Generic Secure Key Sharing Technique for Prevention of Security Attacks on Location based Geo-casting and Forwarding Routing Protocol in Mobile Ad-hoc Networks

A. Amuthan
Associate Professor
Department of CSE
Pondicherry Engineering College

N. Sreenath
Professor
Department of CSE
Pondicherry Engineering College

P.Elango
Assistant Professor
Department of IT
Perunthalaivar Kamarajar Institute of Engineering and Technology

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 an applications in exists such as 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. Along the route, participating nodes will send a Route Reply (RREP) packet to the source via intermediate nodes. With Path Accumulation (PA), these routes will be stored and used in the packet is forwarding has via the routes discovered beforehand [2]. Hence, routing overhead and rushing of packets will 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.

2. IMPLEMENT THE LGF PROTOCOL IN MOBILE AD-HOC NETWORK
The LGF protocol has implemented by GPS-free covered location tracking system with geocast-enhanced AODV[2], if we will be using with GPS means this is an infrastructure not eligible for LGF protocol implementation because it is an infrastructure based. In the proposed work of the LGF protocol is without any infrastructure and centralized system routing protocol in MANET. 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.

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.

2.1 Implementation of the LGF in real MANET test bed

1. Source node S wants to communicate with Destination node D.
2. 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.
3. 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.
4. 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

5. 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 D in the nodes sends Route Error (RRER) packet to the source node.
}
6. 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.
7. The source S node has received from RREP packet to above these IN, after compare its distance from S to D.
8. 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.

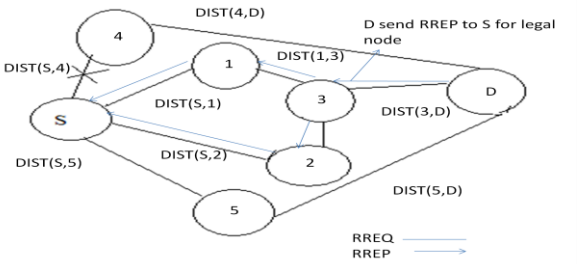

Fig 1: The LGF Protocol Implemented by Real MANET Test Bed without Using GPS- free Covered Location Tracking System

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 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.

4. TRUST BASED SOLUTION FOR BOTH 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 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 2. 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 (AJB). 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.

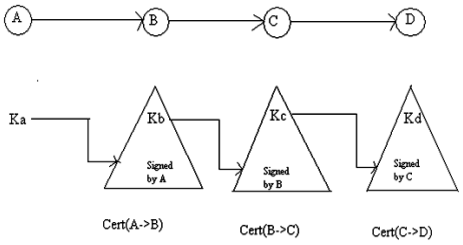

Fig 2: Certificate key chaining

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

4.1 Algorithm to prevent the 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 are issued is convinced about the security level of the node.
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. For, Wormhole timer = 2* transmission range / speed of packet.
7. Certificates issued are stored in the repositories of the issuer.
8. For example if node B is within the range of node A , node A issues certificate to B
9. Cert (A $\rightarrow$ B) = [ID_B, K_b, t , e, S] K_A
10. 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.
11. 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.
12. Since same hash function is used by all nodes, the public key generated by different neighboring node would be same.
13. K_B =H (ID_B)
14. 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.
15. After the certification process the destination node sends the authenticated message append with certificate taken from the corresponding nodes repository.
16. The certified ($JREP_{CERT}$) packet from the destination would be of the form:
17. [Source id, next hop id, final destination id , certificate chain]
18. When this packet reaches the next hop node
19. Next hop node checks its repository to see if the certificate is there.
20. Then it checks the certificate revocation list to find if the destination node is malicious or not.
21. 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.
22. All intermediate nodes perform the same procedure until the final source is reached.
23. 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.
24. 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.

4.2 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

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

---------- *(1)*

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

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 $P = \{P_1 \ldots P_n\}$ 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.

1) Share generation algorithm: The dealer D first selects a random polynomial *f(x)* of degree *t-1*: $f(x) = a_0 + a_1 x + \ldots\ldots + a_{t-1}x^{t-1}$ in which $s = a_0$ and all the coefficients $a_0, a_1 \ldots a_{t-1}$ are in the finite field $F_p = GF(P)$ with *'p'* elements. D computes n shares $(s_1, s_2 \ldots s_n)$ as

$$s_1 = f(1), s_2 = f(2) \ldots\ldots s_n = f(n).$$

The dealer distributes each share s_i to shareholder P_i secretly.

2) Secret reconstruction algorithm: For any t shares $(s_{i1}, \ldots, s_{ik})$ where $(i_1, \ldots, i_t)$ C $\{1,2,\ldots\ldots,n\}$, 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

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

Where $i = 1, 2, 3 \ldots N$, E_{pub} 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*

$$D_i = D_k\,(E_{pub\,(i)}\,(D_i)) \qquad \text{---------- (3)}$$

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.

1. 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.
2. The source node receives the keys from its participating nodes that have been transmitted to them during key generation phase.

3. 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.

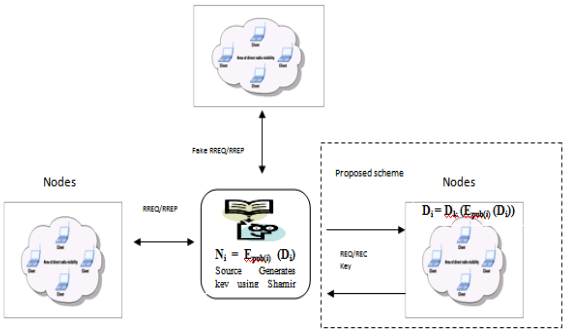

Fig 3: Secure Routing Scheme in MANETs using Secret Key Sharing

Theorem: The super key can be reconstructed from the keys that are collected from the nodes.

Proof:

This scheme is based on polynomial interpolation. Given k points in the 2-dimensional plane $(x_i, y_i)\ldots\ldots\ldots, (x_k, y_k)$, with distinct x_i's, there is one and only polynomial $q(x)$ of degree $k-1$ such that $q(x_i) = y_i$ for all i.

Without loss of generality, we can assume that the data D is number and can be divided into pieces D_i, then pick random $k-1$ degree polynomial $q(x) = a_0 + a_1x + \ldots\ldots\ldots + a_{k-1}x^{k-1}$ in which $a_0=D$, and evaluate

$$D_1 = q(1) \ldots \ldots \ldots D_i = q(i) \ldots \ldots \ldots D_n = q(n).$$

Given any subset of k of these D_i values (together with identifying indices), we can find the coefficient of $q(x)$ by interpolation, and then evaluate $D=q(0)$. Knowledge if those $k-1$ values do not suffice in order to calculate the value D.

Let p be prime number exceeding k and n. Let $D < p$. Choose a random k-1 degree polynomial

$$q(x) = a[0] + a[1]x + a[2]x^2 + \ldots\ldots\ldots + a[k-1]x^{k-1} \quad \text{----------(4)}$$

with $a[0] = D$ and the co-efficients $a[i] \in Z_p$ for $i = 1,2,3, \ldots\ldots\ldots, k-1$.Defining

$$D_i = q(i) \pmod p \quad \text{----------(5)}$$

For $i=1,2,\ldots n$. Then n D_i pieces will be distributed to all nodes .We can construct the number D from any of the k D_i pieces with their node ID's. Consider a subset of k of these D_i pieces, say $D_{i1}, D_{i2}\ldots\ldots\ldots D_{ik}$. By Lagrange's interpolation we can find unique polynomial $f(x)$ of degree at most $k-1$ such that $f(i_j) = D_{ij}$ for $j=1, 2\ldots k$. such that polynomial $f(x)$ is given by

$$f(x) = \sum_{r=1}^{k} Di_r \prod_{\substack{j=1 \\ j\neq r}}^{k} \frac{(x - i_j)}{(i_r - i_j)}$$

---------- (6)

Since $q(x)$ and $f(x)$ satisfy the same hypothesis, by uniqueness of Lagrange's interpolation $f(x) = q(x)$ for all $x \in Z_p$. In particular $q[0] = f[0]$. Hence with this the value of D can be reconstructed. This 'D' value is the value obtained after substuiting the key values that has been received by the source node in the equation (7). Once the value of 'D' is obtained (i.e) the super key from the above equation (7), then the value is compared with super key of the polynomial assumed by the source.

$$D = q[0] = \sum_{r=1}^{k} Di_r \prod_{\substack{j=1 \\ j\neq r}}^{k} \frac{(i_j)}{(i_j - i_r)}$$

---------- (7)

With this the original super key (i.e.) the constant term of the polynomial 'D' value can be reconstructed. The Shamir secret key has been analyzed by scenarios. The source node generates a polynomial of its own and just substitutes the random values for different participating nodes. An attacker cannot impersonate the source because the process of guessing the polynomial is very complicated and very tedious work. After generation of keys for all participating nodes, it then transmits it to the concern node through the communication channel. An attacker tries to capture the packets that transmit to the channel and look for information. If the data is sent as raw data, it is vulnerable and is easier for an attacker node to impersonate the intercepted node on the future. Here in our scheme, we use encrypted transmission using RSA, a public key encryption system. As the source node uses RSA for encryption, the data should be encrypted using the receiver's public key and only the receiver's private key alone can decrypt the value. When the attacker intercepts or interrupts the communication channel, it can receive only the encrypted packet and cannot decrypt because attacker does not possess the corresponding private key. This method, not only provide security to the data using encryption but also it provides security against various attacks such as reply attack etc,

Consider the scenario, where the attacker captures the packets from the communication channel and it tries to reply the same packet to the source or any other node in the network ends up in a failure, because the packet that is sent is encrypted using the corresponding public key of the nodes and cannot impersonate other nodes in the network. The idea of secret sharing is to generate a secret and send it to the participating nodes in the network. But the basic security nature of this scheme lies in the polynomial that is generated by the source node and the consideration of the prime number by the source node. For identification of the malicious nodes in the network, it requires n-1 node values as an input. But the main advantage of this scheme is that, it does not increase the network congestion by repeatedly transmitting values in the network, rather the computation complexity of the source node alone increases, which thereby does not the affect the entire network.

5. SIMULATION RESULTS

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

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 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 the 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.

Table 1. Simulation parameter

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

6. RESULTS

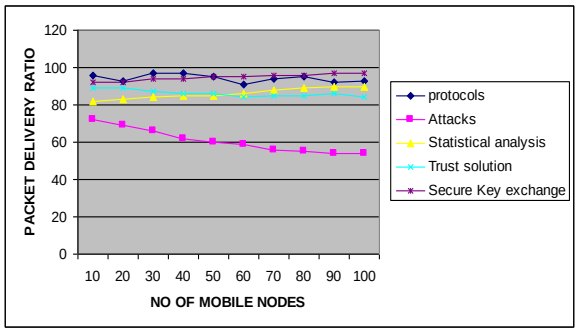

Fig 4: Blackhole Attack – Packet Delivery Ratio

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.

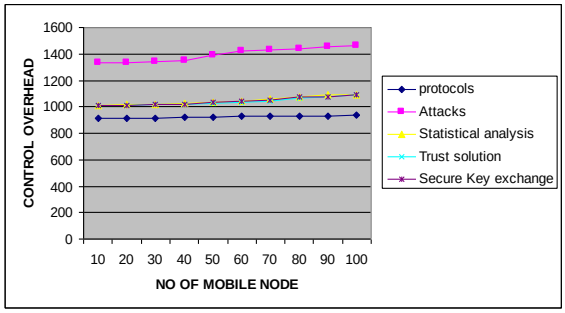

Fig 5: Blackhole Attack – Control Overhead

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**.**

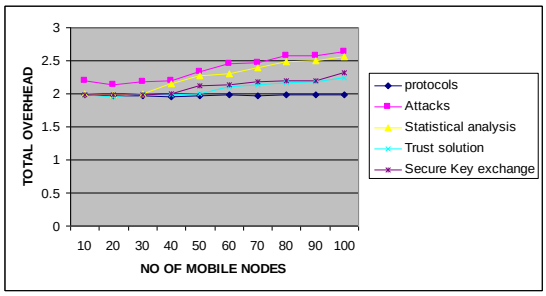

Fig 6: Blackhole Attack – Total Overhead

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

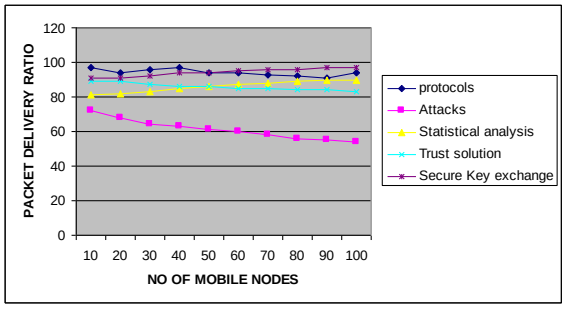

Fig 7: Wormhole Attack – Packet Delivery Ratio

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.

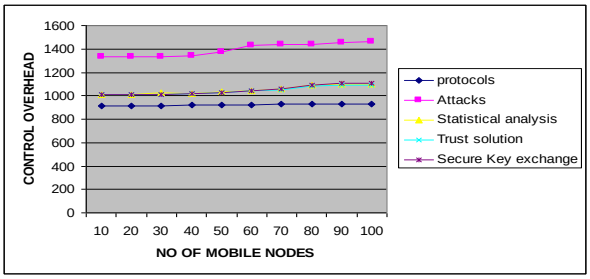

Fig 8: Wormhole Attack – Control overhead

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

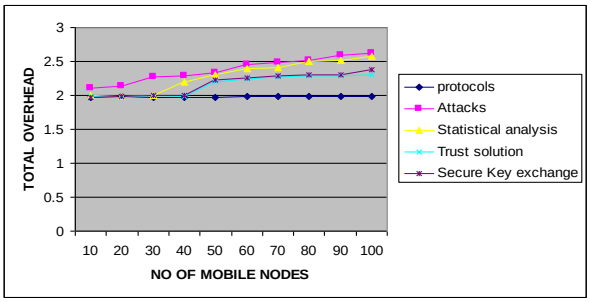

Fig 9: Wormhole Attack – Total Overhead

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

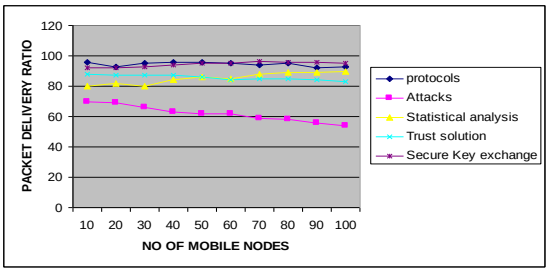

Fig 10: Flooding Attack – Packet Delivery Ratio

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

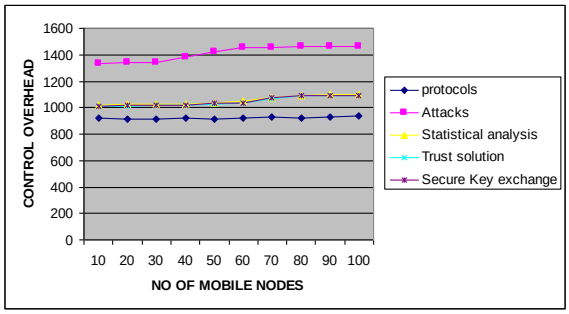

Fig11 : Flooding Attack – Control Overhead

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

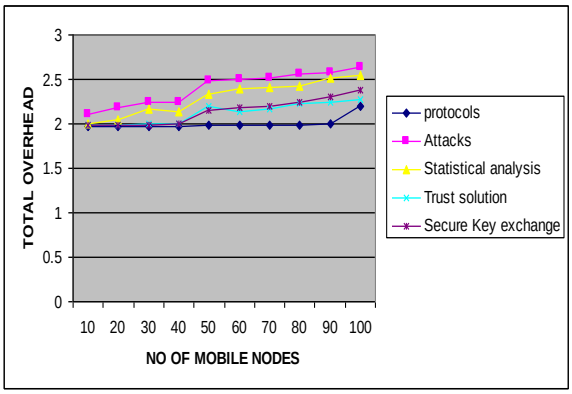

Fig 12: Flooding attack – Total Overhead

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

In this paper is intend to prevent possible types of attacks like flooding, wormhole and blackhole in location-based geocasting and forwarding (LGF) routing protocol in MANETs. In this work two prevention techniques are used for each and every attack in LGF protocol as well as to overcome the impact of attacks in the protocol. 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 it will be making more secure and efficient product to implement in the real time applications. The future work is aimed at extending the proposed solution to the other reactive protocols by actively changing the implementation techniques and to provide some modifications to decrease the control overhead.

8. 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, "Location based 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.