Range	250m
	Bandwidth	2Mbps
	Node Placement	Random
	Radio Propagation Model	TwoRayGround
	MAC Protocol	IEEE 802.11
	Transport Protocol	CBR
XCAST	MEMBER_JOIN_RATE	120s

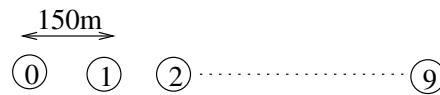
We use 2 Mbps for the channel bit rate. Application generates CBR traffic at the rate of 2 packets per second with payload of size 512 bytes. We have studied the effect of mobility as well as group size on the performance of MMP.

As for the routing protocol, we have employed AODV (Ad hoc on demand distance vector) [13]. In our simulation we consider the transmission range to be 250 m and each node transmits its packet at the highest transmit power level. Some of the simulation parameters are shown in Table I.

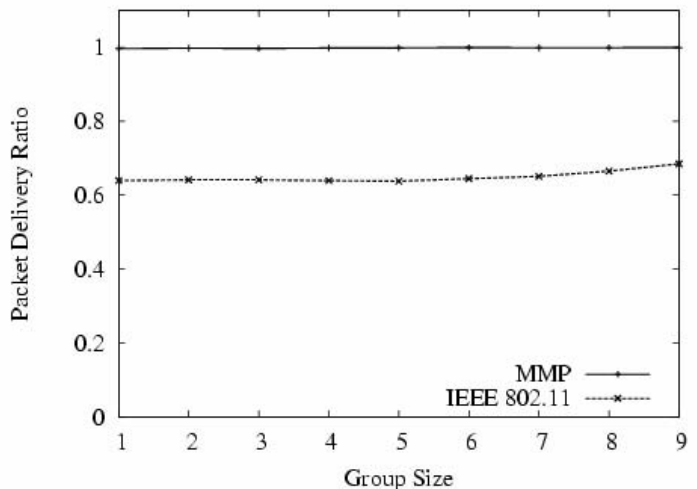
4.1 Linear Topology

To illustrate the impact of hidden terminal problem on multicast packet delivery, we first create a linear topology of 10 nodes as shown in Figure 7(a). In this topology node 9 is the source of a multicast session. We vary the number of members which are supposed to receive the multicast packets from 1 (node 0) to 9 (node 0 to node 8). We then evaluate the packet delivery ratio of MMP and the IEEE 802.11 MAC with no multicast support.

As shown in Figure 7(b), by using an ACK based multicast packet delivery, and corresponding recovery by MRTS the packet delivery ratio in MMP is close to 1, whereas IEEE 802.11 MAC, with no multicast support, the packet delivery ratio is not as impressive and is close to 0.65.



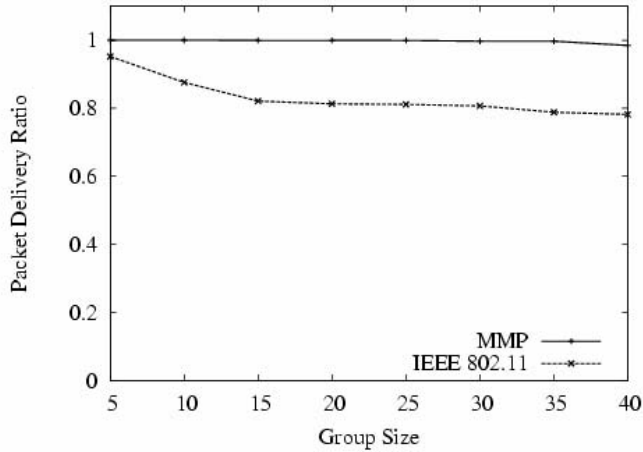
7(a). Linear Topology



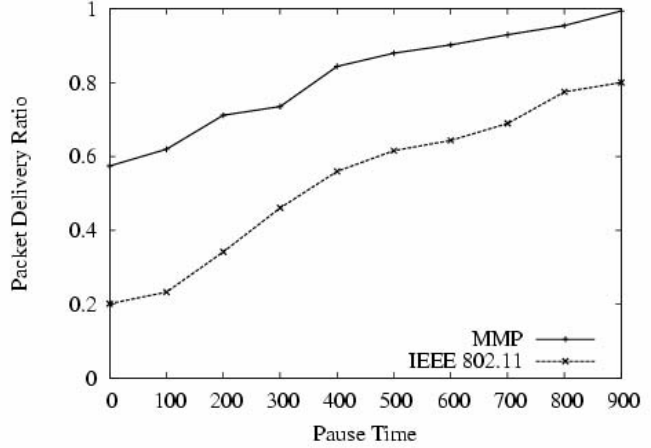
7(b). Packet Delivery Ratio for Figure 7(a)

4.2 Random Topology

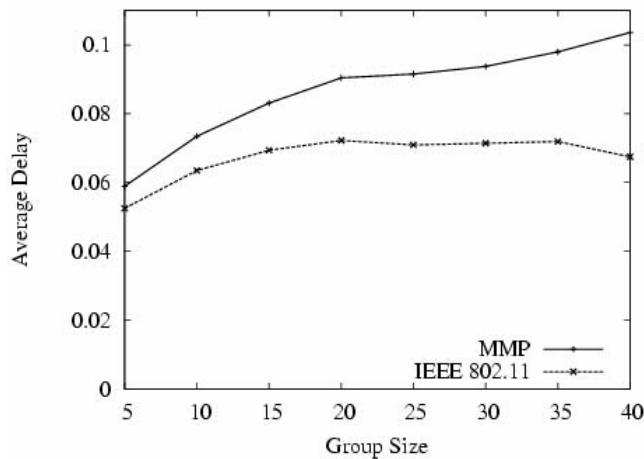
Given this basic illustration on the significance of multicast support in MAC, we will now study the performance of MMP in a random scenario. Here we study the effect of group size as well as mobility on the performance of multicast packet delivery in MMP and IEEE 802.11 for a given multicast session.



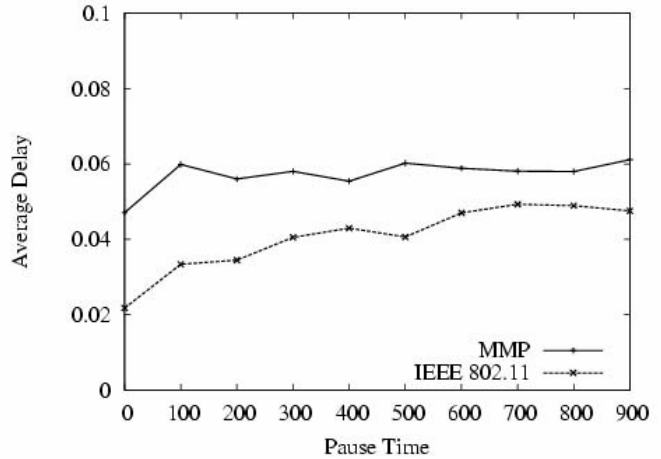
8(a) - Packet delivery ratio with varying group size



8(b) - Packet delivery ratio with varying pause time



9(a) Average packet delay with varying group size



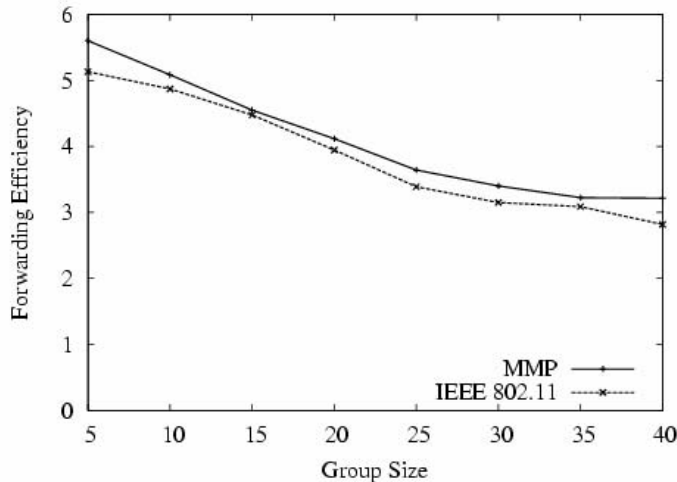
9(b) Average packet delay with varying pause time

In the first group of simulation, we vary the group size (no mobility). The group size considered are 5, 10 ...40 and for a given number of multicast group members we run 10 different simulations, each time selecting a different source, and compute the simulation average for group size. In the second group of simulations, we keep the group size fixed to 25 nodes and vary the node mobility. All the nodes follow the random waypoint mobility model [14] with speed range of 1m/s to 10m/s. We vary the mobility with different pause time as 0, 100, 200 ... 900. For a given pause time, we create 10 different scenarios and finally compute the simulation average for each pause time.

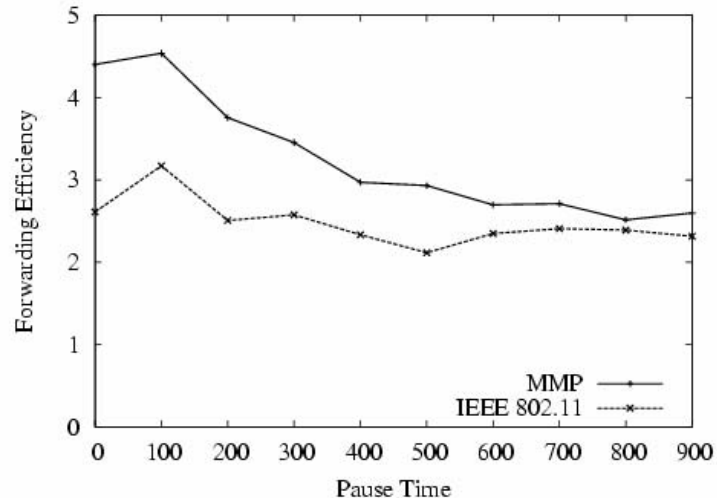
4.2.1 Packet Delivery Ratio

Figure 8(a) and 8(b) compares the packet delivery ratio of MMP with the IEEE 802.11. As evident from the figures MMP achieves a very high packet delivery ratio as compared

to IEEE 802.11 based MAC for both static and mobile scenarios. For static scenario, the high throughput (which is approximately 1) is mainly contributed by the retransmission of multicast packet. The packet delivery for mobile scenario is more interesting. Although the packet delivery ratio for both the schemes goes down as mobility increases, MMP considerably outperforms IEEE 802.11 for all the pause times. For mobile scenario, in MMP a transmitter can detect the movement of its nexthop by SRL retries and hence can try to either find the route to destination again or inform the source without wasting much time. On the other hand in IEEE 802.11, since the packets are transmitted as one hop broadcast, the transmitter has no way to know the movement of its nexthop, and may take MEMBER_UPDATE period. During this vulnerable period all the nodes in the downstream of the nexthop will miss multicast packets.



10(a) - Forwarding efficiency for varying group size



10(b) - Forwarding efficiency for varying pause time

4.2.2 Average packet delay

Next we are going to compare the average packet delay for MMP and IEEE 802.11. We then calculate an average of all such delays. The significance of this result is to account for the delay overhead associated with the additional control packets employed in MMP. To calculate average packet delay we have considered only the packets which have been successfully received. Figure 9(a) and 9(b) shows average packet delivery ratio of MMP and 802.11 based MAC schemes for the static and mobile scenarios. It is to be noted that the average packet delay depends on the distance of a recipient from the source. For both MMP and IEEE 802.11 the average packet delay lies below 100ms, where the delay associated with MMP is more than IEEE 802.11, mainly because of the control overhead and packet retransmission.

4.2.3 Forwarding Efficiency

Finally we compare the forwarding efficiency of MMP with IEEE 802.11. This is a measure of the number of MAC data bytes transmitted per data byte successful received at application and is a good measure to evaluate the overhead involved with control packets and retransmissions in MMP. As shown in Figure 10(a) and 10(b), even by employing an ACK based multicast packet delivery and subsequently using MRTS/CTS for retransmission if needed, the MAC overhead in MMP is considerably closer to basic IEEE 802.11 with no multicast support. It is worthwhile to note that there is a tradeoff between the MAC overhead and the packet delivery ratio, and as evident by the results with a very small MAC overhead in MMP we achieve a very good packet delivery ratio.

V. RELATED WORK

There are several proposed schemes to provide MAC layer support for multicast traffic. In [7] authors suggest a

round-robin polling strategy in the MAC layer to deliver multicast packets. To tackle hidden terminal problem, a transmitter polls each of the neighbors (through RTS/CTS) before sending the DATA. However this amounts to excessive retransmission in case of moderate and high traffic load. Also nodes wastes considerable amount of channel bandwidth just to send RTS. Also the paper does not outline the coordination among the CTS frames or the retransmission strategy.

In continuation of [7], in [10] authors suggests delivering of data packets in sequential order for reliable multicasting. In [8] authors have proposed two schemes to provide a reliable MAC layer multicast. The first scheme, known as Batch Mode Multicast MAC (BMMM), uses a similar mechanism of polling as in [7]. However to avoid the collision of CTS frames as in [7], in BMMW the transmission of RTS/CTS are in a strict sequential order to each of the destinations. To prevent collision among the ACK frames, the transmitter polls each of the neighbors by sending a new packet called RAK (Request to ACK). As evident from the discussion, this scheme adds considerable overhead to transmit a single DATA packet. The second scheme known as Location Aware Multicast MAC (LAMM) tries to avoid the control overhead of BMMW by assuming the location information of each of nodes. It helps the transmitter to poll only a subset of nodes based on their location.

In [9] the authors address the issue of reliability of MAC layer broadcasting in IEEE 802.11 based MANETs. However not specifically tailored to multicasting, authors propose three schemes to increase the reliability of MAC layer broadcast. In first scheme termed as *Duplicated broadcast*, a sender transmits a broadcast packet twice, to increase the chances of reception at the neighboring nodes. The second scheme is termed as *Broadcast Acknowledgement*, where authors propose to use ACK with each broadcast packets. To reduce

the overhead of ACK reception, a single DIFS window is subdivided into many minislots that contain acknowledgment patterns sent by the receivers indicating the correct reception of the message. However it results into extra overhead of synchronization. The third scheme called *priority queue* advocates providing a higher priority to broadcast packets; as compared to a regular unicast packet.

In [11] authors interpret the collision of multiple CTS in response to a RTSm (modified RTS packet) packet sent by the source, as a positive signal provided there is a SIFS period of idle channel before the collision occurs and the duration of the collision is not longer than twice the expected duration of CTS. The drawback of this approach is that there is no way to determine if all the nodes have responded to the RTSm packet. In [15] authors propose Reliable-MAC, a sender initiated protocol which uses separate channels for busy tone to realize the reliability for multicast traffic in MAC layer. Busy tones are used instead of CTS and ACK packets which reduces the physical layer overhead. Similar to [15], authors in [16] also suggest using busy tones in order to provide reliability for multicast traffic in MAC layer. The drawback of these schemes is the implementation of busy tones. Our proposed scheme does not need any support for busy tones.

VI. CONCLUSION AND FUTURE WORK

In this paper we present a novel scheme to support multicasting in IEEE 802.11 networks. The proposed MMP addresses the issues of hidden terminal problem and node movement for multicast packet delivery. The basic objective of MMP is to provide a MAC layer support for multicast traffic. This is done by attaching an Extended Multicast Header (EMH) by the multicast layer, mentioning the names of the nexthops which are supposed to receive multicast packets. The MAC layer in MMP uses the EMH field to support an ACK based data delivery. Through simulation work we have shown that MMP substantially improves the performance of multicast packet delivery in MANETs without creating much MAC overhead. MMP provides a better mechanism to detect the possible movement of its next hop. As future work, we plan to investigate the issue of multiple sources for the same multicast session. Also, we intend to evaluate the performance of MMP with different multicast routing protocols.

VII. ACKNOWLEDGEMENT

This work has been supported by the Ohio Board of Regents Doctoral Enhancement Funds and the National Science Foundation under grant CCR-113361.

REFERENCES

- [1] S. Deering, "Multicast Routing in a Datagram Network," Ph.D. dissertation Stanford University, 1991.
- [2] C. M. Cordeiro, H. Gossain and D. P. Agrawal, "Multicast over Wireless Mobile Ad Hoc Networks: Present and Future Directions", in IEEE Network, Special Issue on Multicasting: An Enabling Technology, Vol. 17, Issue: 1, January/February 2003.
- [3] IEEE Std. 802-11. "IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification," June 1997
- [4] DDM Lusheng Ji, and M S. Corson, "Differential Destination Multicast - A MANET Multicast Routing Protocol for Small Groups", In Proc. of the IEEE Infocom, pp. 1192-1202, 2001.
- [5] H. Gossain, C. Cordeiro, K. Anand, D. P. Agrawal, "E2M: A Scalable Explicit Multicast Protocol for MANETs," In Proc. of IEEE International Conference on Communications (ICC) 2004.
- [6] S. Ray, J. B. Carruthers, and D. Starobinski, "RTS/CTS-Induced Congestion in Ad Hoc Wireless LANs," In Proc. of IEEE Wireless Communications and Networking Conference 2003.
- [7] Ken Tang, and Mario Gerla, "Random Access MAC for Efficient Broadcast Support in Ad Hoc Networks," In Proc. of IEEE Wireless Communications and Networking Conference (WCNC) 2000, Chicago, IL, September 2000.
- [8] M. Sun, L. Huang, A. Arora and T.H. Lai, "Reliable MAC Layer Multicast in IEEE 802.11 Wireless Networks," In Proc. IEEE International Conference on Parallel Processing (ICPP) 2002, pp. 527-536, Vancouver, Canada, August 2002.
- [9] Shiann-Tsong Sheu et al., "A Highly Reliable Broadcast Scheme for IEEE 802.11 Multi-hop Ad Hoc Networks," In Proc. of IEEE International Conference on Communications (ICC)2002, New York, NY, April 2002.
- [10] K. Tang, M. Gerla, "Congestion Control Multicast in Wireless Ad Hoc Networks," Computer Communications, Vol. 26, pp. 278-288, 2003
- [11] K.S.Lau and Derek Pao, "Multicast medium Access Control in Wireless Ad Hoc Network," In Proc. of Wireless Communications and Networking Conference 2004
- [12] NS-2 Network Simulator, <http://www.isi.edu/nsnam/ns/index.html>.
- [13] Charles E. Perkins, Elizabeth M. Belding-Royer, and Samir Das. "Ad Hoc On Demand Distance Vector (AODV) Routing," IETF Internet draft, draft-ietf-manet-aodv-12.txt, November 2002.
- [14] J. Yoon, M. Liu, and B. Noble, "Random Waypoint Considered Harmful," In Proc. of IEEE Infocom, Mar-Apr. 2003.
- [15] Weisheng Si and Chengzhi Li, "RMAC: A Reliable Multicast MAC Protocol for Wireless Ad Hoc Networks," In Proc. of the 2004 International Conference on Parallel Processing (ICPP 2004), Aug, 2004.
- [16] S. Gupta, V. Shankar, and S. Lalwani. "Reliable Multicast MAC Protocol for Wireless LANs," In Proc. IEEE ICC'03, May 2003.