ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Reliable Data Delivery for Highly Dynamic MANETs Using Adaptive Demand Driven Multicast Routing Protocol (ADMR)

[I]Durkadevi K, [II]Maragatharajan M, [III]Balakannan S.P
[I,II,III]Dept. of IT, Kalasalingam University, Krishnankoil, India

Abstract
In highly dynamic mobile ad hoc networks, there exist transmission problems such as delivering data packets, packet delay, time delay, node mobility and so on, particularly in large scale networks. The existing Position-based Opportunistic Routing (POR) protocol makes use of the stateless property of Geographical routing and the broadcast environment of wireless medium. But this protocol is prone to over heading problem as well as lack of data confidentiality. To overcome this problem, the proposed protocol is Adaptive Demand Driven Multicast Routing Protocol (ADMR) has been designed specifically for use in the ad hoc network environment. ADMR, source-based forwarding trees are created whenever there is at least one source and one receiver in the network. Senders are not required to announce their intention to start or stop sending data to the cluster, or to affix the group to that they need to send. Receivers vigorously adapt to the sending pattern of senders and mobility in the network in order to efficiently balance overhead and maintenance of the multicast routing state as nodes in the network move or as wireless transmission conditions in the network change. ADMR also detects when mobility in the network is too high to efficiently maintain multicast routing state.

Keywords
POR, ADMR, Mobile ad hoc network, Multicast Routing, Geographical routing, Opportunistic routing

I. Introduction

A mobile ad-hoc network (MANET) may be a [1] self-configuring infrastructure less network of mobile devices connected by wireless. Every device in a MANET is liberal to move severally in any direction, and can so amendment change its links to different devices frequently. Every node should forward traffic unrelated to its own use, and so be a router. The first challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks might operate by themselves or could also be connected to the larger Internet. MANETs are a unit of wireless ad hoc networks that typically has routable networking environment on top of a Link Layer ad hoc network. The network is specific as a result of it doesn't believe a preexisting infrastructure, like routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, every node participates in routing by forwarding information for alternative nodes, and then the determination of that node forward data is created dynamically supported the network Connectivity. Additionally to the classic routing, ad hoc networks will use flooding for forwarding the data. An ad hoc network usually refers to any set of networks wherever all devices have equal standing on a network and are free to associate with any other ad hoc network devices in link range.

Due to node mobility in traditional topology-based MANET routing protocols [2], Position based mostly routing protocols are achieved, since the network is very dynamic. Maintaining a route is tough in fastly changing network topology. If the path breaks, data packets will get lost and discovery procedures will be time consuming. Dynamically Ad hoc routing protocols make forwarding decisions based on geographical position of a packet's destination. Instead of destination node's position, every node has to know only its own position and therefore the position of its neighbors to forward the packets. When the network is highly dynamic, position-based routing is used. In position based routing a sender can know the present position of the destination. In mobile ad hoc networks (MANETS), geographic routing protocols permit stateless routing. A geographic routing protocol uses the location information of mobile nodes. It has high scalability. Without complex modification to MAC protocol, a position-based opportunist routing is achieved. IEEE 802.11 provides collision avoidance. This scheme uses the advantage of greedy forwarding and opportunist routing.

This POR protocol [3] could collects the data to the all neighboring nodes and send it. And single channel are going to be performed, whenever the link failure is happens best forwarder doesn't forwards the packets then suboptimal candidates as transmit the packets in certain period of time. Here some of the required reliable information is delivered, when a packet loss is occurred.

II. Problem Statement

This paper mainly contributes the problem of data delivery in highly dynamic mobile ad hoc network. The main characteristic of ad hoc network is node mobility. Maintaining a route is difficult one, because of fast changing network topology. Position based opportunistic routing protocol is working well for the network is highly dynamic.POR protocol which takes the advantage of stateless property of broadcast nature.

The POR is designed at based on geographic routing and opportunistic forwarding. In geographic routing uses the location information of mobile nodes. In POR protocol greedy forwarding algorithm is used. Greedy forwarding tries to bring the message closer to the destination in each step using only native information. Thus every node forwards the message to the neighbor that's best suited from a neighborhood purpose of read. The most appropriate neighbor will be the one who minimizes the distance to the destination in every step that node is termed as greedy node. Greedy forwarding will lead into a dead end, wherever there is no neighbor nearer to the destination. If the best forwarder fails to transmit the packet at intervals a particular time, the other candidate that fashioned in the vicinity an order may transmit the packet. So the transmission won't be interrupted, since there are some candidates to transmit packets. POR's first-rate robustness is achieved by exploiting potential multipath on the fly, on a per packet basis. The POR overcomes the limitation of the traditional opportunistic routing and it provides advantages over the system in data delivery in the highly dynamic MANET system. But in terms of packet over heading and security the POR fall miserably

and the system achieves considerable loss.

III. Adaptive Demand Driven Multicast Routing

Adaptive Demand-Driven Multicast Routing protocol [4] (ADMR), a new on-demand multicast routing protocol for wireless ad hoc networks that attempts to reduce as much as possible any non-on demand components among the protocol. In ADMR, source-based forwarding trees are created whenever there is a minimum of one source and one receiver within the network.

ADMR also detects when mobility within the network is just too high to permit timely multicast state setup and maintenance, without requiring GPS or other positioning information or additional control traffic. When such high mobility is detected, ADMR temporarily switches to flooding of every data packet, and after a short time, the protocol once more makes an attempt to operate efficiently with multicast routing, because the mobility within the network may have decreased.

The novel features of ADMR include:

- ADMR uses no periodic network wide floods of control packets.
- ADMR adapts its performance based on application sending pattern.
- Bursty sources are handled.
- ADMR can detect high mobility without the use of GPS or other positioning information.

A. Data Structures

The multicast forwarding state for ADMR is maintained locally by each node within the following three tables:

1. Sender Table

Logically contains one entry for every multicast group address that this node is an active sender. Every entry within the Sender Table includes the current inter-packet time for this node sending to the group, and a count of consecutive keep-alive packets sent to the group since the last data packet sent to the group by this node.

2. Membership Table

Logically contains one entry for every combination of multicast group address and sender address that this node is either a receiver member or a forwarder. Every entry within the Membership Table includes a flag to point if this node may be a receiver, a flag to point if this node may be a forwarder, the current inter-packet time for the sender sending to this group, and the current value of the keep-alive count from packets received for the group.

3. Node Table

Logically contains one entry for every other node in the network from that this node has received a tree flooded or network flooded ADMR packet. Every entry within the Node Table includes the sequence number from the ADMR header of the foremost recent such packet, and a bitmap representing a number of previous sequence numbers of packets from this sender, used to detect and discard duplicate packets throughout a flood: if the bit corresponding to some sequence number during this bitmap is set, the packet is assumed to be a duplicate; all sequence numbers prior to that corresponding to the first bit within the bitmap are also assumed to be duplicates (or are of no any interest and are discarded). This use of a bitmap is similar to the data structure suggested for anti-replay protection within the IP Security protocols [5]. Every entry in the Node Table additionally includes the previous hop address, taken from the MAC-layer sending source address of the packet received from this sender with this sequence number that contained the minimum hop count in its ADMR header. To manage space in the Node Table, new entries ought to be created only as needed and existing entries ought to be retained in an LRU fashion.

B. Multicast Packet Forwarding

Any packet with a multicast or broadcast destination address containing an ADMR header will be flooded. The type of flooding is indicated by the flood type flag in the packet's ADMR header. For most packets, the flood type flag is set to cause a tree flood of the packet, such that the packet will be forwarded only among those nodes belonging to the multicast forwarding tree indicated by the source address (the original sender) and destination address (the multicast group address) in the packet (Figure 2).

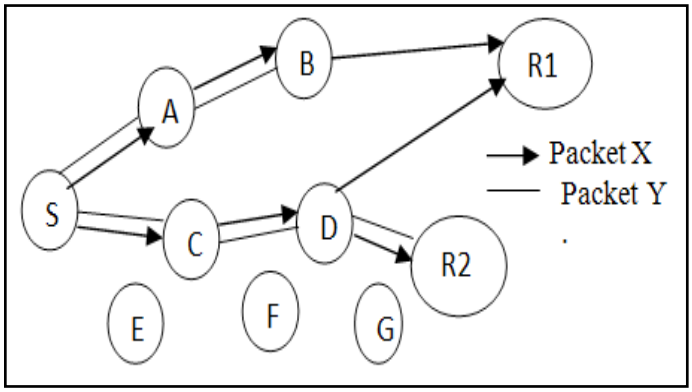

Fig. 1: Multicast data Packet Forwarding

When a node receives such a packet, it checks its Membership Table entry for this group and source to determine if it should forward the packet; the packet thus flows along the tree from the sender to the group receivers but is not constrained to follow specific branches in the tree and is thus able to automatically be forwarded around temporarily broken links or failed forwarding nodes in the tree (Figure 1). If, instead, the flood type flag in the ADMR header indicates a network flood for the packet, the packet will be flooded among all nodes. For either type of flood, each node's Node Table and the sequence number in a packet's ADMR header reliably limit any node that should forward the packet to do so at most once.

The flood of a packet constrained to the nodes in the multicast forwarding tree as a tree flood, and to the more general type of flood of a packet through all nodes as a network flood (Figure 2). This use of flooding within the multicast forwarding tree is similar to the "forwarding group" concept introduced in the FGMP protocol [6] and used also in ODMRP [7], except that our forwarding state is specific to each sender rather than being shared for the entire group. When a sender using ADMR sends a multicast packet, it floods within the multicast distribution tree only towards the group's receivers, whereas with FGMP or ODMRP, the packet also floods back towards any other senders that are not receivers. Although this difference requires us to maintain source-specific state in forwarding nodes, such state is required anyway in order to support the source-specific multicast service model [8]. In addition, even FGMP and ODMRP require source-specific state at each node, since they must detect duplicate packets during a flood within the forwarding group, and any type of packet identifiers used for this duplicate detection when there may be multiple group senders

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

must be source-specific.

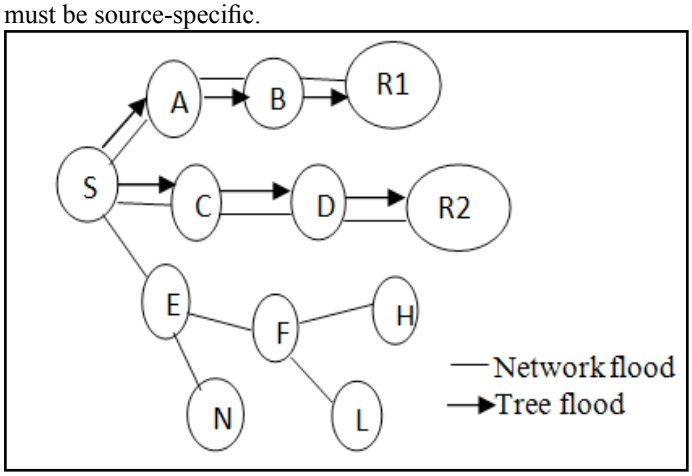

Fig. 2: Tree flood Vs Network flood

C. New Multicast Source

When a node S originates a multicast packet for some group G for which it is not currently an active sender, it will not have a Sender Table entry for G. In this case, node S creates and initializes a new Sender Table entry for G. The inter-packet time in this entry may be set to a default value, may be assumed based on the IP port numbers used in the packet, or may be specified by the sending application if an API is available for this purpose.

After sending this packet, node S buffers for a short time subsequent multicast packets that it might originate to group G, rather than sending them immediately as they are generated, in order to allow the routing state in the network to be formed for receivers interested in this group and sender. Once S receives at least one RECEIVER JOIN packet, S then begins sending any buffered packets to the group as normal multicast packets. The packet exchange which takes place when a new source becomes active is depicted in Figure 3. Most subsequent multicast packets for group G from node S will be flooded only within the members of the multicast forwarding tree established for this group and sender (a tree flood). However, it is possible that some interested receivers did not receive this initial packet from S. To allow for such occurrences, node S uses a network flood rather than a tree flood for certain of its subsequent existing multicast data packets.

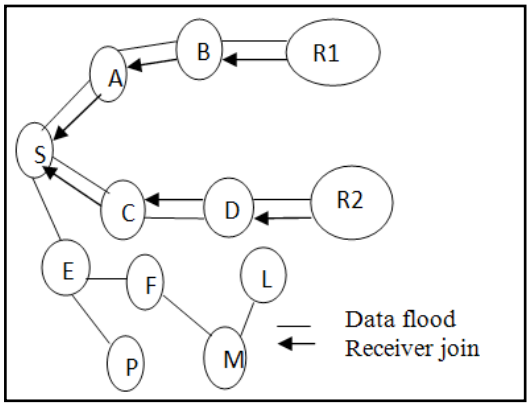

Fig. 3: New Source S

the time between each packet selected to be sent as a network flood is increased until reaching a slow background rate, designed to tolerate factors such as intermittent wireless interference or temporary partition of the ad hoc network.

D. Tree Pruning

Each forwarder node in the multicast forwarding tree for group G and source S automatically expires its own state and leaves the tree when it determines that it is no longer necessary for multicast forwarding. Similarly, the multicast source S automatically expires its state and stops transmitting multicast data packets when it determines that there are no downstream receiver members of the group for this source; the sender continues to send certain of its subsequent

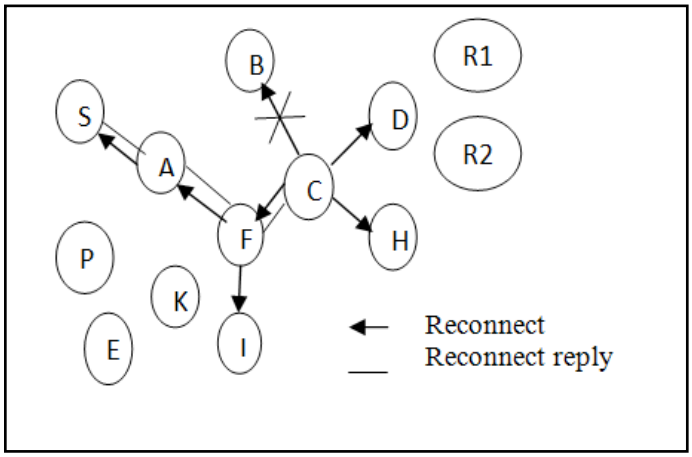

Fig. 4: Source S Responds with Reconnect Reply

multicast packet as infrequent background network flood packets, but otherwise defers sending other multicasts for this group until receiving at least one new RECEIVER JOIN packet, as described in Section III.C.

IV. Simulation Results

The experimental results show the simulation result of the Qos parameters such as Throughput, Packet Delivery Ratio, Delay, Data delivery are achieved with their X Graph using NS2. In ADMR protocol performance results shown in bellow.

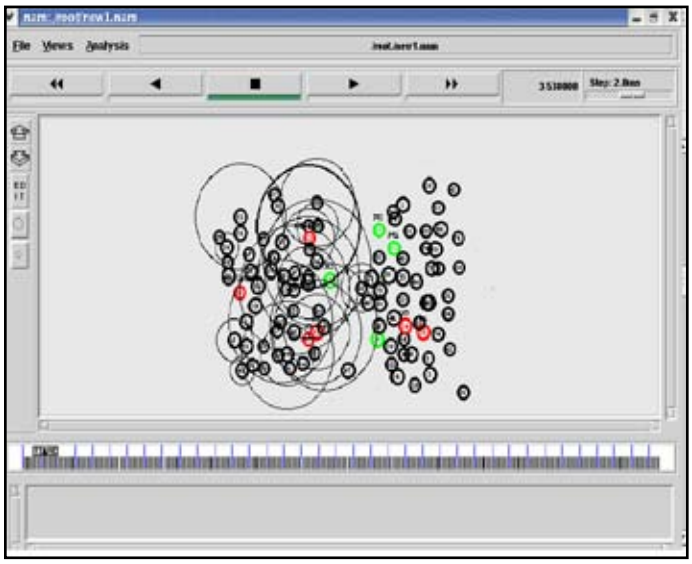

Fig. 5: Data Delivery

The above Figure describes the selection of forwarding nodes for data transmission in a dynamic time. The mobile nodes are mainly used for this transmission.

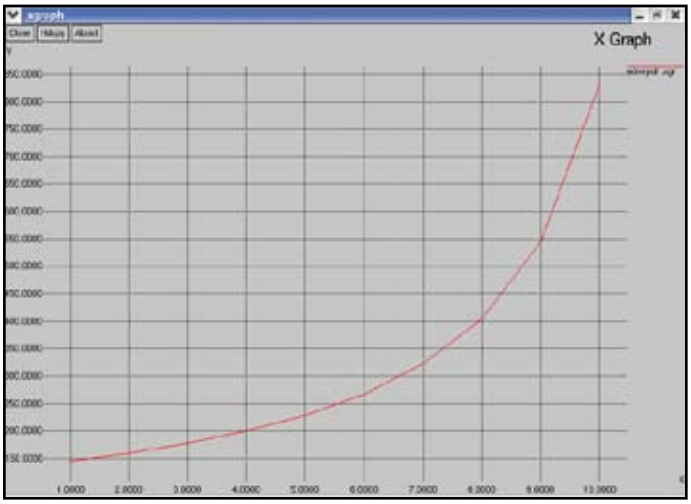

Fig. 6: Packet Delivery Ratio

The above Figure we can see the packet delivery ratio that can be calculated by taking into consideration of the ratio of the number of data packets received at the destination(s) to the number of data packets sent by the source(s).

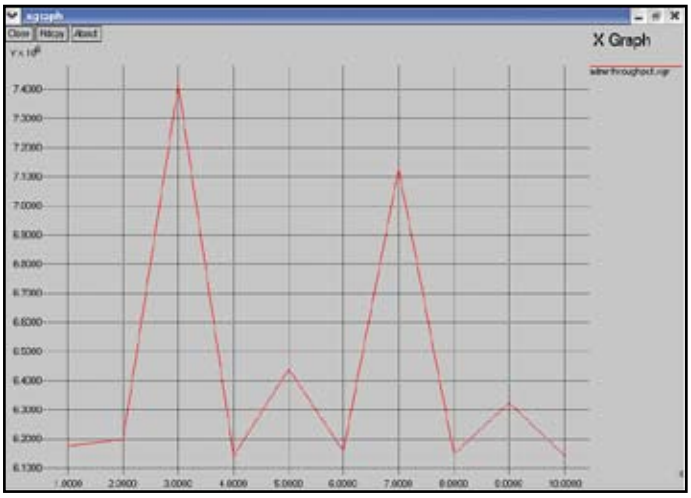

Fig. 7: Throughput

The above Figure we can see the throughput that can be calculated by the amount of data moved from one node to another in a certain period of time.

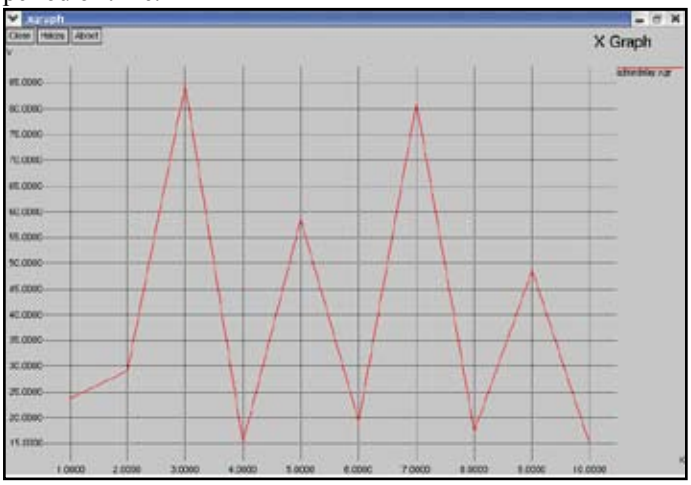

Fig. 8: Delay

The above Figure we can see the Delay that can be calculated by the interval time between sending by the source and receiving by the destination node.

V. Conclusion

The proposed multicast routing protocol Adaptive Demand Driven multicast Routing Protocol [ADMR] transmits a packet from source node to transmits a packet to the destination and it moves to the destination node without communication voids were analyzed by using NS2. By using this protocol the lack of security problem has been found in the previous methods of data delivery will be overcome and the accuracy of data delivery has been increased. The ADMR Protocol provides good packet delivery and reduce duplicate relaying and reduces time delay compare to existing system with using POR.

References

[1] *S.Sharon Ranjini, G.ShineLet, "Position-based Opportunistic Routing for Highly Dynamic MANETS" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 2, February 2013.*

[2] *Karthikeyan.R, Sasikala.K, Reka.R, "A Survey On Position – Based Routing In Mobile Ad Hoc Networks" International Journal of P2P Network Trends and Technology (IJPTT) -Volume3Issue7-August 2013.*

[3] *M. Chandrika , N. Papanna," Comparison and Simulation of POR and E-POR Routing Protocols in MANETs" International Journal of Computer Science and Mobile Computing IJCSMC, Vol. 2, Issue. 5, May 2013, pg.425 – 429.*

[4] *J. G. Jetcheva and D.B.Johnson, "Adaptive Demand driven Multicast Routing in multi-hop wireless ad hoc network," Second Symposium on Mobile Ad Hoc Networking and Computing, pp.33-44,2001.*

[5] *M. Scott Corson and Anthony Ephremides. A Distributed Routing Algorithm for Mobile Wireless Networks. Wireless Networks, 1(1):61–81, feb 1995.*

[6] *C.-C. Chiang, M. Gerla, and L. Zhang, (1998a):" Forwarding Group Multicast Protocol (FGMP) for multihop, mobile wireless networks,"ACM-Baltzer Journal of Cluster Computing, vol. 1, no. 2, pp. 187–196.*

[7] *Sung-Ju Lee, Mario Gerla, and Ching-Chuan Chiang "On demand multicast routing protocol" Wireless Adaptive Mobility Laboratory, Computer Science Department. University of California Los Angeles, CA 90095-1596*

[8] *J.J. Garcia-Luna-Aceves and E.L. Madruga. A Multicast Routing Protocol for Ad-HocNetworks. In Proceedings of the IEEE Con on Computer Communications, INFOCOM 99, pages 784–792, March 1999.*

[9] *Hugh Holbrook and Brad Cain. Source-Specific Multicast for IP. Internet-Draft, draft-holbrook-ssm-arch-01.txt, November 2000. Work in progress.*

[10] *IEEE Computer Society LAN MAN Standards Committee. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std 802.11-1997. The Institute of Electrical and Electronics Engineers, New York, New York, 1997.*

[11] *Jorjeta G. Jetcheva, Yih-Chun Hu, David A. Maltz, and David B. Johnson. A Simple Protocol for Multicast and Broadcast in Mobile Ad Hoc Networks. Internet-Draft, draft-ietf-manet-simple-mbcast-01.txt, July 2001. Work in progress.*

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Author Profile

Durkadevi.K was born in virudhunagar, Tamilnadu, India. She received the B.Tech Degree in Information Technology from Sree Sowdambika college of Engineering, Aruppukottai in 2012. Pursuing M.Tech (IT) in Department of Information Technology Kalasalingam University, Krishnankoil-626126. She was interested in the area of Adhoc Network.

Maragatharajan M received his BE degree in Electronics & Communication Engineering from Anna University by 2007. He has received his Master degree in Information Technology from Kalasalingam University, 2010. He has worked as a Project Associate in TIFAC CORE in Network Engineering, Kalasalingam University from 2007 to 2008. Currently He is working as a Assistant Professor in the department of Information Technology, Kalasalingam University. His areas of interest are Adhoc Networks, Wireless Networks and Network Security.

Balakannan S.P received his Ph.D degree in the department of Electronics and Information Engineering at Chonbuk National University, South Korea (2010). He has received his master degree (5 years integrated) in department of Computer Science and Engineering in the year 2003, from Bharathiar University, India. He has worked as a Project Assistant in Indian Institute of Technology (IIT), Kharagpur, India from 2003 to 2006. Currently he is working as Assistant Professor in the Department of Information Technology at Kalasalingam University, Tamilnadu, India. His area of interest includes Wireless Network, Network Coding, Cloud & Green Computing, Cryptography, and Mobile Communication.