DETECTION AND PREVENTION OF WORMHOLE ATTACK IN STATELESS MULTICASTING

L. Sudha Rani , R.Raja Sekhar (Ph.D)

Abstract: Multicast is an efficient method to implement the group communication. In recent years, a number of different multicast protocols have been proposed for ad hoc networks.Robust and Scalable Geographic Multicast Protocol (RSGM) is one among them. RSGM is a geographic routing protocol which routes the data using the location of the nodes. Geographic routing protocols are known tobe particularly vulnerable to attacks. One of the most powerful and serious attacks in adhoc networks is wormhole attack, preventing this attack has proven to be very difficult.

In this paper, an efficient method namely Multicast Authentication Node Scheme is devised to detect and avoid wormhole attack in theRSGM protocol. This technique uses cryptographic concept to detect and prevent wormhole attack. The proposed system is simulated in network simulator (NS-2).

Keywords: mobile ad hoc networks, multicasting, scalable, robust, security, wormhole attack.

I. INTRODUCTION

In recent years mobile ad hoc networks became a popular subject for research, and various studies have been made to increase the performance of ad hoc networks and support more advanced applications.Applications such as transportation, military, security, health, education, disaster recovery, crowd control, search and rescue, and automated battlefields are typical examples where ad hoc networksare deployed.An Ad hoc network is a dynamically reconfigurable wireless network with no fixed infrastructure or central administration. Each node in a MANET operates not only as an end-system, but also as a router to forward packets.In a typical ad hoc environment, network hosts work in groups to carry out a given task and hence multicast plays an important role in ad hoc networks.

Multicast is a fundamental service for supporting information exchanges and collaborative task executionamong a group of users and aims at identifying one -to-many transmission paths.Multicasting as opposed to (multiple unicasting)preserves network resources by reducing redundant messaging. Robust and Scalable Multicast Geographic Multicast Protocol (RSGM) is one among the Multicast routing protocols.Due to numerous limitations such as lack of infrastructure, dynamic network topology and lack of pre-established trusted relationships between the nodes, most of the envisioned routing protocols for ad hoc networks are susceptible to number of attacks.It is proven that these attacks can potentially degrade the performance of routing protocols and wormhole attack is a much more serious and dangerous attack.

The wormhole attack can form a serious threat in wireless networks, especially against many ad hoc network routing protocols and location-based wireless security systems.So far research has been made regarding security attacks in ad hoc network and concentrated mainly on Non-Geographic Routing protocols (Topology based Routing protocols). Geographic Routing Protocols outperform topology based routing protocol due to the availability of GPS system [10]. Hence it is also equally important for considerable research in Geographic routing protocols.

This paper focuses on wormhole attack on one of the geographic routing protocols namedRobust and Scalable Geographic multicast routing protocol(RSGM) [1].In this devastating attack two or more malicious colluding nodes tunnel traffic from one end of the network to the other end using an out-band link.The main goal of these nodes is to attract traffic to drop,alter or simply look at the packets later on. The cryptographic solution named Multicast Authentication Node Scheme has been proposed to detect and prevent wormhole attack in RSGM protocol.

We organize the rest of the paper as follows: In section II the related work on RSGM protocol is presented .Section III concentrates on Wormhole Attack Analysis where the problem definition is given in detail. The next section consists of approachand methodology for detecting and avoiding wormhole attack. Section V gives simulation results of our proposed system. Section VI is about the conclusion.

II. RELATED WORK ON RSGM ROUTING PROTOCOL

A. Geographic Routing

TheAd hoc network research has resulted in a number of routing protocols suitable for use in MANETs. Most of the research in MANET routing focused mainly on *topology-based* protocols. Thistopology based routing protocols use the information about links that exist in the network to perform packet forwarding. Research has shown that Position Basedrouting protocols or Geographic routingprotocols are a good alternative to topology based routing protocols in many cases[6][7].

In thesePosition-based or Geographic routing protocols routing decisions are made based on the location of the source, destination and intermediate nodes.This results in improved efficiency and performance. The geographical position of the nodes is generally obtained via Global Positioning System (GPS) or some other positioning system. Further this location information is used by these protocols to progressively forward packets through the physical space from the source towards the destination location, with intermediate next-hop routing decisions based on selecting the neighbor that has the closest distance or some other measure of forward progress [2], [3], [4].Geographic forwarding offers a near-stateless, low overhead, and low-latency solution to routing in ad hoc networks and these are scalable even in high dynamic networks.

RSGM protocol is one among these geographic based protocols whichis explained in detail in the following discussion.

B. Features provided by RSGM Protocol:

- Unlike general tree-based multicast protocols where explicit tree structures are built and maintained, RSGM constructs virtual tree paths in order to send data packets and control messages. This greatly reduces the control overhead and increases the reliability and scalability of the protocol.
- The position information is used to design a scalable and reactive zone-based scheme for efficient membership management, and this enables a node to join and leave a group quickly.
- The location service is combined with the membership management in order to support an efficient location search for the group members. This avoids the need and overhead of maintaining a separate location server.
- Introduces a home zone to track the addresses and positions of the sources, this avoids the network-range periodic flooding of source information
- The empty-zone problemsfor both the member zones and home zone are handled very efficiently which iscritical in designing a zone-based protocol.

a) Zone Construction and Maintenance:

RSGM assumes that entire network is divided into zones, where each and every zone is identified by a Zone ID (zID). Each and every node calculates its' zID (a, b) from its' position(x,y) as given in

$$a= [x-x_0/\text{zone-size}] \quad b = [y-y_0/\text{zone-size}] \tag{1}$$

where zone-size=length of the side of the zone square,$(x_0,y_{0)}$=virtual origin.

Each and every zone will have a leader which is elected on demand. Whenever a new member joins the zone it queries the neighbor node for the zone leader (zLdr). If it fails to get the information it announces itself as the leader and sends LEADER message to all the nodes in the zone. In the case of a conflict the member with the largest Id is chosen as the leader. The leader message is flooded for every $\text{Intval}_{\text{refresh}}$time interval.

b) Group Membership Management:

Whenever a member M joins or leaves the group in a zone it sends REFRESH (groupIDs, pos_M) message to the zone leader where pos_M is the position of the member and groupIDs are the addresses where M is a member.

c) Zone Membership Management:

Whenever a zone changes from mZone to non_ mZone the zLdr sends REPORT message to S to notify the change where S is the source.zLdr sends REPORT message for every $\text{Intval}_{\text{refresh}}$ time interval.

d) Empty Zone Handling:

Whenever all the nodes move away from the zone, thezone becomesempty and the moving out zLdr should notify S to stop sending the packets to the emptyzone. In case if the zone leader fails to notify S, then the packets delivered to that zone should be dropped.

e) Multicast Packet Delivery:

From the membership management the source S knows about the mZones and the ZLdrs know about the geographic positions of the local members. The source first transmits the multicast packets to all the member zones towards their zone centers. Zone leaders then send the packets to all the member nodes in their own zones. For each destination next hop is decided by the geographic forwarding strategy and for each and every hop S unicasts a copy of packet which carries the list of the destinations that must be traversed through this hop [5].

f) Session Initiation and Source Tracking:

A multicast session (G) is started by the source S by flooding an ANNOUNCE (S, *posS*, groupIDs) message into the network where groupIDs are IDs of the groups (including G) that S is the source. On receiving this message whichever node (N) is interested to join the group G starts the joining process by unicasting to its zLdr a REFRESH with S's information. Termination of G is also done by S by flooding an ANNOUNCE with G removed from the groupIDs

The source location tracking is facilitated in RSGM by using a home zone(hZone), this avoids network range periodic flooding of source information. Initially there is no hZone in the network. When S announces its' source role it will make its current zone as hZone by inserting its zone ID (zID) and seqNo of hZone in the ANNOUNCE message where seqNo is initialized as zero.When the source moves into a new zone, it unicastsa REGISTER (*zIDnew*) message to hZone. The first hZone node which receives this, floods the message into hZone so that all the hZone nodes can know in which zone the source is currently located. A node just moving into hZone will get the sources' information by querying its neighbors in hZone. Whenever hZone is about to become empty, the last leaving node will announce its entering zone as the new hZone to the network,and floods into the new hZone its source list which contains the sources' information. The seqNo ofhZone is increased by one whenever the hZone changes.

III. WORMHOLE ATTACK ANALYSIS

This is particularly a devastating attack, where two or more maliciouscolluding nodes create a higher level virtual tunnel in the network,which is employed to transport packets between the tunnel end points.Wormhole attack is also known as tunneling attack.In this attack it is possible for the attacker to forward each bit over the wormhole directly, without waiting for an entire packet to be received before beginning to tunnel the bits of the packet, in order to minimize delay introduced by the wormhole.

Due to the nature of wireless transmission, the attacker can create a wormhole even for packets notaddressed to itself, and tunnel them to the colluding attacker at the opposite end of the wormhole.Here thewormhole alwaysputs the attacker in a very powerful position relative to other nodes in the network, and the attacker could exploit this position in a variety of ways. The presence of the wormhole and the two colluding attackers at either endpoint of the wormhole are not visible in the route.

Based on the feature of geographic routing, each node has a propagation radius range(R) and just can broadcastpacket to its neighbors. A wormhole attack can occur if and only if

$\sqrt{(x_d-x_c)^2 + (y_d-y_c)^2} > R*hop\_count$ (2)

where (x_c, y_c) is the source coordinate,

(x_d,y_d) is the destination coordinate andhop_count is the no of hops transmitted.

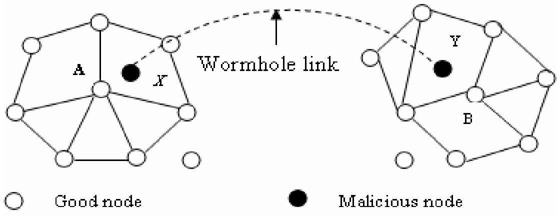

Figure1 Network under Wormhole Attack

IV.PROPOSED SOLUTION

Multicast Authentication Node Scheme is the approach that has been devised to detect and prevent wormhole attack against RSGM Protocol.

A. Multicast Authentication Node Scheme

In this method the wormhole attack is detected byverifying the authentication details of the nodes in theroute which is done by the zone leaders in the destination groups. Here it is assumed that the nodes in the network share their certificates and digital signatures. All the intermediate nodes must add their digital signatures to the datapacket whenever the data packet passes through them. The Signatures are verified by the zone leaders. If any node without digital signature or false digital signature is found in the data packet, the data packet is taken as untrusty packet and a request is sent to the source node from zone leaders to send the data packet in the new route.

According to this approach, the malicious node which does not have a key, cannot impersonate andcannot use the other node authentication. This approach is called pre-processing level and is continued until the packet reaches the destination node which is the zone leader in the destination group. Based on the processing approach and number of hop counts, when the packet is received by the zone leader which is the destination,determines whether the path is trusted or not.

B.Analysis of Proposed Scheme:

The Working of Multicast Authentication Node Schemeis analyzed by taking an example. Let the route throughwhich the data is forwarded be S-A-B-M1-C-D. S is the source and Ddestination where it is a zone leader.Whenthe data is received by A, it adds its digital signature tothe header of the packet then the node B verifies the signature of node A and adds its signature to the packet. The node M1 cannot add its signature to the data packet and therefore it either repeats the signature of other nodes or forwards the packet as it is. The destination D that is the zone leader in the receiving group verifies the signatures of the intermediatenodes in the packet it has received. Ifany fault in the signatures is found, the zone leader asks the source to repeat the packet through other possible route, using data acknowledge packet.The source node resends the untrusty packetthrough another possible route to the destination. Bycomparing the two data packets, the zone leader decidesthe un trusty route and sends the information about the malicious node tothe source node through data_acknowledge. The sourcenode discards the route and informs its neighbors about the malicious node M1. Thus, a malicious node can be avoided from routing in RSGM using Multicast Authentication Node Scheme.

V. SIMULATION RESULTS

A. Simulation Setup:

Simulation parameters are listed in Table 1. The minimum speed for the simulations is 0 m/s while the maximum speed is 10 m/s. To evaluate the schemes we have simulated the schemes in NS2. NS2 (Network Simulator) is an IEEEstandardized simulator for simulating network functions.

Table 1 Simulation Parameters

Examined Protocol	RSGM
Simulation Time	20ms
Simulation Area	1000*1000
Number of Nodes	50,100,150,200
Malicious Node	2,3
No of wormholes	2

Figure 2 demonstrates that packet loss is less in the existing system as each and every packet reaches the destination even though it is forwarded through the untrusted node and in the proposed system packet loss is more as the untrusted nodes are detected and the destination node rejects the packets that are transmitted

through the malicious nodes.

Figure 3 demonstrates that packet delivery ratio is high for the proposed system as security is added and it is low for the existing system as there is no security.

Figure 4 shows that delay increases when the no of nodes increases in the existing system as there is no security and whenever security is added to the protocol delay goes on decreasing

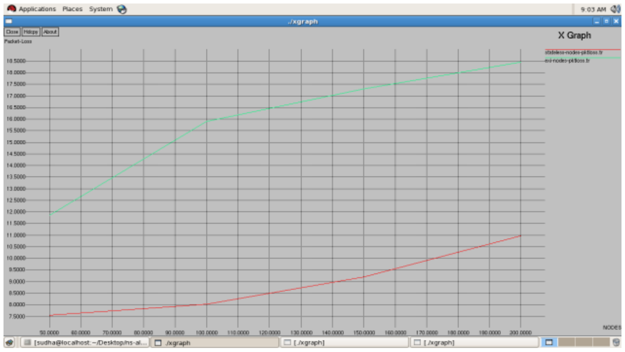

Figure 2

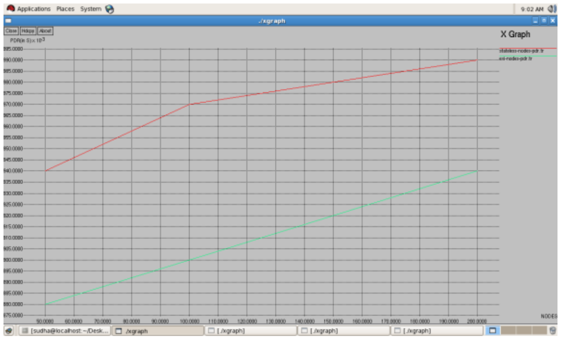

Figure 3

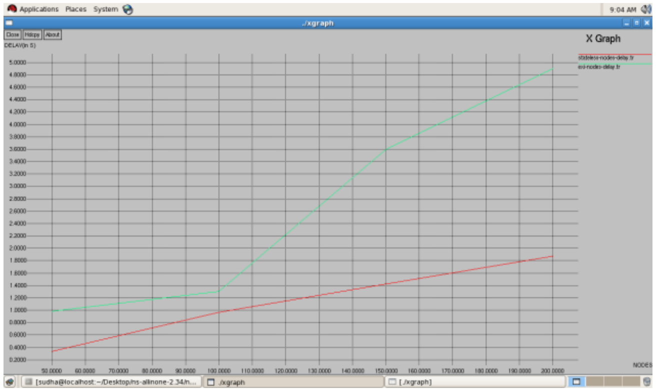

Figure 4

VI. CONCLUSION

The Geographic multicasting routing mechanism has been presented in this paper. Among the existing multicasting routing protocols the reason for selecting RSGM protocol isit handles empty zone problem very efficiently when compared to the other zone based protocols and it has an efficient source tracking mechanism which avoids the periodic flooding of source information. RSGM has the minimum control overhead and joining delay.The protocol can also scale to a large group size and a large network size, and can more efficiently support multiple multicast groups in the network.

One possible attack on the RSGM protocol has been discussed in this paper. The detection of such attack is difficult and is of course very much important. Multicast Authentication Node Scheme is the solution that is proposed to defend against the wormhole attack in RSGM protocol.This solutionclearly shows that the protocol achieves higher Packet Delivery Ratio under all circumstances with different moving speeds, node densities, group sizes, and network sizes.

REFERENCES

[1]Xiaojing Xiang, Zehua Zhou, *Xin* Wang Members of IEEEE "Stateless Multicasting in Manets" IEEE TRANSACTIONS ON COMPUTERS, VOL. 59, NO. 8, AUGUST 2010.

[2]J.C. Navas and T. Imielinski, "GeoCast—Geographic Addressing and Routing," Proc. ACM MobiCom, pp.66-76, 1997.

[3] T. Imielinski and J.C. Navas, GPS-Based Addressing and Routing, IETF RFC 2009, Dept. of Computer Science, Rutgers Univ., 1996.

[4]T.Camp, Location Information Services in Mobile Ad Hoc Networks, Colorado School of Mines, and Oct.2003.

[5] B. Karp and H. T. Kung, "Greedy perimeter stateless routing for wireless networks," in *ACM/IEEE MOBICOM*, August 2000, pp. 243–254.

[6] E. Royer and C-K. Toy, A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks.*IEEE Personal Communications Magazine*, April1999, 46-55.

[7]Y. Ko, and N. Vaidya, Location Aided Routing in Mobile Ad Hoc Networks, *Proceedings of the 4thInternational Conference on Mobile Computing andNetworking*, Dallas, USA, 1998.

[8] W. Wu, J. Cao, J. Yang, and M. Raynal, "Design and Performance Evaluation of Efficient Consensus Protocols for Mobile Ad Hoc Networks," IEEE Trans. Computers, vol. 56, no. 8, pp. 1055-1070,Aug. 2007.

[9] M. Gerla, S.J. Lee, and W. Su, "On-Demand Multicast Routing Protocol (ODMRP) for Ad Hoc Networks,"2000

[10] T. Imielinski and J.C. Navas, GPS-Based Addressing and Routing, IETF RFC 2009, Dept. of Computer Science, Rutgers Univ., 1996.