Gaurav Sharma, Vaishali Sahu, Prashant Kumar Maurya, Mahendra Srivastava, Ashish Allen Robert / International Journal of Engineering Research and Applications (IJERA)
ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 3, May-Jun 2012, pp.1082-1087

Improved Multicast AODV: A Review

Gaurav Sharma[1], Vaishali Sahu[2], Prashant Kumar Maurya[3], Mahendra Srivastava[4], Ashish Allen Roberts[5]
[1,3,4,5] SSET, SHIATS, ALLAHABAD
[2] MNNIT ALLAHABAD

Abstract
A MANET is a mobile ad-hoc network. It allows mobile nodes to set up a temporary network for instant communication without any fixed infrastructure. Nodes with high mobility exchange information very frequently. Many applications such as video conferencing, video-on-demand services, and distributed database applications require multicast communications. Reliable multicast is one of the basic requirements in a MANET for which better routing protocols have to be developed for disaster management, emergency relief, and mobile conferencing and many other applications. As mobile terminals change its position too, frequently, hence, multicast routes have to be updated frequently. This poses several challenges to provide an efficient multicast routing. In this paper, we have reviewed an Improved Multicast Ad hoc On Demand Distance Vector (IMAODV) protocol based on Adhoc On Demand Distance Vector (AODV) and Multicast AODV (MAODV) protocol to support reliability and multicasting for on-line routing of delivery-guaranteed multicasts. Paper reveals that IMAODV performs better in terms of Packet Delivery Ratio (PDR), average End-to-End delay and Network Routing Load (NRL) compared to both AODV and MAODV.

I. INTRODUCTION
MANET is a mobile adhoc network which is designed temporarily for instant communication without any fixed infrastructure. Many applications like rescue operation, military operations, business meetings, etc. demand for an instant configuration of a network and that can be provided by the MANET. In an adhoc network nodes are not familiar of their network topology. Nodes have to identify the topology. A new node joining the network can show its presence by announcing itself and can listen to other neighbors using the process broadcast. An adhoc network can provide both unicast and multicast type of data transfer. Multicast can be implemented using unicast often termed as Multiple unicast. This process increases the end-to-end delay. Multicast also reduces the data transfer cost for applications which need to send the same data to multiple destinations. It also reduces the channel bandwidth, sender and router processing and delivery delay. However, to an extent multicast can utilize the wireless link efficiently by exploiting the inherent nature of broadcast property [1].

There are number of routing protocols for fixed networks but these cannot be efficiently used for routing purposes in adhoc network since the topology of these networks changes too frequently. However, routing protocol as AODV[2] is used for the data transfer in an adhoc network. AODV uses a broadcast route discovery mechanism [2]. It uses RREPs' and RREQ for path discovery [2].

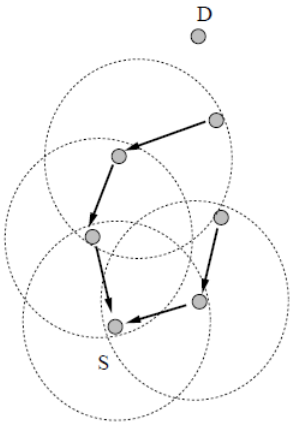

Figure 1. Reverse Path Formation

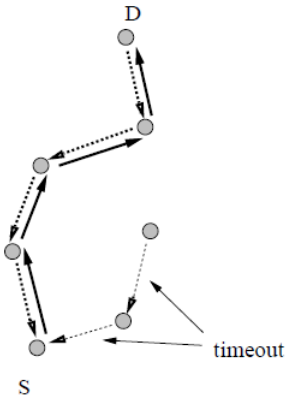

Figure 2. Forward Path Formation

AODV [2] is uniform and destination based reactive routing protocol. It uses table driven routing design work and destination sequence numbers for an on demand protocol. It uses traditional routing tables with one entry per destination. It minimizes the number of required broadcasts, by creating routes on demand basis. For nodes which are not selected in the path, AODV do not maintain any routing information or do not take part in the routing table exchanges. AODV prepares loop free routes. It provides unicast, multicast and broadcast capabilities to all nodes. It disseminates

information about link breakage to its neighboring nodes. In AODV, a routing table expires, if not used recently, thus decreasing the overhead. AODV uses destination sequence numbers to ensure that all routes are loop free and it contains the most recent information. Each node has its own sequence number and broadcast-identifier. The sequence number is used to indicate the latest routing information and to prevent routing loop. All routing packets carry these sequence numbers. The source node includes its own sequence number and broadcast-identifier in the route request and the most recent sequence number for the destination [1]. RERR is used by nodes when the next hop link breaks [2]. MAODV [3] is the multicast extension of AODV. Both AODV and MAODV are routing protocols for ad-hoc networks, with AODV for unicast traffic and MAODV for multicast traffic. It discovers multicast routes on demand. In MAODV, every node maintains two tables, one for unicast routing purpose and other stores the information of multicast routing and path discovery. Every node in a group maintains a multicast table for that particular group[3]. In MAODV, each multicast group has a group leader for that group which maintains and disseminates the sequence numbers to the nodes for the freshness of the information and to prevent loops in the network. Our paper is divided into four sections, we have discussed the introduction in Section I. Section II includes literature review; Section III is about review of the IMAODV. Section IV includes observations of performance parameters for IMAODV. Section V includes future work and finally section VI gives the conclusion.

II. LITERATURE REVIEW

IEEE 802.11was extended as a Round Robin Acknowledgement and Retransmit (RRAR) protocol to improve the reliability of broadcasting [4]. Xie et. al. tested the reliability with PDR and throughput. They introduced the RRAR with ODMRP and shown the improved performance of their protocol. But, the performance of MAODV can still be improved by introducing the acknowledgement from receiver to sender. The sender can resend the data packet if it failed to be delivered correctly. The different performance evaluation parameters can be compared with AODV, MAODV.

Traditional reliable multicast protocols depend on assumptions about flow control and reliability mechanisms, and they suffer from a kind of interference between these mechanisms. This in turn affects the overall performance, throughput and scalability of group applications utilizing these protocols. However, there exists a substantial class of distributed applications for which the throughput stability guarantee is indispensable. Pbcast [5] protocol is a new option in scalable reliable multicast protocols that offers throughput stability, scalability and a bimodal delivery guarantee as the key features. The protocol is based on an epidemic loss recovery mechanism. It exhibits stable throughput under failure scenarios that are common on real large-scale networks. In contrast, this kind of behavior can cause other reliable multicast protocols to exhibit unstable throughput. In this study, Ozkasap et. al. develop an experimental model for Pbcast protocol and virtually synchronous reliable multicast protocols offering strong reliability guarantees. They construct several group communication applications using these protocols on a real system. The aim is to investigate protocol properties, especially the throughput stability and scalability guarantees, in practice. The work has been performed on the IBM SP2 Supercomputer of Cornell Theory Center that offers an isolated network behavior. They use emulation methods to model process and link failures. Ensemble system has been ported on SP2, and a detailed analysis study of Pbcast protocol and its comparison with Ensemble's virtual synchrony protocols has been accomplished.

In [5], they describe experimental study for the protocol and Ensemble's virtually synchronous protocols. The main focus is to investigate and analyze protocol properties, giving attention to stability and scalability, in practice. The experimental work has been performed on the SP2 system of Cornell Theory Center that offers an isolated network behavior. SP2 consists of nodes connected by an Ethernet and a switch. A node is a processor with associated memory and disk. Cornell Theory Center's SP2 system has total 160 nodes that share data via message passing over a high performance two-level cross bar switch. Traditional reliable multicast protocols depend on assumptions about response delay, failure detection and flow control mechanisms. Low-probability events caused by these mechanisms, such as random delay fluctuations in the form of scheduling or paging delays, emerge as an obstacle to scalability in reliable multicast protocols. The reason is as follows. For the reliability purposes, such a protocol requires the sender to buffer messages until all members acknowledge receipt. Since the perturbed member is less responsive, the flow control mechanism begins to limit the transmission bandwidth of the sender. This in turn affects the overall performance and throughput of the multicast group. In effect, these protocols suffer from a kind of interference between reliability and flow control mechanisms. Moreover, as the system size is scaled up, the frequency of these events rises, and this situation can cause unstable throughput.

Based on the results of process group executions, they first examine the throughput behavior of Ensemble's virtually synchronous protocols, then focus on the throughput behavior of Pbcast and also protocol overhead associated with soft failure recovery. During experiments, they varied a number of operating parameters. These are; n: size of process group (8 to 128), f: number of perturbed processes (1to n/4), p: degree of perturbation (0.1 to 0.9).

Study yields some general conclusion about the behavior of basic Pbcast and virtually synchronous multicast protocols. In the first part of the study, focus was on the virtually synchronous Ensemble multicast protocols in the case of soft process failures. They showed that even a single perturbed group member impacts the throughput of unperturbed members negatively. On the other hand, Pbcast achieves the ideal throughput rate even with high percentage of perturbed members. In the second part of the study, they focused on the performance of Pbcast in the case of soft process failures. It is shown [5] that the throughput behavior of Pbcast remains stable as we scale the process group size even with high rates of failures.

An ad-hoc network is the cooperative engagement of a collection of mobile nodes without the required intervention of any centralized access point or existing infrastructure. In [2] Perkin et. al. present Ad-hoc On Demand Distance Vector Routing (AODV), a novel algorithm for the operation of such ad-hoc networks. Each Mobile Host operates as specialized routes, and routes are obtained as needed, that is on demand with little or no reliance on periodic advertisements. This new routing algorithm is quite suitable for a dynamic self starting network, as required by users wishing to utilize ad-hoc networks. This algorithm focuses on, to broadcast discovery packets only when necessary, to distinguish between local connectivity management (neighborhood detection) and general topology maintenance and to disseminate information about changes in local connectivity to those neighboring mobile nodes that is likely to need the information.

It is, however, possible to design a system whereby routes are created on-demand. Such systems must take steps to limit the time used for route acquisition; otherwise, users of the ad-hoc nodes might experience unacceptably long waits before transmitting urgent information. The advantage here is that a smoothly functioning ad-hoc system with on demand routes could largely eliminate the need for periodic broadcast of route advertisements. With the goals of minimizing broadcasts and transmission latency when new routes are needed, they designed a protocol to improve upon the performance characteristics of DSDV in the creation and maintenance of ad-hoc networks.

Although AODV [2] does not depend specifically on particular aspects of the physical medium across which packets are disseminated, its development has been largely motivated by limited range broadcast media such as those utilized by infrared or radio frequency wireless communications adapters. Using such media, a mobile node can have neighbors which hear its broadcasts and yet do not detect each other (the hidden terminal problem). They [2] do not make any attempt to use specific characteristics of the physical medium in our algorithm, nor to handle specific problems posed by channelization needs of radio frequency transmitters. Nodes that need to operate over multiple channels are presumed to be able to do so. The algorithm works on wired media as well as wireless media, as long as links along which packets may be transmitted are available. The only requirement placed on the broadcast medium is that neighboring nodes can detect each other's broadcasts. AODV uses symmetric links between neighboring nodes. It does not attempt to follow paths between nodes when one of the nodes cannot hear the other one; however it may include the use of such links in future enhancements. Some specific features about AODV are nodes store only the routes that are needed [2], AODV avoids problems with previous proposals [2] and has the following need for broadcast is minimized, reduces memory requirements and needless duplications [2], quick response to link breakage in active routes [2], loop free routes maintained by use of destination sequence numbers and scalable to large populations of nodes [2]. AODV is an excellent choice for ad-hoc network establishment. It will be useful in applications for emergency services, conferencing, battlefield communications, and community based networking [2]. They look forward to further development of the protocol for quality of service, intermediate route rebuilding and various interconnection topologies with fixed networks and the Internet.

Zhu et. al. proposed the model for multicast traffic that is extension of AODV, named as Multicast AODV. MAODV [3] is the multicast extension of AODV. Both AODV and MAODV are routing protocols for ad-hoc networks, with AODV for unicast traffic and MAODV for multicast traffic. NS2, a widely used simulation tool, includes a standard implementation of the AODV protocol to analyze its performance, upon which initial MAODV implementations were made. However those implementations face some limitations as only group members can send multicast traffic to the multicast group and the multicast data packets are unicast, resulting in wasted bandwidth. These limitations are avoided in new version of MAODV [3]. It allows each node in the network to send out

multicast data packets, and the multicast data packets are broadcast when propagating along the multicast group tree. Each multicast group has a unique multicast group address. According to the MAODV specification, each multicast group is organized by using a tree structure, composed of the group members and several routers, which are not group member but must exist in the tree to connect the group members, however, [3] states that the group members and the routers are all tree members and belong to the group tree. A group leader is associated with each multicast group, which is responsible for periodically broadcasting Group-Hello (GRPH) messages in the whole network [3]. The group leader also maintains the group sequence number, which is propagated in the network through the GRPH [3]. Each node in the network may maintain three tables. The first one is the Unicast Route Table, recording the next hop for routes to other destinations for unicast traffic. The second one is the Multicast Route Table, listing the next hops for the tree structure of each multicast group. The third table is the Group Leader Table. It records the currently-known multicast group address with its group leader address and the next hop towards that group leader when a node receives a periodic GRPH message.

Proactive connection maintenance feature to the tree maintenance is available in this MAODV implementation [3]. The basic idea is to predict the link breakage time of an active link in the tree before the breakage actually happens, then a new connection, excluding that soon-to-be-broken link, is pro-actively constructed before the old one actually becomes unavailable, in order to avoid the loss of data packets on that link.

Meng et. al. presented a novel Ad hoc On-Demand Vector (AODV) routing protocol based on mobility prediction, named as MAODV[6]. The algorithm controls route discovery, route keeping and route switching according to the distance and mobility estimation of the neighbor nodes. Simulations demonstrate that MAODV reduces the end-to-end delay effectively and enhance the real-time characteristics.

RMAODV [7] describes the reliable use of packet delivery ratio for multicast routing protocol. But it ignored important performance evaluation parameters like NRL and end-to-end delay by increasing the PDR. Further it may increase the end-to-end delay if nodes, which are far away from the existing tree root node, wish to send packets to its multicast group. In the high mobility and large area grid size, the RMAODV also encounters low packet delivery ratio with more end-to-end delay due to the frequent network topological change. Their goal in this work was to overcome such disadvantages and to make it more robust for high mobility ad hoc networks.

III. Review of IMAODV

MAODV [3] has multicasting capability where as IMAODV (Improved Multicast Ad-hoc On Demand Distance Vector) has multicasting and higher reliability in the applications where high mobility rate and large network area are constraints. It is a shared tree based protocol. It builds multicast trees on demand to connect group members from various networks. As nodes join the group, a multicast tree composed of group members is created. Multicast group membership is dynamic, group members have the choice to in and out of the group and group members are routers in the multicast tree. In the case of link breakage, downstream node broadcasts a route request message for repairing the broken link. It responds quickly to link breaks in multicast trees by repairing in time. IMAODV [1] offers some specific features as quick adaptation to dynamic link conditions, has low processing and memory overhead, and low network utilization. These features can result in the form of application in an area where topology of the network changes too frequently, high mobility. IMAODV creates bi-directional shared multicast trees and these trees are maintained as long as group members exist within the connected portion of the network [1]. Each multicast group has a group leader that maintains the group sequence number, which is used to ensure freshness of routing information. The sequence numbers are used to prevent loop in the network. IMAODV [1] enables mobile nodes to establish a tree connecting multicast group members. Multicast trees are established independently in each partition, and trees for the same multicast group are quickly connected if required. However, IMAODV has many features as AODV [2] and MAODV [3]. Every multicast group in IMAODV is identified by its own unique address and group sequence number [1]. If node is not a tree member, it will check its Unicast Route Table to find the next hop for the multicast address. If it has the information, the data packets are forwarded towards the next hop; otherwise, it will send an unsolicited Route Reply (RREP) back to the source node [1]. This make the source node to know about destination is not reachable. If the node itself is a tree member, it will follow its Multicast Route Table to forward the packets. An important feature in IMAODV is Group-Hello Message (GRPH) [1]. These messages are broadcasted throughout the whole network, to indicate the existence of group. When a non-member node receives GRPH first time, it tries to join the group. In the event, where a tree is partitioned

or a group leader revokes its group membership, a new group leader is selected, in the process, each node must update its Group Leader Table to indicate newly elected/ selected group leader.

In IMAODV the multicast data transfer occurs in two different scenarios, first is that when a node wants to send multicast data packets to its multicast group [1] and this node is close to the existing shared-tree root node, it delivers its data packets along the original shared-tree and the second one occurs when a node wants to send multicast data packets to its multicast group and this node is far away from the existing shared-tree root node [1], it initiates a new route discovery. If there exist some potential communication links [8] between any pair of existing nodes which are on the existing tree, and these potential communication links can be used to deliver data from the new source node, they are called forwarding path with respect to the new source node. When a source node that is far away from the group leader, it initiates the new forwarding route discovery; forwarding table will be set up for the nodes that are involved in new route discovery and forwarding path establishment [1]. This new forwarding table [1] contains Source Node IP Address; Next Hops; Group Leader IP Address; Hop Count to Source Node. In the defined forwarding table, source node is the node that initiates a new send and next hops are a list of both the upstream and downstream link nodes. Each next hop contains two fields: next hop IP address and link direction. Link direction is determined upon whether a Forwarding Query Message [1] is received from a requesting node. UPSTREAM indicates receiving and DOWNSTREAM indicates forwarding. Hop Count to Source Node is the number of hops away from source node. If a node is involved in forwarding new data, this forwarding table will be maintained as long as the sending session of the source node continues. After the source node completes its own sending, the forwarding table will be invalidated.

The Query Message consist of destination address, hop count, hop count difference, broadcast identifier, multicast group leader address and the Forwarding Reply Message that contains information like destination address, last hop address, source address, and multicast group leader address. Where destination address is the IP address of multicast group and the hop count is the number of hops that current node is away from the source node. Hop count difference is the distance of the responding node from the last node on the shared multicast tree. Broadcast identifier is used to identify the RREQ each time it is generated by a source node [1]. The source address is the address of the initiating source node. To establish new forwarding path within the near area of the existing shared tree to reduce the average end-to-end delay and therefore, the new route discovery will be exploited when a node that is far away from the group leader wants to send data [1].

In IMAODV, the existing shared tree established by the group leader is maintained for use such as grafting a new branch, pruning an existing branch, forwarding data packets that originated from the group leader or nodes close to group leader, and repairing a broken link [1]. When a link along the forwarding path breaks, the node downstream of the break is responsible for repairing the link which is very much similar to MAODV. The downstream node initiates the repair by broadcasting a RREQ with source address set to the new source node. When a node on the new forwarding tree receives the RREQ, it can reply to the RREQ by unicasting a RREP back to the initiating node. RREP forwarding and subsequent route activation with the MACT [1] message are handled similarly as in MAODV.

It will test for reliability [1] of packet delivery.

[1] Considered that more the Packet Delivery Ratio more is the reliability and implement an Acknowledgement- Retransmit mechanism to ensure correct delivery of the data packets at the receiver node. If the data packet could not be delivered or get delayed, the sender node will not get the acknowledgement from the receiver within a pre-specified time quantum and will be retransmitted again. In case of failure in the transmission, the data packet will be retransmitted once again and this approach improves the packet delivery ratio and reliability as compared with MAODV. The performance of IMAODV [1] is evaluated on the basis of parameter as PDR, End-to-End Delay, and NRL.

Packet Delivery Ratio (PDR): It is defined as the ratio of number of data packets forwarded from a particular node to the number of data packets converging to that node. It is a measure of reliability. If PDR is more, network and data transfer is more reliable.

End-to-End Delay: It is measured as the time elapsed when a multicast packet is sent from a node and is successfully received by all the multicast group members. It includes all possible delays, as delay for route discovery, interface queuing transmission delays, and propagation and transfer times of data packets.

Normalized Routing Load (NRL): The number of route control packets per data packet delivered at destinations. Normalized Routing Load is important to compare the scalability of the routing protocols, the adaption to low bandwidth environments. Sending more routing packets also increases the probability of

packet collision and can delay data packets in the queues.

IV. OBSERVATIONS

A simulation [1] is done in network simulator (NS2) to compare the performance of IMAODV with AODV and MAODV on the basis of parameters as PDR, End-to-End delay, and NRL. With respect to end-to-end delay [1], it is observed, that AODV performs well as compared to IMAODV and MAODV. This is very obvious, since multicast includes number of receivers which increases the delay. However, IMAODV [1] works better than MAODV.

The same is the case with NRL [1], AODV is better than multicast protocols, but IMAODV performs better than MAODV. The main observation is PDR, which is directly related to the reliability, IMAODV is better than both AODV and MAODV protocols for all possible combinations of scenarios [1].

V. FUTURE WORKS

From the observations, we enlighten that IMAODV [1] ensures better reliability by providing more PDR for broadcasting and multicasting purposes. However, for the applications such as audio or video conferencing, the delay is too high. So we plan to modify the IMAODV [1] such that it can be compatible to AODV in terms of End-to-End Delay, to support the services, where delay cannot be tolerated.

VI. CONCLUSION

Reliability is an important aspect for data transfer in MANET and the condition become much important in multicasting. IMAODV provides the better PDR as compared to AODV and MAODV, thus it is more reliable and can be used for applications such as broadcasting and multicasting, but in terms of NRL and delays, it is not comparable to AODV. However, it can be concluded that IMAODV protocol is suitable for reliable and time sensitive multicasting in MANET environment.

Refernces::

1. Srinivasa Sethi and Siba Udagata, “IMAODV: A Reliable and Multicast AODV Protocol for MANET. IEEE 2009
2. Perkin CE and EM Royer, “Ad Hoc on demand distance vector routing”, Proceeding of 2nd IEEE Workshop, Mobile Computing, System Applications, pp:90-100, 1999.
3. Yufang Zhu and Thomas Kunj, “MAODV Implementation for NS-2.26”, Systems and Computer Engineering Carleton University Technical Report SCE-04-01, January 2004.
4. Xie, A. Das, S. Nandi and A. K. Gupta, “Improving the Reliability of IEEE 802.11broadcast scheme for multicasting in mobile and ad hoc networks”, IEEE, Proceeding of Communication, volume 153, No. 2, pp. 207-212, April 2006.
5. Oznur Ozkasap Kenneth P. Birman, “Throughput Stability of Reliable Multicast Protocols”, T Yakhno (Ed.): ADVIS 2000 LNCS 1909, pp. 159-169, 2000.
6. Liming Meng, W Fu, Z Xu, J Zhang and J Hua, “A Novel Ad Hoc routing protocol based on mobility prediction”, Information Technology Journal, vol. 7(3), pp. 537-540.
7. Sun Baolin, Li Layuan, “On the reliability of MAODV in Ad Hoc Networks” Proceeding of IEEE International Symposium on Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications, Vol. 2, pp. 1514-1517, 2005.
8. Ziping Liu and Bidyut Gupta, “A Modified shared-tree multicast routing protocol in Ad-Hoc network”, Journal of Computing and Information technology (CIT), vol. 13 no. 3, pp. 177-193, 2005.