Asian Journal of Information Technology 5(8): 877-883, 2006
Medwell Online, 2006

Implementation of Gossip on ODMRP for Wireless Ad-Hoc Network

P. Latha and R. Ramachandran
Sathyabama Institute of Science and Technology, Deemed University, Chennai, India

Abstract: This study analyses the issue of reliability and to propose a scalable method to improve packet delivery of multicast routing protocols and also to reduce the variation in the number of packets received by different nodes. Multicast protocols that have been proposed provide no reliability guarantee and not suitable when the network topology undergoes frequent changes. Gossip technique has been proposed to construct scalable and reliable multicast protocols. Gossip is well matched to the needs of adhoc networks because it is a controlled form of flooding, propagating the messages without congesting the wireless medium and is independent of topology. So the anonymous gossip technique can be implemented on any of the existing multicast routing protocol in order to improve the reliability and scalability. The proposed work implements the anonymous gossip over the multicast routing protocol ODMRP. The implementation consists of two phases. In the first phase, On Demand Multicast Routing Protocol (ODMRP) is used to multicast a message to the group member, while in the second phase the gossip protocol tries to recover lost messages. When a gossip message is received by a group member, the group member checks information in the message to detect if it is missing some messages. A retransmission request for missing messages is sent directly to the gossip message sender called as gossip push. An alternate technique is gossip-pull method, wherein a gossip sender informs all members of its gossip subgroup about all messages it is missing. Members of a gossip subgroup of a group member can be chosen at random, or from the neighborhood of the group member. This study shows that the packet delivery of ODMRP has been significantly improved .Also the variation in number of packets delivered is decreased .The performance is also analyzed by means of varying the performance metrics.

Key words: Gossip, reliability, multicast, ODMRP

INTRODUCTION

Several multicast routing protocols like AODV[1], ODMRP[2], AMRIS[3], MCEDAR[4] multicast by means of building either a tree or mesh .However maintenance of these tree or mesh pays additional cost and also not suitable for adhoc network .since routes changes very rapidly and the methods used by these protocols are consequently not available to us. Also these protocols do not attempt to ensure packet delivery and packet loss. Gossip is suitable to the needs of ad-hoc networks because it is a controlled form of flooding .Messages are slowly propagated through the network without congesting the wireless medium - and is independent of topology. use a Gossiping mechanism] is used to improve multicast reliability in ad hoc networks. It doesn't reduce the number of messages sent., but rather use the unreliable multicast protocol to multicast a message. They then use gossiping (under the assumption that routes are known) to randomly exchange messages between nodes in order to recover lost messages. Gossip based adhoc routing[5] is nothing but , each node forwards a message with some probability, to reduce the overhead of the routing protocols.This study implements the anonymous gossip on ODMRP which does not require a group member to have any knowledge of the other group members and also the simulation results of[6-7] shows that ODMRP has performed well with respect to throughput and control overhead.

OVERVIEW OF ODMRP

Mesh Creation: ODMRP is a mesh-based, rather than a conventional tree-based, multicast scheme and uses a forwarding group concept (only a subset of nodes forwards the multicast packets via flooding). It applies on-demand procedures to dynamically build routes and maintain multicast group membership. By maintaining and using a mesh instead of a tree, the drawbacks of multicast trees in mobile wireless networks (e.g., intermittent connectivity, traffic concentration, frequent tree reconfiguration, non-shortest path in a shared tree, etc.) are avoided. A soft-state approach is taken to maintain multicast group members.

Corresponding Author: P. Latha, Sathyabama Institute of Science and Technology, Deemed University, Chennai, India

In ODMRP[2], group membership and multicast routes are established and updated by the source on demand. On-demand multicast routing protocol comprise a request phase and reply phase. When a multicast source has packets to send but no route and group membership is known, it floods a control packet with data payload attached. This packet, called "Join Data" is periodically broadcasted to the entire network to refresh the membership information and update the routes. When a node receives a Join Data packet, it stores the source ID and the sequence number to its "Message Cache" to detect duplicates. The upstream node ID is inserted or updated as the next node for the source node in its "Routing Table." If the Join Data packet is not a duplicate and the Time-To-Live value is greater than zero, appropriate fields are updated and it is rebroadcast.

When a Join Data packet reaches the multicast receiver, it creates and broadcasts a "Join Table" to its neighbors. When a node receives a Join Table, it checks if the next node ID of one of the entries matches its own ID. If it does, the node realizes that it is on the path to the source and thus is part of the forwarding group; it sets the FG_FLAG. It then broadcasts its own Join Table built upon matched entries. The next node ID field is filled in by extracting the information from its routing table. This way, the Join Table is propagated by each forward group member until it reaches the multicast source via the selected path. This process constructs (or updates) the routes from sources to receivers and builds a mesh of nodes, the forwarding group.

After this group establishment and route construction process, sources can multicast packets to receivers via selected routes and forwarding groups. While outgoing data packets exist, the source sends Join Data every REFRESH_INTERVAL. This Join Data and Join Table propagation process refreshes forwarding group and routes.

When receiving the multicast data packet, a node forwards it only when it is not a duplicate and the setting of the FG_FLAG for the multicast group has not expired. This procedure minimizes the traffic overhead and prevents sending packets through stale routes.

Adapting the refresh interval via mobility production: ODMRP requires periodic flooding of Join Data to build and refresh routes. Excessive flooding, however, is not desirable in ad hoc networks because of bandwidth constraints. Furthermore, flooding often causes congestion, contention and collisions. Finding the optimal flooding interval is critical in ODMRP performance. In highly mobile networks where nodes are equipped with GPS (e.g., tactical networks with tanks, ships, aircrafts, etc.), we can efficiently adapt the REFRESH_INTERVAL to mobility patterns and speeds by utilizing the location and movement information. Note that ODMRP can still operate efficiently in networks where no such information is available, but the protocol can be further improved if those information can be utilized.

The location and movement information to predict the duration of time routes will remain valid. With the predicted time of route disconnection, Join Data are only flooded when route breaks of ongoing data sessions are imminent.

Routing table: A routing table is created on demand and is maintained by each node. An entry is inserted or updated when a non-duplicate Join Data is received. The node stores the destination (i.e., the source of the Join Data) and the next hop to the destination (i.e., the last node that propagated the Join Data). The routing table provides the next hop information when transmitting Join Tables.

Forwarding group table: When a node is a forwarding group node of the multicast group, it maintains the group information in the forwarding group Table. The multicast group ID and the time when the node was last refreshed are recorded.

Message cache: The message cache is maintained by each node to detect duplicates. When a node receives a new Join Data or data, it stores the source address and the sequence number of the packet. Note that entries in the message cache need not be maintained permanently. Schemes such as LRU (Least Recently Used) or FIFO (First In First Out) can be employed to expire and remove old entries and prevent the size of the message cache to be extensive.

Unicast routing capability: One of the major strengths of ODMRP is its unicast routing capability. Not only ODMRP can work with any unicast routing protocol, it can function as both multicast and unicast. Thus, ODMRP can run without any underlying unicast protocol.

OPERATION

Forwarding group setup: When a multicast source has data a packet to send but no route is known, it originates a "Join Data" packet. The Type field MUST be set to 01. TTL MAY be set to TIME_TO_LIVE_VALUE, but SHOULD be adjusted based on network size and network diameter. The Sequence number MUST be large enough to prevent wraparound ambiguity and the Hop Count is initially set to zero. The source puts its IP address in the

Source IP Address and Last Hop IP Address field. It appends its location, speed and direction into JOIN DATA.

When location and movement information is utilized, it sets the MIN_LET (Link Expiration Time) field to the MAX_LET_VALUE since the source does not have any previous hop node. When the source receives Join Tables from multicast receivers, it selects the minimum RET (Route Expiration Time) among all the Join Tables received. Then the source can build new routes by originating a Join Data before the minimum RET approaches (i.e., route breaks of ongoing data sessions are imminent).

Processing a join data: When a node receives a Join Data packet

- Check if it is a duplicate by comparing the combination with the entries in message cache. If duplicate, then discard the packet.
- If it is not a duplicate, insert an entry into message cache with the information of the received packet and insert/update the entry for routing table (i.e., backward learning).
- If the node is a member of the multicast group, it originates a Join Table packet with the RET value enclosed.
- Increase the Hop Count field by 1 and decrease the TTL field by 1.
- If the TTL field value is less than or equal to 0, then discard the packet. DONE.
- If the TTL field value is greater than 0, then set the node's IP Address into Last Hop IP Address field and broadcast. DONE.

Originating a join table: A multicast receiver transmits a "Join Table" packet after selecting the multicast route. Each sender IP address and next hop IP address of a multicast group are contained in the Join Table packet. The route expiration time is also included if the network hosts operate with GPS.

Processing a join table
When a join table is received:

- The node looks up the Next Hop IP Address field of the received Join Table entries. If no entries match the node's IP Address, do nothing. DONE.
- If one or more entries coincide with the node's IP Address, set the FG_FLAG and build its own Join table. The next hop IP address can be obtained from the routing table.
- Broadcast the Join Table packet to the neighbor nodes. DONE.

Passive acknowledgments: The reliable transmission of Join Tables plays an important role in establishing and refreshing multicast routes and forwarding groups. Hence, if Join Tables are not properly delivered, effective multicast routing cannot be achieved by ODMRP. The IEEE 802.11 MAC protocol, which is the standard in wireless networks, performs reliable transmission by retransmit ting the packet if no acknowledgment is received. However, if the packet is broadcasted, the acknowledgments and retransmissions are not sent. In ODMRP, the transmissions of Join Tables are mostly broadcasted. When a node transmits a Join Table packet to the immediate upstream node of the route, the immediate downstream node can hear the transmission if it is within the transmitter's radio range. Hence, the packet is used as a "passive acknowledgment." We can utilize this passive acknowledgment to verify the delivery of Join Tables. Multicast sources must send active acknowledgments to the previous hops since they do not have any next hops to send Join Tables to unless they are forwarding group nodes. When no acknowledgment is received within the timeout interval, the node retransmits the message. If packet delivery cannot be verified after an appropriate number of retransmissions, the node considers the route to be invalidated. The node then broadcasts a message to its neighbors specifying that the next hop to the source cannot be reached. Upon receiving this packet, the neighboring node builds and unicasts the Join Table to its next hop if it has a route to the multicast source. If no route is known, it simply rebroadcasts the packet specifying the next hop is not available.

In both cases, the node sets its FG_FLAG. The FG_FLAG setting of every neighbor may create excessive redundancy, but most of these settings will expire because only necessary forwarding group nodes will be refreshed in the next Join Table propagation phase.

ANONYMOUS GOSSIP PROTOCOL

Gossip as a general technique has been used to solve a number of problems such as network news dissemination (NNTP), replicated data management and failure detection. Bimodal multicast[8] uses gossip as a technique to achieve probabilistic reliability of multicast in wired networks. Anonymous Gossip protocol[9] achieves a bimodal guarantee i.e., all or no delivery withvery high probability and partial delivery with very low probability, without sacrificing scalability and stable throughput (low jitter). Gossip is used to address the problem of reliable multicast in mobile ad-hoc networks and provide all or no delivery with very high probability and partial delivery with very low probability.

A gossip based reliable multicast protocol involves two phases. In the first phase, any suitable unreliable protocol (ODMRP) is used to multicast the message *m*, to be sent to the group. In the second phase, gossip is used to recover lost messages from other members of the group that might have received it. This phase consists of periodically repeated gossip rounds in the background as more and more messages are multicast. A single gossip round can potentially recover many lost messages. A single round of gossip consists of the node A choosing a member B to send the information about the messages it received, B checks to see if it has received any of the messages listed by A and exchange messages between A and B which are not a part of each other's message history.

AG does not require any member to know the other members of the multicast group. The node attempting to send a gossip message does not even know the identity of the node with which it will gossip until the other node sends back a gossip reply. The gossip message consists of the address of the multicast group , the address of the node sending the gossip message, sequence numbers of messages that the source node believes it has lost, the size of the Lost Array and the sequence number of the next message that the source expects.

Each node randomly selects one of its neighbors and sends a gossip message to it. Any node receiving a gossip message randomly selects one of its neighbors (excluding the neighbor which sent the message) and propagates the message to it. If the receiving node is itself a member of the multicast group then it randomly decides to either accept the gossip or propagate it. The accepting node then unicasts a gossip reply to the initiator of this gossip request. The reply is described in later section. In a general multicast protocol of an ad-hoc network, the nodes themselves participate as routers. Also, only a subset of these nodes/routers would participate in routing any messages meant for a given multicast group. Only participating routers are to be considered while propagating the gossip message. For example, in the implementation of this protocol on ODMRP, only the routers in the multicast tree participate in propagating the gossip. Each router maintains a multicast route table which constitutes the next hops for this router. While propagating the gossip message, one of these next hops is randomly selected. Propagation along the multicast tree prevents gossip messages from reaching the same node twice.

Periodic propagation of gossip messages generates continuous traffic on the network. Hence a scheme is chosen in such a way that gossip takes place locally with a very high probability and with distant nodes occasionally in order to reduce the network traffic. AG protocol is augmented to achieve this optimization. We require each node participating as a router in the multicast tree to maintain one additional field called nearest member. In the implementation over ODMRP, the multicast route table is augmented to have the nearest member field associated with a next hop contains the distance to the nearest group member from this node by taking the link through this next hop node. This adds very little overhead to the existing multicast route table. Whenever a gossip message is received, a next hop node is chosen so that a next hop with a smaller nearest member value is chosen with higher probability than a next hop with a larger nearest member value.

The gossip message propagates only along the multicast tree in the implementation of AG over ODMRP, although other potentially shorter routes may exist between the gossiping members the return path is unaffected by this phenomenon, because gossip replies are unicast. It is efficient to use the unicast routes to gossip with those nodes whose membership is already known. Also these unicast routes may be available for gossip even when the multicast tree is being repaired. This is achieved by a member cache in all the member nodes of each multicast group. The member cache is a bounded buffer containing the address of a group member, the shortest distance between the nodes and the time at which last gossip occurred between these two nodes. The member cache table is updated each time a message is received from a group member. This message could be a data packet meant for this group, a gossip reply, or any other maintenance packet.

Information exchange: A pull mode of message exchange is followed in the implementation of AG over ODMRP. Each node maintains a table called lost table, for every multicast group that it belongs to and it contains the sequence numbers of all the messages this node believes itself to be lacking.

An entry in this table will be made whenever a message is received with a sequence number greater than the expected sequence number. The sequence number is a 2 tuple including the sender address and a sequence number. Each node also maintains a bounded FIFO buffer, called history table containing the most recent messages received. The most recent entries of the lost table are placed in a lost buffer. Whenever a node prepares a gossip message, the lost buffer and a list of expected sequence numbers is added to the gossip message. When a node receives a gossip message, it compares the lost buffer and the expected sequence number list to see if its history table has a copy of any message sought by the

gossip initiator. It then unicasts any message found back to the gossip initiator as the gossip reply.

Anonymous gossip over ODMRP: The issue of improving the packet delivery of multicast routing protocol in mobile adhoc network proposes a reliable protocol Anonymous Gossip Protocol (AGP) implemented over On Demand Multicast Routing Protocol (ODMRP), a mesh based protocol.

This protocol proposes a method by knowing the group membership on sending join query request and getting join reply message from the interested member nodes. Even if the mesh size increases the number of neighbor nodes also increases because of the AG gossips with a randomly chosen neighbor nodes. After multicasting the message loss identification of the packets are identified by comparing the sequence number of the received packet between the nodes and if any packet is not matched then that particular packet will be retransmitted to the victim node through the intermediate node by the source node.

SIMULATION

Simulation of Anonymous gossip technique on on-demand multicast routing protocol is performed using Java[10]. Snapshots produced during the simulation of multicasting a message by the ODMRP and the recovery of lost messages by Anonymous gossip was shown. Figure 1-5 illustrates the various stages in the implementation of AG over ODMRP. Figure 1 shows the nodes placed at random viz, member nodes, non-member nodes and source node. Figure 2 shows the packet loss occurred in second node after the transmission of packets from the source node. Figure .3 illustrates a lost message from node 3 and also it indicates the lost packet.. So far ODMRP has been used to multicast a message and the packets that have been lost have been indicated. Figure 4. represents the recovery phase in which the packets lost have been recovered using AGP.

Simulation environment: All the nodes were initially placed in a fixed area and allowed to move randomly. This study has the assumption of the network consisted of a single multicast group . All the nodes which are green in color are member nodes and the nodes which are violet in color is differentiated as a non member node. The node which is ash in color is the source node which multicast a message. The nodes which joined the group at the beginning of the simulation will not leave and remain through out the simulation.

Fig, 1: Source node is ash in color, member node is green, non member node is violet

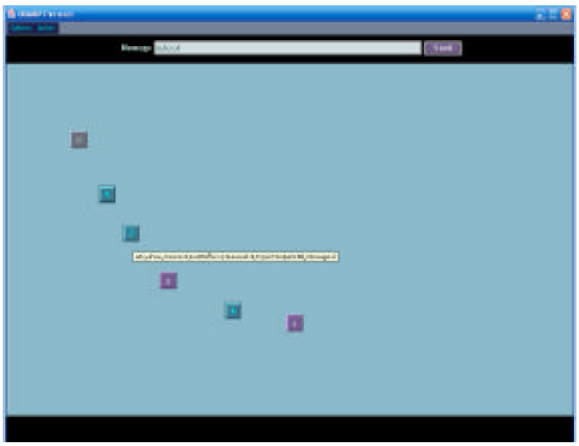

Fig. 2: Shows the packet loss occurred in second node.

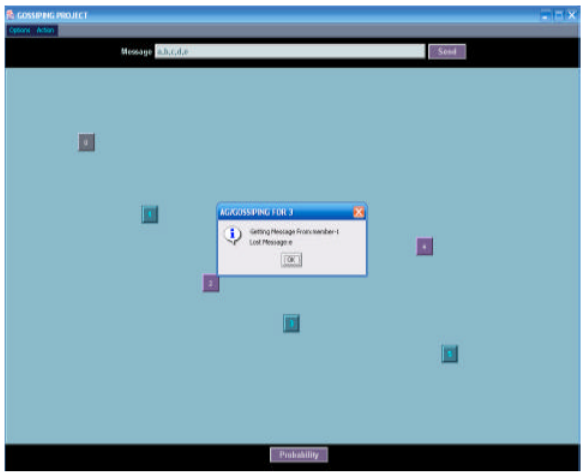

Fig. 3: Getting a lost message from node 3 and also showing the lost packet

Fig. 4: Showing all the packets are recovered successfully using the anonymous gossip protocol.

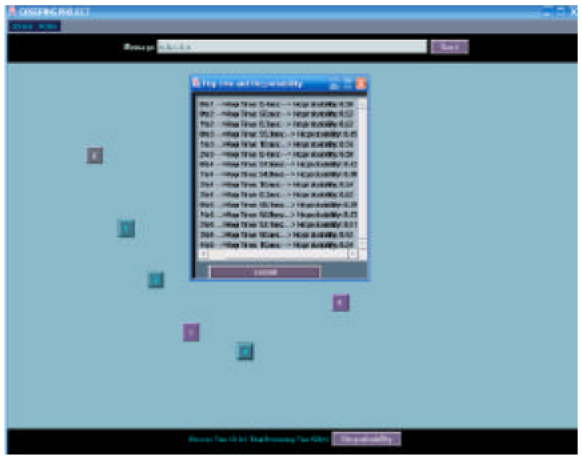

Fig. 5: Showing the heuristic probability for all the routes along the time taken to reach the packets between the nodes.

The transmission range is constant. The maximum number of nodes considered for simulation is 40.

Performance analysis: The performance metrics are analysed in the simulation of anonymous gossip over ODMRP by varying the packets delivered with the number of nodes. The packet delivery of ODMRP has been increased. Figure 6 illustrates the variation of packet delivery with increase in the number of nodes. The number of nodes was varied from 5 to 40.The routing distance between the nodes goes up, as the number of nodes in the network increases. As the number of nodes increases, the packet delivery slightly decreases. Figure 7 depicts the variation in the number of nodes with heuristic probability.

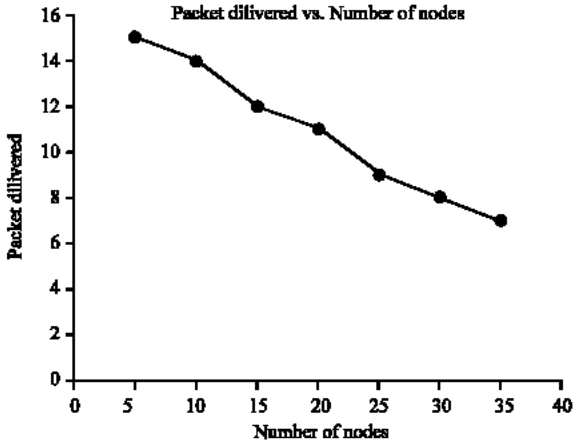

Fig. 6: Number of nodes vs Packet delivery

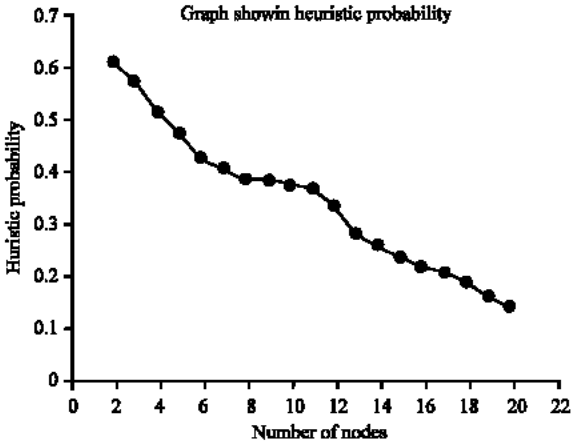

Fig. 7: Number of nodes vs heuristic probability

CONCLUSION

In this study we performed the simulation of anonymous gossip over ODMRP without making any significant changes to existing multicast protocol ODMRP[8]. As a future work , gossip technique can be implemented on MCEDAR and AMRIS. The present study demonstrates the information dissemination through out the network. This may increase the network traffic and congestion may occur. Selective information dissemination can be achieved with any existing multicast protocol. The efficiency and scalability of the protocol itself can be improved. In the context of selective information dissemination ,content based dissemination[12] and location based dissemination has to be considered in order to improve the reliability and scalability.

REFERENCES

1. Perkins, C., E. Royer, S. Das, 2000. Ad-Hoc On Demand Distance Vector (AODV) Routing. IETF Internet Draft, draft-ietf-manet-aodv-05.txt.
2. Lee, S.J., M. Gerla and C.C. Chiang, 1999. On-Demand Multicast Routing Protocol(ODMRP)" Proceedings of IEEE WCNC'99, pp: 1298-1304
3. Chun-Wei Wu, Y.C. Tay, 1999. AMRIS: A Multicast Protocol for Ad-Hoc Wireless Networks". Proceedings of MILCOMM '99.
4. Prasun, S., R. Sivakumar and V. Bhargavan, 1999. MCEDAR: Multicast Core-Extraction Distributed Ad-Hoc Routing". Proceedings of IEEE Wireless Communications and Networking Conference.
5. Li, L. J. Halpern and Z. Haas, 2003. Gossip-based ad hoc routing. In Proceedings of INFOCOM'02, 2002.[50] Y. Sasson, D. Cavin and A. Schiper. Probabilistic broadcast for flooding in wireless mobile ad hoc networks. In IEEE Wireless Comm. and Networking Conference (WCNC, 2003).
6. Kunz, T. and E. Cheng, 2002. On-Demand Multicasting in Ad-Hoc Networks: Comparing AODV and ODMRP. in Distributed computing systems. Vienna: IEEE Computer Society.
7. Lee, S.J., *et al*., 2000. A Performance Comparison Study of Ad Hoc Wireless Multicast Protocols. in Computer communications; IEEE INFOCOM 2000. Tel Aviv, Israel: IEEE.
8. Kenneth, P.B., M. Hayden, O. Ozkasap, Z. Xiao, M. Budiu and Y. Minsky, 1999. Bimodal Multicast. ACM Transactions on Computer Systems, 17: 41-88.
9. Chandra, R., V. Ramasubramanian and K. Birman, 2001. Anonymous gossip: Improving multicast reliability in mobile ad-hoc networks. In Proc. 21st International Conference on Distributed Computing Systems (ICDCS), pp: 275-283.
10. http://java.sun.com/products.
11. Lee, S.J., W. Su and M. Gerla, 1999. On-Demand Multicast Routing Protocol (ODMRP) for Ad Hoc Networks,. Internet-Draft, draft-ietf-manet-odmrp-01.txt, Work in progress
12. Zhou, H. and S. Singh, 2000. Content based multicast (cbm) for ad hoc networks. In Mobihoc.