International Journal of Advanced Information in Engineering Technology (IJAIET) ISSN: 2454-6933
Vol.3, No.9, September 2016

Improved anonymous routing protocol with reduced overhead in Manets

Roshin Pushpan
Computer Science and Engineering
MES College of Engineering
Kuttippuram, India

Neena Susan Alex
Computer Science and Engineering
MES College of Engineering
Kuttippuram, India

***Abstract*—Mobile ad-hoc Networks are used in various fields where it needs anonymous routing for the packets. Since manets are decentralized in nature and due to its free mobility, attacks from malicious nodes are common. This may compromise the communication and leads to the failure in anonymous communication protocol. A lot of researches are being conducted to develop protocols for anonymous communication. Here a location based anonymous communication protocol is developed with reduced overhead, which provides anonymity in node locations and motion patterns. Another feature of the protocol is to provide anonymous routing with shortest path considerations. The protocol provisions certain improved techniques for the achievement of anonymous communication which includes source anonymity, route anonymity and destination anonymity Keywords—anonymous routing, military communication, manets, location based routing.**

I. INTRODUCTION

Wireless communication in manet environment are more vulnerable to both active and passive attacks. In some critical mission like military action scenario, the communication between the friendly nodes should be highly secured. Here it needs the anonymous routing protocol for the message passing. Basically three anonymous conditions are required: (1) source anonymity-to provide anonymity of the location and identity of the source which originates the message, (2) route anonymity-to provide anonymity of the forwarding route nodes and their paths, (3) destination anonymity-to provide anonymity of the location and identity of the final destination node.

II. LITERATURE SURVEY

Researches are always being conducted to improve the security and efficiency of the anonymous routing algorithms. Some of the innovative approaches for anonymity are described in the following sections.

A. ANODR-Anonymous On Demand Routing

ANODR [1], one of the first anonymous routing schemes for mobile ad-hoc networks. ANODR is a unicast anonymous manet routing protocol. ANODR exploits a route pseudo anonymity approach to address the route untraceability problem. It uses a trap-door boomerang onion encryption while forwarding route requests. Main drawback is that during the route request phase, it requires a large processing overhead due to network wide request sending process. Also the protocol does not provide location identity, one of the basic conditions for anonymity.

B. ASR-Anonymous Secure Routing

The functionality of the ASR [2] (Anonymous secure routing) protocol proposed by Zhu is essentially the same as that of ANODR. ASR makes no use of onion encryption as in ANODR that are built up as the Route request progresses through the network, but instead relies on state information that is kept at the forwarding nodes. As the state information is stored in the routing nodes, one or more node will have the knowledge of route used for the communication. If these nodes happened to be an attacker, it will be a serious threat for the anonymous communication. So route anonymity is not provided here.

C. AO2P-Adhoc On demand Position based Routing protocol

A02P [4] works in the network with relatively high node densities, where the positions of destinations are the only position information disclosed in the network for routing. In A02P, route is discovered by delivering a routing request message from the source to the position of the destination. Once a route is built, pseudo IDs and temporary MAC addresses are used for the nodes in the routes, such as sources, destinations, and intermediate forwarders. Since the node identities are not disclosed, communication anonymity can be achieved. For a destination whose position is revealed, its privacy is preserved by hiding the match between a position and its ID through the secure position management scheme. The attackers know that a node at a certain position will receive data. Also route anonymity is not achieved.

D. SDAR-Secure Distributed Anonymous Routing

In contrast to the previously presented protocols, Boukerche proposed SDAR [3] (Secure distributed anonymous routing) which does not use temporary or continuously changing identities. Instead SDAR uses a single fixed identity for every node. Every intermediate node inserts its identity as the source address of every message it broadcast. It requires every forwarding node to perform a public key decryption, a public key encryption and a signature generation for every route request message. The whole process adds overhead to the protocol. Location identity is not achieved due to the insertion of each nodes identity inside the packet.

E. ALARM-Anonymous Location Aided Routing.

ALARM [6] (Anonymous location aided routing) uses nodes current locations 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 untraceability (tracking-resistance). Although it does not provide full security on the location anonymity of source and destination.

F. ALERT-Anonymous Location based Efficient Routing Protocol

Anonymous location based efficient routing protocol in manets-ALERT [7] proposed by Haiying Shen dynamically partitions the network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non traceable anonymous route. ALERT dynamically partitions a network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a nontraceable anonymous route. It then randomly chooses a node in the other zone as the next relay node and uses the GPSR [5] algorithm to send the data to the relay node. In the last step the data is broadcast to k nodes in the destination zone, providing k-anonymity to the destination. A notify and go mechanism is incorporated in order to have the source anonymity. Here it claims to provide source anonymity, but the protocol fails if the attacker may be an insider during the initial original data sending process in notify and go mechanism.

From the literature survey it is clear that no protocol is best amongst all as each has better performance over the other at a particular metric and time. Advantages and disadvantages of those protocols are compared. Some common comparable factors like source, destination, route, end to end data encryption anonymities are analyzed among the different existing protocols and found whether they are providing these or not. Based on this analysis and some general factors which affects the security of anonymous routing protocols, formulates the problems found in the existing anonymous protocol. A detailed analysis of the techniques seen in this chapter are done and based on it we have some results which can be used to determine which protocol is better suited for different manet communication environment. Comparisons are also made with the protocols to check whether they are providing the basic conditions of anonymity in communication. Analysis is summarized as the table below.

TABLE I SUMMARY OF EXISTING ANONYMOUS ROUTING PROTOCOLS

PROTOCOL	IDENTITY	LOCATION	ROUTE
ANODR (TOPOLOGY)	SOURCE DESTINATION	N/A	YES
AO2P (GEOGRAPHIC)	SOURCE DESTINATION	SOURCE DESTINATION	NO
ASR (GEOGRAPHIC)	SOURCE DESTINATION	SOURCE DESTINATION	NO
SDAR (TOPOLOGY)	SOURCE DESTINATION	N/A	YES
ALARM (GEOGRAPHIC)	SOURCE DESTINATION	SOURCE	NO
ALERT (GEOGRAPHIC)	DESTINATION	DESTINATION	YES

III. LOCATION BASED ANONYMOUS ROUTING PROTOCOL

Location based routing protocols differ with each other in a ways of finding and maintaining the route between source to destination and have the aim of reducing control packet overhead, maximum throughput, minimum power consumption and reduction of time delay. Anonymous location based efficient routing protocol (ALERT) is a location based protocol. It dynamically partitions the manet fields into zones and chooses random intermediate nodes for forwarding packets, which provides anonymous route. It relies on GPSR algorithm for the packet forwarding procedure. In the last step of the protocol, the packet is broadcast to all the nodes in that zone, where it also includes the destination node. Thus it claims to provide anonymity. The 'notify and go' mechanism used in ALERT claims that it can provide source anonymity. In this mechanism, the sender itself is revealing that it is going to send message to the destination to other nodes in its communication range. But this method arises some security risk. In this case, if the intruder node is within the range, that intruder will also receive the notify message from sender. This will help the intruder to understand both the sender's identity and its sending time. This may pose serious threat to the purpose of communication. Moreover a separate packet for the 'notify and go' is an overhead. This will create unnecessary traffic. The protocol also faces problems like long duration for communication, due to random selection of nodes without shortest path considerations. This will lead to the development of an improved protocol which provides all the basic conditions for anonymity along with some better performance parameters.

IV. IMPROVED ANONYMOUS ROUTING PROTOCOL WITH REDUCED OVERHEAD IN MANETS

The proposed anonymous routing protocol is meant for a full secure communication in which only the source and destination would benefit from it. The system assumes multi-hop path from source to destination, in which a number of intermediate nodes are there for the forwarding of messages between them. The degree of anonymity increases only if we have sufficient number of intermediate relay nodes. The protocol eliminates the limitations of the existing system in providing anonymity.

A. Implementation

The protocol concentrates on providing source anonymity, destination anonymity and route anonymity. Assume the network field contains a number of manet nodes. The protocol uses hierarchical zone partition method in the network field similar to the ALERT protocol. The total number of partitions can be calculated by node density (d), number of nodes (n) in destination zone and size of the entire network (N), which can be given by the equation:

$$P = \log \frac{d.N}{n} \qquad (1)$$

The basic communication is between the sender and destination through intermediate relay nodes (RN). Every node's identity is protected by a hash function. So dynamic Pseudo identities are passed throughout the communication. Here the source anonymity is achieved by a new method with the support of beacon service rather than using the 'notify and go' mechanism as in ALERT. After that the message will be forwarded to the intermediate nodes. Here the temporary destination is selected random, but with shortest path considerations. These temporary destinations are called random forwarders (RF). Many of the anonymous routing protocol do not consider the path, and it will increase the time delay. Source selects a node in its zone which is closest to RF to forward data packet through GPSR algorithm.

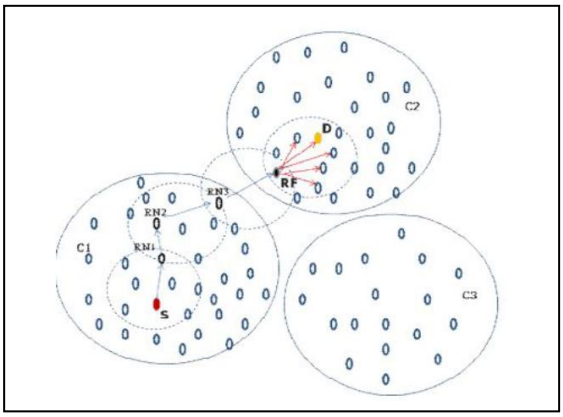

Fig.1. System architecture showing zone partitioning and packet routing

Hierarchical zone partitioning is done as same in ALERT protocol. Here the whole network field is divided into zones, based on equation (1). The condition in zone partitioning is that source/ random forwarders and destination should be in different zones. The improved system uses the advantage of the beacon service for providing source anonymity. In manets, the nodes periodically send beacons. Each beacon transmission identifies the presence of a node. This helps in updating the position information of each node moving across the field. In ALERT protocol, only the original sender is initiating 'notify and go' mechanism. Instead of that here we use Beacon Mode Notification (BMN) mechanism. In this method, every node in the range will periodically send beacon with notification in the payload field indicating the sending time. So here, not only the actual sender, but every node is sending the information, through beacon. So no additional overhead of a separate packet for notification. This will create confusion to intruders if any, that which source is actually sending the original message. During the transmission time, all trusted nodes except trusted nodes except the original source will send the dummy messages and the original source will send the actual message packet along with this. The intruder, if any in this range will only see that everyone is sending notification and message packets and cannot identify which is the original source, since every beacon, it got contain some notification indicates the sending time from different nodes. Thus it provides source anonymity.

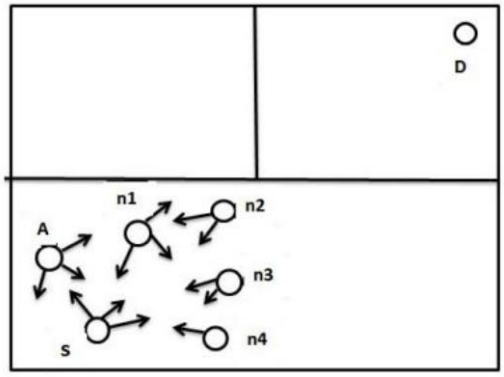

Fig.2. Notification through beacon service

In the figure 2, a number of nodes are present, which periodically send beacons. Suppose S sends a beacon with a notification that it is sending packet at 0.4 ms to A, n1, n2, n3 and n4. So all these nodes will agree to send packet at 0.4 ms. Similarly n2 send BMN to other nodes that it is going to send at the same 0.4 ms. In this way every node will send Beacon Mode Notification (BMN), may be having similar time with others or with different one. Suppose A be an intruder, which gets notification from every nodes and will be in a confusion about the original source.

The protocol also considers the route anonymity. Instead of having a true randomness for the selection of forwarding nodes in the next zone, here it considers directing the packet to the correct destination through shortest yet anonymous path. GPSR forwarding method is used in the protocol. The algorithm consists of two methods for forwarding packets: greedy forwarding, which is used wherever possible, and perimeter forwarding, which is used in the regions greedy forwarding cannot be. Under GPSR, packets are marked by their originator with their destination locations. As a result, a forwarding node can make a locally optimal, greedy choice in choosing a packet's next hop. Specifically, if a node knows its radio neighbor positions, the locally optimal choice of next hop is the neighbor geographically closest to the packet's destination. Forwarding in this regime follows successively closer geographic hops, until the destination is reached.

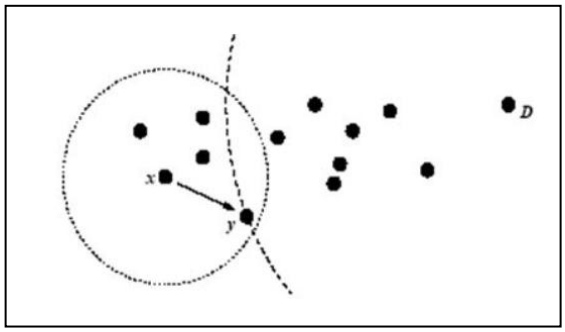

Fig.3. Greedy forwarding: y is x's closest neighbor to D

In ALERT protocol, it finds a node in the next zone, which is called the random forwarder (RF). The node selection is purely random in order to ensure anonymity. But the problem behind this method is that it may cause loop in the network or may be it takes a long route to reach the destination. For a military communication, it is necessary to have faster anonymous communication. So shortest path considerations

have to be taken. In the proposed protocol, it ensures anonymity by combining the random selection technique with shortest path considerations. If a node in a particular zone wants to forward the packet to a node in the next zone, here it first uses the GPSR algorithm to find more than one nodes in the next zone successively running the algorithm and then randomly select any node from these shortest distance nodes from the original destination as the random forwarder.

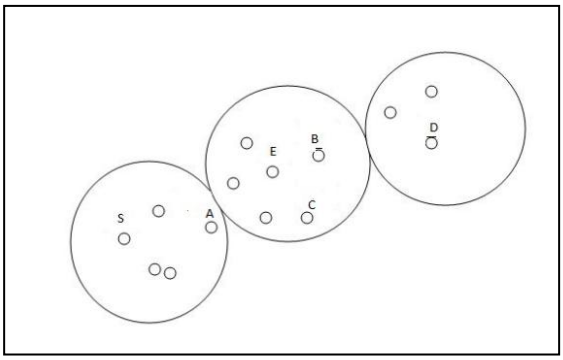

Fig.4. Shortest path random node selection

Consider figure 4, here S wants to send the packet to D through the intermediate nodes. S forwards it to A in the same zone, which is closest to D. Now A wants to select a random forwarder from the next zone. Here it uses GPSR to find a shortest distance node from D. Suppose B is the first shortest node found. Then by keeping aside B, some more nodes closest to D in that zone are found out by the same GPSR algorithm. Say C and E. Now we have B, C and E as the shortest nodes in the path to D. From this node, the protocol randomly selects one node as the random forwarder (RF). This will provide route anonymity in the improved protocol with decrease in communication delay.

Destination anonymity is achieved by the similar method used in ALERT. It provides k-anonymity approach in last zone where destination resides. The random forwarder in the previous zone looks into the last zone, with the knowledge that destination resides in that zone. This means the random forwarder cannot determine the position of destination, only the zone of destination can be determined. The random forwarder broadcasts the packet to k nodes, where k is a predefined integer value. This k node must include the destination. In the last zone, the RF will broadcast the packet to all the nodes in the zone. Here the packet will be received by all nodes but can only open by the intended destination due to the secure key established between the source and destination through the location service.

The whole procedure can be summarized as:
1. Hierarchical zone partitioning of the network field.
2. Transferring of Beacon Mode Notification (BMN) between the nodes.
3. Original source along with others send packets, ensuring the source anonymity.
4. Using GPSR algorithm to find more than 3 nodes in next zone closest to destination.
5. Random selection of one node from these shortest nodes ensures shortest yet anonymous path.
6. Broadcasting to the last zone nodes, which is a predefined number of nodes. This ensures destination anonymity.

V. Results and Discussions

A. Simulation Setup.

The network simulator NS-2.33 was used for simulation. 802.11as the MAC protocol with standard wireless channel and UDP/CBR traffic with maximum packet size 512 bytes. Test field was set to 1000m * 1000m . The simulation sets up 20 nodes for showing the performance of proposed anonymous routing protocol.

B. Results and observations.

Time delay for communication is a major issue in most of the anonymous communication, as its main focus is on anonymity. Here along with full anonymity, protocol also considers the time delay. In protocols, this deals with random selection of nodes for packet forwarding does not consider the shortest one. Merely it finds a random node, and then it forwards the packet towards it. This leads to message looping or it requires long enough time to reach the destination. As the use of anonymous communication is critical and time bound in military environment, this delay may be a problem. In the proposed system, rather than a random forwarder, randomized shortest distance node is considered. Here GPSR shortest routing protocol is used to find k shortest node from the destination, where k is predetermined number more than 1 and then randomly selecting one of the shortest node as forwarder. This will helps in reducing the time delay. The system also shows better performance in case of bandwidth and packet delivery ratio than the existing approaches. Four performance factors of the manet nodes are analyzed. They are packet delivery ratio, overhead, time-delay and the bandwidth. Graphical analysis proves that the method is far better than the existing approach, which does not provide source anonymity.

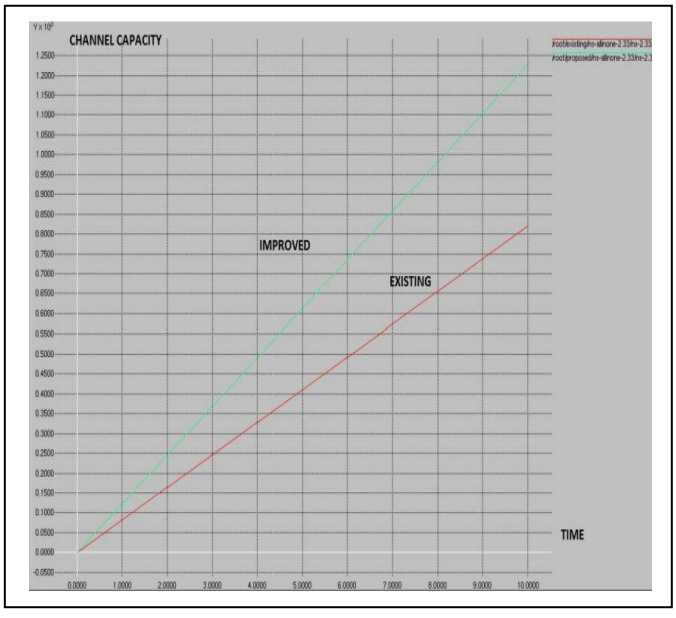

Fig.5. Bandwidth improvement

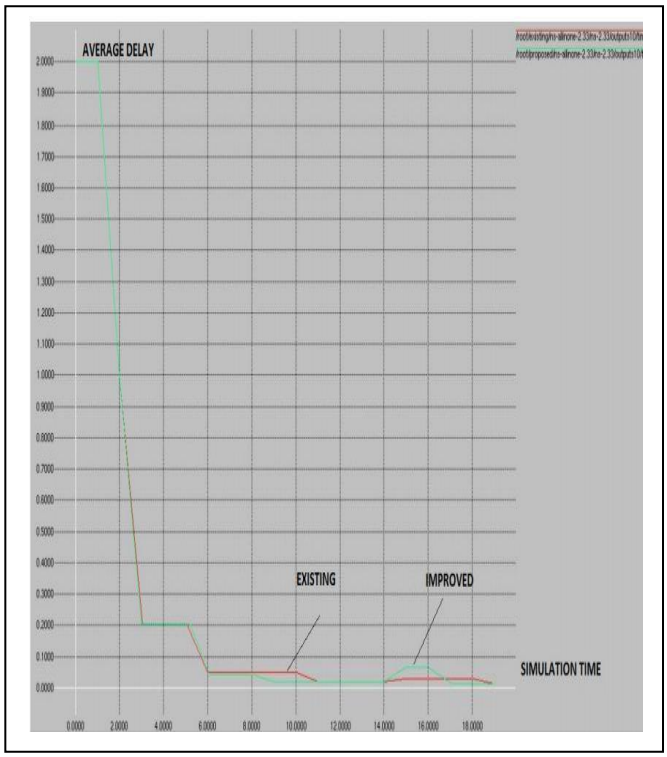

Fig.6. Time delay Comparison

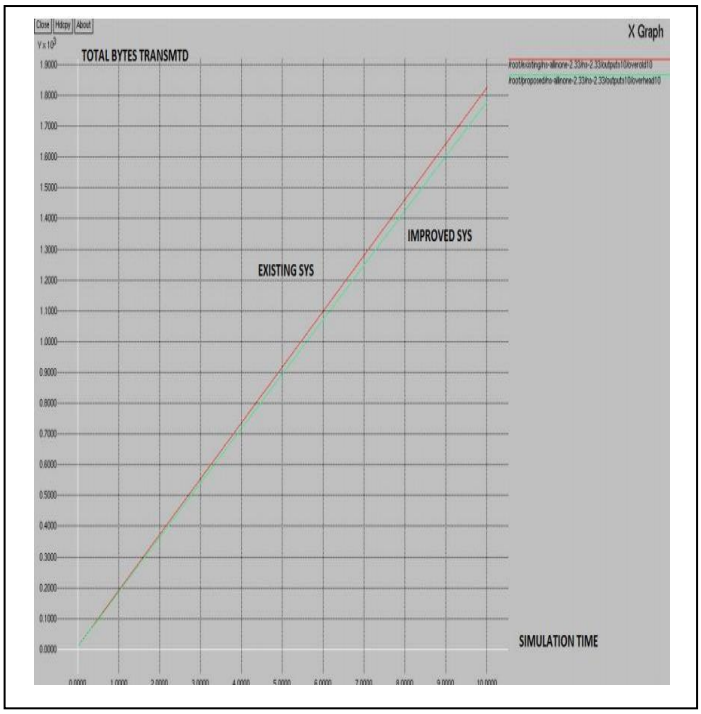

Fig.7. Overhead reduction in proposed system

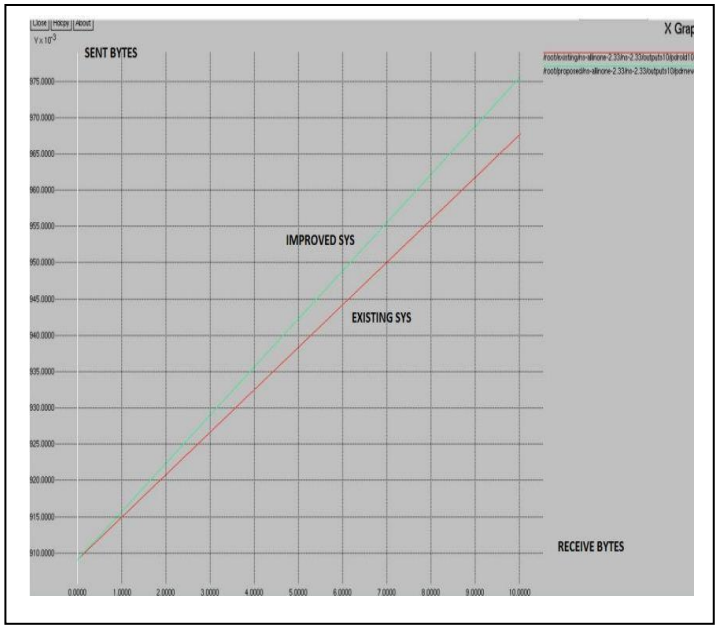

Fig.8. Packet delivery ratio

The graph shows significant changes in the performance between existing and proposed system. The green line shows the improved system and red line shows the existing method. The bandwidth of the proposed system increases as the unnecessary traffic generated by 'notify and go' mechanism has avoided. Overall time delay decreases in the case of improved system, as it takes the shortest path even considering random nodes. Overhead is reduced, which forms an important performance factor in the improved system, due to integrated beacon mode notification system instead of having separate 'notify and go' as in ALERT. The new system almost guarantees better delivery of packets and it is clearly seen in the graph.

VI. Conclusion and Future works

Each protocol has better performance over the other at a particular metric and time. Node locations can be identified through a low cost method and it should be secure enough.

A better anonymous communication is possible if source, destination, route and data packet will be anonymous throughout the network. The proposed method solves the limitations in the existing system and it reduces the overhead and time-delay. The protocol is good for anonymous communication in manet with shortest path considerations. The use of integrated notification with normal beacon service is an important feature of the protocol. Future work lies in reinforcing location based anonymous routing protocol in an attempt to defeat stronger, active attacker.

REFERENCES

[1] X. Hong J. Kong, "Anodr: Anonymous on demand routing with untraceable routes for mobile ad-hoc networks", In ACM MOBIHOC-03, pages 291-302, 2003.

[2] M. S. Kankanhalli F. Bao B. Zhu, Z. Wan and R. H.Deng, " Anonymous Secure Routing in Mobile Ad-Hoc Networks", 29th IEEE International Conference on Local Computer Networks(LC04), pages 102-108, 2004.

[3] L. Xu A. Boukerche, K. El-Khatib and L. Korba, " Sdar: A secure distributed anonymous routing protocol for wireless and mobile ad hoc networks", In 29th IEEE International Conference on Local Computer Networks (LC04), pages 618-624, 2004.

[4] X. Wu, " Ao2p: Ad hoc on-demand position-based private routing protocol", In IEEE Trans. Mobile Computing, vol. 4 no. 4, pp. 335-348, 2005.

[5] H. T. Kung, Brad Karp, "Gpsr: Greedy perimeter stateless routing for wireless networks", In MobiCom ,2000.

[6] K.E. Defrawy and G. Tsudik, "Alarm: Anonymous location- aided routing in suspicious manets", In Proc. IEEE Intl Conf. Network Protocols (ICNP), 2007.

[7] Lianyu Zhao, Haiying Shen, " Alert: An anonymous location-based efficient routing protocol in manets", In IEEE Transactions on mobile computing, vol 6,no.12, 2013

[8] Z. Zhi and Y.K. Choong, " Anonymizing geographic ad hoc routing for preserving location privacy", In Proc. Third Intl Workshop Mobile Distributed Computing (ICDCSW),2005.

[9] D. Yao V. Pathak and L. Iftode, " Securing location aware services over vanet using geographical secure path routing", In Proc. IEEE Intl Conf. Vehicular Electronics and safety (ICVES), 2008

[10] X. Hong X. Wu, J. Liu and E. Bertino, " Anonymous geoforwarding in manets through location cloaking", In International Journal of Innovative Research in Science, Engineering and Technology, 2008

[11] K.E. Defrawy and G. Tsudik, "Prism: Privacyfriendly routing in suspicious manets (and vanets)", In Proc. IEEE Intl Conf. Network Protocols (ICNP), 2008.