International Journal of Computer Network and Security(IJCNS)
Vol5. No.1 – Jan-March 2013 Pp. 16-27
©gopalax Journals, Singapore
available at : www.ijcns.com

Scalable Robust Location Based Geocast Protocol in MANETs

A.Amuthan[1], R.Kaviarasan[2], S.Parthiban[3]
amuthan@pec.edu Kaviarasanr64@pec.edu, Parthi_ns@yahoo.com

ABSTRACT

A Mobile Ad-hoc NETwork (MANET) is composed of Mobile Nodes (MNs) without any infrastructure. MNs self-organize to form a network over radio links. Multicast routing plays a significant role in MANETs. Due to unique characteristics, such as dynamic network topology, limited bandwidth, and limited battery power, routing in MANETs is a particularly challenging task compared to conventional networks. At present, several efficient routing protocols have been proposed for MANETs. Most of these protocols assume a trusted and cooperative environment. However, in the presence of malicious nodes, the network is vulnerable to various kinds of attacks. The success of Mobile Ad-hoc NETwork (MANETs) strongly depends on people's confidence in its security. In large and dense Mobile Ad-hoc NETwork, location-based routing protocols can offer significant performance improvement over topology-based routing protocols. The objective of this paper is to prevent possible types of routing attacks like backhole, flooding and wormhole attack on location- based geocasting and forwarding (LGF) routing protocol in Mobile Ad-hoc NETwork (MANET). However, there are several potential security issues for the development of position-based routing protocols. The routing attacks against location-based geocasting and forwarding is eliminated by Trust based solution and Shamir Secret Key Sharing Scheme. It has been proved that Shamir Secret Key Sharing Scheme is best solution compared with trust based solution on the metrics packet delivery ratio, control overhead and total overhead.

Keywords- Blackhole,Wormhole, Flooding, location- based geocasting and forwarding (LGF), Shamier Secret Key, Certificate,Mobile Ad-hoc NETwork (MANET)

1. INTRODUCTION

Application independence reactive mesh-based multicast routing protocol on location-based geocasting and forwarding (LGF) routing protocol in MANET is a self-organizing system of mobile nodes from a temporary and dynamic wireless network on a shared wireless channel without the aid of a fixed networking infrastructure or centralized administration [1]. Hence, MANET is suitable for applications like military battlefield, emergency rescue, vehicular communications, Urgent Business meetings. Above these applications, communication and collaboration among a group of nodes are necessary. Instead of using multiple transmissions, it is an advantageous use of multicast in order to save network bandwidth and reduce rushing and overhead, since a single message can be delivered into multiple receivers simultaneously. In the LGF protocol routing metrics usually used are shortest path, link stability and minimum number of hops towards the destination. But, power conservation and optimized bandwidth are highlighted because Mobile Node (MN) in MANET is stand-alone devices and operates on batteries [2].

This paper describe the real MANET test bed integration of GPS-free indoor location tracking system with on demand geocasting enhanced AODV. The LGF protocol source node will be multicast the Route Request (RREQ) packet to its entire Intermediate Nodes (IN) within its transmission area. The request packet has additional information send the distance from the source to destination. Hence, every node that receives these packets will compare its distance to the destination. If its distance to destination is less than the distance from the source to destination, the intermediate nodes will be multicast the packets, otherwise it will discard and cancel its scheduled multicast of the packet. The participating nodes will send the router reply to the source. The path with the shortest router reply will be considere by the source and the router will established. The packet will be send to the destination only through that particular path [2]. Hence, routing overhead and rushing of packets will

International Journal of Computer Network and Security(IJCNS)
Vol5. No.1 – Jan-March 2013 Pp. 16-27
©gopalax Journals, Singapore
available at : www.ijcns.com

be reduced extensively. After proposed to generate the possible type's prevention techniques like backhole, flooding and wormhole attack in LGF protocol and also to provide the proactive measures for it.

A. Literature Layout

A Mobile Ad-hoc NETworks (MANETs), sometimes called a mobile mesh network or wireless ad hoc network, is a self-conFigureuring network of mobile devices connected by wireless links. Each device in a MANETs is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a voter. The primary challenge in building a MANETs is equipping each device to continuously maintain the information required to properly route traffic.

Compared to the wireless network or other infrastructure based networks, MANETs has the following advantages:

- They provide access to information and services regardless of geographic position.
- These networks can be set up at any place and time.
- They are flexible and powerful complements with automatic conFigureuration.
- There is no prearrangement.
-

B. Survey on Trust Based Solutions

K. Aishwarya, N.Kannaiah Raju and A. Senthamarai Selvan proposed a solution for blackhole attack in E-ODMRP. According to this proposed solution the Source node in E-ODMRP does not accept every first RREP but calls Previous received RREQ 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. 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.

Dynamic Learning System using DPRAODV: Payal N. Raj, Prashant B. Swadas *proposed* DPRAODV (detection, prevention and reactive AODV) to prevent security of black hole by informing other nodes in the network. It uses normal AODV in which a node receives the Route reply (RREP) packet which first checks the value of sequence number in its routing table. The RREP is accepted if its sequence is higher than that in the routing table. It also check whether the sequence number is higher than the threshold value, if it is higher than threshold value than it is considered as the malicious node. The value of the threshold value is dynamically updated in the time interval. The threshold value is the average of the difference of destination sequence number in each time slot between the sequence number in the routing table and the RREP packet. The node that is detected as the anomaly is black listed and ALARM packet is sent so that the RREP packet from that malicious node is discarded. The routing table for that node is not updated nor is the packet forwarded to others. This solution increases the average end to end delay and normalized routing overhead.

Farid Na¨ıt-Abdesselam, Brahim Bensaou, and Tarik Taleb *proposed a solution for wormhole attack.* When this attack targets specifically routing control packets, the nodes that are close to the attackers are shielded from any alternative routes with more than one or two hops to the remote location. All routes are thus directed to the wormhole established by the attackers. In the optimized link state routing protocol (OLSR), if a wormhole attack is launched during the propagation of link state packets, the wrong link information percolates throughout the network, leading to routing disruption.

They devise an efficient method to detect and avoid wormhole attacks in the OLSR protocol. This method first attempts to pinpoint links that may, potentially, be part of a wormhole tunnel. Then, a proper wormhole detection mechanism is applied to suspicious links by means of an exchange of encrypted probing packets between the two supposed neighbors (endpoints of the wormhole). The proposed solution exhibits several advantages, among which its non-reliance on any time synchronization or location information, and its high detection rate und
er various scenarios.

S.Vijayalakshmi and S.Albert Rabara *proposed a solution for wormhole attack.* Two solution have been proposed for preventing

International Journal of Computer Network and Security(IJCNS)
Vol5. No.1 – Jan-March 2013 Pp. 16-27
©gopalax Journals, Singapore
available at : www.ijcns.com

wormhole attack. First solution is given by the concept of leash for detecting and preventing wormhole attack. A leash is any information added to a packet in order to restrict the distance that the packet is allowed to travel. A leash is associated with each hop. Thus, each transmission of a packet requires a new leash. Two types of leashes are considered, namely geographical leashes and temporal leashes. A geographical leash is intended to limit the distance between the transmitter and the receiver of a packet. A temporal leash provides an upper bound on the lifetime of a packet. As a result, the packet can only travel a limited distance. A receiver of the packet can use these leashes to check if the packet has traveled farther than the leash allows and if so can drop the packet.

Another approach for detecting wormhole attacks is deploying directional antennae. The approach here is based on the use of packet arrival direction to detect that packets are arriving from the proper neighbors. Such information is possible due to the use of directional antennae. This information about the direction of packet arrival is expected to lead to accurate information about the set of neighbors of a node. As a result, wormhole attacks can be detected since such attacks emanate from false neighbors.

Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, And Nei Kato *proposed* a simple solution In this approach, the authors proposed an adaptive technique to mitigate the effect of a flooding attack in the AODV protocol. This technique is based on statistical analysis to detect malicious RREQ floods and avoid the forwarding of such packets. Similar to , in this approach, each node monitors the RREQ it receives and maintains a count of RREQs received from each sender during the preset time period. The RREQs from a sender whose RREQ rate is above the threshold will be dropped without forwarding. Unlike the method proposed in , where the threshold is set to be fixed, this approach determines the threshold based on a statistical analysis of RREQs. The key advantage of this approach is that it can reduce the impact of the attack for varying flooding rates.

Venkat Balakrishnan1, Vijay Varadharajan2, Uday Tupakula3, and Phillip Lucs4 *proposed* a solution on *Trust Integrated Cooperation Architecture* which consists of an obligation-based cooperation model known as *fellowship* to defend against both flooding and packet drop attacks. In this architecture, fellowship enhances its security decisions through a trust model known as *Secure MANET Routing with Trust Intrigue (SMRTI)*. In comparison with related models, SMRTI deploys a novel approach to communicate recommendations such that the deployed approach is free from well-known issues such as honest elicitation, free riding, bias of a recommender, and additional overhead.

C. MANETs has several security issue

- A MANETs system is much more vulnerable to attacks than a wired or infrastructure - based wireless network.
- Designing an effective security protocol for MANETs is a very challenging task.
- Many types of attacks are present in MANETs like black hole attack, rushing attack, jellyfish attack, neighbor attacks, wormhole attacks, and flooding attacks, Repeater attacker. All previous studies have considered only unicast networks in which there is only one sender and one receiver in a communication session and solutions for some of these attacks have been addressed.
- Although many researchers have addressed security issues for unicast, researchers on multicast security in MANETs is still at a very early stage due to several challenges specific to multicast operations such as group key management, Encryption, member access control, and secure routing.
- Eavesdropping on the wireless links. Nodes can be hijacked or captured.
- Dynamic topology. Nodes exchange route update information. Attacker can interfere or modify this.
- Nodes cooperate to make decisions, an attacker can refuse cooperation and disrupt the algorithm causing breakdown.
- MANET has low energy (battery), DoS occurs by making node send many packets until energy depletes causing disconnection of nodes

2. IMPLEMENT THE LGF PROTOCOL IN MOBILE AD-HOC NETWORK

The LGF protocol has been implemented by GPS-free covered location tracking system with geocast-enhanced AODV[2], In the case GPS it an infrastructure which consists be implemented in LGF protocol as MANET networks are infrastructureless and without any centralized authority. So this protocol particular distance only transmit the RREQ packets towards the destination node and also flood the RREP packets towards the source node, because it is GPS-free indoor location tracking system.

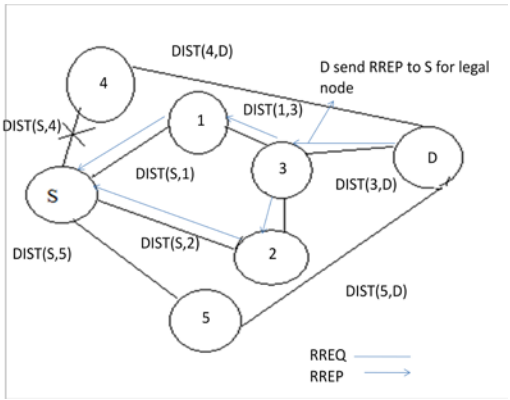
International Journal of Computer Network and Security(IJCNS)
Vol5. No.1 – Jan-March 2013 Pp. 16-27
©gopalax Journals, Singapore
available at : www.ijcns.com

For example Source S to Destination D in between total Distance (DIST), DIST(S,D)=100 meters but DIST(S, 4) =120 meters. Comparing these distance between DIST (S, 4) < DIST (S, D) = 120 < 100, this condition not satisfy and also automatically discard the RREQ packet because it is out of transmission area and another intermediate nodes in transmission coverage area in between source to destination DIST (S, 1)=40M, DIST (S,2)=52M, DIST (S,5)=70M, DIST (1,3) =60M, DIST(2, 3)=65M, DIST (3, D) =80M, DIST (S, 4)=120M, DIST (4,D)=130M, DIST(5,6)=75M, DIST (6,D)=78M

Above these intermediate nodes distance conditions satisfy and also send the route request packets to all intermediate nodes. This is a way of functioning in LGF protocol.

A. Implementation of the LGF in real MANET test bed

- Source node S wants to communicate with Destination node D.
- The source node S will multicasts the RREQ packets to all Intermediate Nodes (IN) with contain the IP address of the destination node D and also distance from the source S to destination D.
- The RREQ packet has received from the intermediate nodes; it will compare the distance in between source to destination. Otherwise ignore it and also drop the RREQ packet.
- Total distance between source to destination where, DIST(S,D)=100, these are all intermediate nodes distance from source to destination, DIST (S, 1)=40M, DIST (S,2)=52M, DIST (S,5)=70M, DIST (1, 3) =60M, DIST(2,3)=65M, DIST(3, D) =80M, DIST (S, 4) =120M, DIST(5,6)=75M, DIST (6,D)=78M
- Now compare the distance of intermediate nodes in between S to D.
  If (IN are 1, 2, 5, 3, 6< Source S to Destination D node distance)
  {
  These are all the IN between S to D, these conditions satisfy and also successfully sends the RREQ packet towards the destination node.
  }
  Else
  {
  Any IN out of the transmission area in between S to in the nodes sends Route Error (RRER) packet to the source node.
  }
- The RREQ packet has received from destination node, after send the RREP packet towards the intermediate nodes are 3, 1and 3, 2 and 6, 5 along with the source S node.
- The source S node has received from RREP packet to above these IN, after compare its distance from S to D.
- Whether the RREP to an intermediate nodes 3 to1 and 3 to 2 and 6 to 5 path has received exactly, which nodes first received via shortest path link from source to destination node, will be come under first in first out policy basis that path only choose of Source S correct route and also send the original data packet to the destination node this is the algorithm for LGF protocol. The LGF protocol process diagram is shown in Figure. 1.



Figureure.1 The LGF Protocol Implemented by Real MANET Test Bed without Using GPS-free Covered Location Tracking System

3. SECURITY THREATS IN MANETS

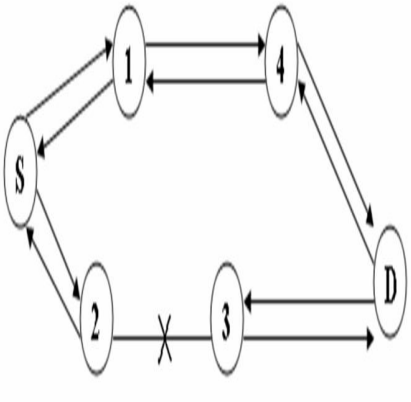
The current Mobile Ad-hoc NETwork allow for many different types of attacks. Although the analogous exploits also exist in wired networks but it is easy to fix by infrastructure in such a network. Current MANETs are basically vulnerable to two different types of attacks: active attacks and passive attacks. Active attack is an attack when misbehaving node has to bear some energy costs in order to perform the threat. On the other hand, passive attacks are mainly due to lack of cooperation with the purpose of saving energy selfishly. Nodes that perform active attacks with the aim of damaging other nodes by causing network outage are

International Journal of Computer Network and Security(IJCNS)
Vol5. No.1 – Jan-March 2013 Pp. 16-27
©gopalax Journals, Singapore
available at : www.ijcns.com

considered as malicious while nodes that make passive attacks with the aim of saving battery life for their own communications are considered to be selfish. This paper focus on vulnerabilities and exposures like backhole, wormhole and flooding attacks in the Mobile Ad-hoc NETwork.

B. Attacks against LGF

Blackhole Attack: In this attack, an attacker uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. An attacker listen the requests for routes in a flooding based protocol. When the attacker receives a request for a route to the destination node, it creates a reply consisting of an extremely short route. If the malicious reply reaches the initiating node before the reply from the actual node, a fake route gets created. Once the malicious device has been able to insert itself between the communicating nodes, it is able to do anything with the packets passing between them. Figure. 2 shows the blackhole attack.



Figureure. 2 The Blackhole attack is demonstrated in this Figureure by considering node 3 as attacker node

Wormhole attack: In a wormhole attack, an attacker receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the network from that point. Routing can be disrupted when routing control message are tunneled. This tunnel between two colluding attacks is known as a wormhole. Figure.3 explains the scenario of wormhole attack.

The wormhole attack is particularly dangerous for many ad hoc network routing protocols in which the nodes that hear a packet transmission directly from some node consider themselves to be in range of that node.

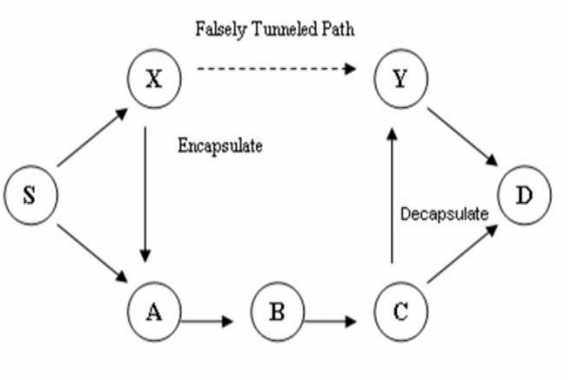


Figure. 3 The Wormhole Attack is demonstrated using a pair of colluding attackers like node X and Y

Flooding attack: The aim of the flooding attack is to exhaust the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance. A malicious node can send a large number of RREQs in a short period to a destination node that does not exist in the network. Because no one will reply to the RREQs, these RREQs will flood the whole network. As a result, all of the node battery power, as well as network bandwidth will be consumed and could lead to denial of service. Figure. 4 explains the state of flooding attack

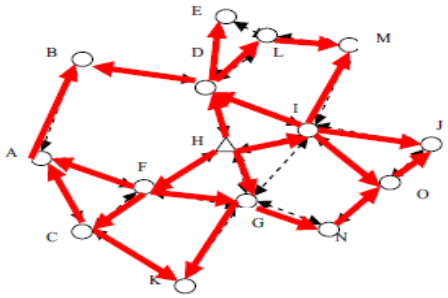


Figure. 4 The RREQ flooding is demonstrated in this Figureure using the attacker node H which continuously floods RREQ to other nodes in the Multicast group

4. TRUST BASED SOLUTION FOR BLACK HOLE, WORMHOLE AND FLOODING ATTACKS

This solution aims at preventing the attacks by establishing a trust relation between the nodes. Certificate chaining is a self organized PKI authentication by a chain of nodes without the use of

International Journal of Computer Network and Security(IJCNS)
Vol5. No.1 – Jan-March 2013 Pp. 16-27
©gopalax Journals, Singapore
available at : www.ijcns.com

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 Figure.5 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.

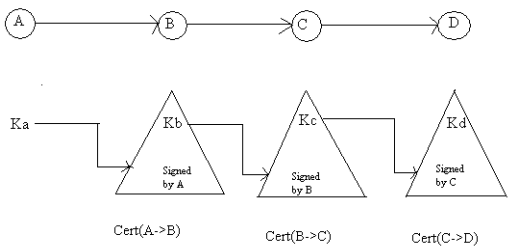


Figure. 5 The Certificate key chaining Figureure demonstrates the certificate issued by the neigbor nodes on taking into account the parameters and process proceeds throught the network for securing the protocol

Ka - public key of A

Kb - public key of B

Kc - public key of C
Kd - public key of D

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.

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.

International Journal of Computer Network and Security(IJCNS)
Vol5. No.1 – Jan-March 2013 Pp. 16-27
©gopalax Journals, Singapore
available at : www.ijcns.com

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.

A. Algorithm to prevent attack

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

  Cert (A 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.
- 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.
- Since same hash function is used by all nodes, the public key generated by different neighboring node would be same.

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

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

  When this packet reaches the next hop node
  - Next hop node checks its repository to see if the certificate is there.
  - Then it checks the certificate revocation list to find if the destination node is malicious or not.
  - If these two verification leads to a positive result, it forwards the $RREP_{CERT}$ to the next hop node .while doing so it appends the certificate from its repository.
- All intermediate nodes perform the same procedure until the final source is reached.
- 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.
- 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.

B. Another solution for LGF to prevent above attacks

This paper proposes Lagrange's interpolation and Shamir secret key sharing scheme solutions for above attacks. Basically, the function of interpolation is to find the missing data or lost data.

Lagrange's interpolation uses Lagrange's interpolating polynomial to find the missing data. This interpolation has been handled differently in modulo arithmetic. The concept of Lagrange's Interpolation is as follows. If $x_1, x_2, \ldots, x_k$ are distinct real numbers and $y_1, y_2, \ldots, y_k$ are real numbers, there is one and only polynomial q(x) of degree at most k-1, such that $q(x_i) = y_i$ for i=1,2,3…, k. The polynomial q(x) is given by

$$q(x) = \sum_{r=1}^{k} y_r \prod_{\substack{i=1 \\ i \neq r}}^{k} \frac{(x - x_i)}{(x_r - x_i)} \qquad (1)$$

International Journal of Computer Network and Security(IJCNS)
Vol5. No.1 – Jan-March 2013 Pp. 16-27
©gopalax Journals, Singapore
available at : www.ijcns.com

This interpolation is used differently in the field of modulo arithmetic. For a prime 'p', let Zp = { 0,1,2,....., p-1}, Zp is a field under addition and multiplication modulo p. If x € Zp and x ≠ 0 then 1/x=y if and only if xy ≡ 1(mod p). On proving the example Z_5. Here p = 5, Z_5 = {0,1,2,3,4}, ½=3 since 2x3 = 6 ≡ 1(mod 5). Similarly for ¼=4. Thus, the proof that the Lagranges interpolation holds good in the finite field Zp. That is if x_1, x_2,….,x_k are distinct elements of Zp and y_1,y_2, …., Y_k € Zp , then there exists one and only polynomial of q(x) of degree at most k-1 such that $q(x_i) = y_i$, where i = 1,2 3,…k.

In Shamir secret key sharing scheme, the source node generates a key and divides into 'n' pieces called shares. These pieces are then transmitted to a destination in different paths. The destination, after receiving these 'n' shares, by using the Shamir secret key sharing scheme, generates the original key. This concept of Shamir secret key sharing has been previously used in multipath routing. Shamir used the idea of interpolation in a different way using modulo arithmetic. The working of Shamir secret key sharing scheme is as follows: Shamir secret sharing (k, n) scheme is based on polynomial interpolation where the information is considered theoretically secure. In general on assumption, the dealer (may be the source) divides the secret and distributes shares to the shareholders. Shareholder must unconditionally trust the received share as a valid one. In Shamir secret sharing based on Lagrange's interpolating polynomial, there are 'n' shareholders P = {P_1 … P_n} and a mutually trusted dealer D. By using (k, n) threshold scheme with n=2k-1, we can recover the original key even when [n/2] = k-1 of the 'n' pieces are destroyed, but the other members cannot reconstruct the key even when keys are expose to [n/2] = k-1 of the remaining 'k' pieces. This scheme basically consists of two algorithms: Share generation algorithm and Secret reconstruction algorithm.

Share generation algorithm: The dealer D first selects a random polynomial f(x) of degree

t-1: f(x) = a0+ a1x +……..+ at-1xt-1in which s = a0 and all the coefficients a0, a1… at-1 are in the finite field Fp = GF (P) with 'p' elements. D computes n shares (s_1, s_2... sn) as

s_1 = f (1), s_2=f (2)…..s_n = f (n).

The dealer distributes each share si to shareholder Pi secretly.

Secret reconstruction algorithm: For any t shares (s_{i1},….,s_{ik}) where (i1,….,it) C {1,2,…..,n}, the secret s can be reconstructed. Thus the basic requirement of the secret sharing scheme is

1) With the knowledge of any 't' or more than 't' shares, shareholders can reconstruct the secret.

2) With the knowledge of any 't-1' or fewer than 't-1' shares, shareholders cannot reconstruct the secret S.

The working of Shamir secret key sharing is handled differently. First, the source node assumes a polynomial p(x) with any degree 'k'. The role of security provided by assuming a polynomial p(x) is that, it is very hard to identify and impersonate the source node with the exact polynomial that has been used for the generation of keys. In the basic Shamir secret key sharing scheme, with the help of this assumed polynomial a single key is generated and it will be divided into many shares for transmitting the key to destination among different paths. Here, instead of creating multiple shares of the same key, the source node creates separate keys for each node that are connected to it. The keys, after generated by the source node, are transmitted to corresponding node for which it has been created. The detailed method followed at the source node is as follows:

1) A polynomial *'P'* is generated by the source with degree *'k'* where the constant term in the polynomial is considered to be the super key.
2) A prime number *'p'* is assumed and the number of nodes that are present in the network is considered for generating keys.
3) The keys are generated using the Shamir secret sharing scheme with the help of the Lagrange's polynomial.
4) These keys are transmitted to the corresponding nodes that are present in the network. Care is taken not to store these keys at the source. This is to avoid one point of failure. (i.e.) if the source node is compromised then the keys that are stored become vulnerable and it may impact the security of the MANETs. The keys are got from the corresponding nodes at the time of verification.
5) The key values are transmitted to nodes in the encrypted form using RSA where in the key for encryption is the corresponding public key of that node. The RSA is used in this proposed scheme for transmission of keys instead of elliptic curve because it is efficient for the data with less time period. It also provides security with reasonable computation that is suitable for MANETs.
6) At source during key generation

$$N_i = E_{pub\ (i)}\ (D_i) \qquad (2)$$

International Journal of Computer Network and Security(IJCNS)
Vol5. No.1 – Jan-March 2013 Pp. 16-27
©gopalax Journals, Singapore
available at : www.ijcns.com

Where i = 1, 2, 3 … N, Epub corresponds to encryption using public key of their corresponding nodes. RSA is used for encrypting the packet, because it is impossible to decrypt the packet without the corresponding private key thereby increasing the security during the packet transmission. This act of encryption provides security against many attacks like replay attacks, packet fragmentation attacks etc. the key size used for the encryption of the packet may be 64 bits or may be lesser because the time to live for the packets is very small and it may not be possible to decrypt the packets within the TTL without the use of corresponding private key. Nodes other than the Source Node performs these following steps: When a packet from the source node is received, it decrypts it with the corresponding private key to get the key as the packet is encrypted with the public key of the corresponding node.

At the corresponding Node i

$$D_i = D_k (E_{pub\ (i)} (D_i)) \quad (3)$$

Where $i = 1, 2, 3 \ldots \ldots N$; D_k corresponds to decryption using private key of their corresponding nodes.

Then the source node verifies the genuineness of the nodes using the following procedure.

- For checking the genuineness of the nodes that are participating in the network, it sends a key request packet in the network. This key request packet is send to [n/2] nodes for which it has transmitted the keys. The following format of the packets is used for requesting the key and the reply for it.
- The source node receives the keys from its participating nodes that have been transmitted to them during key generation phase.
- Then it checks the genuineness of the node by substituting the keys received, in the scheme and if it arrives to the super key then the nodes that have sent the key are said to be genuine nodes. If the super key is not obtained at the first trial, then the different combination of these [n/2] nodes is tried. The super key will be arrived for every combination that is tried with the genuine keys and only single combination does not arrive at the super key is the combination with false values. And then this combination is analyzed and the malicious node is identified.

  After identification of the malicious node, an alternate path is computed in such a way that the malicious node is bypassed. The proposed solution is effective even when more than one attacker is present in the network. This proposed solution is a proactive type of solution because the security is provided at the time of tree or mesh creation.

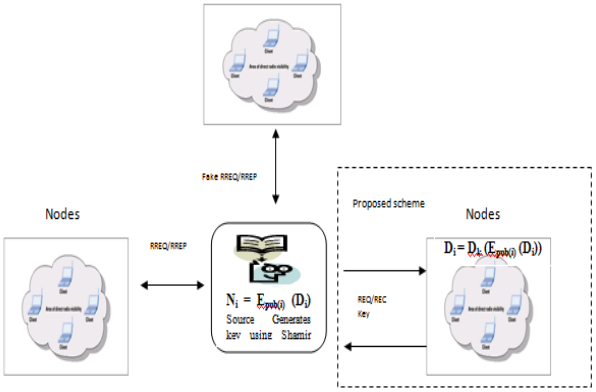


Figure. 6 Secure Routing Scheme in MANETs Figureure depicts how secret key is exchanged and how trusted nodes is manipulated

5. SIMULATION RESULTS

The simulation of work has been done by GloMoSim version 2.03[6], a scalable environment for Mobile Ad-hoc Network.

C. Simulation Parameters

Table I Simulation Parameters

Parameter	Value
Nodes	8
Simulation time	15 sec
Mobility	Random way point model
Packet size	512 bytes
Transmission area	100 m by 100 m
Queuing policy	First-in-first-out

The simulations are done using Glomosim version 2.03. The simulated network consists of 30 mobile nodes placed randomly within a 1000 m x 1000 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. The low traffic load value is used 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 30 seconds. Once this time expires, the mobile node chooses a random destination in the simulation area and then travels toward the newly

International Journal of Computer Network and Security(IJCNS)
Vol5. No.1 – Jan-March 2013 Pp. 16-27
©gopalax Journals, Singapore
available at : www.ijcns.com

chosen destination. Upon arrival, the mobile pauses for 30 seconds before starting the process again.

The attackers were positioned around the center of the multicast mesh in all experiments. The duration of each experiment was 300 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. Table.1 lists the values of the common parameters used in all the experiments.

6. RESULTS

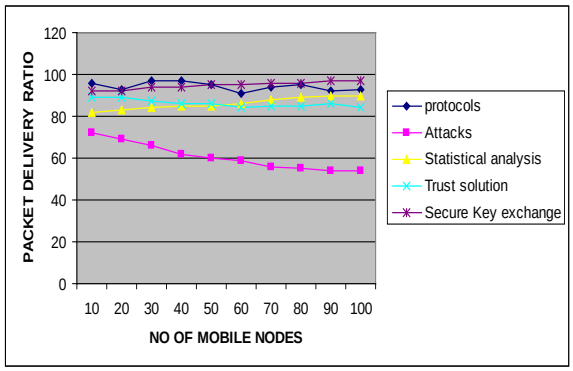


Figure.7 Blackhole Attack – Packet Delivery Ratio

Packet delivery ratio increases on an average by **23.4%** when secure key exchange solution is provided to prevent the black hole attack in LGF Protocol.

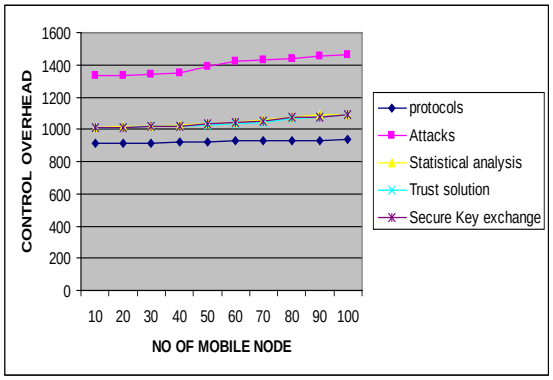


Figure. 8 Blackhole Attack – Control Overhead

Control overhead decreases on an average by **2.5%** when secure key exchange solution is provided to prevent the black hole attack in LGF Protocol.

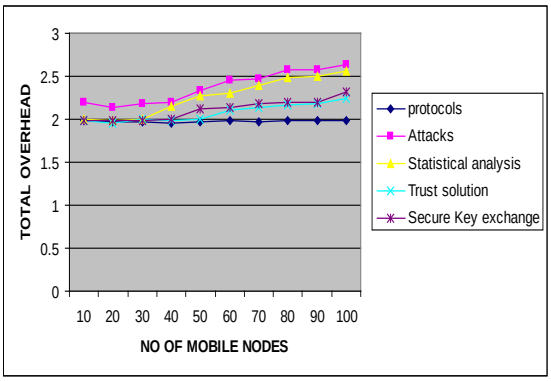


Figure. 9 Blackhole Attack – Total Overhead

Total overhead decreases on an average by **40%** when secure key exchange solution is provided to prevent the black hole attack in LGF Protocol.

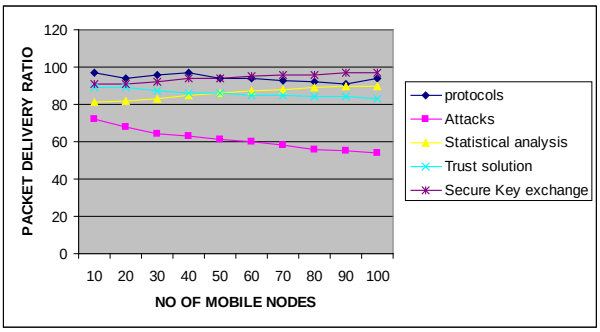


Figure. 10 Wormhole Attack – Packet Delivery Ratio

Packet delivery ratio increases on an average by **20%** when secure key exchange solution is provided to prevent the worm hole attack in LGF Protocol.

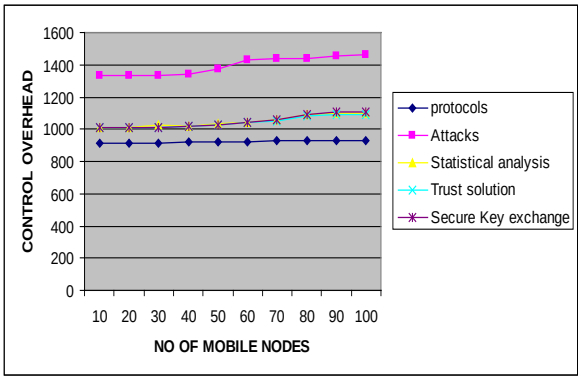


Figure.11 Wormhole Attack – Control overhead

International Journal of Computer Network and Security(IJCNS)
Vol5. No.1 – Jan-March 2013 Pp. 16-27
©gopalax Journals, Singapore
available at : www.ijcns.com

Control Overhead decreases on an average by **3 %** when secure key exchange solution is provided to prevent the worm hole attack in LGF Protocol.

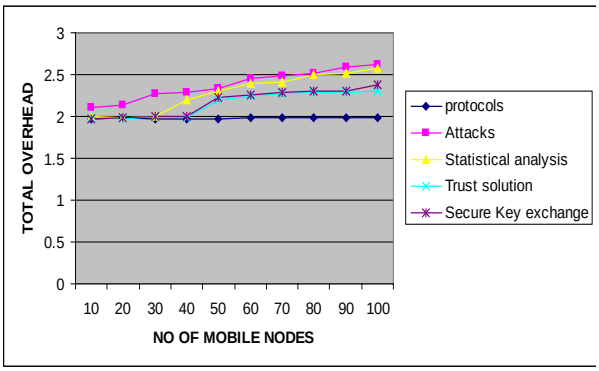


Figure. 12 Wormhole Attack – Total Overhead

Total overhead decreases on an average by **30%** when secure key exchange solution is provided to prevent the worm hole attack in LGF Protocol

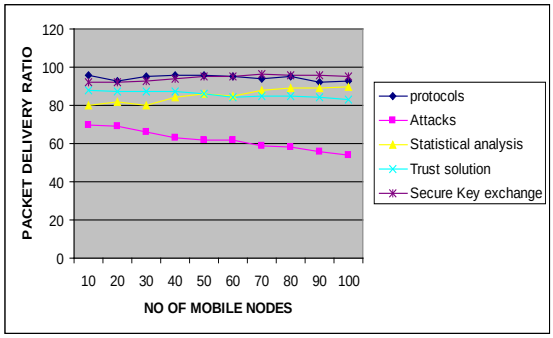


Figure. 13 Flooding Attack – Packet Delivery Ratio

Packet delivery ratio increases on an average by **20%** when secure key exchange solution is provided to prevent the flooding attack in LGF Protocol

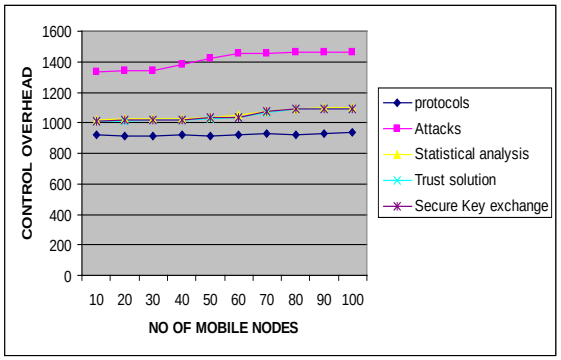


Figure. 14 Flooding Attack – Control Overhead

Control Overhead decreases on an average by **3%** when secure key exchange solution is provided to prevent the flooding attack in LGF Protocol.

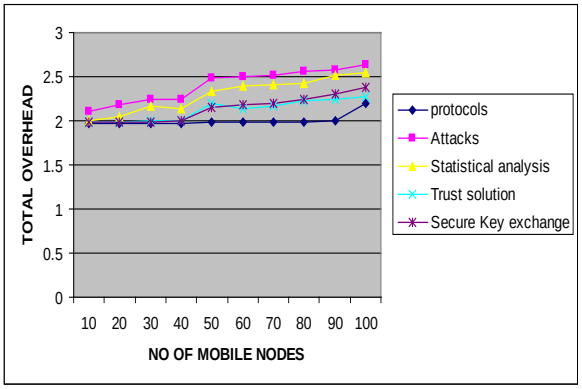


Figure. 15 Flooding – Total Overhead

Total Overhead decreases on an average by **45%** when secure key exchange solution is provided to prevent the flooding attack in LGF Protocol

7. CONCLUSION AND FUTURE WORK

This paper is aimed to preventing possible types of attacks like flooding, wormhole and blackhole in location-based geocasting and forwarding (LGF) routing protocol in MANETs. These attacks are mitigated using trust based solution called Certificate Key Chaining. But the results produced where not convincing, so Shamir Secret Key Sharing technique is incorporated and in the metrics a good convincing results is achieved from the simulated results we infer that Shamir Secret Key Sharing technique achieves a very good rise in PDR (Packet Delivery Ratio) and a reduced control overhead and total overhead when compared to the trust based solution. In future the same solution can be applied to other routing attacks and irrespective of any reactive protocols by actively changing the implementation techniques and to provide some modifications to decrease the control overhead.

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] L.A.Latiff, AAli1, chia-ching,Ooi2, N.Fisal3, "Locationbased Geocasting and Forwarding (LGF) Routing Protocol Mobile Ad hoc Network", Telecommunications, 2005.

Advanced industrial conference on telecommunications/service assurance with partial and intermittent resources conference/e-learning on telecommunications workshop. Aict/sapir/elete2005.Proceedings on 17-20 July 2005.

[3] Shalini Jain, Dr.Satbir Jain, "Detection and prevention of wormhole attack in mobile ad-hoc networks", International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010.

[4] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, And Nei Kato, "A Survey Of Routing Attacks In Mobile Ad Hoc Networks", Wireless Communications IEEE, volume :14, issues:5, 2007.

[5] V. Palanisamy, P.Annadurai, " Impact of Rushing attack on Multicast in Mobile Ad Hoc Network", (IJCSIS) International Journal of Computer Science and Information Security,Vol. 4, No. 1 & 2, 2009.

[6] Jorge Nuevo, "A Comprehensible Glomosim Tutorial", INRS.

[7] Hoang Lan Nguyen and Uyen Trang Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks", Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06).

[8] Garcia- Luna - Aceves and E. Madruga, "The Core Assisted Mesh Protocol", IEEE Journal on Selected Areas in Communications, vol. 17, no. 8, 1999.

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

[10] G.S. Mamatha and Dr. S. C. Sharma, "A Highly Secured Approach against Attacks in MANETS", International Journal of Computer Theory and Engineering, Vol. 2, No. 5, October, 2010.

[11] Li Shi-Chang, Yang Hao-Lan, Zhu Qing-Sheng, "Research on MANET Security Architecture Design", Signal Acquisition and Processing, 2010. ICSAP '10. International Conference on, 10.1109/ICSAP, 2010.19, Page(s): 90 – 93.