A Reactive Protocol for Privacy Preservation using Location-Based Efficient Routing in MANETs

[1] **Shwetha. R,** [2] **Dr. B. G. Prasad**

[1] PG Student, M. Tech (Computer Science & Engineering), B.N.M Institute of Technology
Bangalore, Karnataka, India

[2] Professor & HOD, Computer Science & Engineering, B.N.M Institute of Technology
Bangalore, Karnataka, India

Abstract - Mobile Ad Hoc Networks (MANETs) use anonymous routing protocols that hide node identities and/or routes from outside observers in order to provide anonymity protection. However, existing anonymous routing protocols relying on either hop-by-hop encryption or redundant traffic, either incurs high cost or cannot provide full anonymity protection to data sources, destinations, and routes. The high cost adds to the inherent resource constraint problem in MANETs especially in multimedia wireless applications. To offer high anonymity protection at a low cost, Anonymous Location-based Efficient Routing protocol (ALERT) is proposed. ALERT partitions the network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non-traceable anonymous route and offers anonymity protection to sources, destinations, and routes.

***Keywords* - anonymity, Mobile Ad Hoc Networks, routing protocol, geographic routing.**

1. Introduction

Mobile Ad Hoc Networks (MANETs) feature self-organizing and independent infrastructures, which make them an ideal choice for uses such as communication and information sharing. MANETs has motivated numerous wireless applications that can be used in a various applications such as entertainment, education commerce, military, and emergency services. Because of the openness and decentralization features of MANETs, it is usually not desirable to constrain the membership of the nodes in the network. Nodes in MANETs are vulnerable to malicious entities that aim to tamper and analyze data and traffic analysis by communication eavesdropping or attacking routing protocols. Although anonymity may not be a requirement in civiling applications, it is critical in military applications (e.g., soldier communication).Consider MANET deployed in a battlefield. Through traffic analysis, enemies may intercept transmitted packets, track the soldiers (i.e., nodes), attack the commander nodes, and block the data transmission by comprising relay nodes (RN), thus putting anybody at a tactical disadvantage. Anonymous routing protocols are crucial 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 (i.e., senders) and destinations (i.e., recipients), as well as route anonymity. “Identity and location anonymity of sources and destinations” means it is hard for other nodes to obtain the real identities and exact locations of the sources and destinations. For route anonymity, adversaries, either enroute or out of the route, cannot trace a packet flow back to its source or destination, and no node will have information about the real identities and locations of intermediate nodes enroute. Also, in order to dissociate the relationship between source and destination (i.e., relationship can’t be observed), it is important to form an anonymous path between the two endpoints and ensure that nodes enroute do not know where the endpoints are, especially in MANETs where location devices may be equipped.

Existing anonymity routing protocols in MANETs can be mainly classified into two categories: hop-by-hop encryption [5], [6], [7] and redundant traffic. Most of the current approaches are limited by focusing on enforcing anonymity at a heavy cost to precious resources because public-key-based encryption and high traffic generate significantly high cost. Many anonymity routing algorithms are based on the geographic routing protocol (e.g., Greedy Perimeter Stateless Routing (GPSR) [4]) that greedily forwards a packet to the node closest to the destination.

On the other hand, limited resource is an inherent problem in MANETs, in which each node labors under an energy constraint. MANETs complex routing and stringent channel resource constraints impose strict limits on the system capacity. Further, the recent increasing growth of multimedia applications (e.g. video transmission) imposes higher requirement of routing efficiency. However, existing anonymous routing protocols generate a significantly high cost, which exacerbates the resource constraint problem in MANETs. In a MANET employing a high-cost anonymous routing in a battlefield, a low quality of service in voice and video data transmission due to depleted resources may lead to disastrous delay in military operations.

In order to provide high anonymity protection (for sources, destination, and route) with low cost, an Anonymous Location-based and Efficient Routing protocol (ALERT) is proposed. ALERT dynamically partitions a network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non-traceable anonymous route. Experiments have been conducted to evaluate the performance of ALERT in comparison with other anonymity and geographic routing protocols such as ALARM (Anonymous Location-Aided Routing in Suspicious MANETs) and GPSR (Greedy Perimeter Stateless Routing) respectively.

The contribution of ALERT includes
1. Anonymous routing - ALERT provides route anonymity, identity, and location anonymity of source and destination.
2. Low cost - Rather than relying on hop-by-hop encryption and redundant traffic, ALERT mainly uses randomized routing of one message copy to provide anonymity protection.
3. Extensive simulations - Comprehensive experiments have been conducted to evaluate ALERT's performance in comparison with other anonymous protocols such as ALARM (Anonymous Location-Aided Routing in Suspicious MANETs) and GPSR (Greedy Perimeter Stateless Routing).

1.1 Problem Statement

In order to provide high anonymity protection (for sources, destination, and route) with low cost, an Anonymous Location-based and Efficient Routing protocol (ALERT) is proposed to be implemented. An ALERT partition a network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non-traceable anonymous route.

1.2 Objective

The main objectives of this work are:
1. To provide anonymity protection to source, relay and destination.
2. To achieve higher packet delivery ratio.
3. To achieve minimum end to end delay.

1.3 Motivation

1. Existing anonymous routing protocols cannot provide full anonymity protection to data sources, destinations, and routes. The high cost adds to the inherent resource constraint problem in MANETs especially in multimedia wireless applications.
2. ALERT provides a non-traceable anonymous route. It offers high anonymity protection at a low cost.
3. ALERT achieves better route anonymity protection and lower cost compared to other anonymous routing protocols and offers anonymity protection to sources, destinations, and routes.

2. System Analysis

Analysis phase is a detailed study of various operations performed by a system and their relationships within and outside the system. One aspect of system analysis is defining the boundaries of the system and determining whether or not a candidate system should consider other related systems. The emphasis in system analysis is on identifying what is needed from the system and not how the system will achieve its goal.

2.1 Existing System

Existing anonymity routing protocols in MANETs can be mainly classified into two categories: hop-by-hop encryption and redundant traffic based. Most of the current approaches are limited by focusing on enforcing anonymity at a heavy cost to precious resources because public-key-based encryption and high traffic generate significantly high cost. In addition, many approaches cannot provide all of the aforementioned anonymity protections. For example, (Anonymous Location-Aided Routing in Suspicious MANETs (ALARM) [1]) cannot protect the location anonymity of source and destination, Secure Dynamic Distributed Routing (SDDR) cannot provide route anonymity, and (Zone Based Anonymous Positioning (ZAP) [2]) only focuses on destination anonymity. Many anonymity routing algorithms are based on the geographic routing protocol (e.g., Greedy

Perimeter Stateless Routing (GPSR)) that greedily forwards a packet to the node closest to the destination.

Disadvantages:

1. Existing anonymity routing protocols in MANETs based on Hop-by-hop encryption or redundant traffic based incurs high cost.

2. Cannot provide full anonymity protection to data sources, destinations, and routes.

3. In a MANET employing a high-cost anonymous routing in a battlefield, a low quality of service in voice and video data transmission due to depleted resources may lead to disastrous delay in domains such as military operations.

2.2 Proposed System

In order to provide high anonymity protection (for sources, destination, and route) with low cost, an Anonymous Location-based and Efficient Routing protocol (ALERT) is used. An ALERT partition a network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non-traceable anonymous route. ALERT is compared with recently implemented anonymous geographic routing protocols called Anonymous Location–Aided Routing in Suspicious MANETs (ALARM) (based on hop-by-hop encryption and redundant traffic) and Greedy Perimeter Stateless Routing (GPSR) respectively. ALARM uses current locations of the nodes to securely disseminate and construct topology snapshots and forward data. With the aid of advanced cryptographic techniques (e.g., group signatures), ALARM provides both security and privacy features, including node authentication, data integrity, anonymity, and un-traceability (tracking-resistance). It also offers protection against passive and active insider and outsider attacks. In GPSR, a packet is always forwarded to the node nearest to the destination. When such a node does not exist, GPSR uses perimeter forwarding to find the hop that is the closest to the destination.

Advantages:

1. It provides a non-traceable anonymous route.

2. Offers high anonymity protection at a low cost.

3. ALERT achieves better route anonymity protection and lower cost compared to other anonymous routing protocols such as ALARM and GPSR respectively.

2.3 Proposed System Architecture

In order to provide high anonymity protection (for sources, destination, and route) with low cost, an Anonymous Location-based and Efficient Routing protocol (ALERT) is used. This protocol partitions a network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non-traceable anonymous route.

As shown in figure 1, Source node initiates to transmit the packet to the destination node. So, source node sends the Source ID and Destination ID to the Routing Protocol. The source node broadcasts the route request packet to the intermediate nodes. Then the intermediate nodes receive the route requests and either forwards it or prepares a route reply indicating a valid route to the destination node.

The routing protocol will construct the routing table and select the feasible path based on minimum number of hop nodes and minimum number of hop distance through other nodes. Then the routing protocol sends the next hop information to the source. Routing Protocol performs the zone partitioning based on the zone distance in the network. Zone partitioning provides node type information (i.e. node type 0-Source node zone, node type 1-Relay node zone, and node type 2-Destination node) to the routing protocol.

Packet forwarding logic includes: random forwarder and relay node. In order to forward the packet, the distance between the sender node and the relay node is considered. If the distance is far, then the routing agent selects a feasible node called a random forwarder between sender node and relay node to interface the packet transfer. Later, Source encrypts the packet and forwards it to the random forwarder.

Random forwarder forwards the encrypted packet to the relay node. Relay node requests for next hop information with routing agent. Routing agent provides next hop information to relay node. Later, relay node forwards encrypted packet to the destination node. At the destination node side, decryption and verification takes place. Later, destination node sends an acknowledgement to the source node via relay node and random forwarder.

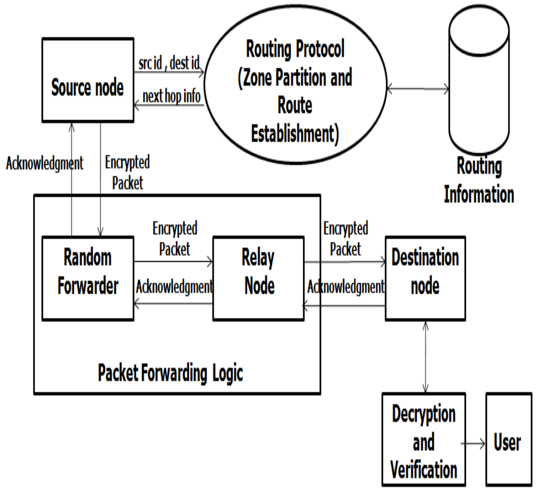

Fig. 1: Proposed System Architecture

3. Implementation

The implementation mainly involves 4 modules and they are:

1. Node Deployment and Configuration
2. Zone Partition
3. Relay Node Selection
4. Source Node Encryption and Packet Forwarding

Routing Protocol - The Adhoc On demand Distance Vector (AODV) routing protocol is a reactive routing protocol. It combines the use of destination sequence numbers in Destination Sequenced Distance Vector (DSDV) routing with the on demand route discovery technique in Dynamic Source Routing (DSR) protocols to formulate a loop-free, on-demand, single path, distance vector protocol. Unlike DSR, which uses source routing, AODV is based on hop-by-hop routing approach. AODV is designed to improve upon the performance characteristics of DSDV in the creation and maintenance of routes.

It is an on demand algorithm, meaning that it builds routes between nodes only as desired by source nodes. It maintains these routes as long as they are needed by the sources. AODV uses sequence numbers to ensure the freshness of routes. It is loop-free, self-starting, and scales to large numbers of nodes. The primary objectives of the AODV protocol are:

1. To broadcast discovery packets only when necessary,
2. To distinguish between local connectivity management (neighbourhood detection) and general topology maintenance.
3. To disseminate information about changes in local connectivity to those neighbouring nodes which are likely to need the information.

In AODV, each node maintains two separate counters:

1. Sequence Number, a monotonically increasing counter used to maintain freshness information about the reverse route to the source.

2. Broadcast-ID, which is incremented whenever the source issues a new Route Request (RREQ) message.

Each node also maintains information about its reachable neighbours with bi-directional connectivity. Whenever a node (router) receives a request to send a message, it checks its routing table to see if a route exists. Each routing table entry consists of the following fields:
• Destination address
• Next hop address
• Destination sequence number
• Hop count

3.1 Node Deployment and Configuration

The node deployment and configuration module involves the deployment of required number of mobile wireless sensor nodes in a predefined topography in NS2 simulator. Sensor nodes are considered to be mobile. Each and every node is configured to the required specifications such as labeling of nodes, defining the color of the node, event occurring time and so on and simulation parameters are defined according to the requirements. The Network Animator (NAM) presents the visual output of the TCL file. The NAM is the front end which presents the animation of all the events taking place in the network.

3.2 Zone Partition

Network area will be partitioned with respect to destination position and sender position which groups the set of nodes called mobile node and relay node zones. Relay nodes are used for forwarding the packets between sender and destination. As shown in figure 2 initially source node broadcast the route request to the neighboring nodes. Later, route request is returned to the base station (Adhoc On demand Distance Vector routing protocol). Routing protocol sends the route reply to the source node and performs the zone partitioning based on the zone distance in the network. Zone partitioning provides node type information (i.e. node type 0-mobile node (source node) zone, node type 1-Relay node zone, and node type 2-Destination node).

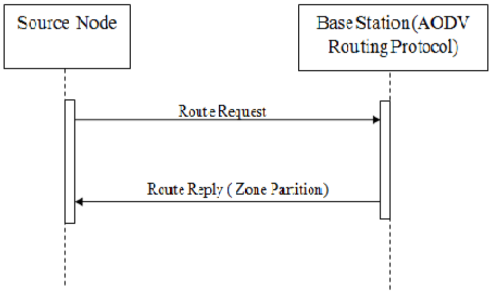
Source Node
Base Station(AODV Routing Protocol)
Route Request
Route Reply (Zone Parition)

Fig. 2 Sequence Diagram for Zone Partitioning

3.3 Relay Node Selection

Based on the zone distance in the network, a node type gets initialized. Node types are Node type 0- mobile node (source node) zone, Node type 1- relay node zone, Node type 2- destination node. If a node resides in the source zone, then it gets the next relay node for the respective node depending on the routing table constructed. As shown in figure 3 initially source node broadcast the route request to the neighboring nodes. Finally route request is returned to the base station (AODV routing protocol). Routing protocol sends the route reply to the source node and performs the zone partitioning based on the zone distance in the network. Zone partitioning provides node type information i.e. node type 0-mobile node (source node) zone, node type 1-Relay node zone, and node type 2-Destination node. Source node requests for the relay node information to the routing protocol. Routing protocol returns the relay node information depending on the routing table constructed.

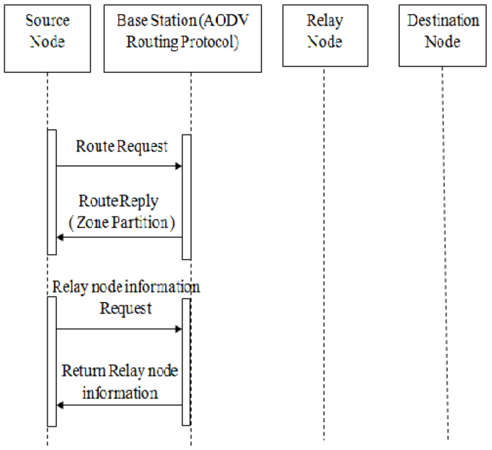
Source Node
Base Station(AODV Routing Protocol)
Relay Node
Destination Node
Route Request
RouteReply (Zone Partition)
Relay node information Request
Return Relay node information

Fig. 3 Sequence Diagram for Relay Node Selection

3.4 Source Node Encryption and Packet Forwarding

In order to provide source, router and destination anonymity, the sender packets are encrypted by using polynomial key generated using the combination of sender, relay and destination identities.

1. Data Encryption Standard (DES) algorithm is used for Encryption and Decryption of the packets.
2. RSA algorithm is used for generating the Polynomial Key Generation.

Packet Forwarding - In order to identify, group and to separate the received packets in the zone, the following conditions are checked:

1. Depending on the node types, the packets are classified as route request packet and user packet. If a packet arrives to any node is a broadcast packet that is, if (packet==255) then the broadcast is replied to the neighboring nodes in that zone.
2. If a packet arriving to any node is a user packet that is, if (packet! =255) then the packet is set to free.

The packet which is set to free must hold 2 conditions, which are,

1. To check whether the packet has been reached the destination. If reached, then the packet is stored in the stack.
2. If the packet has not reached the destination, then the packet is delivered via random forwarder, then relay node and finally to the destination.

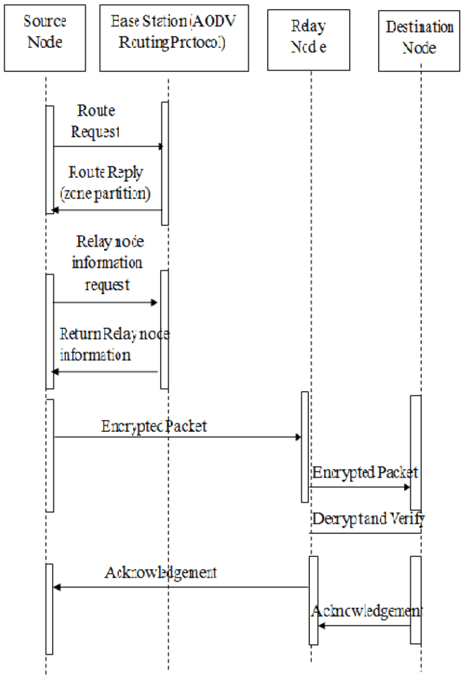

Fig. 4 Sequence diagram for Encryption and Decryption of a packet

As shown in figure 4, initially source node broadcasts the route request to the neighboring nodes. Finally route request is returned to the base station (AODV routing protocol). Routing protocol sends the route reply to the source node and performs the zone partitioning based on the zone distance in the network. Zone partitioning provides node type information (i.e. node type 0-mobile node (source node) zone, node type 1-Relay node zone, and node type 2-Destination node). Source node requests for the relay node information to the routing protocol. Routing protocol returns the relay node information depending on the routing table constructed. Later, source node forwards the encrypted packet to relay node. Relay node forwards the encrypted packet to destination. As soon as the encrypted packet arrives to the destination node, at the destination node side decryption and verification of the packet takes place. Later, Destination node sends an acknowledgement to source node via relay node.

4. Results

The environment of Anonymous Location-based and Efficient Routing protocol (ALERT) is simulated using NS2 simulator. The results are analyzed using graphs and there are many tools for graph designing in NS2 like x-graph, trace graph, gnuplot etc. Here x-graph is used for graph generation. X-graph is a plotting program which is used to create graphic representations of simulation results.

4.1 Simulation

The nodes are randomly placed in a 300 x 300 m^2 field area. The sensor nodes are mobile in nature. Total simulation time is 30 seconds. The different simulation parameters that are set are described below:

Simulation Parameters:
1. Number of nodes = 51
2. Geographical area (m^2) = 300 * 300
3. Channel type = Wireless Channel
4. Queue type = Drop Tail/PriQueue
5. Routing Protocol = AODV
6. MAC type = IEEE 802.11
7. Simulation time = 30 s

4.2 Performance Analysis

The following are some of the performance metrics evaluated to analyze the simulation results:
1. Packet delivery ratio
2. End-to-End delay

1. Packet Delivery Ratio
Packet Delivery Ratio (PDR) is defined as the ratio of data packets received by the destination to those generated by the sources. Mathematically, it is defined in Eq. (1) as follows:

$$PDR= (S1/S2)* 100 \qquad (1)$$

Where, S1 is the sum of data packets received by the each destination and S2 is the sum of data packets generated by the each source. The graph shows the fraction of data packets that are successfully delivered during simulation time versus the PDR (%). The fig 5 highlights the relative performance of existing method (ALARM and GPSR) with our implemented method (ALERT) for Packet Delivery Ratio with varying time and PDR. As the time increases, packet delivery ratio also increases. It is observed that our implemented method has a higher Packet Delivery Ratio compared to the existing method.

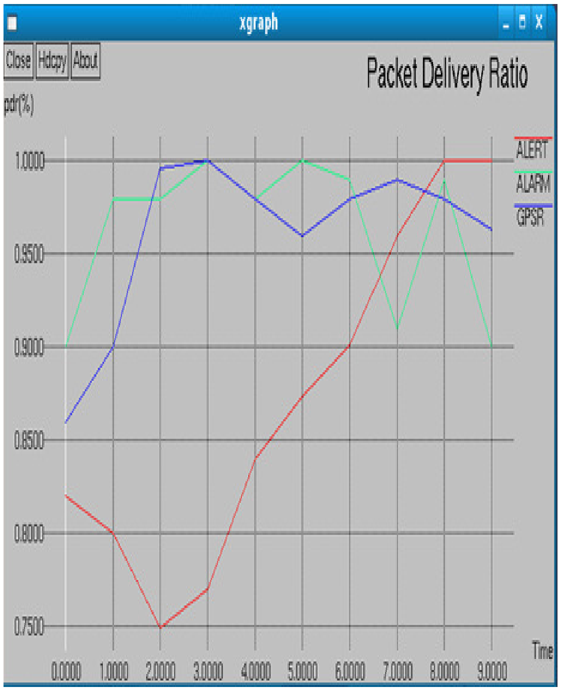

Fig. 5 – Graphical Performance Comparison1 (Packet Delivery Ratio) of the Implemented Method (i.e. ALERT) with the Existing method (i.e. ALARM and GPSR)

2. End-to-End Delay

End-to-End delay is defined as the average time it takes a data packet to reach the destination. This includes all possible delays caused by buffering during route discovery latency and queuing at the interface queue. Mathematically, it is defined in Eq. (2) as follows:

$$\text{Avg. End to end delay} = (S/N) \qquad (2)$$

Where S is the sum of the time spent to deliver packets for each destination, and N is the number of packets received by the destination nodes.

The fig 6 highlights the relative performance of existing method (ALARM and GPSR) with implemented method (ALERT) for Average End To End delay with varying time and number of nodes. As the number of nodes increases, delay decreases. It is observed that our implemented method has a lower End-to-End Delay compared to the existing method.

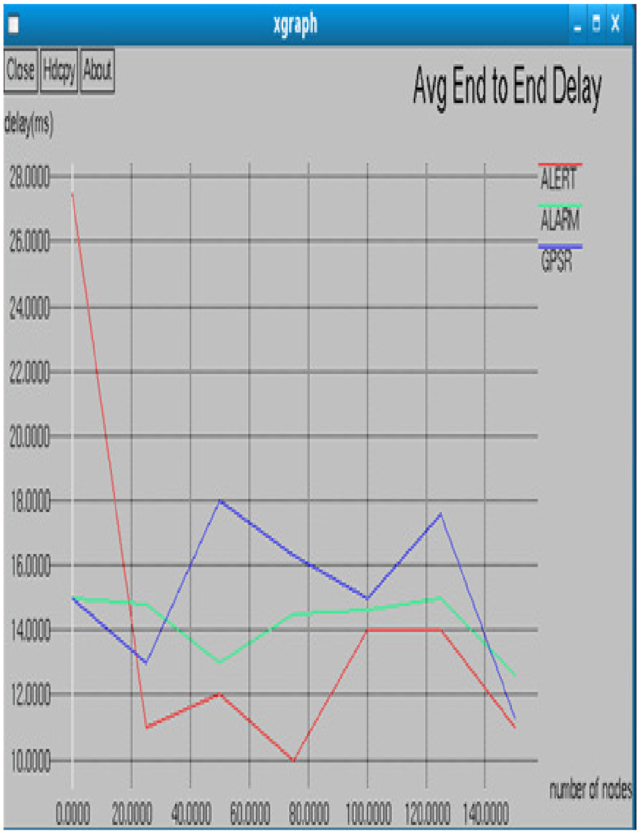

Fig. 6 – Graphical Performance Comparison2 (Average end to end delay) of the Implemented method (i.e. ALERT) with the Existing method (i.e. ALARM and GPSR)

5. Conclusion

Anonymous Location Based Efficient Routing Protocol is implemented using Network Simulation (NS2) tool. Initially, the nodes are deployed and configured in a predefined topography. Later, Network area will be partitioned with respect to destination position and sender position which groups the set of nodes called mobile node and relay node zones. Based on the zone distance in the network, node types get initialized. Node types are Node type 0- Mobile node (source node) zone, Node type 1- Relay node zone, Node type 2- Destination node. In order to provide source, route and destination anonymity, the sender packets are encrypted (DES algorithm) by using polynomial key generated using the combination of sender, relay and destination identities by the RSA algorithm. Our implemented method (ALERT) is compared with the existing methods (ALARM and GPSR) Comparison is based on the performance metrics such as packet delivery ratio and end to end delay. Using X-graph tool in Network Simulator (NS2), the simulation results are shown graphically. Results indicate that our implemented method (ALERT) has a higher packet delivery ratio and lower end to end delay compared to the existing method (ALARM and GPSR).

References

[1] K. E. Defrawy and G. Tsudik, "ALARM: Anonymous Location- Aided Routing in Suspicious MANETs," Proc. IEEE Int'l Conf. Network Protocols (ICNP), 2007.

[2] X. Wu, J. Liu, X. Hong, and E. Bertino, "Anonymous Geo- Forwarding in MANETs through Location Cloaking," IEEE Trans. Parallel and Distributed Systems, vol. 19, no. 10, pp. 1297-1309, Oct.2008.

[3] X. Wu, "AO2P: AdHoc On-Demand Position-Based Private Routing Protocol," IEEE Trans. Mobile Computing, vol. 4, no. 4, pp. 335-348, July/Aug. 2005.

[4] S. Ratnasamy, B. Karp, S. Shenker, D. Estrin, R. Govindan, 1 L. Yin, and F. Yu, "Data-Centric Storage in Sensornets with GHT, a Geographic Hash Table," Mobile Network Applications, vol. 8, no. 4, pp. 427-442, 2003.

[5] Sk. Md. M. Rahman, M. Mambo, A. Inomata and E. Okamoto. "An Anonymous On-Demand Position-Based Routing in Mobile Ad Hoc Networks," Proc. Int'l Symp. Applications on Internet (SAINT) 2006.

[6] V. Pathak, D. Yao and L. Iftode. "Securing Location Aware Services over VANET Using Geographical Secure Path Routing," Proc. IEEE Int'l Conf. Vehicular Electronics and safety (ICVES), 2008.

[7] 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.

[8] S. Ratnasamy, B. Karp, S. Shenker, D. Estrin, R. Govindan, L. Yin, and F. Yu, "Data-Centric Storage in Sensornets with GHT, a Geographic Hash Table," Mobile Network Applications, vol. 8, no. 4, pp. 427-442, 2003.

[9] L. Zhao and H. Shen, "ALERT: Anonymous Location Based Efficient Routing Protocol in MANETs," Proc. Int'l Conf. Parallel Processing (ICPP), 2013.

R. Shwetha B.E in Computer Science in the year 2008, MTech (pursuing) Computer Science & Engineering in B.N.M Institute of Technology. Previously worked as lecturer in Government Polytechnic for Women (2009-2010) and Brindavan College of Engineering (2010-2012).

Dr. B. G. Prasad Ph.D currently working as Professor & Head of Department in CSE at B.N.M Institute of Technology. He has over 25 years of academic experience in Computer Science. Has published 24 journals / conference papers. His areas of interest encompass Computer Networks, Image Processing, CBIR, Operating Systems and Computer Vision.