©gopalax -International Journal of Technology And Engineering System(IJTES):
Jan –March 2011-

Counter Measures Against Multicast Attacks on Enhanced-On Demand Multicast Routing Protocol In Mobile AD-HOC Networks

Aishwarya .K[1], Kannaiah Raju .N [2] and Senthamarai Selvan .A[3]

1P.G. Student, M.E .CSE Department of CSE, AMACE, Vadamavandal- 604410
aishumecse@gmail.com
2Assistant Professor, Department of CSE, AMACE, Vadamavandal- 604410
kanniya13@hotmail.com
3 Assistant Professor, Department of CSE, AMACE, Vadamavandal- 604410
senselvana@gmail.com

***Abstract*— A Mobile Ad-hoc Networks (MANETs) is composed of Mobile Nodes without any infrastructure. Mobile Nodes self organize to form a network over radio links. A multicast routing protocol are faced with the challenge of producing multi-hop routing under host mobility and bandwidth constraint. In addition, within a wireless medium, it is even more crucial to reduce the transmission overhead and power consumption. Multicasting can be used to improve the efficiency of the wireless link when sending multiple copies of messages to exploit the inherent broadcast property of wireless transmission. The multicasting plays an important role in MANETs. The Enhanced-On Demand Multicast Routing Protocol (E-ODMRP), a mesh based multicast routing protocol which retains all of the advantages of the On-Demand Multicast Routing Protocol (ODMRP) such as high packet delivery ratio under high mobility and high throughput. Moreover it significantly reduces the control overhead, one of the main weaknesses of ODMRP, under the presence of multiple sources. The objective of this paper is to develop a secured multicast network, which will be tolerant to the attacks that are currently present in the multicast Mobile Ad-hoc Networks and for that studying the various vulnerabilities present in E-ODMRP, a mesh based multicast routing protocol and simulate the suitable attacks like flooding attack, black hole attack and put forth a defence mechanism to improve packet delivery ratio, number of control packets and average throughput.**

***Keywords*— E-ODMRP, MANET, Multicasting Routing Attack, Black hole and Flooding attack**

I. INTRODUCTION

A Mobile Ad-hoc Network or MANET[1] is defined as a wireless network of mobile nodes communicating with each other in a multi-hop fashion without the support of any fixed infrastructure such as base stations, wireless gateways or access points.[4] For this reason, MANETs [1]are also called infrastructure less or non-infrastructure wireless networks. The term ad-hoc [6] implies that this network is a network established for a special, often extemporaneous service customized to specific applications. Manets enable wireless networking in environments where there is no wired or cellular infrastructure; or, if there is an Infrastructure, it is not adequate or cost effective. The absence of a central coordinator and base stations makes operations in MANETs [1] more complex than their counterparts in other types of wireless networks such as cellular networks or wireless local area networks.

II . E-ODMR PROTOCOL

E-ODMRP an enhanced version of ODMRP with adaptive refresh. Adaptation is driven by receivers' reports on link breakages rather than mobility prediction. And the adaptive refreshing mechanism is seamlessly integrated with a simple and unified" (i.e., combined) local recovery and receiver joining scheme. As the time between refresh episodes can be quite long, a new node or a momentarily detached node might lose some data while waiting for the route to it to be refreshed and reconstructed. Upon joining or upon detection of a broken route, a node performs a local route recovery procedure instead of flooding to proactively attach itself to a forwarding mesh or to request a global route refresh from the source. Compared to ODMRP [2], a slightly lower packet delivery ratio might be expected in E-ODMRP in light load since the new scheme uses packet loss as a indicator of a broken link. The major advantage is reduced overhead (by up to 90%) which translates into a better delivery ratio at high loads.

A. ODMRP

On Demand Multicast Routing Protocol (ODMRP)[2] is a multicast routing protocol for mobile ad hoc networks. Its efficiency, simplicity, and robustness to mobility render it one of the most widely used MANET multicast protocols. At the heart of the ODMRP's robustness is the periodic route refreshing. ODMRP rebuilds the data forwarding “mesh" on a fixed interval and thus the route refresh interval is a key

parameter that has critical impact on the network performance. If the route refresh rate is too high, the network will undergo too much routing overhead wasting valuable resources. If it is too low, ODMRP cannot keep up with network dynamics resulting in packet losses due to route breakages. In this paper, we present an enhancement of ODMRP with the refresh rate dynamically adapted to the environment. E-ODMRP compares favourably with other published multicast schemes.

B. ENHANCED ODMRP with Motion Adaptive Refresh

Creating a Forwarding Mesh by Source Initiation Same as the original ODMRP, a forwarding mesh structure between sources and receivers is initiated by a source. When a new source has data to transmit to a multicast group, it starts with flooding the entire network with the first data packet piggybacking the control/signalling information. We refer to the first data packet as the Join Query packet for convenience hereafter. Upon reception of the first, non duplicate, Join Query packet, every node sets pointers to its upstream node, i.e. the sender of the Join Query packet, and rebroadcasts it. Once the Join Query reaches a receiver, the receiver sends a Join Reply packet back towards the source. The Join Reply is relayed by the intermediate nodes all the way to the source following the pointers set when the Join Query was propagated through the network. The intermediate nodes which have relayed the Join Reply become the forwarding group (or mesh). All nodes in the forwarding mesh are collectively in charge of delivering multicast data to receivers and achieve such goal by transmitting non-duplicate data packet once. A source refreshes the forwarding mesh, i.e., floods the Join Query, on variable-interval schedules and the interval can vary from the prefixed minimum to maximum values. The initial creation of the forwarding mesh is the same for ODMRP and E-ODMRP but the nodes' behaviour in the mesh is quite different due to the difference in the mesh maintenance mechanism. All nodes in the E-ODMRP mesh, intermediate and leaf nodes, forward received non-duplicated data packets. The leaf nodes' data forwarding is to implement the passive acknowledgement (ACK) which is a general mechanism widely used in various MANET protocols for various reasons. In the data packet's header, there is a field indicate the packet sender's upstream node. By overhearing every data packet transmission and from the field in the packet, a node can know whether its transmission was a success and whether it is a valid forwarder, that is, some node is actually receiving data from it. Forwarders in the E-ODMRP mesh do not have the forwarder life-time whereas ODMRP's forwarder has a timeout which is a parameter usually set to 3 times the refresh interval. In ODMRP forwarder nodes discharge themselves when the forwarding state expires by a timeout. In E-ODMRP [2], intermediate nodes forward data packets as long as downstream receivers exist otherwise they prune themselves. Nodes realize whether receivers exist in the downstream sub-tree using the passive ACK mechanism.

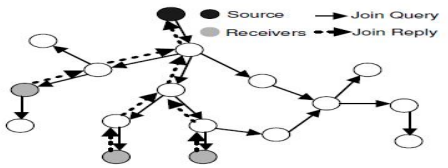

Figure. 2.1 E-ODMRP mesh construction: Join Query and Join Reply

C. Receiver Joining

When a receiver wants to join a multicast group, it performs a local search to graft onto the existing multicast mesh. The receiver broadcasts a Receiver Join packet first with limited Time-To-Live (TTL). When a Listener node, defined to be a neighbour of any forwarder or receiver nodes, receives a Receiver Join packet, it sets itself up as a Temporary Forwarder and immediately starts forwarding data packets. While Temporary Forwarders forward next several non-duplicate packets, the receiver chooses one of them as a regular forwarder being part of the forwarding group. Other Temporary Forwarders clear their status and go back to Listeners.

The Receiver Join packet's TTL is 1 in E-ODMRP, but disconnected node can grab into a forwarding mesh that is 2 hops away due to the definition of the Listener. In Figure 2.2 (a), node A wants to join the multicast mesh and transmits a Receiver Join packet. Upon receiving the Receiver Join, Listeners, node B and C, relay next several packets. In Figure 2.2 (c), node B becomes a Forwarder and node A is connected to the forwarding mesh. Therefore, E-ODMRP's Local Recovery scheme performs the same effect as other protocols' local recovery that a recovery control packet travels up to 2 hops. If such a local search fails, the disconnected receiver floods a Refresh Request packet. Sources, if exist, will receive the packet and refresh the multicast forwarding group by flooding with a Join Query packet. When multiple receivers simultaneously issue Refresh Request floods, huge traffic overhead occurs through the network. It may degrade protocol performance to waste resources and block other traffics. To prevent this harmful network wide flooding, E-ODMRP nodes relay only one of such Refresh Request packets when multiple receivers broadcast Refresh Request packets in a short time frame, i.e., a minimum refresh time

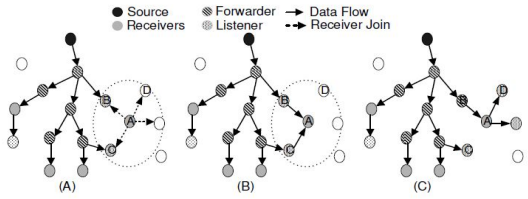

Figure. 2.2 Illustration of receiver join/local recovery process

(Dotted circles denote the same distances.) Node A wants to join the forwarding mesh, so node A floods the Receiver Join packet. Node B, and C hear it and set themselves up as Temporary Forwarders. (b) Now node B and C transmit a packet to the node A, but node D cannot. (c) Node A chooses the node B as a upstream node. Node C goes back to a Listener due to Temporary Forwarder timeout. The node D becomes a Listener since it overhears data transmission from the node A. In other words, a node relays the first Refresh Request packet and drops any other Refresh Request packets arrived within a short time period even though they have been generated by different nodes. If timeout occurs without receiving any data packet, the receiver refloods the Refresh Request. If timeout occurs again, it waits for the next Join Query without flooding since it means that the network is completely divided or there is no source. If a forwarder or a listener wants to join a multicast group, it simply updates its status as a receiver without the joining process.

D. Detecting a Link Break and a Local Recovery

An intermediate node or a receiver can be disconnected from the mesh due to mobility. For unicast transmission, detection of a broken route is fairly easy and provided by the MAC layer. If a node does not return a MAC layer ACK, the link incident on the node is considered to be broken. But in multicast, a link break should be detected in different ways since MAC broadcast has no ACK. ADMR monitors the traffic to detect malfunctioning links. We take a similar approach. Assuming that traffic is frequent enough to serve as indicator for any route break, each source estimates its own inter packet arrival time and informs receivers by recording it in Join Query packets. Based on source's value, each node calculates and updates own inter packet arrival time until receiving the next Join Query. If a node in the mesh does not receive any data during a multiple of the packet arrival interval e.g., 5 times arrival interval in our simulation, the node considers itself to be detached from the mesh and performs the recovery procedure. It is the same as the receiver join process except sending a Dummy packet. When the node receives a Receiver Join packet from a parent node, it generates a Dummy packet and transmits to a sub-tree to prevent recovery explosion. Nodes received the Dummy packet wait for a next packet without a local recovery. However, they start the local recovery, if they have timeout without receiving a new packet. A source generates the Dummy packet when no packet is coming from the application. All nodes in the mesh wait without the local recovery. If timer expires again, the source re-sends the Dummy packet. Upon receiving the second Dummy packet from the source, all nodes in the multicast group realize that the data transmission sends and they remove information related to the multicast group by the next timeout. During the route refresh and the recovery period, the forwarder mesh becomes larger since new forwarders are emerged. Though redundant data forwarding leads to high delivery ratio, it also generates high overhead that may degrade performance. Pruning removes unnecessary data forwarding using the passive ACK scheme. As mentioned earlier, in the every data packets, the address of the next-hop to the upstream direction is written. Each node records upstream and downstream node's addresses in its Multicast Routing Table to be explained in the next section that is updated and maintained during the route refresh and the recovery process. Intermediate nodes overhear packet transmission from the downstream nodes so that they can confirm whether their transmission is valid by checking the recorded address in the packet. Thus each sent packet serves as a passive ACK eliminating any explicit control packet. If a forwarder misses several passive ACKs continuously, it prunes itself from the mesh. Though the passive ACK removes unnecessary forwarding, the overhead may be still high since all nodes including the leaf nodes in the mesh forward packets. To reduce the overhead, a passive ACK suppression technique is employed in the leaf nodes. The leaf nodes forward packets after short delay whereas intermediate nodes forward as soon as receiving packets. If a leaf node receives duplicated packets during the short delay, it skips sending a passive ACK for this packet since another receiver may send a passive ACK or the leaf node may change a upstream forwarder due to mobility.

III . ATTACKS AND ITS COUNTER MEASURES

The different types of attacks involved in this project are:

1.Flooding Attack

2.Black hole Attack

A. Black hole Attack

A black hole attack is one in which a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. This attack aims at modifying the routing protocol so that traffic flows through a specific

node controlled by the attacker. The attacker drops the received messages instead of relaying them as the protocol requires. Therefore the quantity of routing information available to other nodes is reduced. The attack can be accomplished either selectively or in bulk. Selective dropping means dropping packets for a specified destination or a packet every‘t’ seconds or a packet every ‘n’ packets or a randomly selected portion of packets. Bulk attack results in dropping all packets. Both result in degradation in the performance of the network. [6]

B. Black hole Problem in E-ODMRP

E-ODMRP is an important on demand routing protocol that creates routes only when desired by the source node. E-ODMRP does not include any provisions for security and hence it is susceptible to attacks .When a node requires a route to a destination it initiates a route discovery process within the network. Any malicious node can interrupt this route discovery process by claiming to have the shortest route to the destination thereby attracting more traffic towards it. For example, source A wants to send packets to destination D, in fig.3.1, source A initiates the route discovery process. Let M be the malicious node which has no fresh route to destination D. M claims to have the route to destination and sends join reply JREP packet to S. The reply from the malicious node reaches the source node earlier than the reply from the legitimate node, as the malicious node does not have to check its routing table like the other legitimate nodes. The source chooses the path provided by the malicious node and the data packets are dropped. The malicious node forms a black hole in the network and this problem is called black hole problem..

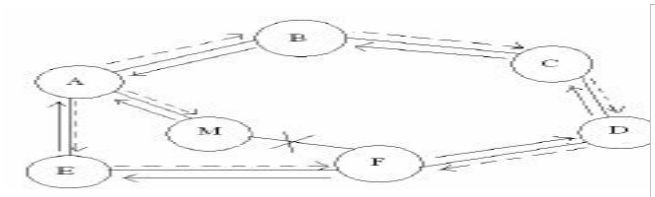

Figure 3.1 Black hole attacks

A-Source node, M-Malicious node D-Destination node - - - - JREQ ____ JREP

C. Solution to the Black hole Attack

Source node in E-ODMRP does not accept every first RREP but calls Pre_ReceiveRREP (Packet p) which stores all the RREPs in the newly created(EODMRP_RREP_Tab) table till ODMRP_WAIT_TIME. Then it analyses all the stored RREPs from EODMRP_RREP_Tab table and discards the RREP having exceptionally high destination sequence number. The node that sent this RREP is suspected to be the malicious node. EODMRP maintains the identity of the malicious node as Mali_node [6] so that in future it can discard any RREPs from that node. Now since malicious node is identified the routing table for that node is not maintained and also control messages from the malicious node will not be forwarded in the network. EODMRP_RREP_Tab is flushed once an RREP is chosen from it. Our solution after detecting the malicious node acts as normal EODMRP by accepting the RREP with lower destination sequence number.

D. Pseudo code for black hole attack solution:

```
At Source Node: E-ODMRP
    Pre_ReceiveRREP (Packet P){
                        t0 = get(current time value)
 Set timer (t0 + EODMRP_WAIT_TIME)
till timer expires Store P.Dest_Seq_No and
P.NODE_ID in EODMRP_RREP_Tab table
aftertimerexpireswhile(EODMRP_RREP_Tabisnotemp
ty){
Select Dest_Seq_No from table
                    if(Dest_Seq_No>>>=Src_Seq_No){
                     Mali_Node=Node_Id
                    discard entry from table
select Packet q for Node_Id having
            lowest value of Dest_Seq_No
            ReceiveRREP(Packet q)
```

E.stimulation and results

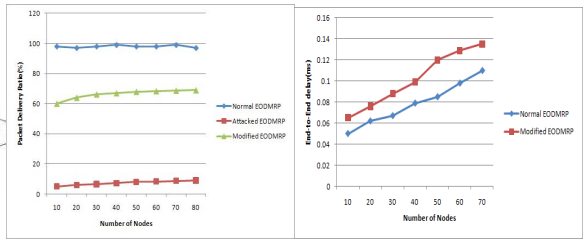

Figure3.2 black hole attack

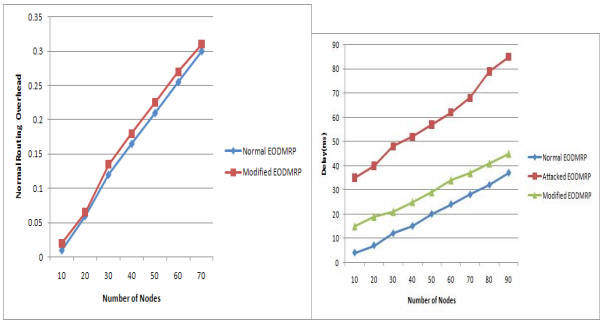

Figure3.3 black hole attack

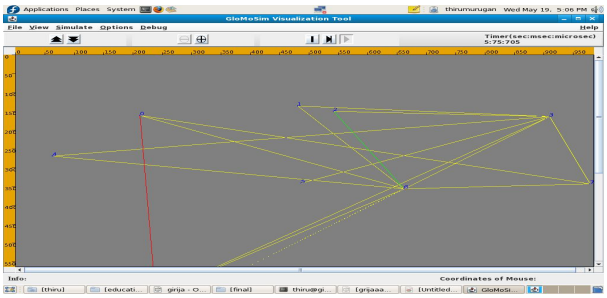

Figure 3.4 stimulation result

IV. CONCLUSION AND FUTURE WORK

The development in computing environments, the services based on ad hoc networks have been increased. Wireless ad hoc networks are vulnerable to various attacks due to the physical characteristic of both the environment and the nodes. blackhole attack solution inclusion of EODMRP_WAIT_TIME variable and DMRP_RREP_Tab table, helps us to suspect malicious node. From the experimental results, it shows that the solution achieves a very good rise in PDR (Packet Delivery Ratio). The solution we have proposed have decreased the delay to a greater extent .The future work is aimed at extending the solutions we have proposed to the other proactive protocols by actively changing the implementation techniques and to some reactive protocols as well.

V. REFERENCES

[1] Luo Junhai, Ye Danxia, Xue Liu and Mingyu, " A Survey of Multicast Routing Protocols for Mobile Ad-Hoc Networks", IEEE Communications Surveys & Tutorials, vol.11 No. 1,First Quarter 2009.

[2] Y. O. Soon, J.-S. Park, and M. Gerla, "E-ODMRP: Enhanced ODMRP with motion adaptive refresh," in Proc. ISWCS, 2005, pp. 130–134.

[3] Bounpadith Kannhavong, Hhidehisa Nakayama, Yoshiaki Nemoto and Nei Kato, "A survey of routing attacks in mobile ad hoc networks",IEEE Wireless Communications on October 2007.

[4] Patroklos G. Argyroudis and Donal O'Mahony, "Secure Routing For Mobile Adhoc Networks", IEEE Communications Surveys & Tutorials, Third Q5] M. Gerla, S. J. Lee, and W. Su, "On-demand multicast routing protocol (ODMRP) for ad-hoc networks," Internet draft, draft-ietf-manet-odmrp-02.txt, 2000.

[5] N. H. Mistry, D. C. Jinwala and M. A. Zaveri, "MOSAODV: Solution to Secure AODV againstBlackhole Attack", (IJCNS) International Journal of Computer and Network Security, Vol. 1, No. 3, December 2009

[6] Saman Desilva ,RajendraV. Boppana, " Mitigating Malicious Control Packet Floods in Ad Hoc Networks", IEEE Communications Society/WCNC 2005.