I.J. Information Technology and Computer Science, **2013, 10, 92-102**
Published Online September 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2013.10.10

Secluding Efficient Geographic Multicast Protocol against Multicast Attacks

A. Amuthan
Department of Computer Science & Engineering, Pondicherry Engineering College, Puducherry, India
E-mail: amuthan@pec.edu

R. Kaviarasan
Department of Computer Science & Engineering, Alpha College of Engineering & Technology, Puducherry, India
E-mail: kaviarasanr64@pec.edu

S. Parthiban
Department of Computer Science & Engineering, PondicherryUniversity , Puducherry, India
E-mail: parthi_ns@yahoo.com

Abstract— A Mobile Ad-hoc Network (MANETs) is composed of Mobile Nodes without any infrastructure. The network nodes in MANETs, not only act as ordinary network nodes but also as the routers for other peer devices. The dynamic topology, lack of a fixed infrastructure and the wireless nature make MANETs susceptible to the security attacks. To add to that, due to the inherent, severe constraints in power, storage and computational resources in the MANET nodes, incorporating sound defense mechanisms against such attacks is also non-trivial. Therefore, interest in research of Mobile Ad-hoc NETworks has been growing since last few years. Security is a big issue in MANETs as they are infrastructure-less and autonomous. The main objective of this paper is to address some basic security concerns in EGMP protocol which is a multicast protocol found to be more vulnerable towards attacks like blackhole, wormhole and flooding attacks. The proposed technique uses the concepts of certificate to prevent these attacks and to find the malicious node. These attacks are simulated using NS2.28 version and the proposed proactive technique is implemented. The following metrics like packet delivery ratio, control overhead, total overhead and End to End delay are used to prove that the proposed solution is secure and robust.

Index Terms— MANETs, EGMP, Certificate Key Chaining

I. Introduction

A MANET [6] 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. The term *Adhoc*[9] implies that this network is established for a special, often extemporaneous service customized to specific applications.

Mobile Ad-Hoc NETworks (MANET) is a collection of wireless mobile nodes forming a temporary network without using any centralized access point, infrastructure [11], or centralized administration. To establish a data transmission between two nodes, typically multiple hops are required due to the limited transmission range. Mobility of the different nodes makes the situation even more complicated. Multiple routing protocols especially for these conditions have been developed during the last years, to find optimized routes from a source to some destination. In MANETs, routing and resource management are done in a distributed manner; that is, all nodes coordinate to enable communications among themselves. This requires each node to be more intelligent so that it can operate both as a network host for transmitting and receiving data, and as a network router for forwarding packets for other nodes.

Security is a big concern in MANETs and prone to many security attacks [1] [8] [13] as its application extends in military application and these attacks are the challenging issues faced by researches of all times. In this paper, advanced routing attacks based on their vulnerabilities which caused by them in the network have been taken up. The attacks are chosen based on the impact which is made by them in the network. The first attack chosen is flooding attack [15], this attack will exhaust the network resources such as energy and bandwidth which leads to denial of service attack. The next most vulnerable attack is blackhole [2] attack in which rushing attack [7] has to be implemented in which it has to invade the forwarding group and then blackhole attack will be implemented. The last attack which is chosen is wormhole attack in which a pair of colluding attackers is present and this too will lead to low packet delivery ratio.

1.1 Multicast Routing Protocol Design - Issues and Challenges

Limited bandwidth availability, an error-prone shared broadcast channel, the mobility of nodes with limited energy resources, the hidden terminal problem , and limited security make the design of a multicast routing protocol for ad hoc networks a challenging one. Several issues involved in the routing protocol are discussed below.

Robustness: Due to the mobility of the nodes, link failures are quite common in ad hoc wireless networks. Thus, data packets sent by the source may be dropped, which results in a low packet delivery ratio. Hence, a multicast routing protocol should be robust enough to sustain the mobility of the nodes and achieve a high packet delivery ratio.

Efficiency: In an ad hoc network environment, where the bandwidth is scarce, the efficiency of the multicast protocol is very important. Multicast efficiency is defined as the ratio of the total number of data packets received by the receivers to the total number of (data and control) packets transmitted in the network.

Control overhead: In order to keep track of the members in a multicast group, the exchange of control packets is required. This consumes a considerable amount of bandwidth. Since bandwidth is limited in ad hoc networks, the design of a multicast protocol should ensure that the total number of control packets transmitted for maintaining the multicast group is kept to a minimum.

Quality of service: One of the important applications of ad hoc networks is in military/strategic applications. Hence, provisioning quality of service (QoS) is an issue in ad hoc multicast routing protocols. The main parameters which are taken into consideration for providing the required QoS are throughput, delay, delay jitter, and reliability.

Dependency on the unicast routing protocol: If a multicast routing protocol needs the support of a particular routing protocol, then it is difficult for the multicast protocol to work in heterogeneous networks. Hence, it is desirable if the multicast routing protocol is independent of any specific unicast routing protocol.

Resource management: Ad hoc networks consist of a group of mobile nodes, with each node having limited battery power and memory. An ad hoc multicast routing protocol should use minimum power by reducing the number of packet transmissions. To reduce memory usage, it should use minimum state information.

Security and Reliability: Security provisioning is a crucial issue in MANET multicasting due to the broadcast nature of this type of network, the existence of a wireless medium, and the lack of any centralized infrastructure. This makes MANETs vulnerable to eavesdropping [5], interference, spoofing, and so forth. Multicast routing protocols [4] should take this into account, especially in some applications such as military (battlefield) operations, national crises, and emergency operations. Reliability is particularly important in multicasting, especially in these applications, and it becomes more difficult to deliver reliable data to group members whose topology varies.

The remainder of this paper is organized as follows: Section 2 gives a complete description on working of Efficient Geographic Multicast Protocol. Section 3 describes the Trust based solution to mitigate the multicast attacks. Section 4 presents the experimental set up and evaluation results. Conclusion and future work are given in the final section.

II. Efficient Geographic Multicast Protocol

2.1 Overview of EGMP

This section deals with the entire description of the EGMP (EFFICIENT GEOGRAPHIC MULTICAST PROTOCOL) and its various flaws found in the security mechanism that makes us the protocol more vulnerable to attacks and also the details of the EGMP functionalities, exploited by the malicious nodes to stage a blackhole attack, wormhole attack and flooding attack in the network

EGMP supports scalable and reliable membership management and multicast forwarding through a two-tier virtual zone-based structure. At the lower layer, in reference to a predetermined virtual origin, the nodes in the network self organize themselves into a set of zones as shown in Fig: 1 and a leader are elected in a zone to manage the local group membership. At the upper layer, the leader serves as a representative for its zone to join or leave a multicast group as required. As a result, a network wide zone-based multicast tree is built. For efficient and reliable management and transmissions, location information will be integrated with the design and used to guide the zone construction, group membership management, multicast tree construction and maintenance, and packet forwarding. The zone-based tree is shared for all the multicast sources of a group.

To further reduce the forwarding overhead and delay, EGMP supports bidirectional packet forwarding along the tree structure. That is, instead of sending the packets to the root of the tree first, a source forwards the multicast packets directly along the tree. At the upper layer, the multicast packets will flow along the multicast tree both upstream to the root zone and downstream to the leaf zones of the tree. At the lower layer, when an on-tree zone leader receives the packets, it will send them to the group members in its local zone.

Many issues need to be addressed to make the protocol fully functional and scalable. The issues related to zone management include: the schemes for more efficient and robust zone construction and maintenance, the strategies for election and

maintenance of a zone leader with minimum overhead, zone partitioning as a result of severe wireless channels or signal blocking, potential packet loss when multicast members move across zones. The issues related to packet forwarding include: the efficient building of multicast paths with the zone structure, the handling of empty zone problem, the efficient tree structure maintenance during node movements, the reliable transmissions of control and multicast data packets, and obtaining location information to facilitate our geometric design without resorting to an external location server.

For the convenience of presentation, let's first introduce the terminologies used in the paper. In EGMP, every node is aware of its own position through some positioning system or other localization schemes are assumed. The forwarding of data packets and most control messages are based on the geographic unicast routing protocol GPSR described. EGMP, however, does not depend on a specific geographic unicast protocol. Some of the notations to be used are:

Zone: The network terrain is divided into square zones

r: Zone size, the length of a side of the zone square.

The zone size is set to r<rt /√2 , where rt is the transmission range of the mobile nodes. To reduce intrazone management overhead, the intrazone nodes can communicate directly with each other without the need of any intermediate relays.

Zone ID: The identification of a zone. A node can calculate its zone ID (a, b) from its position coordinates (x, y) as: a= $(x-x_0)/r$, b = = $(y-y_0)/r$ where (x_0, y_0) is the position of the virtual origin, which can be a known reference location or determined at network setup time. A zone is virtual and formulated in reference to the virtual origin. For simplicity, let assume the entire zone IDs are positive.

Zone center: For a zone with ID (a,b), the position of its center xcyc can be calculated as: $x = x_0 + (a*0{:}5) *r$; $y_c = y_0 + (b*0.5)$. A packet destined to a zone will be forwarded toward the center of the zone.

zLdr: Zone leader. A zLdr is elected in each zone for managing the local zone group membership and taking part in the upper tier multicast routing

Tree zone: The zones on the multicast tree. The tree zones are responsible for the multicast packet forwarding. A tree zone may have group members or just help forward the multicast packets for zones with members.

Root zone: The zone where the root of the multicast tree is located.

Zone depth: The depth of a zone is used to reflect its distance to the root zone. For a zone with ID (a, b) , its depth is

$$Depth = max\ (|a_0 - a|, |b_0 - b)|)$$

Where (a_0, b_0) is the root-zone ID. For example, in Fig. 1, the root zone has depth zero, the eight zones immediately surrounding the root zone have depth one, and the outer seven zones have depth two.

In EGMP, the zone structure is virtual and calculated based on a reference point. Therefore, the construction of zone structure does not depend on the shape of the network region, and it is very simple to locate and maintain a zone. The zone is used in EGMP to provide location reference and support lower-level group membership management. With the introduction of virtual zone, EGMP does not need to track individual node movement but only needs to track the membership change of zones, which significantly reduces the management overhead and increases the robustness of the proposed multicast protocol. To design the zone without considering node density, it must provide more reliable location reference and membership management in a network is chosen with constant topology changes.

Table 1: Illustrates the neigboring nodes associated with the node 18 and the position of neigboring nodes are mentioned in the table.

Table 1: The Neighbor Table of Node 18

NODE ID	POSITION	FLAG	ZONE ID
16	(x16 ,y16)	1	(1,1)
1	(x1 ,y1)	0	(1,1)
17	(x7,y7)	1	(0,1)
13	(x13 ,y13)	1	(1,2)

2.2 Neighbor Table Generation and Zone Leader Election

For efficient management of states in a zone, a leader is elected 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 reduce overhead, EGMP simply inserts in the BEACON message a flag indicating whether the sender is a zone leader. With zone size ≤ r <rt, a broadcast message will be received by all the nodes in the zone. To reduce the beaconing overhead, instead of using fixed interval beaconing, the beaconing interval for the underneath unicast protocol will be adaptive. A non-leader node will send a beacon every period of Intvalmax or when it moves to a new zone. A zone leader has to send out a beacon every period when Intvalmin to announces its leadership role.

A node constructs its neighbor table without extra signaling. When receiving a beacon from a neighbor, a node records the node ID, position, and flag contained in the message in its neighbor table. Table.1 shows the neighbor table of node 18. The zone ID of the sending node can be calculated from its position, as discussed

earlier. To avoid routing failure due to outdated topology information, an entry will be removed if not refreshed within a period TimeoutNT or the corresponding neighbor is detected unreachable by the MAC layer protocol.

A zone leader is elected through the cooperation of nodes and maintained consistently in a zone. When a node appears in the network, it sends out a beacon announcing its existence. Then, it waits for an Intvalmax period for the beacons from other nodes. Every Intvalmin a node will check its neighbor table and determine its zone leader under different cases:

The 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 the leadership role. If the node is closer to the zone center than other nodes, it will announce its leadership role through beacon message with the leader flag set. More than one node in the same zone have their leader flags set, the one with the highest node ID is elected.Only one of the nodes in the zone has its flag set, then the node with the flag set is the leader.

2.3 Zone Supported Forwarding

In EGMP, to avoid the overhead in tracking the exact locations of a potentially large number of group members, location service is integrated with zone-based membership management without the need of an external location server. At the network tier, only the ID of the destination zone is needed. A packet is forwarded toward the center of the destination zone first. After arriving at the destination zone, the packet will be forwarded to a specific receiving node or broadcast depending on the message type. Generally, the messages related to multicast group membership management and multicast data will be forwarded to the zone leader to process.

In the above design, for scalability and reliability, the center of the destination zone is used as the landmark for sending a packet to the group members in the zone although there may be no node located at the center position. This, however, may result in the failure of geographic forwarding.

To avoid this problem, we introduce a zone forwarding mode in EGMP when the underlying geographic forwarding fails. Only when the zone mode also fails, the packet will be dropped. In zone mode, a sender node searches for the next hop to the destination based on its neighbor table, which can more accurately track the local network topology. The node selects as its next hop the neighboring node whose zone is the closest to the destination zone and closer to the destination zone than its own zone. If multiple candidates are available, the neighbor closest to the destination is selected as the next hop.

2.4 Multicast Tree Construction

In this section, the multicast tree creation and maintenance scheme is presented. In EGMP, instead of connecting each group member directly to the tree, the tree is formed in the granularity of zone with the guidance of location information, which significantly reduces the tree management overhead. With a destination location, a control message can be transmitted immediately without incurring a high overhead and delay to find the path first, which enables quick group joining and leaving. In the following description, except when explicitly indicated, we present G, S, and M, respectively, to represent a multicast group, a source of G and a member of G.

2.5 Multicast Session Initiation and Termination

When a multicast session G is initiated, the first source node S (or a separate group initiator) announces the existence of G by flooding a message NEW SESSION (G, zoneIDS) into the whole network. The message carries G and the ID of the zone where S is located, which is used as the initial root-zone ID of group G. When a node M receives this message and is interested in G, it will join G using the process described in the next section. A multicast group member will keep a membership table with an entry (G, root zID, Acked), where G is a group of which the node is a member, root_zID is the root-zone ID, and is Acked is a flag indicating whether the node is on the corresponding multicast tree. A zone leader (zLdr) maintains a multicast table. When a zLdr receives the NEW_ SESSION message, it will record the group ID and the root-zone ID in its multicast table. Table 2 describes the multicast table.

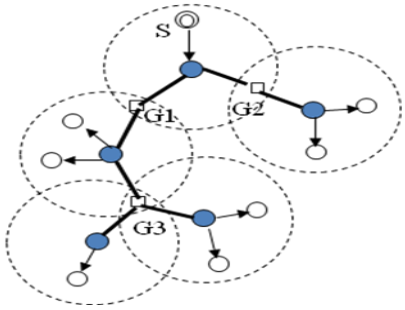
Table 2: Multicast Table

Multicast Table Format				
Zone id	Upstream zone id	Group zone id	Downstream zone list	Downstream node list

2.6 Multicast Group Join

When a node M wants to join the multicast group G, if it is not a leader node, it sends a JOIN REQ (M, PosM, G, Mold) message to its zLdr, carrying its address, position, and group to join. The address of the old group leader Mold is an option used when there is a leader handoff and a new leader sends an updated JOIN_REQ message to its upstream zone. If M did not receive the NEW_SESSION message or it just joined the network, it can search for the available groups by

querying its neighbors. If a zLdr receives a JOIN_REQ message or wants to join G itself, it begins the leader joining procedure as shown in Fig.1 If the JOIN_REQ message is received from a member M of the same zone, the zLdr adds M to the downstream node list of its multicast table.



S→Source G_1, G2, G3-→Group members

Fig. 1: Multicast Group Join

In, Fig: 1 describes the multicast group join scenario. If the message is from another zone, it will compare the depth of the requesting zone and that of its own zone. If its zone depth is smaller, i.e., its zone is closer to the root zone than the requesting zone, it will add the requesting zone to its downstream zone list; otherwise, it simply continues forwarding the JOIN_REQ message toward the root zone. If new nodes or zones are added to the downstream list, the leader will check the root-zone ID and the upstream zone ID. If it does not know the root zone, it starts an expanded ring search. As the zone leaders in the network catch the root-zone ID, a result can be quickly obtained.

With the knowledge of the root zone, if its upstream zone ID is unset, the leader will represent its zone to send a JOIN_REQ message toward the root zone; otherwise, the leader will send back a JOIN_REPLY message to the source of the JOIN_REQ message. When the source of the JOIN_REQ message receives the JOIN_REPLY, if it is a node, it sets the Acked flag in its membership table and the joining procedure is completed. If the leader of a requesting zone receives the JOIN_REPLY message, it will set its upstream zone ID as the ID of the zone where the JOIN_REPLY message is sent, and then send JOIN_REPLY messages to unacknowledged downstream nodes and zones.

2.7 Multicast Group Leave

When a member M wants to leave G, it sends a LEAVE (M, G) message to its zone leader. On receiving a LEAVE message, the leader removes the source of the LEAVE message from its downstream node list or zone list depending on whether the message is sent from an intrazone node or a downstream zone. Besides removing a branch through explicit LEAVE, a leader will remove a node from its downstream list if it does not receive the beacon from the node exceeding 2* Intervalmax. If its downstream zone list and node list of G are both empty and it is not a member of G either, the leader sends a LEAVE (zoneID, G) message to its upstream zone. Through the leave process, the unused branches are removed from the multicast tree.

2.8 Packet Sending from the Source

After the multicast tree is constructed, all the sources of the group could send packets to the tree and the packets will be forwarded along the tree. In most tree-based multicast protocols, a data source needs to send the packets initially to the root of the tree. The sending of packets to the root would introduce extra delay especially when a source is far away from the root. Instead, EGMP assumes a bi-directional tree- based forwarding strategy, with which the multicast packets can flow not only from an upstream node/zone down to its downstream nodes/zones, but also from a downstream node/zone up to its upstream node/zone.

2.9 Multicast Data Forwarding

Maintain the multicast table, and the member zones normally cannot be reached within one hop from the source. When a node N has a multicast Packet to forward to a list of destinations (D1; D2; D3), it decides the next hop node towards each destination (for a zone, its center is used) using the geographic forwarding strategy. After deciding the next hop nodes, N inserts the list of next hop nodes and the destinations associated with each next hop node in the packet header. In Fig: 2 depicts the multiple clusters in one zone.

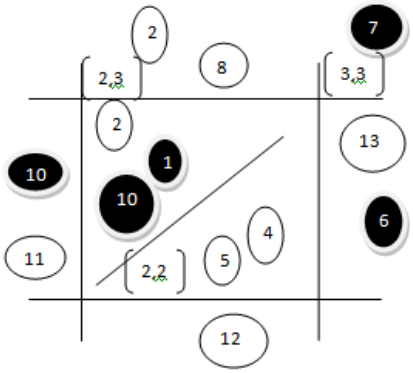


Fig. 2: Multiple Clusters in One Zone

An example list is (N1:D1; D3; N2:D2; :), where N1 is the next hop node for the destinations D1 and D3, and N2 is the next hop node for D2. Then N broadcasts the packet promiscuously (for reliability and efficiency). Upon receiving the packet, a neighbor node will keep the packet if it is one of the next hop nodes or destinations, and drop the packet otherwise. When the node is associated with some downstream destinations, it will continue forwarding packets similarly as done by node N.

2.10 Multicast Route Maintenance and Optimization

In the zone structure, due to the movement of nodes between different zones, some zones may become empty. It is critical to handle the empty zone problem in a zone-based protocol. Compared to managing the connections of individual nodes, however, there is a much lower rate of zone membership change and hence a much lower overhead in maintaining the zone-based tree.

When a member node moves to a new zone, it must rejoin the multicast tree through the new leader. When a leader is moving away from its current zone, it must handover its multicast table to the new leader in the zone, so that all the downstream zones and nodes will remain connected to the multicast tree.

III. Trust Based Solution to Mitigate Attacks

This solution aims at preventing the attacks by establishing a trust relation between the nodes [14]. Certificate chaining is a self organized PKI authentication by a chain of nodes without the use of a trusted third party. Here authentication is represented as a set of digital certificates that form a chain. Each node in the network has identical roles and responsibilities thereby achieving maximum level of node participation. Every node in the network can issue certificates to every other node within the radio communication range of each other.

A certificate is a binding between a node, its public key and the security parameters. Certificates are stored and distributed by nodes themselves. Every node participating in certificate chaining must be able to authenticate its neighbors, create and issue certificate for neighbors and maintain the set of certificates it has issued. The issue of certificates can be on the basis of security parameters of the node. Each node has a local repository consisting of certificates issued by the node to other nodes and certificates issued by others to the particular node. Therefore each certificate is stored twice, one by the issuer and the other for whom it is issued.

Periodically certificates from neighbors are requested and repository is updated by adding new certificates. If any of the certificates are conflicting, i.e., same public key to different nodes or same node having different public key, it is possible that a malicious node has issued a false certificate. A node then labels such certificates as conflicting and tries to resolve the conflict. If certificates issued by any node are found to be wrong, then that node may be assumed to be malicious. If multiple certificate chains exist between a source and destination, the source selects a chain or a set of chains for authentication.

Consider nodes A, B and C in a network as shown in Fig: 3 Node A issues certificate to node B if it is convinced about the security level of node B. The security parameters to counter the effect of black hole attack may be node id, location of the node and the delay in processing the RREQ packet. The delay for malicious nodes is zero as these nodes do not refer the routing table and respond immediately with a RREP message. The legitimate nodes would have a certain delay time in referring the routing table. The certificate contains the security parameters and the public key of B signed by A. Every other node in the network can verify the signature using A's public key. Certificate issued from node A to node B is represented as cert (A→B). Here A is the issuer and B is the subject of the certificate. Every node forming the route has to prove its identity and obtain a certificate from its neighboring node. Each certificate is issued with a limited validity period and contains the time of issue and expiration time. Before a certificate expires, the issuer issues an updated version of the same certificate with an extended time of expiry if the issuer node is still convinced of the security level of the subject node. This updated version of certificate is called certificate update. When node A wants to communicate with node D, it finds a chain of valid public key certificates leading to D. The chain is such that the first hop uses an edge from A i.e., a certificate issued by node A and the last hop leads to D i.e., certificate issued to D. All intermediate nodes are trusted through the previous certificates in the path. The last certificate contains the public key of the destination.

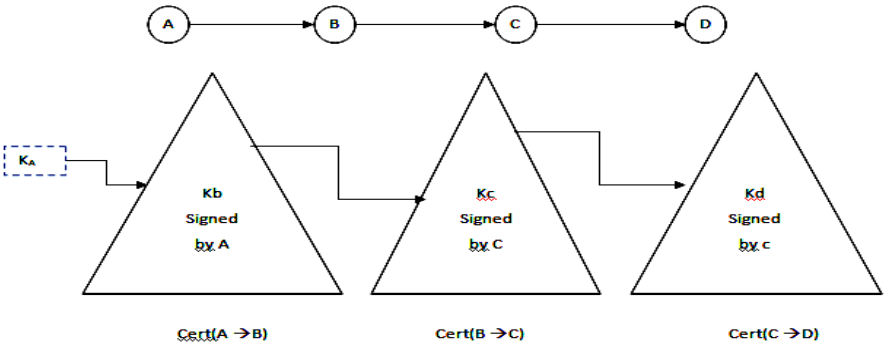


Fig. 3: Certificate Key Chaining

K_a - public key of A K_b - public key of B K_c - public key of C K_d - public key of D

3.1 Certificate Update

Each certificate has an expiry time after which it becomes invalid. If the certificate is still required to be used, the issuer has to update the certificate if it is still convinced about the security level of the subject node. On the other hand, if the issuing node feels that the subject node is compromised, it will not provide the certificate update.

3.2 Certificate Revocation

When the binding between a node and its key is found to be invalid, the issuing node can revoke the certificate. The revoked certificate is not usable.

3.3 Authentication Phase

The authentication phase follows the certification phase. When a source node A wants to find a route to a destination node D, it broadcasts a JREQ packet. The destination node or any other node that has a valid route to the destination now replies to the JREQ. Any malicious node may reply to the request from the source by claiming to have the shortest path to the destination. To overcome this black hole attack, source node does not initiate the data transfer process immediately after the routes are established. Instead it waits for the authenticated reply from the destination. After the certification process, the destination node sends authenticated messages appended with certificates taken from the corresponding node's repository.

3.4 Algorithm to Mitigate Attacks

1) The route is established between the source and destination
2) The nodes forming the routes enter into certificate phase
3) The security parameters of the next hop nodes are requested and public key certificates will be issued if the security level of the node is convinced.
4) The time difference between sending of JREQ packet and receipt of the same next hop node is used as a measure of security level.
5) If the security level is set as 1 it is considered as genuine node. If not malicious node
6) Certificates issued are stored in the repositories of the issuer
7) For example if node B is within the range of node A , node A issues certificate to B

$$\mathbf{Cert\ (A \rightarrow B) = [ID_B,\ K_b, t, e, S]\ K_A}$$

The certificate contains identity of node B, the public key of B , the time of issue of certificate , the time of expiry and security level of node signed by node A.

8) Public key is calculated by applying a one way hash function H, to the identity of the node. The identity may be either IP address or MAC address
9) Since same hash function is used by all nodes, the public key generated by different neighboring nodes would be the same.

$$\mathbf{K_B = H\ (ID_B)}$$

10) Each certificate has an expiry time, if the certificate has still required to be used the issuer has to update the certificate by checking the security parameters.
11) After the certification process the destination node sends the authenticated message append with certificate taken from the corresponding nodes repository.
12) The certified ($JREP_{CERT}$) packet from the destination would be of the form:

[Source id, next hop id, final destination id, certificate chain]

13) When this packet reaches the next hop node

Next hop node checks its repository to see if the certificate is present.

14) Then it checks the certificate revocation list to find if the destination node is malicious or not
15) If these two verification leads to a positive result, it forwards the $JREP_{CERT}$ to the next hop node .while doing so it appends the certificate from its repository.
16) All intermediate nodes perform the same procedure until the final source is reached
17) When the source receives the packet it checks the whole certificate chain. If there is no problem with the certificate chain data packets are sent through this route.
18) In case of legitimate node turning malicious over a period of time, the nodes behavior is recorded and the certificate would be revoked, thus isolating the node from further participation of network activities

3.5 Analysis of Certificate Key Chaining

The certificate key chaining solution protects the network through a self organized, fully distributed and localized procedure. The additional certificate publishing happens only for a short duration of time during which almost all nodes in the network get certified by their neighbors. After a period of time each node has a directory of certificates and hence the

overhead incurred in this process is reasonable with a good network performance in terms of security. To believe this is an acceptable performance, given that the attack prevented has a much larger impact on the performance of the protocol. As certificates are stored in repository of the issuer, it can be revoked at any point of time, if the node is found to be malicious. The certificate issued by the node cannot be forged, as time of expiry of the certificate and security level of the parameter are considered to be challenging tasks and they cannot be compromised at any point of time in the network The proposed mechanism can also be applied for securing the network from other routing attacks [12] by changing the security parameters in accordance with the nature of the attacks. This proposed solution can be applicable to all attacks and can be applied irrespective of the protocol to make the protocol more secure against attacks. This solution results in high packet delivery ratio and reduced control overhead, Total overhead and End to End delay.

IV. Simulation Settings

NetworkSimulator-2.28 is used for simulating the parameters in the proposed experiments.

Table: 3 Illustrates the simulation settings used during the simulation scenario.

Table 3: Common Simulation Parameters

Parameters	Values assigned
EGMP refreshment interval	0.33seconds
Channel capacity	2 Mbps
Packet size	128 bytes
Traffic model	Multicast constant bit rate
Mobility model	Random way-point
Queuing policy	First-in-first-out

The simulated network consists of 50 mobile nodes placed randomly within a 500 m x 500 m area. Each node has a transmission range of 250 m and moves at a speed of 1 m/s. The total sending rate of all the senders of the multicast group, i.e., the traffic load, is 1 packet/s. We use a low traffic load value to highlight the effects of the attacks on packet loss rate, as opposed to packet loss due to congestion and collisions resulting from a high traffic load.

The mobility model chosen for a mobile node was the *random way-point* model. A mobile node begins by staying in one location for a pause time of 0.33 seconds. Once this time expires, the mobile node chooses a random destination in the simulation area and then travels toward the newly chosen destination. Upon arrival, the mobile pauses for 0.33 seconds before starting the process again.

The attackers were positioned around the center of the multicast tree in all experiments; the duration of each experiment was 100 seconds in simulated time. Every experiment was repeated 10 times using 10 different randomly generated seed numbers, and the recorded data was averaged over those runs.

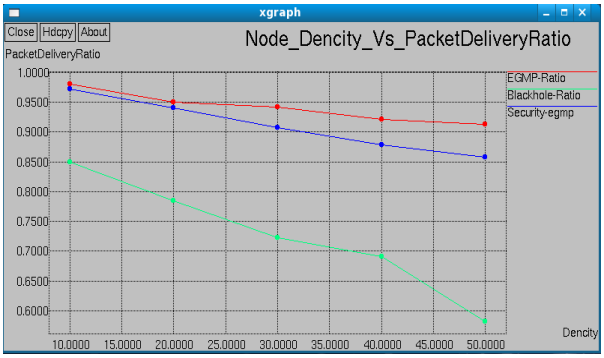


Fig. 4: Packet Delivery Ratio- Blackhole Attack

Packet Delivery Ratio increases on an average by **13%** when certificate key chaining solution is provided to prevent the Blackhole attack in EGMP.

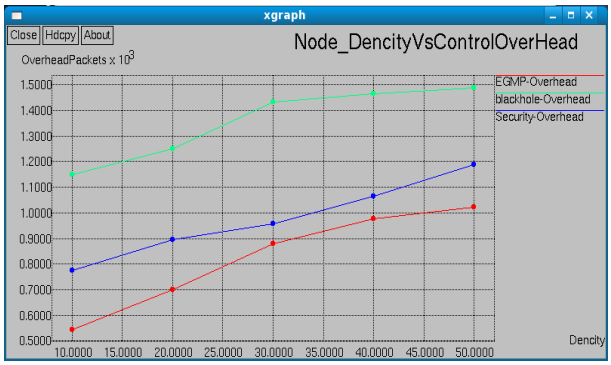


Fig. 5: Control Overhead - Blackhole Attack

Control Overhead decreases on an average by **3.7%** when Certificate key chaining solution is provided to prevent the Blackhole attack in EGMP.

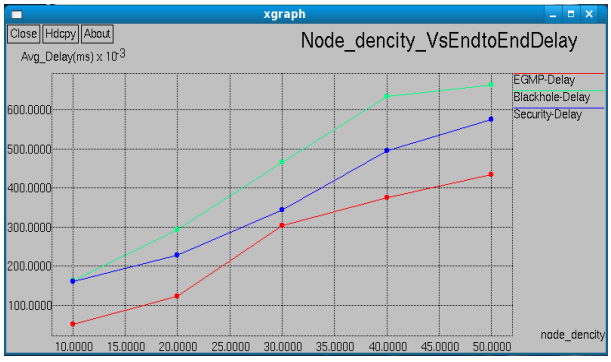


Fig. 6: End to End Delay- Blackhole Attack

End to End Delay decreases on an average by **10%** when Certificate key chaining solution is provided to prevent the blackhole attack in EGMP.

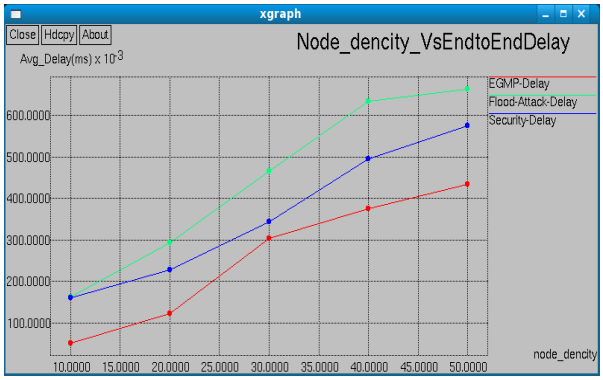


Fig. 7: End to End Delay-Flooding attack

End to End Delay decreases on an average by **10.2%** when Certificate key chaining solution is provided to prevent the flooding attack in EGMP.

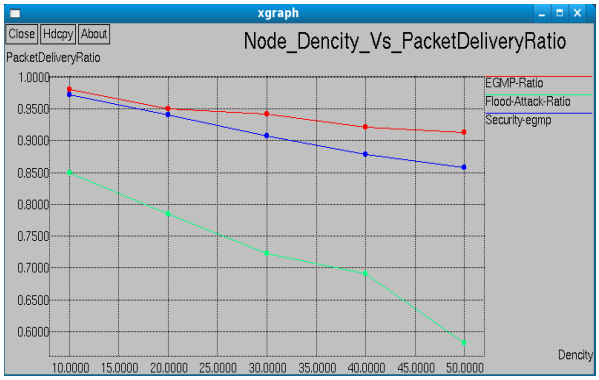


Fig. 8: Packet Delivery Ratio-Flooding attack

Packet Delivery Ratio increases on an average by **12.8%** when certificate key chaining solution is provided to prevent the Flooding attack in EGMP.

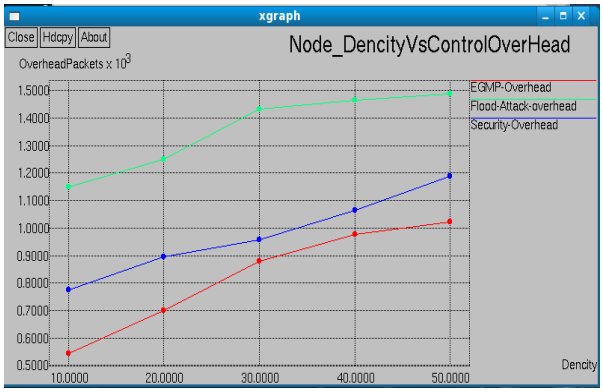


Fig. 9: Control Overhead –Flooding attack

Control Overhead decreases on an average by **3.5%** when Certificate key chaining solution is provided to prevent the flooding attack in EGMP.

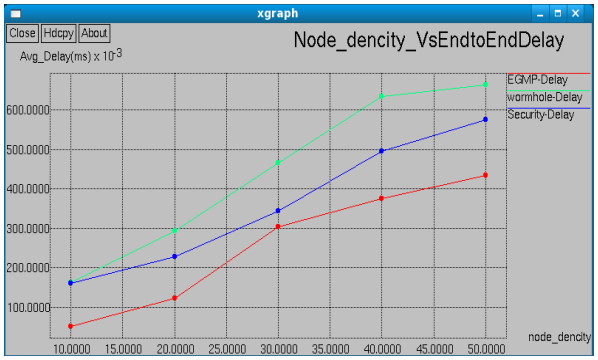


Fig. 10: End to End Delay- Wormhole attack

End to End Delay decreases on an average by **10.8%** when Certificate key chaining solution is provided to Prevent the wormhole attack in EGMP.

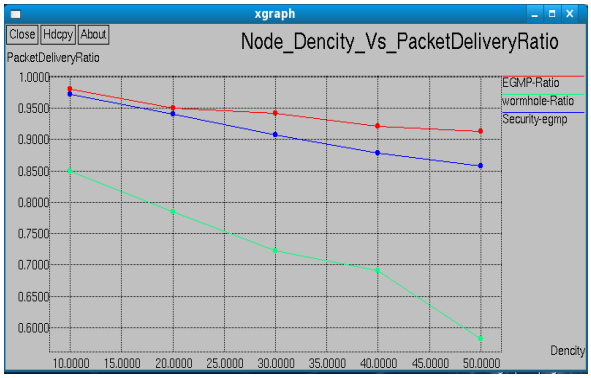


Fig. 11: Packet Delivery Ratio - Wormhole attack

Packet Delivery Ratio increases on an average by **13.2%** when certificate key chaining solution is provided to prevent the wormhole attack in EGMP

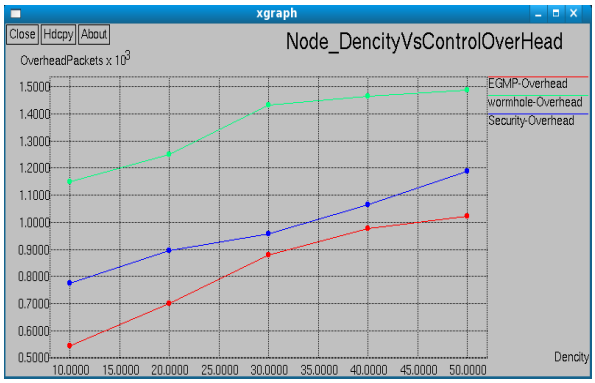


Fig. 12: Control Overhead- Wormhole attack

Control Overhead decreases on an average by **3.5%** when secure key exchange solution is provided to prevent the wormhole attack in EGMP.

V. Conclusion and Future Works

MANETs can be deployed and operated without depending on a fixed backbone. However, their features

of open medium, absence of infrastructure, dynamic changing network topology, cooperative algorithms, lack of centralized monitoring and management point, resource constraints and lack of a clear line of defense, are vulnerable to many attacks.

An in-depth analysis is done on the EGMP protocol and the vulnerabilities of the protocol such as blackhole attack, wormhole attack and flooding attack are identified. A trust based secure solution has been proposed to mitigate these attacks. Certificate key chaining solution aims in making the protocol more secure which achieves a very good rise in PDR (Packet Delivery Ratio) and a reduced control overhead and total overhead. This solution can be applied irrespective of the protocol and on any routing attack and a good convincing result can be achieved. The future work is aimed at extending the proposed solution to the other reactive protocols.

References

[1] K.Aishwarya, N.KannaiahRaju and A. SenthamaraiSelvan, "Counter Measures Against Multicast Attacks on Enhanced-On Demand Multicast Routing Protocol In Mobile AD-HOC Networks" -International Journal of Technology And Engineering System(IJTES) Jan –March 2011

[2] Payal N. Raj, Prashant B. Swadas "DPRAODV: A dyanamic learning system against blackhole attack in aodv based manet IJCSI International Journal of Computer Science Issues, Vol. 2, 2009

[3] NitalMistry, Devesh C Jinwala, Member, IAENG, MukeshZaveri"Improving AODV Protocol against Blackhole Attacks" IMCES 2010, MARCH 2010.

[4] Zhaoyu Liu, AnthonyW. Joy, Robert A. Thompson "A Dynamic Trust Model for Mobile Ad Hoc Networks"IEEE International Workshop on Future Trends of Distributed Computing Systems (FTDCS'04).

[5] Feng Li, Jie Wu and AvinashSrinivasan "Struggling Against Selfishness and Black Hole Attacks in MANETs"IJCNS 2010.

[6] Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park "Black Hole Attack in Mobile Ad Hoc Networks" ACM April-2004.

[7] DrKarim KONATE andAbdourahime GAYE "A Proposal Mechanism against the Attacks: Cooperative Blackhole, Blackmail, Overflow and Selfish in Routing Protocol of Mobile Ad Hoc Network", International Journal of Future Generation Communication and Networking Vol. 4, No. 2, June, 2011.

[8] A.Amuthan and D. NagamaniAbirami "Multicast security attacks and its counter measures for puma protocol" Int. J. Comp. Tech. Appl., Vol 2 (3), 594-600, 2011.

[9] FaridNa¨ıt-Abdesselam, BrahimBensaou, and TarikTaleb"Detecting and Avoiding Wormhole Attacks in Wireless Ad Hoc Networks" (IEEE WCNC), Mar. 2005.

[10] S.VijayalakshmiandS.AlbertRabara "Weeding Wormhole Attack in MANET Multicast Routing using Two Novel Techniques - LP3 and NAWA2" International Journal of Computer Applications (0975 – 8887) Volume 16– No.7, February 2011

[11] Shang-Ming Jen, Chi-Sung Laih and Wen-Chung Kuo "A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET" ISSN 1424-8220. 2010

[12] WassimZnaidi, Marine Minier and Jean-Philippe Babau "Detecting Wormhole Attacks in Wireless Networks Using Local Neighborhood Information" IEEE 2008.

[13] BounpadithKannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, And Nei Kato "A Survey Of Routing Attacks In Mobile Ad Hoc Networks" IEEE Wireless Communications October 2007.

[14] VenkatBalakrishnan, Vijay Varadharajan, UdayTupakula, and Phillip Lucs "Trust Integrate Co-Operative Architecture For Mobile Adhoc Networks"IEEE-2007.

[15] Jian-Hua Song, Fan Hong1, Yu Zhang"Effective Filtering Scheme against RREQ Flooding Attack in Mobile Ad Hoc Networks", Springer-2004.

Authors' Profiles

A. Amuthan, currently working as Associate Professor in the department of Computer Science & Engineering, Pondicherry Engineering College, Puducherry. Completed his Under graduate B.Tech in Computer Science & Engineering from Pondicherry Engineering College, M.E. from College of Engineering, Anna University, Chennai. He has obtained his doctorate in the area of Information Security at Pondicherry Engineering College under Pondicherry University.

R. Kaviarasan, currently working as Assistant Professor in the department of Computer Science & Engineering, Alpha College of Engineering & Technology, Puducherry. Completed his under graduate B.Tech in Information Technology from Bharathiyar College of Engineering & Technology and M.Tech Information Security from

Pondicherry Engineering College under Pondicherry University.

S. Parthiban, currently working as Senior Technical Assistant in the Department of Computer Science, Pondicherry University, Puducherry. Completed his M.E. in Computer Science & Engineering from Anna University, Chennai.

How to cite this paper: A. Amuthan, R. Kaviarasan, S. Parthiban,"Secluding Efficient Geographic Multicast Protocol against Multicast Attacks", International Journal of Information Technology and Computer Science(IJITCS), vol.5, no.10, pp.92-102, 2013. DOI: 10.5815/ijitcs.2013.10.10