Journal of Telecommunications System & Management

Augustine and Sebastian, J Telecommun Syst Manage 2016, 5:2
DOI: 10.4172/2167-0919.1000130

Research Article Open Access

Routing Mechanism for Mobile Ad Hoc Networks with Improved Security Features

Augustine A* and Sebastian EJ

Department of ECE, Wireless Network Research Centre, Vimal Jyothi Engineering College, Kerala, India

Abstract

MANET is a type of wireless network without a fixed topology and consists of set of self-organized nodes. The nodes are randomly, frequently and unpredictably mobile. The inherent features make them an ideal choice in military and civilian communication applications. Major performance constraint of these types of networks comes from security attacks due to the dynamic topology and lack of centralized monitoring authority. Both passive and active attacks adversely affect the normal functionality of the network. Passive attackers monitor the network traffic and nodes in the networks. Active attacks like Blackhole attackers can drop packets partially or completely from the network. Secure routing protocol can conceal the identities and locations of route, source and destination to provide security and privacy from intruder's attacks. So in this paper, a route selection method is introduced for MANET which improves the security features for source, destination and route against passive attacks and specified active attacks. The developed method dynamically partitions the entire communication area in to different zones and randomly chooses a position from the divided zones as the temporary destination. The node which is very close to the position is selected as the random forwarder node and data is transmitted through random forwarder node using GPSR. The proposed method provide both identity and location anonymity to nodes. Methods are also proposed for avoiding the timing attacks. Position of active attacker like Blackhole attackers in the route are obtained and eliminated by using Homomorphic Message Authentication method.

Keywords: Mobile Ad Hoc networks; Routing protocols; Security; Passive and active attacks

Introduction

Without a fixed topology collection of mobile nodes forming an instant network is called MANET. The nodes are randomly and unpredictably mobile can move out or join in the network freely [1]. In the communication field the importance of MANET are very high because of the self-organizing ability of the networks. These networks are very attractive in military applications because of rapid deployment and reconfiguration capabilities. In tactical communications with unfavorable environments, security sensitive operations are essential. MANET is an open environment and it is susceptible to many security attacks due to dynamic topology and lack of centralized monitoring authority. Secure routing protocols conceal the identities about the route, source and destination to provide security and privacy from the attacks. Both active and passive attackers can affect the performance of the routing protocols. Limited resource is an inherent problem in MANETs, in which each node operates under an energy constraint situation. The scalability and energy efficiency of existing secure routing protocols are poor while considering the delays and overhead introduced by the cryptographic methods, and also the cost of implementation is a major drawback.

For providing high degree of security against both passive and active attacks [2] for the routing path and nodes in the network with low cost and high efficiency, this paper introduced an algorithm. This algorithm can select a secure and non-traceable route for the data transmission and performs some security methods for the source and destination node anonymities [3-5]. The developed algorithm for the route selection under both passive and active attacks is referred to as Improved Security Providing Routing method (ISPR) in this paper.

Secure route selection method used in ISPR method is the dynamic zone partition and randomized temporary destination position selection from the partitioned zones. In this method the network area is partitioned dynamically in to vertical and horizontal zones in each step of route selection. Then it selects any position from the partitioned zone as the temporary destination position and a node very close to this temporary destination position as the random forwarder node. Selection of temporary destination positions is carried out randomly, so the route formed by this method is strictly secure and unpredictable by an attacker.

For providing identity anonymity to nodes, ISPR uses the pseudo identity for a node. Notify and Go and Destination Zone Broadcasting scheme are the two methods used for providing anonymity to source and destination nodes against timing attacks.

An active attacker can modify, reroute or drop the packets from the networks depends on its nature. Blackhole attacks are very common in MANETs. All the nodes in the route calculation the packet delivery rate in each step. If the packet delivery rate is too small, then the node can assume the presence of Blackhole attacker in the route dropping the packets. Active attacker like Blackhole attacker's position can be efficiently found out by the using the Homomorphic Message Authentication method in ISPR algorithm. Homomorphic Message Authentication is a concept derived from the Homomorphic encryption method. The main advantage of Homomorphic encryptions is that, it allows complex mathematical operations to be performed on encrypted data without compromising the encryption. So the route selected and nodes in the network are secure from both passive and active attacks by ISPR methods.

The rest of the paper organized as follows. In section 2 we review some security protocols like AO2P, ANODR, ALARM and ALERT.

***Corresponding author:** Augustine A, Department of ECE, Wireless Network Research Centre, Vimal Jyothi Engineering College, Kerala, India, Tel: 0460 221 3399; E-mail: anupriyaaugustine@gmail.com

Received August 01, 2015; **Accepted** February 17, 2016; **Published** February 28, 2016

Citation: Augustine A, Sebastian EJ (2016) Routing Mechanism for Mobile Ad Hoc Networks with Improved Security Features. J Telecommun Syst Manage 5: 130. doi: 10.4172/2167-0919.1000130

Proposed methodology is detailed in section 3. Simulation and discussion are presented in section 4 and section 5 is the conclusion.

Literature Review

Security is a major performance factor for reliable communication in MANET. The inherent features of MANET make it susceptible to many security attacks which may completely or partially destroys and changes the information contents and networks. This will demands secure routing protocols to provide a very high level of security in MANET. Different techniques are used in secure protocols to achieve the goal of security [6-10]. Secure routing protocols conceal the identities about the route, source and destination to provide security and privacy from intruder's attacks. Both active and passive attackers can affect the performance of the routing protocols and may leads to fatal effects in the communication. There are so many secure routing protocols are used to prevent the disastrous consequences by these attackers.

Routing protocols in MANET which provides security features for the rote and nodes in the network are called anonymous routing protocols. Anonymous routing protocols are important in MANETs to provide secure communications by hiding node identities and preventing traffic analysis attacks from outside observers. Anonymity in MANETs includes identity and location anonymity of data sources that is the sender of data and destinations that is the recipients of the data, as well as route anonymity. Identity and location anonymity of sources and destinations means it is very difficult to for other nodes to obtain the real identities and exact locations of the sources and destinations in the network. Route anonymity means that the attackers, either in the route or out of the route, cannot trace a packet flow back to its source or destination, and any node has no information about the real identities and locations of intermediate nodes in the route.

The scalability and energy efficiency of existing secure routing protocols are poor, while considering the delays and overhead introduced by the cryptographic methods. Also the cost of implementation is a major drawback to provide high security in MANET. AO2P, ANODR, ALARM, ALERT etc. are some recently proposed anonymous routing protocols in MANET.

Ad Hoc on-demand position based private routing protocol

Xiaoxin Wu and Bharat Bhargava proposed a protocol called Ad Hoc On-Demand Position Based Private Routing Protocol (AO2P) [11]. In addition to node ID, extra information, such as the positions of the nodes, is used for making routing decisions. Since it is unlikely that two ad hoc nodes are concurrently at exactly the same position, the match between a position and an ID is unique. Therefore, in position based routing algorithms, if the positions have been exposed for routing, node IDs do not need to be revealed. If an adversary cannot match a position to a node ID correctly, node anonymity can be achieved.

In AO2P route discovery is done by using only the position of the destination. Real identities of source, destination and forwarding nodes are confidential and data packet uses the pseudo identifiers of the source, destination and forwarding nodes. Route is established by receiver contention scheme in AO2P. R-A02P is another, in which the position of a reference point is used for establishing the route instead of destination position.

Anonymous on demand routing protocol

Jiejun Kong, Xiaoyan Hong introduced an anonymous routing protocol for MANET is called Anonymous On Demand Routing (ANODR) [12]. ANODR have three phases on this routing mechanism. That is the anonymous route discovery, anonymous route maintenance and anonymous route forwarding. Anonymous route discovery establishes an on demand route. Trapdoor is a common concept in cryptographic functions for providing security in route discovery. The intermediate nodes embedded a cryptographic onion and symmetric key on the route request packets for back route selection and security. Except the first route discovery, ANODR is identity free and incurs no public key encryption overhead in route request broadcasted. For anonymous route maintenance, the routing table entries are recycled upon timeout.

Anonymous location aided routing protocol

Defrawy and Tsudik proposed a topology based secure routing protocol for MANET named as Anonymous Location Aided Routing (ALARM) [13]. Nodes authentication and locations secure data forwarding in ALARM is by using the node's current locations. Identification of nodes at certain locations in ALARM is relies on Group Signature to create pseudonyms. Group Manager helps to identify the nodes which are provided with the Group Signature. A private key is generated by all the group members and this key is concealed from other nodes. Group signature is produced from this private key. Each node also creates a public key and is revealed only for the group manager. Group public key is common to all members in the group. This provides identity and location anonymity in ALARM.

Anonymous location based efficient routing protocol

Haiying Shen and Lianyu Zhao introduced Anonymous Location Based Efficient Routing Protocol (ALERT) [14]. ALERT provides both identity and location anonymity to the route and nodes in the networks without using any complex cryptographic techniques. Hierarchical partition is the main technique used in ALERT for implement security to the route. This dynamic zone partition and randomized temporary destination position selection methods used in ALERT can create a route, which is undetectable by the attackers. For the identity anonymity of nodes networks, ALERT uses a dynamic pseudonym as its node identifier.

ALERT provides security against the passive attacks in the networks only. ALERT takes some assumptions about the networks such as, attackers cannot issue strong active attacks like as Blackhole attacks, attackers can only perform intrusion to a proportion of all nodes and the encrypted data are secure to a certain degree when the key is not known to the attackers. But in the real scenario, the MANET routing can be affected with different types of active attacks also.

Observations

MANET is a dynamic, infrastructure less and decentralizes network. The self-configuration ability of MANET constitutes a wide variety of applications in tactical and civilian fields. So the development of a routing protocol which satisfies all the performance enhancement features have great impact in networking fields. Security is the major problem in the reliable communication in MANET. The inherent features of MANET makes it susceptible to many security attacks which may completely or partially destroys and changes the information contents. This demands a secure routing protocol to provide a very high level of security in MANET.

Existing anonymous routing protocols uses different techniques to provide anonymity [15]. Most of the current approaches provide anonymity to the routing mechanisms based on high cryptographic methods or complex algorithms. Existing anonymous routing protocols

uses either the hop by hop encryption or redundant traffic method, which generate high cost in the networks. Also, some protocols are unable to provide complete source, destination, and route anonymity protection. AO2P, ANODR, ALARM and ALERT are some of the recently developed anonymous routing protocol for MANET.

Table 1 shows the comparison of these protocols based on the anonymity provided to the nodes and route. From these observations it can be concluded that, the existing anonymous protocols in MANET are not completely bulletproof from all the attacks. Some of the method can provide better security to the network, but they are unable to handle both passive and active attacks in the networks. Limited computational and resource availability of the nodes in the networks stops the implementation of complex algorithms for security. Traffic overhead created du tot the security algorithm and cost generated by the algorithm are two important parameters in the networks, which describe the efficiency of anonymous routing protocols.

Improved Security Providing

Routing method in MANET

Wireless ad hoc networks are an open environment and it is susceptible to many security attacks due to dynamic topology and lack of centralized monitoring authority. Secure routing protocols conceal the identities about the route, source and destination to provide security and privacy from intruder's attacks. So a secure route selection method is introduced for Mobile Ad Hoc network with improved security features against both passive and active attacks. The resulting method is referred to as Improved Security Providing Routing method (ISPR) in this paper.

Figure 1 shows the block diagram of the work. The block diagram contains two phases. In the first phase of the works concentrated on the secure route selection and source and destination protection methods against passive attacks. On the second phase, is the extension phase of the work mainly focused on providing security against active attacks like Blackhole attacks in the networks?

The methodologies used for the proposed method are pseudo node identity instead of real MAC address of the node in order to provide identity anonymity for the nodes. The secure route selection methodologies are based on the dynamic zone partitions of the network area and randomized selection of temporary destination position from the partitioned zones. This route selection procedure creates a non-traceable route and provides security to the route formed from passive and active attackers. Source and destination node required some protection techniques against timing attacks. Notify and Go mechanism at the source node and Destination Zone Broadcasting at the destination provides security against the timing attacks.

As the extension part of the work, concentrated on the active attacker security problems. Active attacker like Blackhole attacker drops packets from the nodes. This attacker's presence in the network can be identified by the packet delivery ratio calculation and attacker position is obtained by a method called Homomorphic Message Authentication scheme. So by using these techniques a new route can be selected without the presents of attacker node in it. The proposed method not based on any high cost encryption techniques for providing security against Blackhole attacks. The existing works provides security with high cost cryptographic methods. The Homomorphic Message Authentication scheme can provide a new route which eliminated the presence of the attacker node, with low cost and low latency in the networks. So the two phases of the works completely protect the data transmission through the networks from active and passive attacks.

The attacker node in the network is a battery powered node and usually it has limited resources like a normal node in the network. The passive attacker can only monitor the nodes and data transmitted through the network. They cannot able to induce any modifications in the data packets. But the passive attacker can induce some active attack in the network. The active attacker node can able to modify the packets, rerouted the packets and drop the packets. That means the active attackers affect the complete functionality and reliability of the entire networks. Due to the limited available resources and computational ability the attacker node cannot brutally decrypts the encrypted data packets within a reasonable time. So the encrypted data packets are secured to an extent. But some attackers can induce some adverse effects on the nodes in the networks. Therefore the nodes in the networks should also secure to provide successful communication. With the continuous observation of the networks and traffic in network, an attacker node can find the position of source, relay and destination nodes. It may results some serious attacks in the networks. So the location anonymity of the nodes in the networks is also very important. For that purpose the secure route selection method and source and destination protective techniques are developed in this work, which provides location and identity anonymity for all the nodes in the networks.

A transmission session is the time period that a source and destination interacts with each other. For providing identity anonymity for a node in the network the ISPR method uses a pseudonym as its node identifier instead of the real MAC address. The pseudonym is generated by using the real MAC address and the current time stamp. The time stamp is precise enough to avoid the re computation of the pseudonym by the attacker nodes. There are so many nodes are present in the network for an attacker to listen. This will creates high computational overhead for the attacker nodes and the attacker node do not successes to re compute the pseudonym of the nodes in the networks. This method provides some identity anonymity for the nodes in the route and in the networks.

For the communication session, the routing method needs the location and public key of all the nodes in the networks. Distributed secure position service method can be used for obtain the location and public keys of the nodes. An Ad Hoc node can able to obtain its position through GPS. Each node has a geographic region around a fixed center called virtual home region. A number of trusted nodes are distributed in the networks, which are acts as the location servers. A node periodically updated its position to the servers located in its virtual home region. If a node wants to get the position and public key

Protocol	Proactive/ Reactive	Routing Mechanism	Topology/ Geographic	Identity anonymity	Location anonymity	Route anonymity
AO2P	Reactive	Hope by hope encryption	Geographic	Source, Destination	Source, Destination	No
ANODR	Reactive	Hope by hope encryption	Topology	Source, Destination	No	Yes
ALARM	Proactive	Redundant traffic	Topology	Source, Destination	Source	No
ALERT	Reactive	Randomize	Geographic	Source, Destination	Source, Destination	Yes

Table 1: Comparison of anonymous routing protocols in MANET.

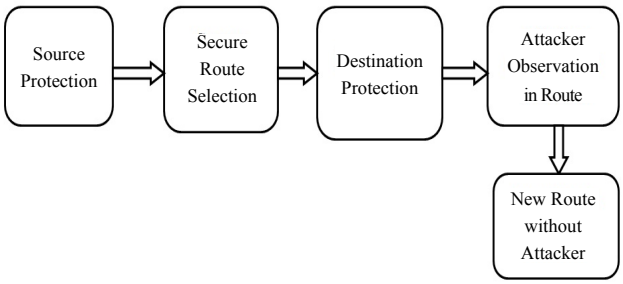

Figure 1: Block diagram of proposed mechanism.

of another node in the network, it sends a request to the corresponding node's server. The server node will return the encrypted position and public key to the requested node. The cost of pseudonym and location exchange is used as performance metrics to analyze the efficiency of the route selection method. The cost should be low compared to the regular communication message to provide high performance efficiency and reduced latency. This method provides a secure location service in the Ad Hoc networks. In this paper, concentrates on the secure route selection method and nodes anonymity protection schemes.

Destination zone creation

In the ISPR method a secure route is selected to avoid the passive attacks. The route formed by the dynamic zone partition and randomized temporary destination position selection created a highly secure and untraceable route. So the nodes in the route are secure and can avoid the attacker's interaction with the nodes in the route.

The first step of route selection process is the destination zone creation. The zone in which the destination node resides is called the destination zone (Z_D). The destination zone contains the destination node along with some other nodes in the network. For the destination zone creation the source node consider the entire network area as a rectangle in shape. The information of the bottom right and upper left boundary of the network area is configured in to each node when it joins the system to locate its position in the network. The source node portioned the network area in to two zones alternatively in horizontal and vertical manner to separate it from the destination node. The zone in which destination node presented is portioned in each steps for the creation of the destination zone. The number of partitions required to generate the destination zone is represented as H. H is calculated by using the equation,

$$H = \log_2\left(\frac{\rho.G}{k}\right)$$

Where ρ is the network density, G is the size of the entire network area and k is a predefined integer which represents the number of nodes needs to be in the destination zone.

After H number of partitions in the network, destination zone is created. The size of the destination zone created is, $\frac{G}{2^H}$.

Figure 2 shows the network area partition process to create the destination zone. The source first partitioned the entire network area horizontally in to two zones. Then there are three more partitions are conducted for the destination zone creation. The shaded region in the Figure 2 shows the formed destination zone, where destination node presents after the four partitions in the network.

The equations used for calculating the two side length of the H th partitioned zones are,

$$b(h, l_B) = \frac{l_B}{2^{h/2}}$$

Where a (h, l_A) and b (h, l_B) are the side length of the destination zone after H partitions. l_A and l_B are the actual side length of the entire network.

Secure route selection algorithm

After the destination zone creation the ISPR method selected the secure route for the data transmission. The method used for the unpredictable route formation is the dynamic zone partition and randomized temporary destination position selection from the portioned zone.

In the route selection algorithm, at first the source node checks whether it is located inside the destination zone or not. If the source node is not located inside the destination zone, then the source node divides the network area in to two zones either horizontally or vertically to separate itself and destination zone. Then the source and destination node are located in different portioned zones. After the zone partition, the source node selected any position from the other partitioned zone as the temporary destination position (TD). The node which is very close to this temporary destination position selected as the first random forwarder node (RF1). The data packets are forwarded from the source to the first random forwarder node using GPSR routing mechanism through the relay nodes. Between any two random forwarders, the relays perform GPSR routing. Each relay node has no information on the source or destination node and its routing action is based on coordinates of the next temporary destination position.

In the next step the first random forwarder checks whether it is located inside the destination zone or not. If it is not in the destination zone, the previous steps are repeated. Here the zone partitions are conducted in an alternative horizontal and vertical manner. Due to this alternative partition method, the packets reach to the destination at each step. The random forwarder node repeats the zone partition process until itself finds located inside the destination zone.

The route created by this dynamic method is secure due to the unpredictable temporary destination position selection. An attacker cannot trace the route in any observation and the nodes in the route are secure. With this method a secure route is created without any complex

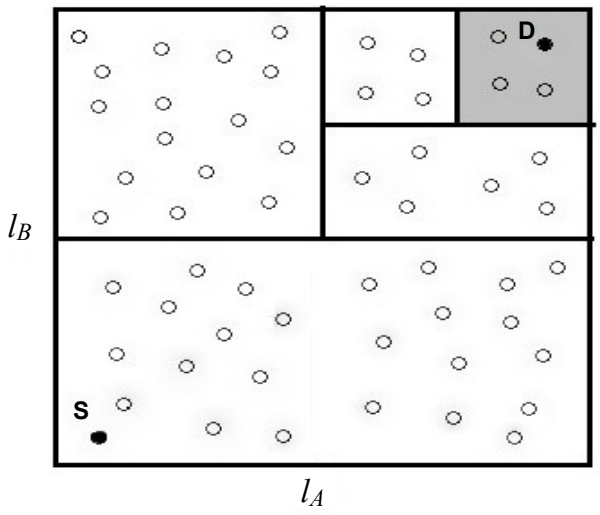

Figure 2: Destination zone creation.

algorithms. The route selection procedure followed in ISPR method does not induce any overhead in the network or high cost. Figure 3 shows the route selection steps in the ISPR algorithm.

For successful communication between source and destination, source and each packet forwarder embedded the following information into the transmitted packet.

- The zone position of *Z D*, that is the *H* th partitioned zone.
- The encrypted zone position of the *H*th partitioned zone of *S* using *D*'s public key, which is the destination for data response.
- Pseudonym of source and destination.
- The current randomly selected *TD* for routing.
- A bit (0 or 1), which is flipped by each *RF*, indicating the partition direction (horizontal or vertical) of the next *RF*.

The number of participating nodes in the route formation is higher very in ISPR method. The participating nodes in the route include the random forwarder nodes and the relay nodes. When more number of nodes is included in the route, it became more secure and unpredictable. Because the nodes that actually conduct routing are not easily discovered among the many possible participating nodes and this makes the routing pattern undetectable.

Theoretically, it is possible to calculate the total number of participating nodes in the route. For that, it is required to calculate the probability that σ partitions are needed to separate source and destination and is represented as $P_s(\sigma)$,

$$p_{s(\sigma)} = \frac{1}{2^{\sigma}} \quad 0 < \sigma \le H$$

Where σ is the closeness between source and destination and $P_s(\sigma)$ is the probability that destination is located in a position that can be separated from source using σ partitions. We can calculate the expected number of nodes participating in the route denoted by $N_e(\sigma)$ as,

$$N_e(\sigma) = a(\sigma, l_A) b(\sigma, l_B) \rho$$

Where ρ is the node density in the network, a (h, l_A) and b (h, l_B) are the side length of destination ones after σ partitions. By using these two equations, the final expected number of possible participating nodes in the route is calculated as,

$$N_e = \sum_{\sigma=1}^{H} N_e(\sigma) p_s(\sigma) = \sum_{\sigma=1}^{H} \left(a(\sigma, l_A) b(\sigma, l_B) \rho \right) \frac{1}{2^{\sigma}}$$

The number of random forwarders in the route is used to calculate the length of the routing path from source to destination. More random forwarder offers higher anonymity to the route. But a network with fixed number of nodes, the higher number of random forwarders will reduce the number of nodes in the destination zone. So the anonymity protection of the destination zone is reduced. For calculating the number of random forwarders, the probability of i random forwarders in source to destination routing is used and is represented as $P_i(\sigma,i)$. $P_i(\sigma,i)$ is determined by i random forwarder choices that leads to RF^+ and by (H- σ-i) random forwarder choice leads to RF^-. In case of each random forwarder selection, the probability of resulting RF^+ and RF^- is same and it is ½. So $P_i(\sigma,i)$ can be calculated as,

$$p_i(\sigma, i) = C_{H-\sigma}^{i} \left(\frac{1}{2}\right)^{i} \left(\frac{1}{2}\right)^{H-\sigma-i} = C_{H-\sigma}^{i} \left(\frac{1}{2}\right)^{H-\sigma}$$

The expected number of random forwarders is represented as $N_{RF}(\sigma)$ and is calculated as,

$$N_{RF}(\sigma) = \sum_{i=1}^{H-\sigma} p_i(\sigma, i) i = \sum_{i=1}^{H-\sigma} C_{H-\sigma}^{i} \left(\frac{1}{2}\right)^{H-\sigma} i$$

By considering the different probability of closeness between source and destination the equation for expected number of random forwarder nodes can be rewritten as,

$$N_{RF} = \sum_{\sigma=1}^{H} \sum_{i=1}^{H-\sigma} C_{H-\sigma}^{i} \left(\frac{1}{2}\right)^{H-\sigma} \frac{i}{2^{\sigma}}$$

When the number of partitions increases, the number of random forwarder also increases. Each partition creates one more random forwarder and provides higher security to the untraceable route. But the nodes in the destination zone are reduces and it reduces the destination anonymity protection. The selection of number of partitions required for the network area needs high attention. Many partitions in the network induce higher overhead in the network and reduce the performance of the selected route.

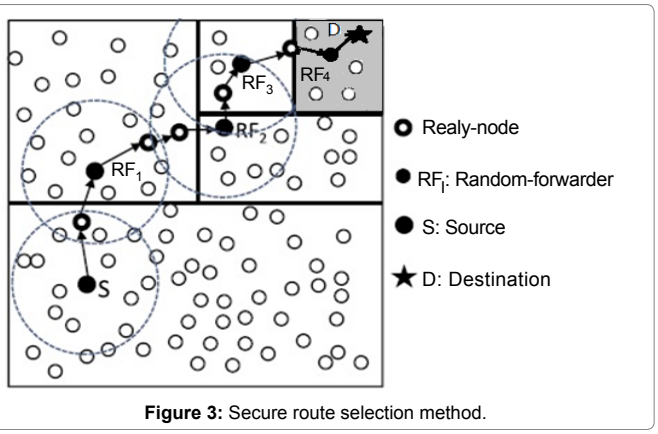

Figure 3: Secure route selection method.

Source security algorithm

The dynamic route selection method provides high security to the route formed. But with the continuous observations of the network an attacker can able find the locations of the source and destination nodes. This types of attacks are called timing attacks in the Ad Hoc environments. If the transmission session duration between a source and destination node is 5 seconds, then by the continuous monitoring an attacker observes that there is a data transmission between source and destination in each 5 seconds. So the attacker concludes the position of source and destination nodes in the network and injects some attacks in the source and destination nodes.

To avoid timing attacks in the source, a mechanism is used in ISPR method is called Notify and Go. The anonymity of source can be provided with this mechanism. The Notify and Go contains two phases. In the first Notify phase, the source sends a data transmission notification message to its neighbours. The message contains a time t, is the time at which the source node started the data transmission and a small offset time t_0. All the neighboring nodes receive this message and generated some random data packets. In the second Go phase, source and its neighbours selects a time from [t, t+t_0] for their data transmission. All the nodes send their data packets at this selected times. The neighbours send some random data generated only to cover the traffic of the source node. Then by the continuous observation of the network an attacker cannot able to find the source node among this group of nodes transmitting their data packets at the selected times. Therefore the Notify and Go mechanism protects the source node from timing attacks.

Destination security algorithm

The destination node position can also obtained by the attacker node by timing attacks in the networks. Therefore a security method is necessary for the destination also to cover the exact position of the destination node in the network. For that purpose ISPR introduced a method called the Destination Zone Broadcasting.

In the usual data transmission process, the packets are forwarded from the last relay node to the destination node only. But in the Destination Zone Broadcasting scheme, the data packets are broadcasted to the destination zone rather that a giving it to a specified destination node. Only the destination node can decrypt the data and other nodes will discarded the data packets received. The timing attacker fails to locate the exact position of the destination node from the group of nodes receiving the packets at the same time.

The Destination Zone Broadcasting also improves the packet delivery rate under high node mobility. It is because the packets are broadcasted to the destination zone and the probability of data reception is higher in this method. There are k nodes are present at the destination zone and it provides k anonymity to the destination node. Each relay node has no information on the source and destination node except the destination zone information. In the packet header, the destination zone position is embedded instead of the destination node position and forwarded to the destination zone. The developed Destination Zone Broadcasting method improves the destination anonymity protection against timing attacks. Figure 4 shows the Destination Zone Broadcasting method for the destination node protection. From the last random forwarder node, the data packets are broadcasted in to the destination zone which is represented as a shaded region in the Figure 4.

Destination security is obtained by the number of nodes in the destination zone, which is related to the node density and the size of the destination zone. The probability of a node with moving speed v, remains in the destination zone after time period t is denoted as $P_r(t)$ and here the destination zone is a circular area with radius r. $P_r(t)$ can be calculated as,

$$p_r(t) = e^{-t/\beta(r)}$$

Where,

$$\beta(r) = \frac{\pi r}{2v}$$

For using this equations in the destination zone created using ISPR method, assumes that the H^{th} partitioned destination zone as a circle covering approximately the same area. This assumption is possible with $l_A = l_B$ and a $(H, l_A) = b (H, l_B)$. 2r' is the side length of the destination zone formed. The radius of the assumed circular destination zone can be calculated as,

$$\pi r^2 = (2r')^2 \rightarrow r = \frac{2r'}{\sqrt{\pi}}$$

and

$$\beta(r) = \frac{\sqrt{\pi}\, r'}{v}$$

The number of nodes remaining in the destination zone after a time period t is denoted as $N_r(t)$ and can be calculated as,

$$N_r(t) = P_r(t)\, a(H, l_A)\, b(H, l_B)\, \rho = e^{\frac{-tv}{\sqrt{\pi}r'}}\, a(H, l_A)^2\, \rho$$

The number of remaining nodes in the destination zone decreases when the time goes on increasing. Also the number of remaining nodes in the destination zone decreased with decrease in the node density and increase in the node moving speed. Anonymity of the destination zone is depends on the node moving speed, node density in the network and destination zone size.

Figure 5 shows the flow chart of the secure route selection method. The mechanisms used for the source, destination and route anonymity are included in the steps of the flow chart.

Attacker observation

There may be so many active attackers in the networks and they affect the communication efficiency of the networks. Active attackers create a highly disastrous effect in the network. They can modify, drop or reroute the packets in the networks. The protection against the active attackers can provide by a highly sophisticated algorithms. Most of the current approaches are limited by providing anonymity at a heavy cost to precious resources. Because the encryption

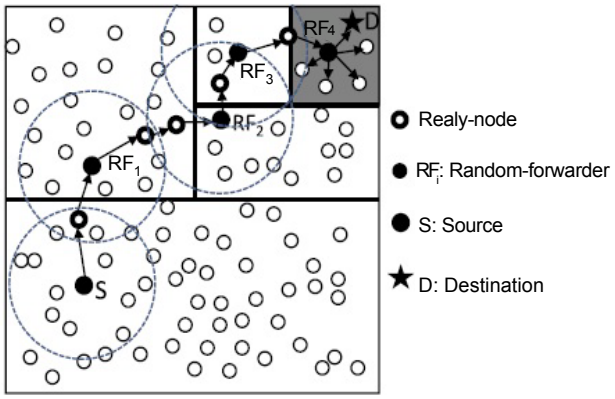

Figure 4: Destination zone broadcasting.

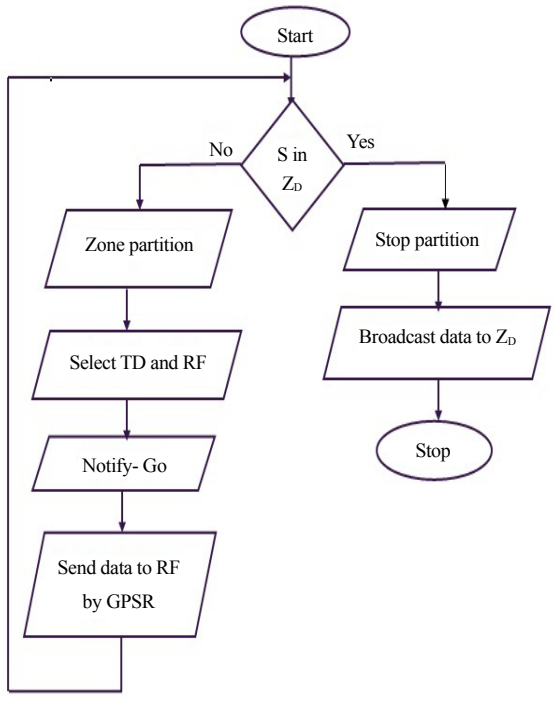

Figure 5: Flow chart of secure route selection.

techniques used and high traffic generate significantly high cost in the data transmission.

Blackhole attackers are very common in wireless Ad Hoc environments. The attacker uses the routing protocol to advertise itself as having the best path to the node whose packets it want to intercept. The Blackhole attacker can create a route through the attacker node. Once the attacker has been able to insert himself between the communications node, then attacker may able to do anything with the packet which is send by the initiator for the receiver. The packets transmitted along the route can be dropped by the attacker completely or partially.

However, if the Blackhole attacker begins dropping packets on a specific time period or over predefined number of packet, it is often harder to detect because some traffic still flows across the network. So for a Blackhole attack, the encrypted data also can be dropped by the attacker. The highly secure encryption procedures cannot avoid the dropping of packets and it is very difficult to obtain the location of this active Blackhole attackers. In ISPR method, the Homomorphic Message Authentication technique is used to find the position of active attackers in the route and selected the new route without attacker node.

Homomorphic message authentication: Homomorphic encryption is the conversion of data into ciphertext that can be analyzed and worked in the encrypted form itself without decrypting the data. Homomorphic encryptions allow complex mathematical operations to be performed on encrypted data without compromising the encryption. The aim of Homomorphic cryptography is to ensure privacy of data in communication, storage or in use which is similar to conventional cryptography. But the Homomorphic encryption has an added capability of computing over encrypted data, searching an encrypted data, etc. than the conventional methods. In Homomorphic cryptography, the result produced by an operation on the encrypted data is same as that of the result produced from the plain text. Many conventional encryption schemes possess either multiplicative or additive Homomorphic property and are currently in use for respective applications.

In Homomorphic cryptography anybody can perform arbitrary computations over authenticated data and produce a short tag that authenticates the result of the computation without knowing the secret key. This tag can be verified using the secret key to ensure that the produced result is indeed the correct output of the specified computation over previously authenticated data without knowing the underlying data. For example, Alice can upload authenticated data to the cloud, which then performs some specified computations over this data and sends the output to Bob, along with a short tag that convinces Bob about the correctness of the result. Alice and Bob only share a secret key, and Bob never needs to know Alice's underlying data. Homomorphic encryption techniques are widely used in case of cloud computing applications to securely outsource the data. Anyone can perform any operations on the data in the cloud without the need of decryption. So the data in the cloud are secure and need not decrypts the important data from the open environments. For the encryption of data, existing encryption method like RSA can be used. In ISPR method, used the most common and efficient RSA algorithm is used for the Homomorphic encryption of the data. If the RSA public key is modulus m and exponent e, then the encrypted message x is given by, $C=x^e \bmod m$ and decrypted message is given by $x= C^d \bmod m$. The Homomorphic property is:

$$C(x_1).C(x_2) = x_1^e x_2^e \bmod m = (x_1 x_2)^e \bmod m = C(x_1.x_2).$$

Concept based on this Homomorphic encryption technique called Homomorphic Message Authentication (HMA) is used for obtain the attacker position. In Homomorphic Message Authentication method, all the valid nodes and the attacker node in the network can perform operations on the Homomorphically encrypted data without the need of any decryption. By analyzing the result of operation from all the nodes the, the attacker node position can be understand. This method of authentication of the valid nodes in the network is called the Homomorphic Message Authentication.

Attacker elimination algorithm: Homomorphic Message Authentication scheme is used for obtaining the active attacker position in the route. In ISPR, assume the attacker node as a Blackhole attacker which is very common in the wireless Ad Hoc environments. The Blackhole attacker can drop packets from the networks partially or completely. Usually it is very difficult to obtain the attacker presence in the networks because there may be traffic in the networks under the presence of attacker node also. The packet delivery rates of the network are reduced due to the packet drop by the Blackhole attacker in the route. It is necessary to obtain the position of the attacker node in order to eliminate that node from the route. That is, after finding the attacker node position the ISPR can select a new route which avoids the attacker from the route vicinity.

The nodes in the route calculated the packet delivery rate (PDR) in each steps and send a confirmation message to the sender about the PDR of data transmission. If the PDR is too low and below a threshold value, then the sender node can assumes the presence of a Blackhole attacker in the route. The Blackhole attacker can generate a route through the attacker node and can drops the packets continuously from the nodes. Due to the reduced PDR, the sender observed the presence of active Blackhole attacker in the route. The attacker node position is needed to create a new route without the presence of attacker node. For that, the sender node used the Homomorphic Message Authentication (HMA) scheme.

In the first step of HMA scheme, the sender node generated a request message and sends it to all the neighbouring nodes. The broadcasted request message contains a data, a mathematical operation and a request for resending the result of this mathematical operation performed on the data present in the message and the nodes position. The data and mathematical operation in the request message is Homomorphicaly encrypted with an asymmetric key algorithm like RSA method. All the neighbouring nodes and the attacker node receive this request message and analyze the message. All the nodes performed the mathematical operation on the encrypted data and resend the result and its location to the sender in order to authenticate itself as a valid node. The attacker node also performs these operations to authenticate itself as a valid node in the route. But the mathematical operation present in the request message is not the actual operation need to perform on the encrypted data. The valid nodes have a pre distributed mathematical operation corresponding to the operation present in the request. This will creates a wrong result from the attacker node only.

The sender node receives all the reply messages from the neighbouring nodes and attacker node. Then the sender checks the result of the mathematical operations from each node. By this analysis the sender can find the wrong result from a particular node and can selected that node as the attacker node. From the reply message of the attacker node, its position can be obtained. With this scheme the position information of the attacker nodes can be obtained by an efficient way. Sender node avoids the attacker's location during the coming temporary destination position selections. Finally the sender

creates a new route without the presence of this attacker node. Figure 6 shows the flow chart of the attacker observation and new route selection in the network using HMA scheme.

Advantages of the algorithm: Homomorphic Message Authentication effectively observed the presence of attacker node in the route and obtained the position of the attacker node. With this scheme ISPR can eliminate the attacker node from the route without a high cost encryption on the message. The main advantage of Homomorphic encryption used in ISPR is that it need not required the decryption of the request message at the receiver. So the algorithm works very fast without the creation of any extra delay in the network. The key distribution overhead in the networks can be avoided with this Homomorphic Message Authentication method. The request message can be broadcasted to the neighbours including the attacker due this Homomorphic nature. Homomorphic encryption allows mathematical operations to be performed on the encrypted data itself without its decryption and produces an encrypted result. On decryption, the result matches the result of operations performed on the plaintext.

Performance Evaluation

The simulations are conducted in network simulator 2.35. Channel type used for the simulations is wireless and the simulation duration is set as 200 seconds. The simulation area defined is 1000 m × 100 m and the transmission range of the node is 100 m. MAC type used in simulation is 802.11. Total number of nodes in the network is taken as 34 and 54. Constant bit rate traffic is used for the simulations and the packet size is 512 bytes. The packet transmission rate is set as 4 packets/second. NAM window outputs and the performance analysis of the developed method are shown in the below figures.

Simulation is carried out to experimentally evaluate the performance of the route selection method. For the analysis, uses different performance metrics to evaluate the routing performance in terms of effectiveness on anonymity protection and efficiency. Total number of nodes participating in the route under different network density and number of random forwarders under different number of zone partitions are used as a performance metric to analyze the intractability of the route. Delivery rate under different node mobility and different nodes density in the networks are also used as a performance metric. Another factor used for the evaluation is the latency of the network in varying node densities.

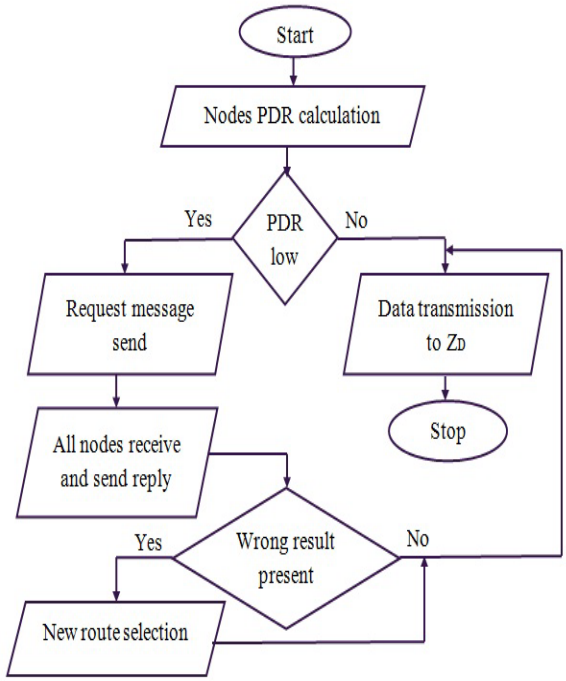

Figure 6: Flow chart of attacker observation and new route selection.

The developed route selection method is also compared with the baseline GPSR protocol to analyses its improved performance under varying node mobility and density. Results show the improved performance of the developed mechanism than the GPSR under varying network conditions. Latency is slightly greater than GPSR but it provides improved anonymity and attack prevention without any high cost encryption techniques, compared to GPSR and other existing anonymous routing protocols.

The following graphs show the performance analysis results.

When the node density in the network increases, the total number of participating nodes in the route also increases. Because each routing involves more new random forwarders and relay nodes. It improves the anonymity of the route selection to a high degree. When the nodes included in the route is higher, the route formed became more untraceable and secure. For the performance analysis, the node density of the network is varied from 50 to 120. Graph in Figure 7 shows the relationship between the total numbers of nodes participating in the route selection process under different node density in the network.

In the base line GPSR, the route selected is always the shortest one. The greedy forwarding selected a relay node which is very close to the destination. So the increased node density does not create a secure route in GPSR protocol. In such an analysis the security protection provided by the random route selection by ISPR is more than the GPSR route selection.

When the number of region partitions increased, the number of random forwarders nodes is also increased and it creates a more secure route. The graph of this increase is shown in Figure 8. Each network partition generates one extra random forwarder node and the associated relay nodes. More participating nodes leads to more randomized routes that are difficult to detect or intercept. So the attacker cannot easily find out the path and the successful delivery rate improved to a great extends when the total nodes participation increases. In the simulation the network partitions varied from zero to seven partitions. Every partition increases the total nodes in the nodes.

The latency of data transmission is decreased when the node density in the network increases and is shown in the Figure 9. This is because a higher node density provides more options for relay nodes selection leading to shorter routing paths. The data transmission between two random forwarder nodes is based on GPSR, so the latency is reduced as well. In the proposed method do not uses any high cost encryption and decryption techniques. So the latency due to the cryptography is also very less. Here the data packet must go through all the random forwarder and relay nodes to create the secure path. It may increases the latency to a small extends than the shortest path created by the GPSR. But the route created is very secure and an attacker cannot follow the route selected. So the probability of successful data delivery is higher than the route selected by GPSR. So the slight increase in the latency can be neglected due to the more secure route selection. This simulation results shows the improved performance of the route selection by ISPR method than the GPSR in terms of delivery rate under different node density in the network.

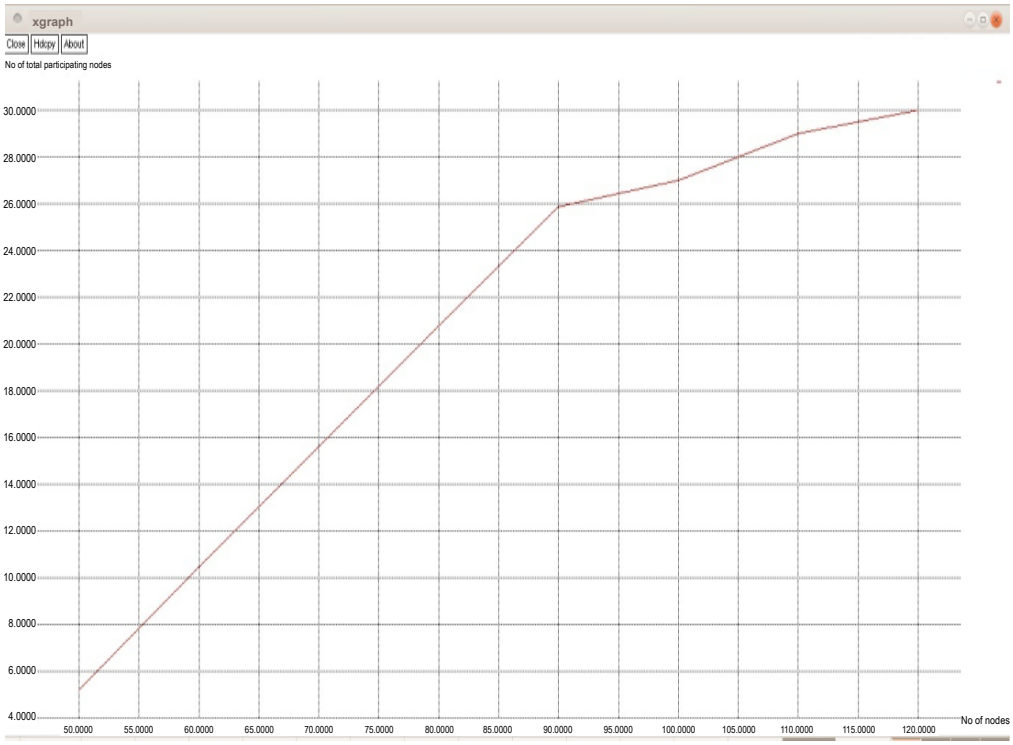

Figure 7: Total number of nodes participating under different number of nodes.

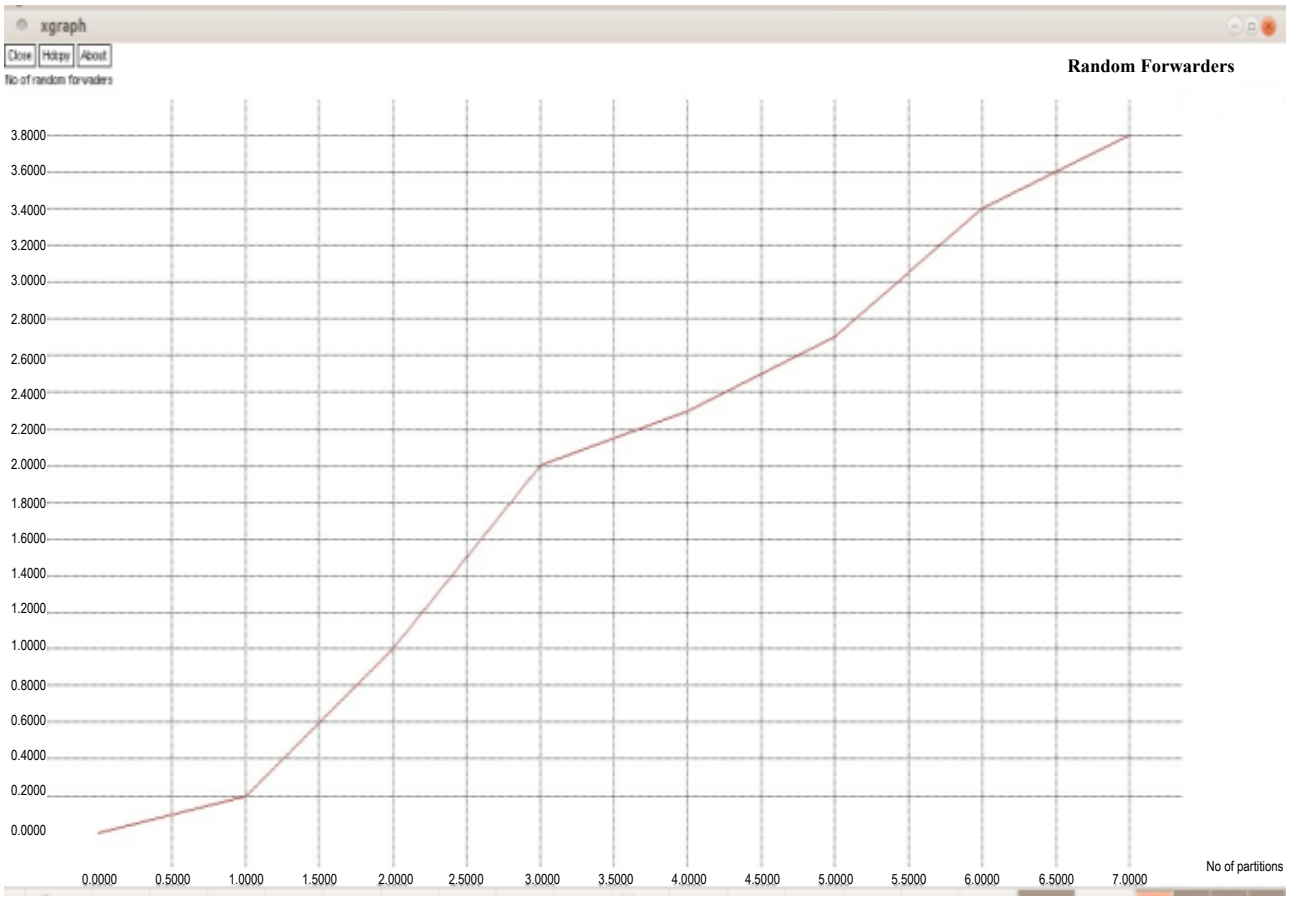

Figure 8: Number of random forwarders under different number of partitions.

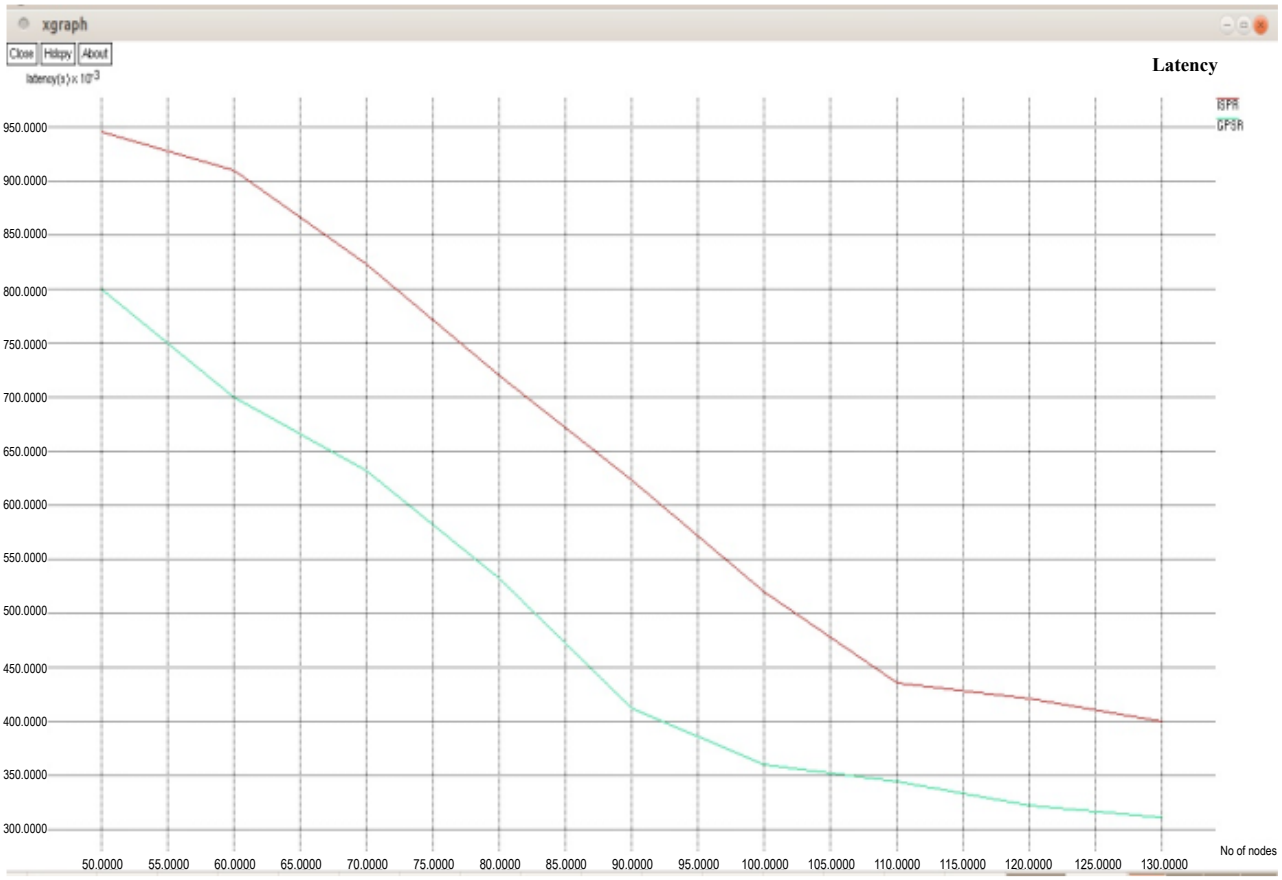

Figure 9: Latency under different number of nodes.

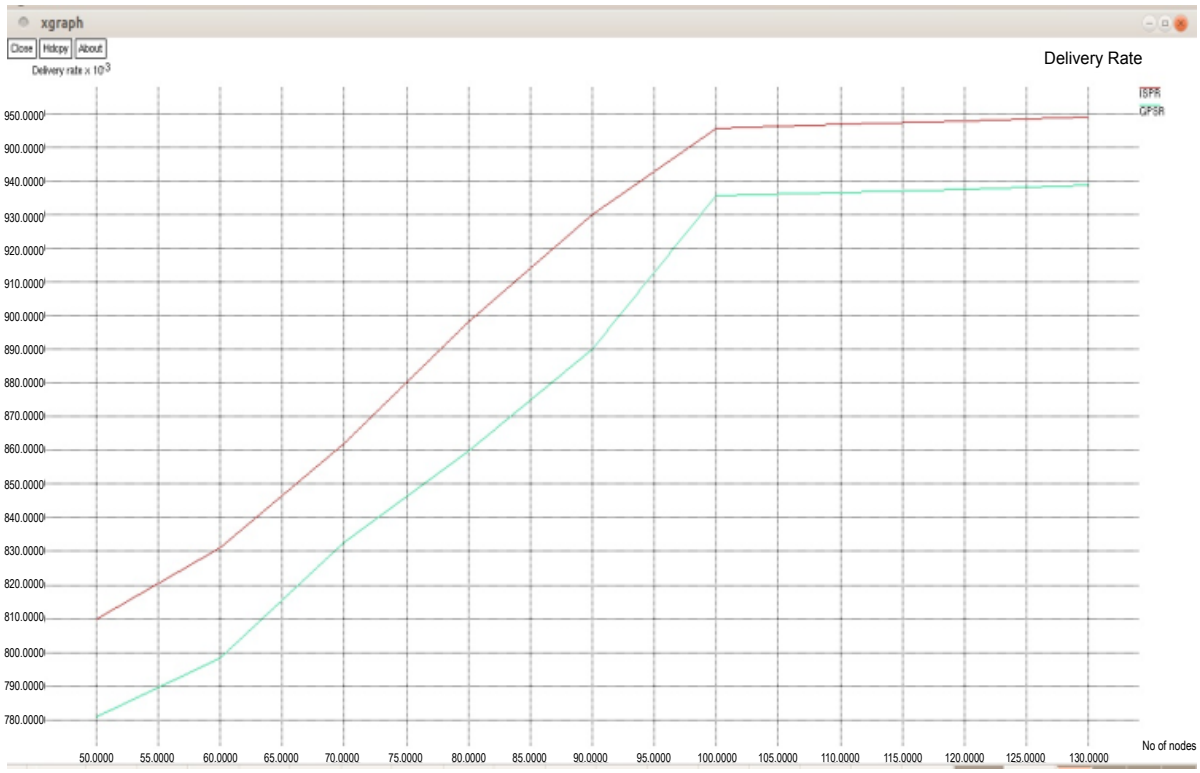

Figure 10: Delivery rate under different number of nodes.

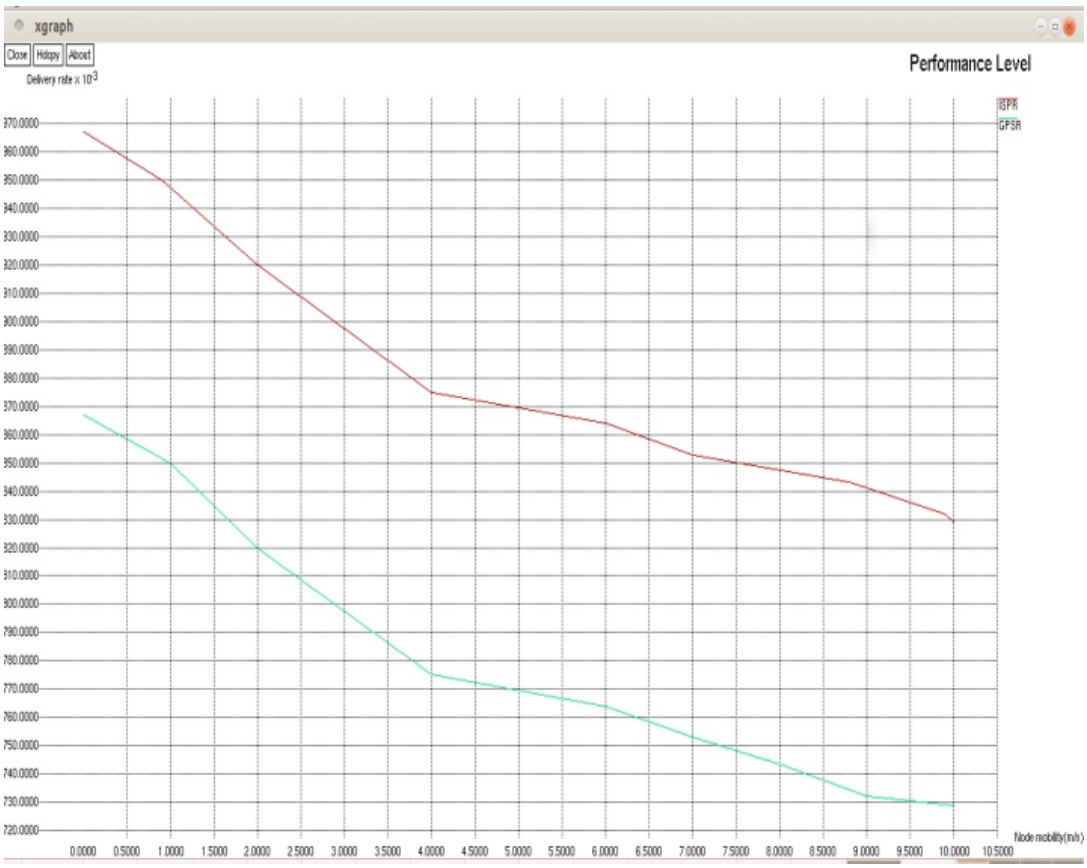

Figure 11: Delivery rate under different node mobility.

Another performance metric used to analyze the randomized route selection by ISPR is the delivery rate under different node density and mobility of the in the network. When the network density is increased, delivery rate is also increased because of the availability of more relay nodes for the route selection in the network. This relationship between delivery rate and number of nodes in the networks is shown in Figure 10. In the case of secure route selection and the GPSR, delivery rate increased with increase in the node density. The increase in the delivery rate is higher for ISPR route selection method that the GPSR because the route created is very secured and unpredictable by an attacker. So the attacker cannot affect the data transmission and the rate of successful data transmission is more than the shorter GPSR route selected. When more nodes are available in the network the route created is more secure and an attacker cannot implement any passive and active attacks in the nodes.

In the route selection by ISPR method, if there is an active Blackhole attacker in the route it reduces the packet deliver rate, and then the ISPR method can select the new route without attacker. This will always increase the delivery rate in this method. But in the GPSR routing, if there is a Blackhole attacker drop the packet from the network it cannot select the new route and the delivery rate is reduced in the network.

Delivery rate under different node mobility is also used as a performance metric. When the node mobility is increased, the delivery rate of both the ISPR route selection and GPSR route selection methods are reduced. It is shown in the graph of Figure 11. This is because of the mobility of the destination node during the data transmission. The proposed method have higher delivery rate than the GPSR because of the data broadcasting from the last relay node to the destination zone instead of a destination node. In the GPSR, the data is transmitted to a particular destination node at the last step of data forwarding. So the increased destination node mobility reduces the successful delivery rate. But in randomized secure routing method, the data are broadcasted to the entire destination zone at the last step. So the probability of data reception by the destination nodes is higher than the GPSR and the delivery rate is higher under increased node mobility.

In summary, the experimental results exhibit the improved performance factors of the proposed secure route selection method compared with the baseline GPSR protocols. The secure methods used for the route discovery, source and destination anonymity protection and attacker observation are capable of giving efficient performance.

Conclusion

Mobile Ad Hoc networks is a dynamic, infrastructure less and decentralized network. The self-configuration ability of Ad Hoc networks constitutes a wide variety of applications in tactical and common life. Security is major problem faced by the Ad Hoc networks due to its open environments. The inherent features of Mobile Ad Hoc networks make it susceptible to many security attacks which may completely or partially destroys and changes the information contents and functionality of the networks. So the development of a secure routing method which satisfies all the performance enhancement features have great impact in Ad Hoc networks. Different techniques are used for providing security from attackers in different existing methods.

In this papers, developed a secure randomized route selection method which provides higher security for the source, destination and routing path. Both passive and active attack like Blackhole attacks can be efficiently identified and avoid by this method. It observes the presence of active Blackhole attacker in the selected route and creates new route without the attacker node. Performance of underlying GPSR routing can be improved by this new method and can avoid adverse attacker effects. The main technique which provides security to the route selected is the dynamic zone partition and randomized selection of intermediate nodes. Passive attacks like timing attacks can be avoided with the Notify and Go mechanism at the source and Destination Zone Broadcasting at the destination. Active attacks like Blackhole attacks in the routes can be observed and selected a new route without attacker by the Homomorphic Message Authentication scheme. Experimental results show the improvements in the secure route selection method than the baseline GPSR in terms of network performance factors and security.

References

1. Pfitzmann A, Hansen M (2005) Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management - A consolidated proposal for terminology. Technical report.
2. Raymond J (2001) Traffic analysis: Protocols, attacks, design issues, and open problems. Proc Int'l workshop designing privacy enhancing technologies: Design issues in anonymity and unobservability (WDIAU) pp: 10-29.
3. Camp T, Boleng J, Davies V (2002) A survey of mobility models for ad hoc network research. Wireless Communications and Mobile Computing 2: 483-502.
4. Kong J, Hong X, Sanadidi MY, Gerla M (2005) Mobility changes anonymity: Mobile ad hoc networks need efficient anonymous routing. ISCC pp: 57-62.
5. Murthy S, Aceves GL (1996) An efficient routing protocol for wireless networks. Mobile Networks and Applications 1: 183-197.
6. Karp B, Kung HT (2000) GPSR: Greedy Perimeter Stateless Routing For wireless networks. Proceedings of 6th Annual International Conference on Mobile Computing and Networking pp: 243-254.
7. Zhi Z, Choong YK (2005) Anonymizing geographic ad hoc routing for preserving location privacy. Proc 3rd Intenational Workshop, Mobile Distributed Computing.
8. Wu X (2006) Disposer: Distributed secure position service in mobile ad hoc networks: Research articles. Wireless Communication and Mobile Computing 6: 357-373.
9. Zhang Y, Liu W, Luo W (2005) Anonymous communications in mobile ad hoc networks. Proc IEEE INFOCOM.
10. Khatib K, Korba L, Song R, Yee G (2003) Anonymous secure routing in mobile ad-hoc networks. Proc Int'l Conf. Parallel Processing Workshops.
11. Wu X, Bhargava B (2005) A02P-Ad Hoc on-demand position-based private routing protocol. IEEE Transaction on mobile computing.
12. Kong J, Hong X (2003) ANODR: Anonymous on Demand Routing with Untraceable Routes for mobile ad-hoc networks. Proc Mobile Ad Hoc Networking.
13. Defrawy KE, Tsudik G (2007) ALARM: Anonymous Location-Aided Routing in Suspicious MANETs. Proc. IEEE Int'l Conf. Network Protocols (ICNP).
14. Zhao L, Shen H (2013) ALERT-An Anonymous Location Based Efficient Routing Protocol in MANETs. IEEE Mobile Computing.
15. Liu J, Kong J, Hong X, Gerla M (2006) Performance evaluation of anonymous routing protocols in MANETs. IEEE Wireless Communications and Networking Conference.