An Anonymous Security to Routing Protocol in MANET

[1]Pallavi M. Kulkarni, [2]Mr. S. A. Hashmi

[1]M.E. Student, [2]Assistant Professor & Head
Department of Information Technology,
MGM College of Engineering, Nanded, Maharashtra,

***Abstract*: The nodes of a Mobile Ad Hoc Network cannot be trusted for the correct execution of critical network functions and therefore security in MANETs is an essential component for maintaining data secrecy. MANETs do not have perfect security policy, but it is important to establish secure communication between parties in MANETs. So it is necessary to provide anonymities in networks. Previous anonymous routing protocols are unable to provide complete source, destination and route anonymities. Mobile Ad-hoc Network is the branch of Ad-hoc Networks that deals with communication among the Mobile nodes. In Mobile Ad-Hoc Network (MANET) , anonymous routing protocols used for security purpose. These protocols hide node's original identity from outsider, so that observer cannot threaten the security of network. There are few existing anonymous routing protocols available for MANET. From these anonymous routing protocols, some are relying on hop-by-hop encryption or redundant traffic, but having high cost and provide low anonymity. Therefore to provide high anonymity protection with low cost, we propose an Anonymous Location Based Efficient Routing Protocol. In this protocol entire network area is dynamically partitioned into different zones. Every zone includes nodes which act as intermediate nodes. These nodes get randomly selected for routing so that observer cannot indentify route. Source and destination identity is hiden using pseudonym which changes frequently.**

***Index Terms*: Mobile ad hoc network, anonymity, routing protocol, geographical routing**

I. INTRODUCTION

MANET It is an ad hoc wireless network that can change locations and configure itself. The topology of MANET changes constantly due to the mobility of nodes. Because of that mobility, nodes can move out of coverage range of each other, so that some links break while new links between nodes are created. Devices can move independently in any direction and therefore can change their links to other devices frequently.

MANET (mobile ad hoc networks) uses anonymous routing protocols that hide the node's identities and routes from outside observers to provide anonymity protection. ALERT offers anonymity protection to source, route, and destination. "Identity and Location anonymity of sources and destinations" means it is hard to obtain the real identities and exact locations of the sources and destinations. For route anonymity, either en route or out of route an adversary cannot trace a packet flow, or no node has information about the real identities and locations of intermediate nodes. This work includes:

i. *Anonymous routing:* ALERT provides route anonymity, identity, and location of source and destination.
ii. *Low Cost:* Rather than using hop-by-hop encryption and redundant traffic, ALERT mainly uses randomized routing of one message copy to provide anonymity protection.
iii. *Resilience to Intersection attacks and Timing attacks:* ALERT has an ability to counter intersection attacks. ALERT can also avoid timing attacks because of its non- fixed routing paths for a source and destination pair.
iv. *Extensive simulation:* To evaluate ALERT's performance in comparison with other anonymous routing protocols.

II. RELATED WORK

Existing anonymity routing protocols in MANETs may be principally classified into two categories: hop-by-hop cryptography [4] and redundant traffic [5],[6],[9]. Most of the present schemes are limited by specializing in imposing anonymity at a significant cost to precious resources as a result of public key-based cryptography and generate considerably high traffic cost.

1. In GSPR [4] packets in all time follow the minimum hop count paths so it does not provide route anonymity. In a long term communication the route can be determined by malicious node.

2. In the AO2P [5] geographic routing algorithm, pseudonyms are used to protect nodes' real identities, and a node chooses the neighbor that can reduce the greatest distance from the destination. So AO2P cannot offer anonymity protection to route.

3. In ALARM [9] offers source identity and location anonymity, destination identity anonymity. In ALARM using map construction malicious nodes can get destination node locations so it cannot provide destination location anonymity. ALARM does not provide the route anonymity.

4. Anonymous Location-based Efficient Routing protocol (ALERT) [10] to offer high anonymity protection at a low cost. It is not complete bulletproof to all attack.

III. ANONYMOUS LOCATION BASED EFFICIENT ROUTING PROTOCOL IN MANET

Pseudonym and Location services

Pseudonym is another name or identity given to node. In ALERT, pseudonym used as node identifier with replacement of its real MAC address. Node's MAC address can be used to trace nodes existence in the network. Therefore replacing MAC address with pseudonym is the main advantage of ALERT protocol. This pseudonym is the combination of MAC address and Current time stamp. But if this information is known by attacker then it can easily find out the node. Therefore, to prevent this problem, time stamp can be randomly selected. This pseudonym should not permanent; it should expire after a certain time period so that attacker cannot identify the pseudonym of nodes. Considering the network delay, the attacker needs to compute, e.g., 10^5, times for one packet per node. And this should be applied for number of nodes in network, so the computing overhead is not acceptable by an attacker, and the success rate is low from attacker side. There is one problem with this pseudonym and it is that if pseudonym is changed frequently then routing becomes uneasy. To make it more difficult for an attacker to compute the timestamp, we can increase the computation complexity by using randomization for the time stamps. Specifically, we keep the time stamp in a certain range of values, say 1 second, and randomize the digits within 1/10th. So, the pseudonyms cannot be easily reproduced. A node's pseudonym expires after a specific time period in order to prevent adversaries from associating the pseudonyms with nodes. If pseudonyms are changed too frequently, the routing may get disturbed and if pseudonyms are changed too infrequently, then the adversaries can identify pseudonyms of nodes. Therefore this pseudonym change frequently should be properly determined. To avoid pseudonym collision, we use a collision resistant hash function, such as SHA-1, to hash a node's MAC address and current time stamp. Each node updates its position and pseudonym to "hello" messages, and sends the messages to its neighbors periodically. Also, every node maintains a routing table that keeps its neighbor's pseudonyms with their locations.

Components and phases of ALERT

Now to understand the ALERT routing algorithm we should study the following components.

i. *Temporary Destination (TD):* A node that randomly chooses from other zone is called as Temporary destination.

ii. *Random Forwarder (RF):* This is a node that randomly chooses closest to the temporary destination is called as Random Forwarder.

iii. *Relay Node (RN):* Relay nodes are the nodes which are participate in information routing.

iv. *Destination Zone (Z_D):* It is last zone after the partition in which destination node is present is called as destination zone.

Phases of ALERT are as follows:

i. Hierarchical Zone Partition

ii. Selection of Random Forwarders

iii. Selection of relay nodes

iv. Route Formation

v. Broadcasting

IV. ALERT ALGORITHM

Hierarchical Zone Partitioning

Hierarchical means the total network area gets partitioned in zones but in alternative manner. Zone partitioning continuously splits the smallest zones in an alternating manner. And this process is called as hierarchical zone partitioning.

We assume the entire network area is generally a rectangle, in which nodes are randomly spread over this rectangular area. 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 position of nodes in the entire area for zone partitions in ALERT.

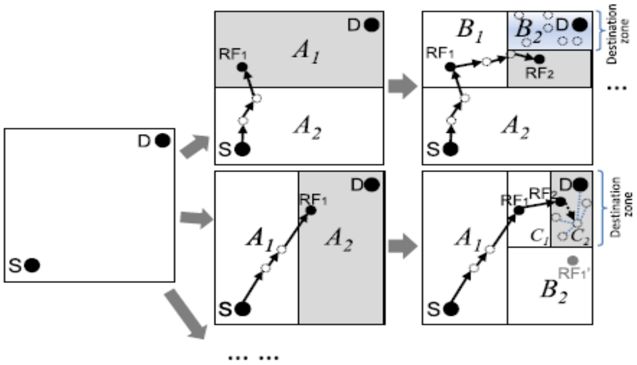

Fig. 1 Example of different zone partition

As shown in the figure 1, part1, we horizontally partition into zones that is A1 and A2. We then vertically partition zone A1 into B1 and B2. After that we horizontally partition zone B2 into two zones. This is related to as hierarchical zone partitioning. Now in lower part of this figure shows another routing path based on different partition pattern. After source vertically partitions the whole area to separate itself from destination zone, it randomly chooses temporary destination 1 (TD1) and sends packet to random forwarder 1 (RF1). RF1 partitions zone A1 into B1 and B2 horizontally and then partitions B1 into C1 and C2 vertically. So itself and destination zone are separated.

Note that RF1 could vertically partition A2 to separate itself from destination zone in two zones but may choose a TD further away from the destination than the TD that resulted from the horizontal partition. Therefore, ALERT sets the partition in the alternative horizontal and vertical manner in order to ensure that a packet approaches D in each step. We assume that destination node will not move away from its position during data transmission, so it can successfully receive the data. But small problem is that number of hierarchies generates more routing hops. Because of increase in number of hops , increases anonymity and delay also.

To ensure the delivery of packets, the destination sends a confirmation to the source upon receiving the packets. And if the source has not received the confirmation during a predefined time period, it will resend the packets.

Formula for Partition

To partition the entire network in different zones we have one formula which is explained below. H denotes the total number of partitions in order to produce Z_D. Using the number of nodes in destination zone Z_D (i.e., k), and node densityρ, H is calculated by,

$$H = log_2(\frac{\rho * G}{k})$$

H: Total no. of partitions

ρ: Node Density

G: Size of entire network area

k: No. of nodes in destination zone

By using values of these parameters, we can calculate total number of zones. We should calculate the position of destination zone Z_D also. Size of destination zone: $\frac{G}{2^H}$

Example of Alert Routing Algorithm

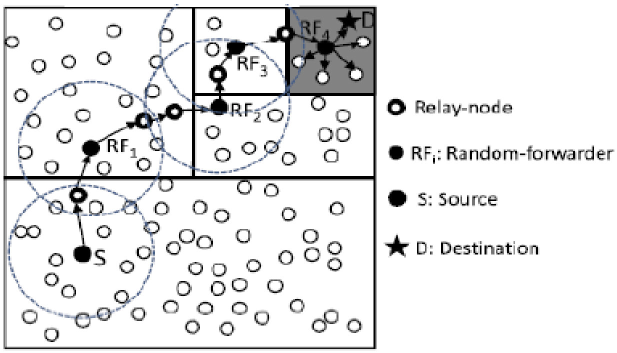

Fig. 2 Routing among zones in ALERT

Figure 4.2 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 figure is the destination zone. It first checks whether itself and destination are in the same zone. If so, it divides the zone alternatively in the horizontal and vertical directions. The node repeats this process until itself and destination are not in the same zone. It then randomly chooses a position. Routing among zones in ALERT zone is called temporary destination (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 (RF).
Thus, in the last step, the data is broadcasted to k nodes in Z_D, providing k-anonymity to the destination.

Source Anonymity

In ALERT, By hiding the nodes view of source node and forwarded node, ALERT can give source anonymity. And this makes it difficult for an attacker to identify whether the node is source node or forwarding node. To strengthen the anonymity protection of the source nodes, author proposes lightweight mechanism, “Notify and Go”.
In first phase “Notify” phase, source attach its data transmission notification with periodical update packets to notify its neighbors that it will send out a packet. The packet includes two back off time periods “t” and “t_0”.
Now in second phase “Go” phase, source and its neighbors wait for certain period of time that is randomly chosen before sends out messages. Example, t,(t+t_0), (t+t+t_0),…
Source’s neighbors generate only several bytes of random data just to cover the traffic of the source. “t” should be a small value that does not affect the transmission latency. Latency is the average time taken by a data packet to arrive in the destination. Now “t_0”, long “t_0” may lead to long transmission delay while short “t_0” may result in interference due to many packets being sent out simultaneously. Thus, “t_0” should be long enough to minimize interference and balance out delay between source and source’s nearest neighbor to prevent any intruder from understand the source.

Route Anonymity

ALERT can give route anonymity and this is the specialty of ALERT protocol.ALERT features a dynamic and unpredictable routing path, which consist of a number of dynamically determined intermediate relay nodes. The resultant different routes for transmission between a given source and destination pair make it difficult for an attacker to observe a statistical pattern of transmission. This is because the RF sets changes due to the random selection of RF during the transmission of each packet.
in ALERT, the routes between two communicating nodes are constantly changing, so it is difficult for attackers to predict the route of the next packet for packet interception.
Attacker can identify the packets transmitted between source and destination through packet departure and arrival times, from it can detect source and destination. For example, two nodes communicate with each other A and B at an interval time of 5 seconds. After long observation time, the attacker finds A’s packet sending time and B’s packet receiving time have a fixed 5 seconds difference. Then attacker would suppose that A and B are communicating with each other. The routing path between given source-destination pair and the communication delay changes constantly, which again keep away an attacker from identifying the source and destination.

Destination Anonymity

Attacker can identify destination from repeated observations of node movements and communication, destination always stays in destination zone during a transmission session.
This is because, destination is conducting communication for long time, the attacker can monitor the change of the members in the destination zone containing destination. As time elapsed, node and all other members may move out of the destination zone except destination. As a result destination is identified as destination because it always appears in the destination zone.

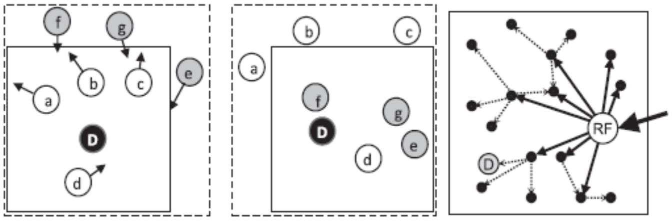

Fig 3 .Destination Anonymity

Figure 4.5 shows the status of destination zone after a packet is broadcasted to the zone. The arrow shows the moving directions of nodes. We can see that nodes a, b, c, d and D are in same destination zone. The second block of figure shows the status of the zone next time a packet is transmitted between same source and destination pair. This time nodes d, e, f, g and D are in destination zone. Since, the intersection of both zones, nodes in both figure include d and D.
So, the destination D can be identified by attacker. Therefore, attacker watches longer time the process the easier it is to identify the destination node.

Packets are delivered to destination zone constantly in long-duration sessions rather than using direct local broadcasting in the zone, the last RF multicasts packets pkt1 to a partial set of nodes say m nodes out of the k nodes in the zone. The m nodes hold the packets pkt1 until the arrival of the next packet pkt2. Upon the arrival of the next packet, m nodes conduct one hop broadcasting to enable other nodes in the zones to also receive the packet in order to hide the destination.
Now the 3rd block of figure shows two step processes 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 delivery of packet 1 and packet 2 are mixed. So, the attackers suppose that D is not in the recipient set of pkt1, though D receives pkt1 in the delivery time of pkt2. Therefore, the attacker would think that D is not recipient of every packet in Z_D in transmission session. And in this way we can protect the destination from an attacker.

V. Performance Evaluation

The default simulation parameters are presented in Table 1. The tests were carried out on NS-2.29 simulator using 802.11 with a standard wireless transmission range of 250 m and UDP/CBR traffic with a packet size of 512 bytes. The test field in our experiment was set to a 1,000 m *1,000 m area with 200 nodes moving at a speed of 2 m/s. The density was set to 50, 100, 150, and 200 nodes per square meters. The duration of each simulation was set to 100 s unless otherwise indicated. The final results are the average of results of 30 runs.
In the ALERT protocol, we evaluate the performance under the following metrics

i. Number of actual participating nodes.

ii. Number of Random Forwarders.

iii. Number of remaining nodes in a destination zone.

iv. Number of hops per packet.

v. Latency per packet.

vi. Delivery rate

(i) Number of actual participating nodes: These nodes include RFs and relay nodes that actually participate in routing. This metric demonstrates the ability of ALERT's randomized routing to avoid routing pattern detection.

(ii) Number of Random Forwarders: This is the number of actual RFs in a S-D routing path. It shows routing anonymity and efficiency.

(iii) Number of remaining nodes in a destination zone: This is the number of original nodes remaining in a destination zone after a time period. A larger number provides higher anonymity protection to a destination and to counter the intersection attack. We measure this metric over time to show effectiveness on the destination anonymity protection.

(iv) Number of hops per packet: This is measured as the accumulated routing hop counts divided by the number of packets sent, which shows the efficiency of routing algorithms.

(v) Latency per packet: This is the average time elapsed after a packet is sent and before it is received. It includes the time cost for routing and cryptography. This metric reflects the latency and efficiency of routing algorithms.

(vi) Delivery rate: This is measured by the fraction of packets that are successfully delivered to a destination. It shows the robustness of routing algorithms to adapt to mobile network environment.

VI. Simulation Analysis

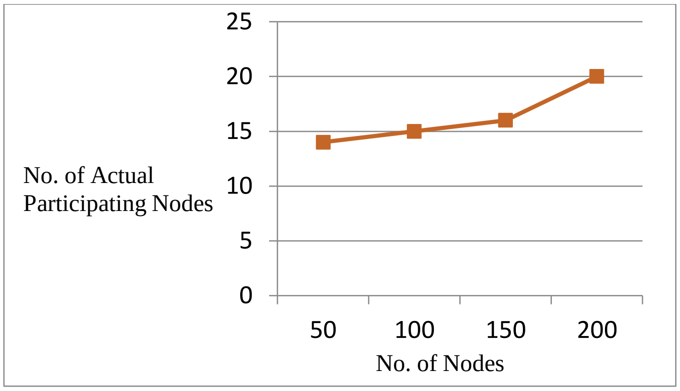

Figure.4 Comparison of Actual participating nodes With Number of nodes

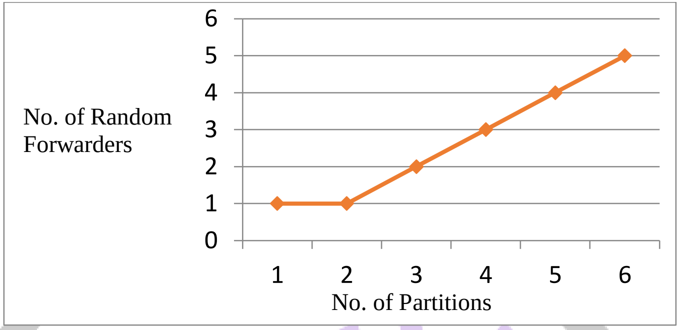

Figure 5 Comparison of Number of partitions With Number of Random forwarders

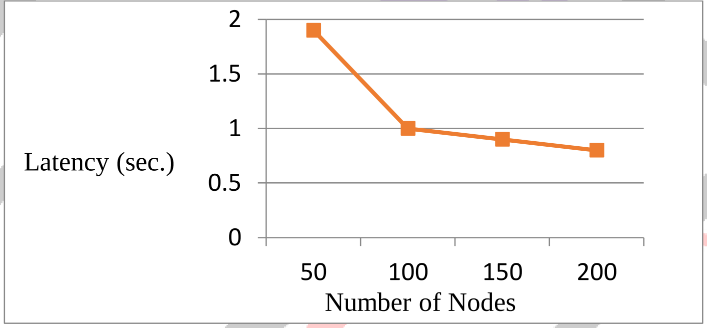

Figure 6 Comparison of Latency with Number of nodes

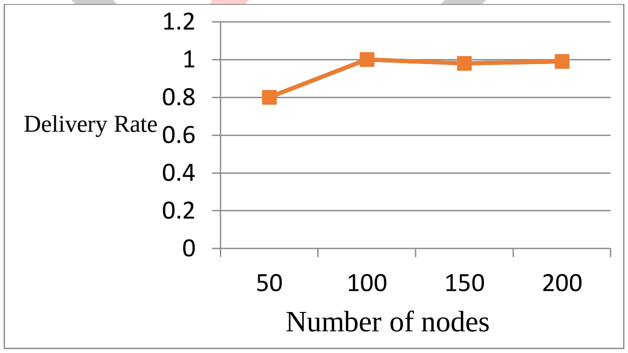

Figure 7 Comparison of Number of Nodes with Delivery rate

VII. Conclusion

ALERT uses dynamic hierarchical zone partitions and random relay node selections. ALERT is protocol which provide better anonymity to source, route as well as route.

Experiment results show that ALERT can offer high anonymity protection at low cost when compared to other anonymity algorithms. In ALERT, the Random Forwarder (RF) node is selected randomly without considering the capacity (Energy level and memory capacity). So there may be a chance of node failure during the transmission. To avoid that, in our work the capacity of the node should be considered while selecting the random forwarder node. To increase the route efficiency, the Random forwarder will be selected by considering the parameter Transmission capability (Power level). Future work relies on choosing a deputy RF node having the second energy value when the RF becomes dead due to the attack from a hacker.

REFERENCES

[1] L. Zhao and H. Shen, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs," IEEE transactions on mobile computing, Vol.12, No.6, June 2013.
[2] K.E. Defrawy and G. Tsudik, "ALARM: Anonymous Location- Aided Routing in Suspicious MANETs," Proc. IEEE Int'l Conf. Network Protocols (ICNP), 2007.
[3] 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.
[4] J. Kong, X. Hong, and M. Gerla, "ANODR: Anonymous on Demand Routing Protocol with Untraceable Routes for Mobile Ad-Hoc Networks," Proc. ACM MobiHoc, pp. 291-302, 2003.
[5]Y. Zhang, W. Liu, and W. Luo, "Anonymous Communications in Mobile Ad Hoc Networks," Proc. IEEE INFOCOM, 2005.
[6] X. Wu, "AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol," IEEE Trans. Mobile Computing, vol. 4, no. 4, pp. 335-348, July/Aug. 2005.
[7] 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.
[8] 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.
[9]"TheNetworkSimulator-ns-2,http://www.isi.edu/nsnam/ns, 2012.
[10] K. El-Khatib, L. Korba, R. Song, and G. Yee, "Anonymous Secure Routing in Mobile Ad-Hoc Networks," Proc. Int'l Conf. Parallel Processing Workshops (ICPPW), 2003.
[11] I. Aad, C. Castelluccia, and J. Hubaux, "Packet Coding for Strong Anonymity in Ad Hoc Networks," Proc. Securecomm and Workshops, 2006.
[12] 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.
[13] 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.
[14] M. Priya and S. Vasantmohan, " Zone Partition Based Routing Protocol in MANETs", International Journal of Innovative Research in Science, Engineering and Technology Volume 3, Special Issue 3, March 2014
[15] Namrata R. Borkar and Avinash P. Wadhe, " Implementation of an Anonymous Location based Eifficient Routing Protocol in Mobile Adhoc Networks", Volume 3, Issue 5, May 2015 International Journal of Advance Research in Computer Science and Management Studies