ISSN:0975-9646

A Location Based Protocol for Anonymity Protection of Nodes and Routes at Low Cost

M.Bhavana, M.R.Pavan Kumar

Department Of Computer Science and Engineering
Sree Vidyanikethan Engineering College, Tirupati, India

***Abstract*----Mobile Ad Hoc Networks (MANETs) use various anonymous routing protocols in order to provide security from outside observers. To offer high anonymity protection at low cost, An Anonymous Location Based Efficient Routing Protocol (ALERT) is proposed. ALERT dynamically partitions the network area into zones and randomly chooses the intermediate relay nodes to form a anonymous route. ALERT achieves a better routing efficiency comparable to the GPSR geographic routing protocol. Even though ALERT offers anonymity protection at low cost, it is not completely resistant to all attacks. To prevent the happening of stronger attackers, a Secure Cryptographic Based Mix zones (SCBMIX) routing is used. So to achieve anonymity protection at low cost ALERT is used and to provide stronger anonymity protection SCBMIX is used. The idea of SCBMIX is to mask the adversary from accessing the content of the messages. Thus ALERT with SCBMIX offers higher anonymity protection.**

***Index Terms* - MANETs, Anonymity, routing protocol, GPSR.**

I.INTRODUCTION

A Mobile Ad Hoc Network is an autonomous and short-lived association of group of mobile nodes that communicate with each other over wireless links. A node can directly communicate to the nodes that lie within its communication range; it uses intermediate nodes as routers. Nodes in MANETs are endangered to malicious entities that aim to tamper the data by attacking routing protocols. Anonymous routing protocols are very important in MANETs to provide secure communication by masking the node identities and prohibiting traffic analysis attacks from the attackers. Anonymity in MANETs means identifying and tracing the anonymity of sources, destinations as well as routes.

Routing in MANETs

Routing in a MANET generally depends up on several factors such as topology, selection of routers, location of request initiator, and specific underlying characteristics that could serve as a heuristic in finding the path quickly and efficiently. One of the major challenges in designing a routing protocol for MANETs is that a node should at least needs to know the reachability information of its neighbors for finding a packet route, while the network topology often changes in a MANET.

Routing in Adhoc networks are broadly classified into Topology based or Position based approaches. Topology based routing protocols depend up on the information of the existing links in the network and use that information to perform the task of packet forwarding. They are further classified as proactive, reactive and hybrid protocols. The position-based protocols require that the physical location information of the nodes be known. Typically, each or some of the MHs determine their own position through the use of the Global Positioning System (GPS) or some other type of positioning technique. The sender normally uses a location service to determine the position of the destination node, and to incorporate it in the packet destination address field. Here, the routing process at each node is based on the destination's location available in the packet and the location of the forwarding node's neighbors.

Existing anonymity routing protocols in MANETs are broadly categorized into hop-by-hop encryption and redundant traffic. In hop-by-hop encryption routing, a packet is encrypted in the transmission of two nodes en route, preventing adversaries from detecting the packet contents to interrupt the communication or identify the two communicating nodes. Hop-by-hop encryption can be classified further as onion routing and hop-by-hop authentication. Several existing protocols do not provide full anonymity protection to the source, destination and routes. For example ALARM provides only route anonymity, ZAP focuses on destination anonymity and SDDR provides the source and destination anonymity.

In order to provide the high anonymity protection with low cost, Anonymous Location-based and Efficient Routing Protocol (ALERT) is proposed. The ALERT protocol divides a network field dynamically into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a nontraceable anonymous route. In each routing step, a data sender partitions the network area so as to separate itself and the destination into two zones. It then randomly selects a node called as the next relay node in the other zone and uses the GPSR algorithm to send the data to the relay node. In the final step, the data is broadcasted to k nodes in the destination zone, providing k-anonymity to the destination. In addition, ALERT provides a mechanism to hide the data initiator among several senders to strengthen the anonymity protection of the source. ALERT is also elastic to intersection attacks and timing attacks. As other various anonymity routing algorithms, ALERT is not completely bulletproof to all attacks. ALERT can be applied to random way point and group mobility network models. To prevent the happening of stronger and active attackers, ALERT is mixed with SCBMIX. An unidentified zone functions as a mix zone where the nodes change their pseudonym and combine with each other. The mobile nodes do not know where the mix zone is. Mix zones [3] are created at predefined locations and to force pseudonym changes to take place within those regions. Since the location of mix-zone is fixed, the adversary can identify them and thus

could easily attempt to eavesdrop transmissions originating in the mix-zone area. The attacker observes the timing and the location of entering and exiting nodes depends upon their trajectory in an intersection. The idea for mix-zones is to prevent the attacker from accessing the messages including their signatures. All the authorized nodes within the mix-zone obtain a symmetric key and use this key to encrypt messages within the zone.

II. RELATED WORK

Anonymous routing schemes in MANETs have been investigated in recent years. By the different usage of topological information, they can be classified into on-demand or reactive routing methods, and proactive routing methods. Also there are anonymous middleware working between network layer and application layer.

ALARM (Anonymous Location Aided Routing in Suspicious MANETs):

ALARM [4] uses proactive routing, where each node broadcasts its location information to its authenticated neighbors so that each node can build a map for later anonymous route discovery. However, this map construction leaks destination node locations and compromises the route anonymity. Thus, ALARM cannot protect the location anonymity of source and destination. In ALARM, each node at times disseminates its hold identity to its genuine neighbors and continually collects all other nodes' identities. Hence, nodes can assemble a secure map of other nodes for geological routing.

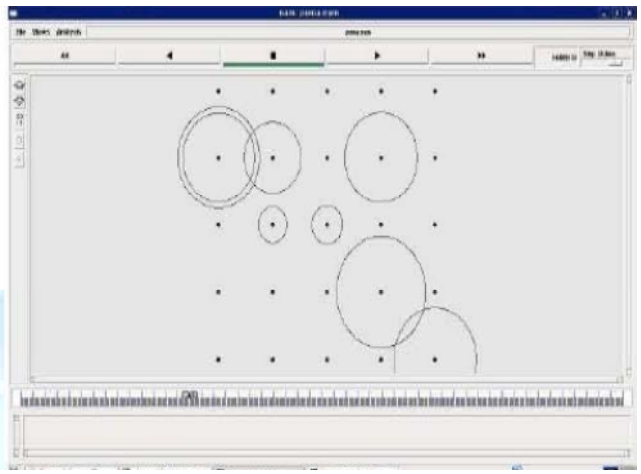

Fig.1: Implementation of ALARM protocol

ZAP (Zone based Anonymous Routing Protocol):

Zone based Routing Protocol, or ZAP is a hybrid Wireless Networking routing protocol that combines the proactive and reactive routing protocols when sending the data over the network. ZAP was designed to speed up the delivery rate and reduce the processing overhead by selecting the most efficient type of protocol to use throughout the entire route.ZAP uses a destination zone, and locally broadcasts to a destination zone in order to reach the destination without leaking the destination identity or position. A disadvantage of redundant traffic-based methods is the very high overhead incurred by the redundant operations or packets, leading to high cost. Although some methods such as ZAP only perform local broadcast in a destination zone, these methods cannot provide source or routing anonymity.

GLS (Grid Location Service):

GLS is a zone-based location service. The Grid Location Service (GLS) divides the area that contains the MANET into a hierarchy of squares. In this hierarchy, n-order squares contain exactly *(n* - l)-order squares, forming a so-called quadtree. Each node maintains a table of all other nodes within the local first-order square. The table is constructed with the help of periodic position broadcasts scoped to the area of the first order square. Although GLS also uses hierarchical zone partitioning, its use is for location service while in ALERT; its use is for anonymous routing.

GPSR (Greedy Perimeter Stateless Routing) Protocol:

In GPSR protocol, the packets are routed geographically. All the packets are marked with the positions of their destinations. All the nodes know their own positions and the positions of the nodes a single hop far away from them. GPSR uses two different algorithms for routing: a greedy forwarding algorithm that moves packets progressively closer to the destination at each hop and a perimeter forwarding algorithm that forwards packets where greedy forwarding is not possible. Especially, in every routing step, a data sender partitions the network area in order to divide itself and the destination into two zones. It then randomly chooses a node in the new zone as the subsequent relay node and uses the GPSR algorithm to forward the data to the transmit node. In the final step, the data is broadcasted to k nodes in the destination zone, providing k-anonymity to the destination.

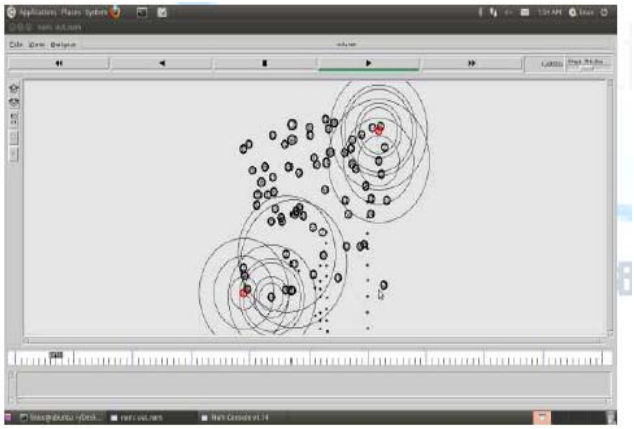

Fig 2. Implementation of GPSR protocol

Mobility Models:

Mobility models represent the movement of mobile user, and how their location, velocity and acceleration change over time. Such models are frequently used for simulation purposes when new communication or navigation techniques are investigated. Mobility management schemes for mobile communication systems make use of mobility models for predicting future user positions. The mainly used mobility models are Synthetic entity mobility models and group mobility models.

Random way point model:

The Random waypoint is the most widely used synthetic entity model. The Random waypoint model [5] includes the pause times between the changes in directions and/or speed. The Mobile nodes are initially distributed randomly around the simulation area. A Mobile node (MN) begins by staying in one location for a certain time period (i.e pause time). Once this pause time expires, the MN chooses a random destination in the simulation area and a speed that is distributed uniformly between [minspeed, maxspeed]. The MN then travels with the selected speed towards the newly chosen destination. Upon arrival, the MN pauses for a specific time period before starting the process again.

Group Mobility Model:

In an adhoc network, however there are many situations where it is necessary to model the behavior of MNs as they move together. A Group mobility model [6] is used to simulate this cooperative characteristic. The Reference Point Group Mobility (RGPM) model is widely used mobility model. The RGPM model represents the random motion of a group of MNs as well as the random motion of each individual MN within the group. Group movements are based upon the path travelled by a logical center for the group. The logical center for the group is used to calculate the group motion via a group motion vector. The motion of the group center completely characterizes the movement of its corresponding group of MNs, including their direction and speed. Individual MNs randomly move about their own pre-defined reference points, whose movements depend on the group movement. As the individual reference points move from time t to t+1, their locations are updated according to the group's logical center.1once the updated reference points are calculated, they are combined with a random motion vector, to represent the random motion of each MN about its individual reference point.

III ALERT PROTOCOL

Dynamic pseudonym and Location service:

In ALERT, each node uses a dynamic pseudonym as its node identifier instead of using its real MAC address, which can be used to trace nodes' existence in the network. To avoid pseudonym collision, collision resistant function such as SHA-1 is used to hash the nodes' MAC address and current time stamp. To prevent an attacker from recomputing the pseudonym, the time stamp should be precise enough (e.g. nano seconds). A Secure Location Service is used to provide the information of each of nodes' location and public key. Such a location service enables a source node, which is aware of the identity of the destination node, to securely obtain the location and public key of the destination node. The public key is used to enable two nodes to safely establish a symmetric key for secure communication. The destination location enables a node to determine the next hop in geographic routing. Generally, trusted normal nodes or dedicated service provider nodes are used to provide location service. Each node has a location server. When a node A wants to know the location and public key of node B, it will first sign the request containing B's identity using its own identity. Then the location server of A will return an encrypted position of B and its public key, which can be decrypted by A using the predistributed shared key between A and its location server. When node A moves, it will also periodically update its position to its location server.

The Destination Zone Position:

The reason we have used Z_D rather than D is to avoid exposure of D. Zone position describes the upper left and bottom-right coordinates of a zone. One disadvantage is how to find the position of Z_D, which is needed by each packet forwarder to check whether it is separated from the destination after a partition and whether it resides in Z_D. Let H denote the total number of partitions in order to produce Z_D. Using the number of nodes in Z_D (i.e., k), and node density þ, H is calculated by

$$H = \log_2 (þ.G/k)$$

G is the size of the entire network area

þ is the node density

k is the number of nodes in Z_D

The size of the destination zone is $G/2^H$.

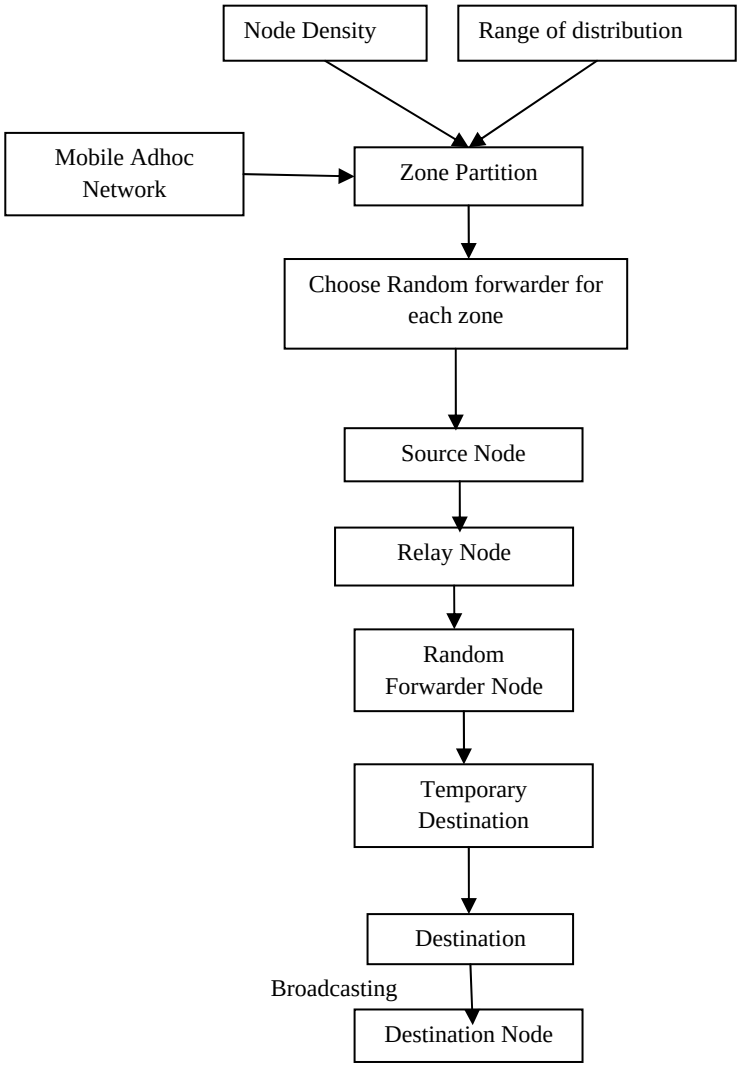

Fig 3: Block diagram of ALERT

The ALERT Routing Algorithm:

Initially, the entire network area is generally assumed as a rectangle in which nodes are randomly distributed. The information of the bottom-right and upper left boundary of the network area is configured into each node when it joins in the system. This information enables a node to locate the positions of nodes in the entire area for zone partitions in ALERT. ALERT[7] features a dynamic and unpredictable routing path, which consists of a number of dynamically determined intermediate relay nodes.

The given network area is horizontally divided into two zones A_1 and A_2. Then the A_1 zone is vertically partitioned into B_1 and B_2. After that B_2 is horizontally divided into two zones as shown in the fig.1. Such zone partitioning consecutively splits the smallest zone in an alternating horizontal and vertical manner called as hierarchical zone partition. ALERT uses the hierarchical zone partition and randomly chooses a node in the partitioned zone in each step as an intermediate relay node (i.e., data forwarder), thus dynamically generating an unpredictable routing path for a message.

Fig. 4 shows an example of routing in ALERT. We call the zone having k nodes where D resides the destination zone, denoted as Z_D. k is used to control the degree of anonymity protection for the destination. The shaded zone in Fig. 4 is the destination zone. Specifically, in the ALERT routing, each data source or forwarder executes the hierarchical zone partition. It first checks whether itself and destination are in the same zone. If the source and destination are in the same zone, it divides the zone alternatively in the horizontal and vertical directions. The process is repeated until itself and Z_D are not in the same zone. It then randomly chooses a position in the other zone called temporary destination (TD), and uses the GPSR routing algorithm to send the data to the node closest to TD. This node is called as a random forwarder (RF).

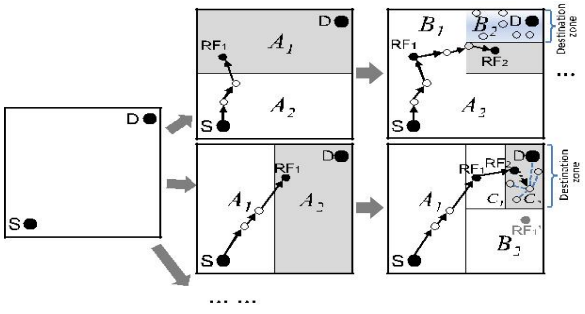

Fig.4. Examples of different zones in a network

Packet Format of ALERT:

RREQ/RREP/NAK		Ps	P_D	L_{ZS}	L_{ZD}	L_{RF}
h	H	K^S_{pub}	$(TTL)_K{}^{RN}{}_{pub}$	$(Bitmap)_K{}^D{}_{pub}$		data

Fig 5. Packet format of ALERT

The above Fig. 5 shows the packet format of ALERT, which does not contain the MAC header. Because of the randomized routing in ALERT, we have a universal format for RREQ/RREP/NAK. A node uses NAK to acknowledge the lost packets. The data field of RREQ/RREP is left blank in NAK packets. Flooding-based anonymity routing usually uses ACKs, while NAKs are often implemented in geographic routing-based approaches to reduce the traffic cost. For the same purpose, we use NAKs. In the packet, P_S represents the pseudonym of a source; P_D is the pseudonym of the destination; L_{ZS} and L_{ZD} are the positions of the Hth partitioned source zone and destination zone, respectively; L_{TD} is the currently selected TD's coordinate; h gives the number of divisions so far, H is the maximum allowed number of divisions; and K_s^S describes the symmetric key of a source. Particularly, $(TTL)_K{}^{RN}{}_{pub}$ is used for the protection of source anonymity, and $(Bitmap)_K{}^D{}_{pub}$ is used for solving the intersection attack.

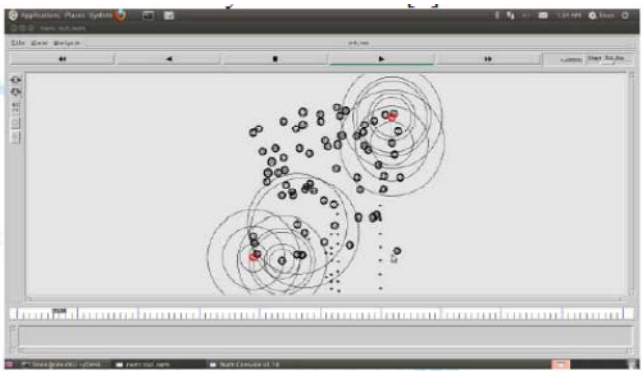

Fig 6: Implementation of ALERT protocol

Anonymity protection:

ALERT provides the identity and location anonymity of the source node, destination node, as well as the route anonymity. Unlike geographic routing, which always uses the shortest path, ALERT makes the route between a S-D pair which is difficult to discover by randomly and dynamically selecting the relay nodes. The resultant distinct routes for transmissions between a given S-D pair make it more difficult for an intruder to observe a statistical pattern of transmission. This is because the RF set changes continuously due to the random selection of RFs during the transmission of each packet. Even if an intruder detects all the nodes along a routes once, this detection does not help it in finding the routes for subsequent transmissions between the same S-D pair.

Additionally, since an RF is only aware of its proceeding node and succeeding node in route, the source and destination nodes cannot be differentiated from other nodes en route. Also, the anonymous path between S and D ensures that nodes on the path do not know where the endpoints are. ALERT strengthens the privacy protection for S and D by the unlinkability of the transmission endpoints and the transmitted data. That is, S and D cannot be associated with the packets in their communication by adversaries. ALERT uses the "notify and go" mechanism to prevent an attacker from identifying which node within the source neighborhood has initiated packets. ALERT also provides k-anonymity to destinations by hiding D among k receivers in Z_D. Thus, an eaves-dropper can only obtain information on Z_D, rather than the destination position, from the packets and nodes en route.

The route anonymity due to random relay node selection in ALERT prevents an intruder from intercepting packets or compromising vulnerable nodes en route to issue DoS attacks. In ALERT, the routes between two communicating nodes are constantly changing, so it is difficult for the intruders to predict the route of the next packet for packet interception. Similarly, the communication of two nodes in ALERT cannot be completely stopped by compromising certain nodes because the number of possible participating nodes in each packet transmission is very large due to the dynamic changes of the routes. In contrast, these attacks are very easy to perform in geographic routing, since the route between a given S-D pair does not change for different packet transmissions, and thus, the number of involved nodes is much smaller than in ALERT.

Resistant to Timing Attacks:

In timing attacks, through packet departure and arrival times, an unauthorized user can identify the packets transmitted between S and D, from which it can finally detect S and D. For example, two nodes A and B communicate with each other at an interval of 5 seconds. After a repeated observation time, the intruder finds that A's packet sending time and B's packet receiving time have a fixed five second difference such as (19:00:55, 19:01:00) and (20:01:33, 20:01:38). Then, the intruder would suspect that A and B are communicating with each other. Avoiding the exhibition of interaction between communication nodes is a way to counter timing attacks. In ALERT, the "notify and go" mechanism and the broadcasting in Z_D both put the interaction between S-D into two sets of nodes to confuse the intruders. Mainly, the routing path between a given S-D and the communication delay (i.e., time stamp) change constantly, which again keeps an intruder from identifying the S and D.

Strategy to Counter Intersection Attacks:

In an intersection attack, an attacker with information about active users at a predefined time can determine the sources and destinations that communicate with each other through the repeated observations. Intersection attacks are the most common problem and have not been well resolved. Though ALERT offers k-anonymity to D, an intersection attacker can still identify D from repeated observations of node movement and communication if D always stays in Z_D during a transmission session. This is because as long as D is conducting communication, the attacker can monitor the change of the members in the destination zone containing D. As time elapses and nodes move, all other members may move out of the destination zone except D. As a result, D is identified as the destination because it always appears in the destination zone.

Fig 7.a gives the status of a Z_D after a packet is broadcasted to the zone. The arrows indicate the moving directions of the nodes. We can see that nodes a, b, c, d, and D are in Z_D. Fig. 7.b is the subsequent report of the zone the next time a packet is transmitted between the same S-D pair. This time, nodes d, e, f, g, and D are in Z_D. Since the intersection of the in-zone nodes in both figures includes d and D, D could be identified by the attacker. Therefore, the longer an attacker observes the process, the easier is to identify the destination node.

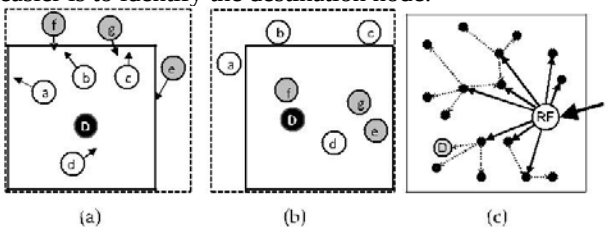

Fig 7: Intersection attack and solution.

Fig. 7.c shows the two-step process with the first step in solid arrows and the second step in dashed arrows. We can see that the first step reaches a number of nodes in the destination zone, but the destination is reached in the second step. Because the deliveries of pkt_1 and pkt_2 are mixed, an attacker observes that D is not in the recipient set of pkt_1 though D receives pkt_1 in the delivery time of pkt_2. Therefore, the attacker would think that D is not the recipient of every packet in Z_D in the transmission session, thus foiling the intersection attack.

Because the attacker may grab and analyze the packets on air, the last forwarding node alters a number of bits in each packet to prevent the attacker from identifying identical packets in one broadcasting. This function is provided by the field $(Bitmap)_{K^{D}_{pub}}$ in each packet. The Bitmap filed records the changed bits and is encrypted using the destination's public key K_{pub}^{D} for recovering the original message. Since destination is not always within the recipient set, and also the packet forwarded to a destination is different from the original packet, the attacker cannot identify the destination from its observation history by calculating the intersection set of nodes. This approach incurs two extra costs. One is the one-hop broadcasting of the recipients in the destination zone. The other is the encryption cost of changed bits.

Routing Performance:

The routing performance of the ALERT protocol is compared with the different routing protocols such as GPSR, AO2P and ALARM in terms of latency, number of hops per packet and delivery rate. The latency of ALERT with SCBMIX is much lower than the ALARM and AO2P. This is because of the time and cost of encryption. ALERT uses symmetric key encryption for packets, which takes shorter time than the public key encryption used in ALARM and AO2P. Also, ALERT encrypts packets only one time, while in the previous routing protocols encryption takes place in each hop and has to periodically authorize its neighbors. Even though ALERT generates more number of hops than AO2P and ALARM, the latency of ALERT is still significantly less. ALERT generates a slightly longer latency than GPSR.

In summary, we can say that ALERT with SCBMIX achieves better route anonymity protection compared with the existing anonymous routing protocols.

IV.COMPARISON ANALYSIS

We compare ALERT with two newly proposed anonymous geographic routing protocols: ALARM and GPSR. ALARM is based on hop-by-hop encryption and unnecessary traffic. All of the protocols are geographic routing, so we also evaluate ALERT with the location based routing protocol GPSR in the experiments. In GPSR, a packet is constantly forwarded to the node nearest to the destination. When such a node does not exist, GPSR uses edge forwarding to locate the hop that is closer to the destination.

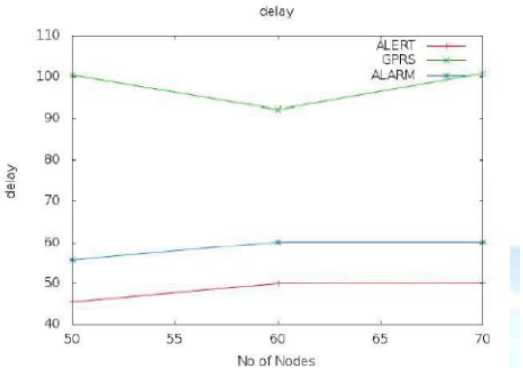

Fig. 8: Comparison graph of Average Delay

The average delay parameter shown by above graph presents that ALERT protocol is much highly efficient in this parameter than GPRS.

Output for GPRS Delivery ratio:

a. 50 100.30230044208847
b. 60 92.199800651124704
c. 70 100.66228088219775

In ALARM, each node generates its own identity to its genuine neighbors and constantly collects all other nodes' identities. Thus, nodes can form a secure map of other nodes for geological routing. In routing, each node encrypts the packet by its key which is confirmed by the next hop en route.

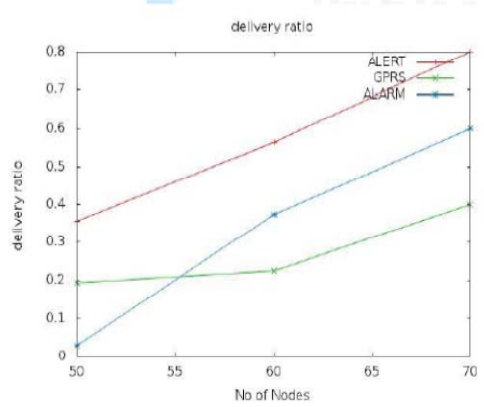

Fig 9: Comparison graph of Packet Delivery Ratio

Output for ALERT Delivery Ratio

a. 50 0.29354838709677422
b. 60 0.52631578947368429
c. 70 1.0

The above graph result shows that Packet Delivery Ratio of ALERT protocol is higher than in GPRS protocol. The results from the comparison graph clearly show that ALERT protocol is better in delivery ratio as well as packet delivery ratio than GPRS.

IV. CONCLUSIONS

The existing anonymous routing protocols depend upon either hop-by-hop encryption or redundant traffic and do not provide the complete protection to the source, destination and routes. ALERT provides protection for the source, destination and as well as routes. As ALERT is not completely bullet proof to all attacks Secure Cryptographic Based Mix-Zones routing protocol (SCBMIX) is used. The concept of mix zones refers to a service restricted area where mobile users can change their pseudonyms and the new pseudonyms are not revealed. SCBMIX protocol distributes keys for encrypting beacon messages while in the mix-zone.

ACKNOWLEDGEMENTS

I am thankful to the authors Haiying Shen, Lianyu Zhao for their research.

REFERENCES

[1] Z. Zhi and Y.K. Choong, "Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy," Proc. Third Int'l Workshop Mobile Distributed Computing (ICDCSW), 2005.
[2] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Wireless Networks, vol. 11, pp. 21-38, 2005.
[3] A.R. Beresford and F. Stajano, "Mix Zones: User Privacy in Location-Aware Services," Proc. IEEE Second Ann. Conf. Pervasive Computing and Comm. Workshops (PERCOMW), 2004.
[4] K.E. Defrawy and G. Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs," Proc. IEEE Int'l Conf. Network Protocols (ICNP), 2007.
[5] T. Camp, J. Boleng, and V. Davies, "A Survey of Mobility Models for Ad Hoc Network Research," Wireless Communications and Mobile Computing, vol. 2, pp. 483-502, 2002.
[6] X. Hong, M. Gerla, G. Pei, and C.C. Chiang, "A Group Mobility Model for Ad Hoc Wireless Networks," Proc. Second ACM Int'l Workshop Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM), 1999.
[7] L. Zhao and H. Shen, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs," Proc. Int'l Conf. Parallel Processing (ICPP), 2011.