Efficient and Secured Multicasting over Mobile Ad-Hoc Networks

Thenmozhi S[1], Anitha G[2]
[1]ECE, *Sri Krishna College of Technology, Tamil Nadu, India,* s.thenmozhi@skct.edu.in
[2]ECE, *Sri Krishna College of Technology, Tamil Nadu, India*, g.anitha@skct.edu.in

***Abstract* – Now-a-days group communications are playing a vital role in Mobile Ad hoc Networks. An efficient method for implementing group communications is multicasting. However, it is a big challenge to implement efficient and secured multicast in MANETs due to the mobility of the nodes, limited resources, difficulty in group membership management and multicast packet forwarding. This has lead to the development of alternative protocols. In this paper a virtual-zone-based structure is formed to implement scalable and efficient group membership management. MANETs are easily prone to a number of security threats. Black hole attack is one of the severe security threats which can be easily employed by exploiting the vulnerability of on- demand routing protocols. An Intrusion Detection System (IDS) is designed to detect the malicious nodes. The efficiency and security of the protocol is evaluated through simulations and quantitative analysis.**

***Keywords*—multicast, Mobile Ad Hoc Networks, protocol, security, black hole attack, IDS.**

I. INTRODUCTION

Multicasting is different from unicasting and broadcasting. Unicasting is a one-one communication. Broadcasting is one-to-all communication. Whereas multicasting is the transmission of packets from a single node to many nodes (one-to-many) or between many nodes (many-to-many). There are astounding interests and importance in supporting multicasting over Mobile Ad Hoc networks. Some of the applications include the exchange of messages among a group of committee members in an office, and the support of multimedia games and teleconferences. Multicast is an efficient method to realize group communications, with a one-to-many or many-to-many transmission. Yet, there is a big challenge in enabling efficient multicasting over Mobile Ad Hoc networks.

Generally there are two types of multicast routing protocols in wireless networks - Tree-based multicast routing protocol and mesh based multicast routing protocol [7]. The tree-based protocols (e.g. MAODV [9], AMRIS [11], MZR [2] and MZRP [13], establish and maintain a shared multicast routing tree to deliver data from a source to receivers of a multicast group. But the structure can be highly unstable in multicast ad-hoc routing protocols, as the network is dynamic.

The mesh-based protocols (e.g., FGMP [1], CAMP [4], and ODMRP [5]) are proposed to enhance the robustness with the use of redundant paths between the source and the destination pairs. Multicast protocols generally do not have good scalability due to the overhead incurred for route searching of the destination, group membership management, and creation and maintenance of the tree/mesh structure over the Network.

II. RELATED WORK

For MANETs, geographic routing protocols have been proposed in recent years for more scalable and robust packet transmissions. The existing routing protocols generally assume that nodes are aware of their own positions through certain positioning system (e.g., GPS [6]), and a source can obtain the destination position through some type of location service. An intermediate node makes its forwarding decisions based on the destination position inserted in the packet header by the source and the positions of its one-hop neighbors learned from the periodic beaconing of the neighbors.

Similarly, to reduce the topology maintenance overhead and support more reliable and efficient multicasting, an alternative is to make use of the position information to guide multicast routing. However, there are many difficulties in implementing an efficient and secured geographic multicast scheme in MANETs. For example, in unicast geographic routing, the destination is a single member; while in multicast routing the destination is a group of members.

A straight forward way to extend the geography based transmission from unicast to multicast is to put the addresses and positions of all the members into the packet header. However, the header size will increase significantly as the group size increases, which will force the application of geographic multicasting only to a small group. Besides requiring efficient packet forwarding, a scalable and highly secured geographic multicast protocol also needs to efficiently manage the membership of a large group, obtain the positions of the members and build routing paths to reach the members distributed in a possibly large network terrain. The existing geographic multicast protocols normally address only part of these problems.

III. PROTOCOL OVERVIEW

In this paper, we propose an efficient geographic multicast protocol, which can scale to a large group size and large network size. The protocol is designed to be simple and efficient for more reliable operation. Instead of addressing only a part of the problem, it includes a zone-

based structure to efficiently handle the group membership management. The zone structure is formed virtually and the zone where a node is located can be calculated based on the position of the node and a reference origin. There is no need to involve an overhead to create and maintain the geographic zones proposed in this work, which is vital to support more efficient and reliable communications over MANETs. By making use of the location information, the protocol designed could quickly and efficiently build packet distribution paths, and effectively maintain the forwarding paths. In summary, the work includes:

- Making use of the position information to design a virtual-zone-based scheme for efficient membership management, which allows a node to join a group as and when needed.
- Supporting location search of the multicast group members, to avoid the need and overhead of using a separate location server.
- Evaluating the performance of the protocol through quantitative analysis and extensive simulations. Simulation studies confirm the efficiency of the proposed protocol.

IV. PROPOSED MODEL

The protocol proposed supports efficient and reliable membership management and multicast forwarding through a two-tier virtual zone-based structure. At the lower layer, the nodes in the network organize themselves into a set of zones and a leader is elected in a zone to manage the local group membership. At the higher layer, the zone leader serves as a representative for its zone. As a result, a network wide zone-based multicast tree is built.

For efficient and secured management and transmissions, location information will be used to guide the zone formation, multicast tree construction and maintenance, and packet transmission. The zone-based tree is shared by all the multicast sources of a group.

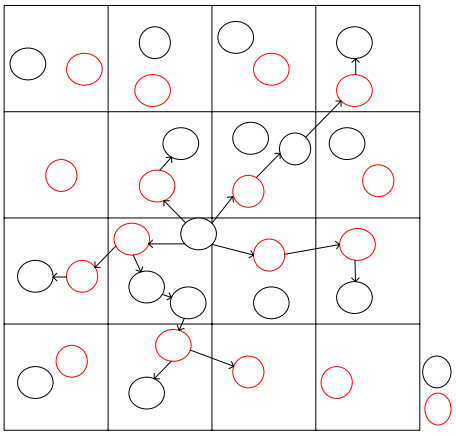

Fig 1: Zone formation and multicast tree construction [12]

Some of the notations used in the paper are:

zone: The network terrain is divided into square zones as shown in Fig. 1.
r: Zone size, the length of a side of the square zone. The zone size is set to $r \geq r_t / \sqrt{2}$, where r_t is the transmission range of the mobile nodes. To reduce intra-zone management overhead, the intra-zone nodes can communicate directly with each other without the need of any intermediate relays.
zone ID: The identification of a zone.
zLdr: Zone leader. A zLdr is elected in each zone for managing the local zone group membership and taking part in the multicast routing.
tree zone: The zones on the multicast tree. These zones are responsible for the multicast packet forwarding. These zones may have group members or just helps to forward the multicast packets for zones with members.
root zone: The zone in which the root of the multicast tree is located.

In the proposed protocol, the zone structure is virtual and calculated based on source as the reference point. Hence, the formation of zone structure does not depend on the shape of the network region, and it is simple to locate and maintain a zone. A multicast group can cross multiple zones. Hence, it is not necessary to track individual node movement but the membership change of zones alone has to be tracked, which will reduce the management overhead and increase the robustness of the proposed multicast protocol.

A. Neighbor Table Generation and Zone Leader Election

For efficient management of states in a zone, a leader is elected by the source with minimum overhead. As a node employs periodic BEACON broadcast to distribute its position in the underneath geographic unicast routing, to facilitate leader election and to reduce overhead, BEACON message with a flag indicating whether the sender is a zone leader is inserted. The message will be received by all the nodes in the zone. To reduce the the number of beacons, instead of using fixed interval beaconing, the adaptive beaconing interval is employed.

A node will check its neighbor table and determine its zone leader under different cases:

- If neighbor table contains no other nodes in the same zone, it will announce itself as the leader.
- The flags of all the nodes in the same zone are unset, which means that no node in the zone has announced itself as the leader. If the node is closer to the zone center than other nodes, it will announce itself as the leader through a beacon message with the leader flag set.
- If only one of the nodes in the zone has its flag set, then the node with the flag set is the leader.

B. Zone-Supported Geographic Forwarding

With a zone structure, communication can be of two types-an intrazone transmission and an interzone transmission. In the proposed zone structure, as nodes from the same zone are within each other's range and are aware of each other's location, only one transmission is required

for intrazone communications. Transmissions between nodes in different zones may be needed for the network-tier forwarding of control messages and data packets. But in this paper we are mainly concentrating on intra- zone communication, as inter-zone communication is quite a rare case.

Generally, the messages related to multicast group membership management and multicast data will be forwarded to the zone leader for processing. A packet is considered to be successfully delivered if it is received by any node in the destination zone. The simulation results confirm that zone forwarding mode helps to reduce the number of undelivered packets.

V. BLACK HOLE ATTACK

Security is a great issue in MANETs. A malicious node can exploit the vulnerability of zone leader election process. A malicious node may send a RREP (Route Reply) with FAKE parameters to the source and get elected as a zone leader [10]. Once it gets elected as zone leader, it may perform passive or active attacks depending on the level of importance of the message

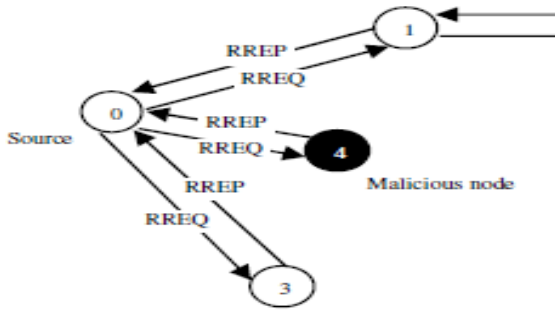

Fig 2: RREQ broadcast

VI. IDS FOR ENHANCED SECURITY

IDS uses Host-based IDS schema as a Network-based IDS schema cannot be employed to mobile ad-hoc networks where there is no central access point that monitors traffic flow. IDS assumes that every activity of an user or a system can be monitored and anomaly activities of an intruder can be identified from normal activities. Hence, by identifying anomaly activities of a malicious node, it is possible to detect a possible intrusion and isolate it. To do so an IDS has to be provided with a pre-collected set of anomaly activities, called audit data. Once audit data is collected and is given to the IDS system, the IDS system is able to compare every activity of a host with the audit data on a fly. If any activity of a host (node) resembles the activities listed in the audit data, the IDS system isolates the particular node by forbidding further interaction. Furthermore, IDS works in a principle that trusts no peer. This means mobile nodes do not rely on other nodes to prevent intrusions.

Algorithm of IDS to prevent black hole attack:
Notations

SN: Source Node
AD: Audit Data
DP: Data Packet
RT: Routing Table
1. SN broadcasts RREQ
2. SN receives RREP
3. IF (RREP (e1, e2, e3 …en) is different from AD (a1, a2, a3…an))
4.{
5. save route to RT
6. WHILE (size of BUFFER is not zero)
7. send DP
8. }
9. ELSE
10. discard RREP
11. goto step3
12. }

In a black hole attack, a malicious node deceives source nodes by sending a fake RREP message. Fake RREP messages from a malicious node contain the following parameters:

- maximum destination sequence number − to make the route up to data
- single hop-count − to make a route with the shortest path
- life-long route − informs a route will exist as long as the network
- destination IP address − address of the destination node copied from RREQ
- time-stamp − the time the RREP was generated

These entries of an RREP message from a malicious node can be collected as audit data to differentiate anomaly activities from normal activities.

In summary an IDS (Intrusion Detection Systems) [14] can be added to detect the malicious nodes. IDS can be trained with a set of audit data [8]. When the parameters in the BEACON is different from the audit data above a threshold value an intrusion is detected. IDS notifies the detected intrusion to the source. Source sets the particular zone leader as a malicious node and informs the other members in the zone. Apart from this, the source re-elects a different zone leader and multicast transmission takes place as explained earlier.

VII. PERFORMANCE EVALUVATION

The proposed protocol is simulated using NS2. The algorithm has three phases: zone formation, zone-leader election and data communication phase. We simulate the proposed method under certain ideal conditions.

The throughput parameter of the protocol designed is compared under 3 conditions

- under normal condition,
- under black hole attack,
- under prevention of black hole attack by IDS

We are mainly interested in the protocol's efficiency and security in dynamic environment. The simulation was run with 48 nodes randomly distributed in an area of 650m x 650m. The simulation lasted for 45 simulation seconds. The

performance of the protocol designed is evaluated via network simulator.

Measured metrics are utilized for the multicast performance evaluation. Simulation results prove that the protocol designed performs better in terms throughput.

Throughput

Throughput is defined as the number of packets received per second. Throughput of the network designed using the proposed protocol is measured in simulation, and is shown in Fig. 3.

$$\text{Throughput} = \frac{\text{Packets received}}{\text{Time in seconds}} \qquad (1)$$

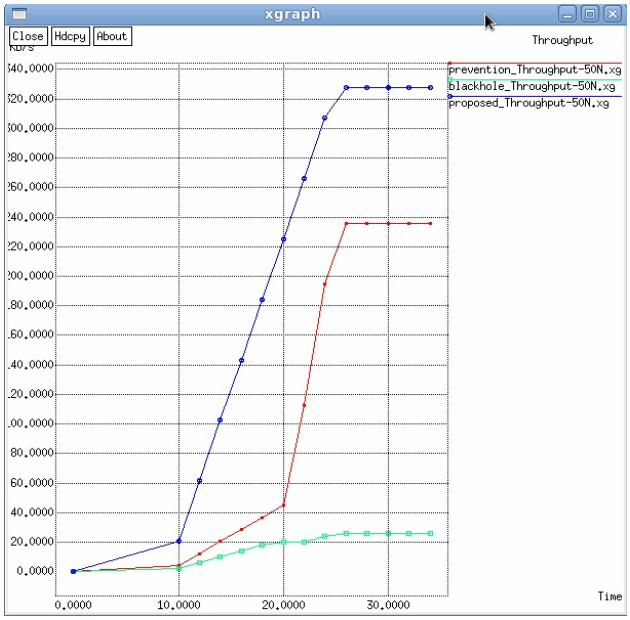

Fig 3: Performance analysis of Throughput

In summary, the protocol designed performs much better in a large network, and has a significantly higher throughput due to its virtual-zone-based geometric membership management and transmission infrastructures.

VIII. CONCLUSION

In this paper, we propose an efficient and secured multicast protocol for MANET. A zone-based multicast tree is built at the upper tier for more efficient multicast membership management and the lower tier to realize the local membership management. The location information is used in the protocol to guide the zone structure building, multicast tree formation, maintenance, and packet forwarding.

Results indicate that geometric information can be used more efficiently to construct and maintain multicast structure, and to achieve more efficient and reliable multicast transmissions in the presence of constant topology change of MANETs. The simulation results demonstrate that the protocol designed has high throughput. The self protection principle of IDS where every single mobile node is responsible for protecting itself effectively prevents a black hole attack regardless of the black hole nodes. The protocol is also scalable to both the group size and the network size.

REFERENCES

[1] Chiang C.-C., Gerla M., and Zhang L., "Forwarding Group Multicast Protocol (FGMP) for Multihop Mobile Wireless Networks," ACM J.Cluster Computing, special issue on mobile computing, vol. 1, no. 2, pp. 187-196, 1998.

[2] Devarapalli V. and Sidhu D.,"MZR: A Multicast Protocol for Mobile Ad Hoc Networks," Proc. IEEE Int'l Conf. Comm. (ICC '01), (2001).

[3] Dokurer S., "Simulation of black hole attack in wireless ad-hoc networks," Master thesis, Atilim University, Turkey, Sep 2006.

[4] Garcia-Luna-Aceves J.J. and Madruga E., "The Core-Assisted Mesh Protocol (CAMP)," IEEE J. Selected Areas in Comm., vol. 17, no.8, pp.1380-1394.3, Aug 1999.

[5] Gerla M. Lee S.J. and Su W., "On-Demand Multicast Routing Protocol (ODMRP) for Ad Hoc Networks," Internet draft, draftietf-manet-odmrp 02.txt, 2000.

[6] Kaplan E., Understanding GPS. Artech House, 1996.

[7] Lee S. Su W. Hsu J. Gerla M. and BagrodiaR., "A Performance Comparison Study of Ad Hoc Wireless Multicast Protocols," Proc. IEEE INFOCOM, 2000.

[8] Raj P. and Swadas P., "A dynamic learning system against black hole attack in AODV based MANET," IJCSI International Journal of Computer Science, Vol. 2, pp. 54-59, 2009.

[9] Royer E.M. and Perkins C.E., "Multicast Operation of the Ad Hoc On Demand Distance Vector Routing Protocol(MAODV)," Proc. ACM/IEEE MobiCom, pp. 207-218, Aug 1999.

[10] Sharma S. and Gupta R. , "Simulation study of black hole attack in the mobile ad-hoc networks," Journal of Engineering Science and Technology, Vol. 4, No. 2 pp. 243-250, 2009.

[11] Wu C. Tay Y. and Toh C.-K.,"Ad Hoc Multicast Routing Protocol Utilizing Increasing Id-Numbers (AMRIS) Functional Specification," Internet draft, Nov 1998.

[12] Xiang. X and Wang X.,"Supporting efficient and scalable multicasting over mobile ad hoc network", IEEE Transactions on mobile computing, vol. 10, No. 4, PP. 544-559, April 2011.

[13] Zhang X. and Jacob L. "Multicast Zone Routing Protocol in Mobile Ad Hoc Wireless Networks (MZRP)," Proc. Local Computer Networks (LCN '03), Oct. 2003.

[14] Zhang Y. and Lee W., "Intrusion detection in wireless ad-hoc networks," Sixth Annual International Conference on Mobile Computing and Networking (MobiCom'2000), Boston, August 6-11, 2000.

AUTHORS PROFILE

S.Thenmozhi completed her B.E. degree and M.E. degree in 2011 and 2013 respectively. She is currently working as an Assistant Professor in Sri Krishna College of Technology, Coimbatore. Her research area is Mobile Ad-Hoc Networks, Wireless Sensor Networks.

G.Anitha completed her B.E. degree and M.E. degree in 2001 and 2007 respectively. She is currently working as an Assistant Professor in Sri Krishna College of Technology, Coimbatore. Her research area is Wireless Sensor Networks.