ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

IJIRSET

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)
On 21st & 22nd March Organized by

K.L.N. College of Engineering , Madurai, Tamil Nadu, India

Location Based Anonymous Routing Protocol for MANETS

P.Dhivya[1] M.Rajakani[2]

[1]PG Scholar, Department of Computer Science and Engineering, Mepco Schlenk Engineering College, Sivakasi, India

[2]Asst.Professor, Department of Computer Science and Engineering, Mepco Schlenk Engineering College Sivakasi, India

Abstract - Privacy is needed in ad hoc networks. In order to provide anonymous routing protocol in MANETs the location of source and destination can be concealed by using "notify and go" mechanism and broadcasting. In this paper, we address some of the issues arising in MANETs by using an anonymous routing protocol. Location Based Anonymous Routing Protocol partitions the network into zones for anonymity protection. The destination position is identified to separate the source node from destination node by clustering, which is needed by the packet forwarder to check whether it is separated from the destination. The packet which is forwarded from source to destination can be encrypted by using asymmetric encryption algorithm. Location Based Anonymous Routing Protocol forwards a packet to the neighbor to the destination through the randomly selected relay nodes. Thus, it provides anonymous protection to source, destination, and routes at a low cost. It takes advantage of geographic routing protocol and also provides reliable communication. For routing anonymity temporary destination can be randomly chosen in other zone and relay nodes are selected in the same zone to transfer the data to temporary destination. Owe to the vulnerable nature of the mobile ad hoc network, there are various security threats that disturb the development of it. Location Based Anonymous Routing Protocol also has strategies to effectively counter the intersection and timing attacks.

Keywords - Ad hoc wireless network, anonymity, geographic routing, identity.

I. INTRODUCTION

MANETs Stands for "Mobile Ad Hoc Network". It is an ad hoc wireless system that can change locations and configure itself on the fly. Because MANETs are ambulatory, they use wireless connections to connect to various networks. The topology in an ad hoc network may change constantly due to the mobility of nodes. Because of that mobility, nodes can move in and out of coverage region of each other, so that some links break while new links between nodes are created. MANETs feature self-organizing and independent infrastructures, which make communication and information sharing in wireless network. In MANETs nodes are not in safe, there is a malicious activity such as communication eavesdropping or attacking routing protocol to steal the data forwarded through the network. In MANETs anonymity is require in tactical networks (military battlefields), emergency services, commercial and civilian. In Exiting system security is not provided completely, there is neither source nor destination anonymity. It is multi-hop routing. So the message is send from anyone to anywhere. It has high capability. If node location information is sufficiently granular, a physical map of a MANET can be constructed and node locations is identified, instead of node identities, can be used in place of network addresses. In fact, in some application settings, such as law enforcement and search-and-rescue, node identities might not be nearly as important as node locations. In addition, if the operating environment is hostile, node identities must not be revealed. We use the term "hostile" to mean that communication is being monitored by adversarial entities which are not part of the MANET [2]. Hiding the location of the node help to make more difficult for adversary to focus attacks.

In ad hoc networks, geographic routing protocols [3], [11] which uses geographical information to route the data and queries. Each node periodically updates its current location to its neighbors node. It exposure the node location and create a way for abuse. GPSR routing protocol also called position based routing algorithm [5] for ad hoc networks. 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 location and an ID is unique [6]. Therefore, in position-based routing algorithms, if the positions have been exposed for routing, node IDs do not need to be revealed. If an attacker cannot match a position to a node ID correctly, then node anonymity can be achieved. In ad hoc routing protocol, there is necessary security is needed in source, route and destination. That can be achieved by anonymity to the location of source and destination and randomness in choosing the forwarding node. That cannot obtain completely in existing system neither source nor destination anonymity provided by the existing routing protocol in MANETs. Also, in existing system uses public key based encryption, it increases the cost.

To solve this problem, develop a location based anonymous routing protocol in MANETs. That provides anonymity protection to source, route and destination. Full anonymity protection in MANETs means, it includes identity and location of data source and destination as well as route anonymity.

II. Proposed System

The network route from sender node to a destination node may require a number of intermediate nodes to forward packets to create a ‘‘multihop’’ path from a sender to destination. The role of the routing protocol in an ad hoc network is to allow nodes to learn such multihop paths. Since the nodes in the network may move at any time, or may even move continuously the routing protocol must also be able to react to these changes and to learn new routes to maintain connectivity. Ad hoc networks require no centralized administration or fixed network infrastructure such as base stations or access points, and can be quickly and inexpensively set up as needed. Dynamically partitions the network into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a nontraceable anonymous routing.

In addition, it hides the data initiator/receiver among many initiators/receivers to strength ensource and destination anonymity protection. Randomly chooses a node in the other zone as the next forwarding node and uses the GPSR algorithm to send the data between that node.

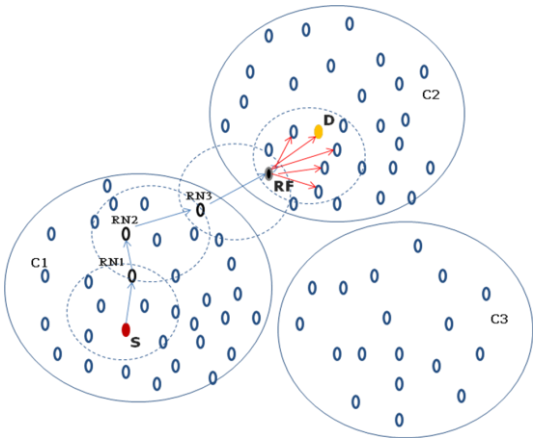


Fig. 1 System Architecture

The intermediate node in the other zone act as a Temporary Destination (TD). Source can send the data to the TD through the number of intermediate relay node (RN) in the same zone. TD can forward the data closest to the destination. In the destination zone the data can be broadcast to few nodes to obtain the destination anonymity. The source can be hidden in the number of initiator to obtain the source anonymity. Location based anonymous routing protocol uses symmetric key encryption for transmitted data. In a S-D communication, S first embeds a symmetric key Ks, encrypted packet using D’s public key. Later, D sends S its requested contents, encrypted with Ks, decrypted by its own public key. Therefore, the communicated between S and D can be efficiently and securely protected using Ks.

A. Our Assumption

MANET deployed in a large field where geographic routing is used for node communication in order to reduce the communication latency. In anonymous communication protocol that can provide untraceability of routing that can be needed to strictly ensure the anonymity of the sender when the sender communicates with the other node. A malicious observer may also try to detect destination nodes through traffic analysis by launching an intersection attack. Therefore, the destination node also demands the protection of anonymity. By eavesdropping, the adversary nodes can analyze any routing protocol and obtain information about the communication packets in their vicinity and positions of other nodes in the network. They can also analysis data transmission on the air when a node is communicating with other nodes in the wireless network and record the historical communication of nodes. They can interfere on some specific weak nodes to control their behavior, e.g., with Denial-of-Service (DoS) attacks, which may break the routing in existing anonymous geographic routing methods.

1) *Intersection Attack:* A communication between the source and destination can be repeatedly observed by the attackers. So that which source encode the message and which node receive the message can be identified by intruders. This intersection attack can be avoided in Location based anonymous routing protocol by destination anonymity protection method. In the existing system, ZAP (Zone based Anonymous Position routing) to counter the intersection attack. It enlarge the area of destination zone to broadcast the message. It will increases the communication overhead in the destination zone, that reduce the performance of routing.

2) *Intersection Attack:* In the time of packet departure and arrival, an attacker can identify the source and destination by observing the time interval between the start of the transmission up to the end. In this, attacker work backward to the input. This attack can be avoided by providing the anonymity to the source.

B. Dynamic Pseudonym and Location Service

Communication between two nodes, a sender node (S) send a request to the destination node (D) and then the destination node send a replay to S. A transmission session is the time period that S and D interact with each other continuously until they stop. In Location based anonymous routing protocol, each node uses a dynamic pseudonym as its node identifier rather than using its real address, which can be used to trace nodes' existence in the network. The public key is used to enable two nodes to securely establish symmetric key Ks for secure communication.

III. Routing In Location Based Anonymous Routing Protocol In MANETs

In Location Based Anonymous Routing Protocol a dynamic and unpredictable routing path, that is a number of dynamically determined intermediate relay nodes. In this protocol the area of the network can be partitioned into number of zone in horizontal and vertical manner this process is called hierarchical zone partition. Source (s) can first checks whether itself and destination are in the same zone, if it is in same zone then it can divide the zone into horizontal and vertical manner. It can separate the source and destination. This process of partition can be performed until it reaches the Destination Zone (D_Z).

Forwarding the packet from source to destination can be performed by using the intermediate nodes. Source can select the neighbor node which is closest to the destination to forward the data .Intermediate node selected in other zone is TD that act as a Random Forwarder (RF). Then the source can select the RN in the same zone to forward the data to the TD.

In Fig. 1, the source (s) is in the zone c1 destination (D) is in the zone c2. The source can select the RF in the other zone c2 which is closest to the destination and then randomly select several intermediate relay node (RN). Forwarding node can be selected by setting the flag value for all nodes in the source cluster. If the node is within the coverage region of the source node then set the flag value as 1 else set the value as 0. A malicious observer may also try to detect destination nodes through traffic analysis by launching an intersection attack. Therefore, the destination node also needs the protection of anonymity. For that Destination zone the packet can be broadcast to few nodes to provide the destination anonymity.

A. Destination Zone Position

Each packet forwarder can check whether the destination position is reached or not, this can be identified by calculating the D_Z position. That D_Z can be produced by total number of partitions in the network. The total number of partitions (P) can be calculated by node density ρ, the number of nodes (n) in D_Z, and the size of the entire network area N.

$$P=\log_2(\rho \cdot N / n) \quad (1)$$

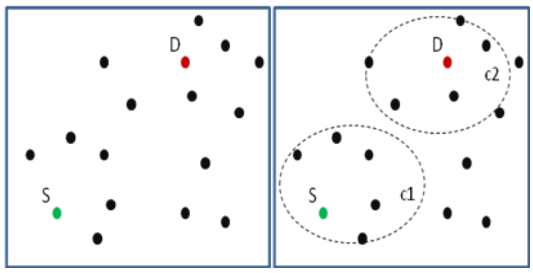
B. Packet Format

For reliable communication between the source and destination ACK can be send to the source to check whether the packet reach the destination correctly or not. The packet can be encrypted by using the destination public key so that packet can be only accessed by the destination node. In the packet, PS is the pseudonym of a source; PD is the pseudonym of the destination; L_S and L_D are the positions of the P^{th} partitioned source zone and destination zone, respectively; L_D is the currently selected TD's coordinate; P is the number of divisions so far, and K^S_s denotes the symmetric key of a source. Particularly, Time To Live (TTL) is used for the protection of source anonymity. At first create a wireless network with 50 nodes and uniquely identify each node by dynamic pseudonym. Every node maintains a routing table. The source and destination can be identified and classify the position of that node. The public key and location of the destination of a data transmission can be known by others, but its actual identity desire protection. That protection can be provided by the destination anonymity. The source can identify the temporary destination (TD) and the intermediate relay node that can be used to forward the packet to the destination node. Intermediate node can be randomly selected on the basic of the coverage region. TD can be selected as, which is closest to the destination node. Between source node and TD node the transmission can be performed by randomly selected several RN.

For successful communication between S and D, S and each packet forwarder uses the GPSR routing algorithm to send the data to the node closest to TD. In order to hide the packet content from adversaries, in my work employs cryptography. The work in experimentally proved that generally symmetric key cryptography costs hundreds of times less overhead than public key cryptography while achieving the same degree of security protection. Therefore, the packets communicated between S and D can be efficiently and securely protected using K^S_s. NAKs/ACK used in geographic routing-based approaches to reduce traffic cost. In this paper, use NAK in order to identify the packet loss in the transmission.

IV. Zone Partitioning

In my project zone partitioning can be performed partitioning the network. The separation between the source node and destination node for anonymity protection.



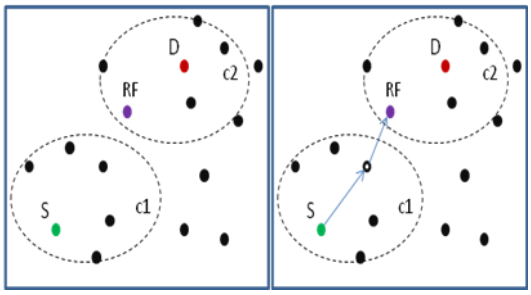


Fig. 2 Zone partition

First the source can check whether the destination can present in the same zone, if it is in same zone then source can partition the network. In the D_Z, there are a number of nodes to provide high anonymity to the destination zone. In the source zone each node can communication with the neighbor's node. Each node maintains the routing table that contains the neighbor node detail and the distance between those nodes. One zone node can communicate with other zone nodes by the neighbors node of that zone that means some node is within the coverage region of the other zone node. Fig. 2 show the partition method, in the first diagram the source and destination in the same zone and then in the second diagram source can partition the network into two zones by clustering the group of node such as C1 and C2 and select the intermediate node in the other zone (C2) as random forwarder. In the third diagram select the intermediate relay node forward the data to RF this process is continue until the destination can be reached.

A. Source Anonymity

The contribution of the Location based anonymous routing protocol is to provide the location anonymity to the source and destination. The anonymity protection of location can confuse the intruder to decide if a node is source or a forwarding node. To provide the source anonymity, the source node location can be hide by lightweight mechanism called "notify and go". In this mechanism the source node can send a notification message to a neighbor's node with piggybacks its update packet. After the receiving of notification the source node and neighbors node can wait for some random time and then that all neighbors' nodes can send a packet at the time of source send in order to hide the packet among other packets. Before send the packet can be encrypted by asymmetric encryption algorithm AES (Advanced Encryption Standard) to reduce the cost. That encrypted packet can be decrypted only by the destination node.

1) Time to live: That packet contain the TTL (time to live) field. The source can set a valid TTL value and the neighbor node covering packet contain the value TTL=0 and the node which is selected as the next TD, packet forward through a intermediate relay node contain the non-zero value for TTL. The intermediate node can be selected on the basic of GPSR routing protocol which select the node that is closest to the destination. Only the destination node can contain the valid TTL and decrypt the packet by its own private key.

B. Distance Calculation

The distance between the nodes can be calculated and find the shortest path to reach the destination. Every node periodically updates the location information about its neighbor's node. Based on this information, a sender selects the path and list of next hop nodes that are eligible for forwarding the data. In the distance calculated table from source node which node has small value can be selected as next hop node and the data can be forwarded to that node. In that table the reachable node can be set flag as 1 and other are set to 0.

In the source anonymity method the timing attack can be avoided by "notify and go" method. At the time of source send, its neighbors node also send a covering packet. So the intruder cannot identify the exact location of the source, because of traffic generated in source cluster.

C. Node Selection

Location based routing protocol features a dynamic and unpredictable routing path, which consists of a number of dynamically determined intermediate relay nodes. It makes the route between a S-D pair difficult to discover by randomly and dynamically selecting the relay nodes. relay node means that is in the same zone of the source and RF means which is selected as intermediate forwarder node in the other zone that is also called TD. The resultant different routes for transmissions between a given S-D pair make it difficult for an intruder to observe a statistical pattern of transmission. This is because the RF set changes due to the random selection of RFs during the transmission of each packet. Even if an adversary detects all the nodes along a route once, this apprehension does not help in identify 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. Location based anonymous routing protocol 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. Source can randomly choose a position in the other zone called TD, and uses the GPSR routing algorithm to send the data to the node closest to TD. This node is defined as a random forwarder.

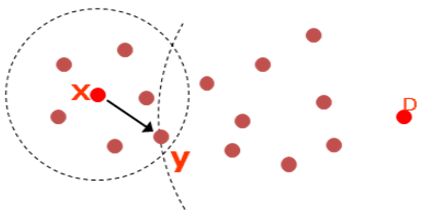


Fig. 3 intersection node selection

X-source node, D-destination node and Y-relay node. Fig. 3 shows the GPSR routing process of neighbor node

selection. X select neighbor Y, which is closest to the destination. That Y is in the coverage of X and that is reachable by D. This selection process is called GPSR routing.

1) Routing Table: Routing table is maintained in each node that contains the information about source node and the next neighbor node to transfer the packet and the position of that node. Routing table can be obtained by the distance table, which nodes contain the value within the coverage region of the source can be present in the routing table and randomly select the intermediate node in that node. After the packet reach the next hop node in the routing table of source, then that node act as a source and contain the routing table information. This process is performed until reach of destination zone. Routing table is created for each node by that each node in the path known the next hop node to forward the packet.

V. Destination Anonymity

Destination anonymity is determined by the number of nodes in the destination zone, which is related to node density and the size of the destination zone. In the destination zone broadcast packet to a set of few nodes out of n nodes. The few nodes to broadcast include the destination node. The last RF node in the destination zone can broadcast the packet to few nodes in that zone to provide destination anonymity.

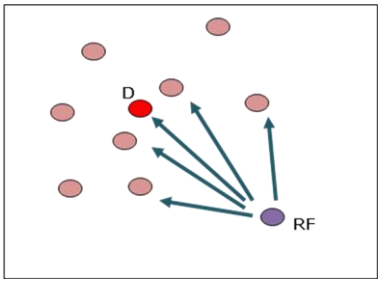


Fig. 4 Message broadcasting

A. Counter the Intersection Attacks

Location based anonymous routing protocol 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 D_Z 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 a result, D is identified as the destination because it always appears in the destination zone. In fig. 4, it shows the broadcasting of packet in the destination zone. The arrows show the moving directions of nodes.

To counter the intersection attack, ZAP [2] dynamically enlarges the range of anonymous zones to broadcast the messages or minimizes communication session time. However, the former strategy increases the communication overhead, while the latter may not be suitable for long duration communication. In the existing system ALERT broadcast the packet to m nodes out of k nodes in the destination. m node receives the packet and hold the packet pkt1 until reaching of next packet. After arrival of pkt2 it can transmit one hop to enable the other nodes to receive the packet. Due to that each node load is increased it decrease the performance of the protocol. Instead of adopting such a mitigating mechanism, we use another strategy to resolve this problem. Rather than using direct neighborhood broadcasting in the zone, the last RF multicasts packet pkt1 to a partial set of nodes, out of the total n nodes in the destination zone that set of node also contain the destination node to receive the data. It enables other nodes in the zone to receive the packet in order to hide D.

VI. Results And Discussion

The distance between the nodes can be calculated by using Euclidean distance calculation**.** By using that identifies the neighbor node to forward the data from source. Intermediate node selection can be performed carefully by setting the flag value because some nodes are in the same cluster of source but it far away from the source node. Table.1 describes the flag value set for the nodes which are in the path from source to destination. If the node is neighbor to the source to transfer then it set as flag value 1for that node otherwise set flag value as 0. If source node is n1 then its neighbor node distance is calculated in that n12 has small distance and within the coverage region of the source so its flag value is 1. So source can forward data to n12 then find the next intermediate node from n12 by using same method.

Table.2 shows the path form source n1 to destination n45. Routing path through the nodes are n12, n19, n32, n42, n44, n45. Passing through cluster 1, cluster 3 and cluster 4. In that routing data is passed through cluster 1, cluster 3 and cluster 4. Cluster 1 is a source zone and cluster 4 is a destination zone.

TABLE.1
Flag Value TO Discover The Route

Source	Neighbor	Distance	Cluster	Flag
n1	n2	361	Cluster1	0
n1	n3	668.2	Cluster1	0
n1	n4	420.8	Cluster1	0
n1	n12	24.8	Cluster1	1
n32	n33	196.5	Cluster3	0
n32	n41	370.1	Cluster4	0
n32	n42	172.2	Cluster4	1
n32	n43	688	Cluster4	0
n19	n35	580.4	Cluster3	0
n19	n32	196.5	Cluster3	0

VII. Performance Evaluations

In this section, experimental evaluation of the routing protocol, which exhibit consistency with our analytical results. Both prove the superior performance of routing in providing anonymity with low cost of overhead. Recall that anonymous routing protocols can be classified into hop-by-hop [2], [3], [4], [5], [11] encryption and redundant traffic [6], [7], [12], [10]. We compare Location based anonymous routing protocol with two recently proposed anonymous geographic routing protocols: AO2P [3] and ALARM [4], which is based on hop-by-hop encryption and redundant traffic, respectively. All of the protocols are geographic routing, so we also compare it with the baseline routing protocol GPSR [2] in the experiments.

TABLE. 2
Route Discovery

Source node	Destination node	Distance	Zone position
n1	n12	24.8	Cluster1
n12	n19	92.9	Cluster1
n19	n32	154.4	Cluster3
n32	n42	172.2	Cluster4
n42	n44	619.0	Cluster4
n44	n45	256.8	Cluster4

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. In ALARM, each node periodically disseminates its own identity to its authenticated neighbors and continuously collects all other nodes' identities. Thus, nodes can build a secure map of other nodes for geographical routing. In routing, each node encrypts the packet by its key which is verified by the next hop en route. Such dissemination period was set to 30 s in this experiment. The routing of AO2P is similar to GPSR except it has a contention phase in which the neighboring nodes of the current packet holder will contend to be the next hop. This contention phase is to classify nodes based on their distance from the destination node, and select a node in the class that is closest to destination. Contention can make the ad hoc channel accessible to a smaller number of nodes in order to decrease the possibility that adversaries participate, but concurrently this leads to an extra delay. Also, AO2P selects a position on the line connecting the source and destination that is further to the source node than the destination to provide destination anonymity, which may lead to long path length with higher routing cost than GPSR.

Fig.5 shows the delivery rate versus the number of nodes with destination update. We see that delivery rate of all methods are close to 1, except in the sparse environment where node density is only 50 nodes=km2. This is due to the unavailability of relay nodes in a sparse environment sometimes. In fig.6 shows the execution time compare to the existing system.

VIII. Conclusion And Futurework

This research proposes a routing algorithm, named Location Based Anonymous Routing Protocol, to achieve anonymity protection to source, destination and routes. Some protocol unable to provide the source, destination and route anonymity that means not provide full anonymity protection. Location Based Anonymous Routing Protocol is distinguished by its low cost and anonymity protection for sources, destinations, and routes. It partitions the network by clustering and random relay node selections to make it difficult for an intruder to detect the two endpoints and nodes en route. A packet in Location Based Anonymous Routing Protocol includes the source and destination zones rather than their positions to provide anonymity protection to the source and the destination. Location Based Anonymous Routing Protocol further strengthens the anonymity protection of source and destination by hiding the data initiator/receiver among a number of data initiators/receivers. It has the "notify and go" mechanism for source anonymity, and uses local broadcasting for destination anonymity. It also counters the intersection and timing attacks. Future work lies in reinforcing Location Based Anonymous Routing Protocol in an attempt to defeat stronger, active attackers.

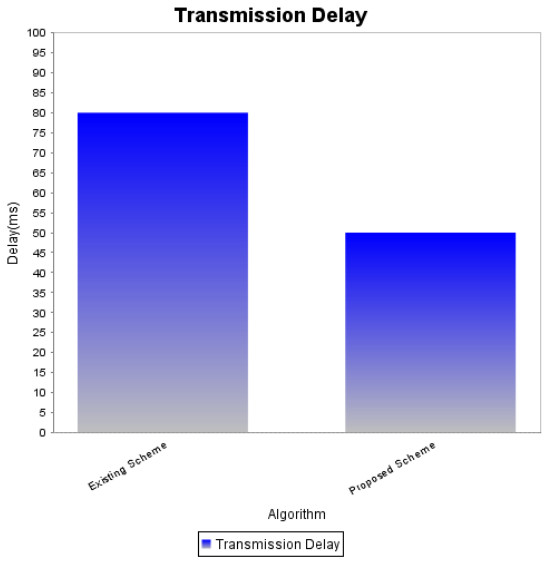


Fig. 5 Transmission delay

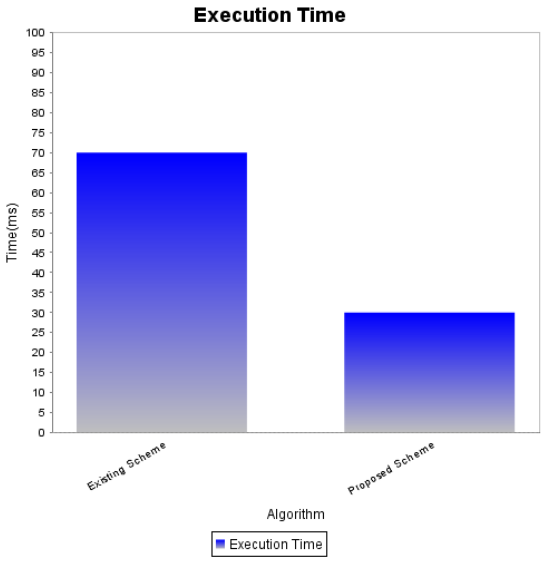


Fig. 6 Execution time

ACKNOWLEDGMENT

The authors wish to express their heartfelt thanks and gratitude to the Department of Computer Science and Engineering of Mepco Schlenk Engineering College, Sivakasi for providing good support and encouragement for this work. The authors also thank their principal and management for providing the necessary facilities to carry out this work.

REFERENCES

[1] Haiying Shen and Lianyu Zhao, " ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs " IEEE Transaction on Mobile Computing, Vol. 12, No. 6, June 2013.

[2] 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.

[3] 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.

[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] K.E. Defrawy and G. Tsudik, "PRISM: Privacy-Friendly Routing in Suspicious MANETs (and VANETs)," Proc. IEEE Int'l Conf.Network Protocols (ICNP), 2008.

[6] 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.

[7] Stefaan Seys and Bart Preneel K.U.Leuven, "ARM: Anonymous Routing Protocol for Mobile Adhoc Networks".

[8] C.-C. Chou, D.S.L. Wei, C.-C. Jay Kuo, and K. Naik, "An Efficient Anonymous Communication Protocol for Peer-to-Peer Applications over Mobile Ad-Hoc Networks," *IEEE J. Selected Areas in Comm.,vol. 25, no. 1, pp. 192-203, Jan. 2007.*

[9] 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.*

[10] B. Zhu, Z. Wan, M.S. Kankanhalli, F. Bao, and R.H. Deng, "Anonymous Secure Routing in Mobile Ad-Hoc Networks," *Proc.IEEE 29th Ann. Int'l Conf. Local Computer Networks (LCN), 2004.*