A Security System for MANETs Using ALERT Protocol

[1]Shruthi M., [2]Ramamurthy K.N.,
[1]PG Student, [2]PG Student
[1]Department of Electronics and Communication,
[1]Vivekananda Institute of Technology, Bangalore, India

***Abstract* - Mobile Ad-hoc Network is the collection of the mobile users that communicate over the various bandwidths of the constrained wireless links. To offer high anonymity protection at a low cost, we propose an Anonymous Location-based Efficient Routing proTocol (ALERT). ALERT dynamically partitions the network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which forms a nontraceable anonymous route. In addition, Experimental results which exhibits the analysis and in future the attacker in whole network topology is find out by using an algorithms and the scheme which makes more secure the whole network topology.**

***Index Terms* – Mobile Ad-hoc Networks, Anonymity, Routing protocols.**

I. INTRODUCTION

The communication over packets between source and destination in an environment associated with MANETs as shown in Figure 1. The mobile nodes which spread in the entire network and the router are used in order to transmit the packet from source to a destination and randomly that will be changing with period of time. The packet is established between source and destination through the transmission range.

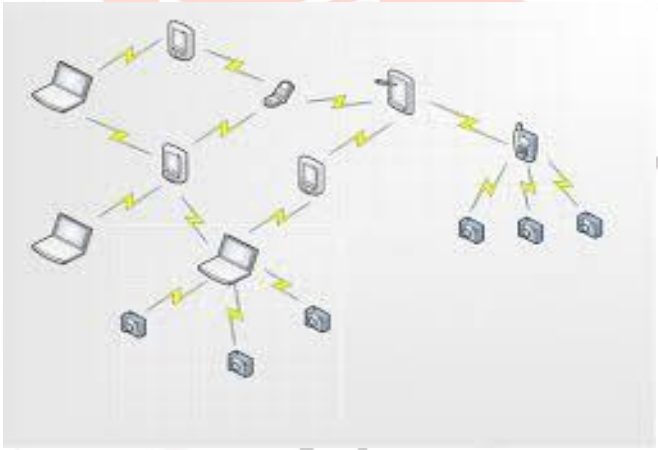


Fig 1: Mobile Ad-hoc Network

The area of the mobile users that is communicating over the source and destination of the individual mobile users and Mobile Ad-hoc Network also be used in the commercial sectors by providing the information about the rescue operations such as fire and flood in the case of local level they can be used to share the information among the participants such as classroom and conferences and in the personal area network they can be used to intercommunication between the various mobile nodes such as electronic devices they are laptop , computers and the phone etc. So that it can also be used in the various communication channels to share the information among each other.

For anonymity point of view that includes the path which cannot trace a packet to transmission between their sources and destinations and the locations and associated path that will used for transmission. Also the relationship between the sources and destinations which is the relationship of an unobservability and to ensure that the nodes and routes are does not know where the endpoints lies in an MANETs because it won't be having any fixed arrangement of nodes because mobile nodes will be moving from one place to another since the environment is an mobile ad-hoc network and where the location devices are connected together.

The anonymous routing protocols which the mobile ad-hoc network by setting the design and analysis for an security purpose by using the protocol that securely disseminate construct topology with the information. It uses advance crypto graphical such as group signatures, existing anonymous routing protocols includes that comes when the MANET settings by designing the protocols which provides security for authentication and integrity and also provides protection for passive and active attack.

ALARM featuring including of a location, identity and nontraceability such as tracking resistance . The other routing protocols are Anonymous Secure Routing (ASR) which provides the property of anonymity which includes the privacy and position of a routing protocol and also it has route anonymity problem.

For route anonymity, adversaries, either en route or out of the route, cannot trace a packet flow back to its source or destination, and no node has information about the real identities and locations of intermediate nodes en route. Also, in order to dissociate the relationship between source and destination i.e., relationship unobservability , it is important to form an anonymous path between the two endpoints and ensure that nodes en route do not know where the endpoints are, especially in MANETs where location devices may be equipped.

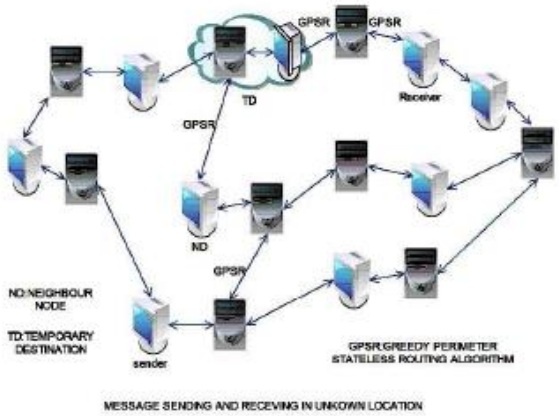


Fig 2: System Architecture

The system architecture which consists of geographic routing protocol for example Greedy Perimeter Stateless Routing (GPSR) that greedily forwards a packet to the node closest to the destination and the protocol's strict relay node selection makes it easy to reveal source and destination and to analyze traffic. Greedy Perimeter Stateless Routing is a responsive and efficient routing protocol for mobile and wireless networks. it uses shortest path to find routes an makes position of nodes to make packet forwarding decisions and it use to recover by forwarding in perimeter mode.

II. LITERATURE SURVEY

L.Zhao and H. Shen *An Anonymous Location-Based Efficient Routing Protocol in MANETs* [3] proposed that Greedy Perimeter Stateless Routing, GPSR, is a responsive and efficient routing protocol for mobile, wireless networks. Unlike established routing algorithms before it, which use graph-theoretic notions of shortest paths and transitive reachability to find routes, GPSR exploits the correspondence between geographic position and connectivity in a wireless network, by using the positions of nodes to make packet forwarding decisions. GPSR uses greedy forwarding to forward packets to nodes that are always progressively closer to the destination. In regions of the network where such a greedy path does not exist (i.e., the only path requires that one move temporarily farther away from the destination), GPSR recovers by forwarding in perimeter mode, in which a packet traverses successively closer faces of a planar sub graph of the full radio network connectivity graph, until reaching a node closer to the destination, where greedy forwarding resumes. GPSR will allow the building of networks that cannot scale using prior routing algorithms for wired and wireless networks. Such classes of networks include:

We are extending GPSR:

- **Geographic provisioning:** We use geographic forwarding via a waypoint not on the path found by GPSR to distribute load on the network. This approach is promising because on a wireless network, position and capacity are correlated; distributing load geographically leverages spatial reuse, and cuts the average load in regions where traffic is concentrated.
- **Obstacles:** We are investigating GPSR's behavior in the presence of obstacles to radio propagation, which introduce the risk that the planar subgraph used by GPSR's perimeter mode may not be connected. We are investigating both deterministic and randomized algorithms for recovering from such disconnections when they occur. We plan to build novel wireless network systems in the above categories that use GPSR.

A.Pfitzmann et.al.,[1] proposed that due to a less dynamic and behaviors in the radio transmission of the system it will communicates this difficult analysis when congestion happens hence after analyzing attacker which determines the nodes which conducting an attack against which is known as target-orientation attacks. This analysis have been used in the method through which the attack that are known as difficult and includes the protocols order to provide an security through the routing protocols hence the information of routing is very informative to the data in a network topology .Therefore, proposed an protocol that keeps nodes and don't know where the end points are lies in the entire area. Hence analysis shows for both routes and nodes in the target orientation attacks.

Sk.Md.M.Rahman et.al.,[2] proposed that location privacy which an network and that depends on routing hence presence which makes servers concern about the location privacy and which is upon ideas proposed protocol provides anonymity as well as efficiency of an topology. Broadcast nature in the radio transmissions, which provides communication in which proposed a nature in the traffic analysis .The new cryptographical concept which is called as an pairing hence proposed as an anonymous authentication protocol which allows an node to authenticate each other nodes without their identities. Hence the secret key which is established between the neighborhood authentication process, and the routing and packet forwarding tasks which disclosing the identities of the topology, which provides information about the sender and the receiver anonymity, with the information between the sources and destinations.

III. PROPOSED SYSTEM

The ALERT Routing Algorithm

1. Routing in ALERT

Given an area, we horizontally partition it into two zones A1 and A2 and again vertically partitioned zone A1 to B1 and B2 . After that, it horizontally partition zone B2 into two zones. Such zone partitioning consecutively splits the smallest zone in horizontal and vertical manner hence this partitioned process called as a hierarchical zone partition. ALERT uses the hierarchical zone partition and randomly chooses a node in the partitioned zone in each step as an intermediate relay node (i.e., data forwarder), thus dynamically generating an unpredictable routing path for a message.

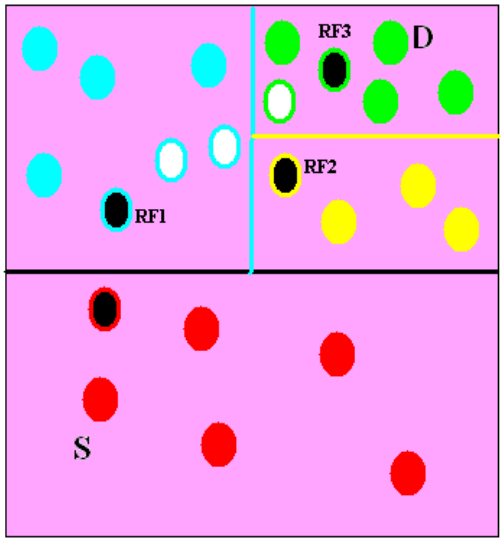


Fig 3: Routing among zones

2. Zone Partitioning

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

In the upper routing flow the data source S first horizontally divides the area into two equal-size zones, A1 and A2 , and in order to separate source and zone destination. Source then randomly selects the first temporary destination T D1 in zone A1 where ZD resides. Then, Source which relies on GPSR to send packet to TD1 . The packet is forwarded by several relays until reaching a node that cannot find a neighbor closer to T D1 . This node is considered to be the first random-forwarder RF 1.After RF 1 receives packet, it vertically divides the region A1 into regions B1 and B2 so that ZD and itself are separated in two different zones. Then, RF 1 randomly selects the next temporary destination T D2 and uses GPSR to send packet to TD2.This process is repeated until a packet receiver finds itself residing in ZD , i.e., a partitioned zone is ZD having k nodes. Then, the nodes that broadcasts the packet to the k nodes .

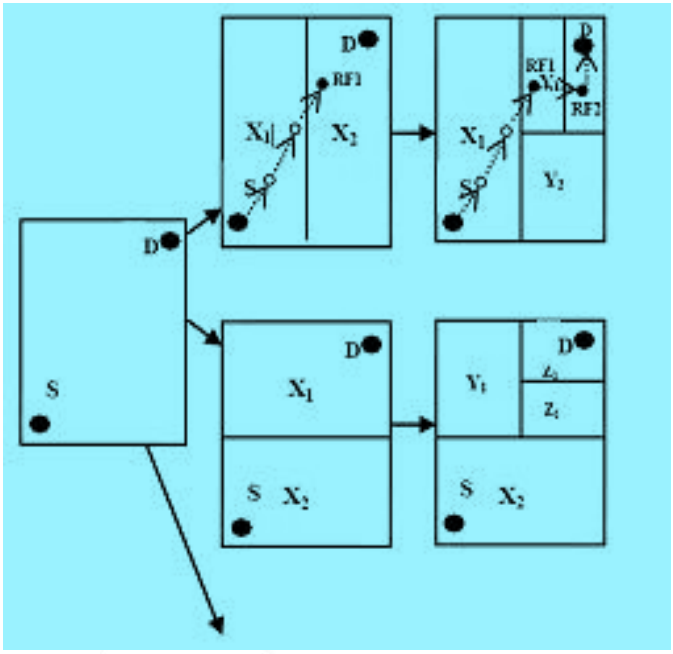


Fig 4: Examples of different zone partitions

The another routing path based on a different partition pattern. After S vertically partitions the whole area to separate itself from ZD , it randomly chooses TD1 and sends pkt to RF 1 . RF 1 partitions zone A2 into B1 and B2 horizontally and then partitions B1 into C1 and C2 vertically, so that itself and ZD are separated. Note that RF 1 could vertically partition A2 to separate itself from ZD in two zones but may choose a TD further away from the destination than the TD that resulted from the horizontal partition.

3. Structure of Packet in an ALERT

For communication between source and destination, source and each packet forwarder embeds the following information into the transmitted packet.

- The zone position of zone destination , i.e., the Hth partitioned zone.
- The encrypted zone position of the Hth partitioned zone of S using's public key, which is the destination for data response.
- The current randomly selected TD for routing.
- A bit (i.e., 0/1), which is flipped by each RF, indicating the partition direction (horizontal or vertical) of the RF.

With the encrypted Hth partitioned zone in the information of an attacker needs very high computation power to be able to launch attacks such as dictionary attack to decrypt it in order to discover the source S of a session with a specific destination D. The Hth partitioned zone is the position of a zone rather than a position, which makes it even harder to locate the source S.

RREQ/RREP/NAK		P_S	P_D	L_{Z_S}	L_{Z_D}	L_{RF}
h	H	K^S_{pub}	$(TTL)_{K^{KI}_{pub}}$	$(Bitmap)_{K^D_{pub}}$		data (NULL in NAK)

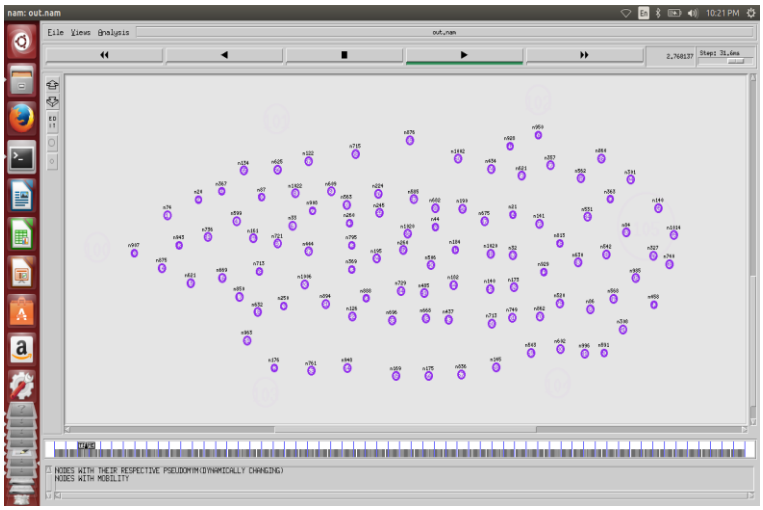
Fig 4: Structure of Packet in an ALERT

Figure shows the Structure of Packet in an ALERT, which omits the MAC header. Because of the randomized routing nature in ALERT, we have a universal format for RREQ/RREP/NAK. A node use NAK to acknowledge the loss of packets. The data field of RREQ/RREP is left blank in NAK packets.

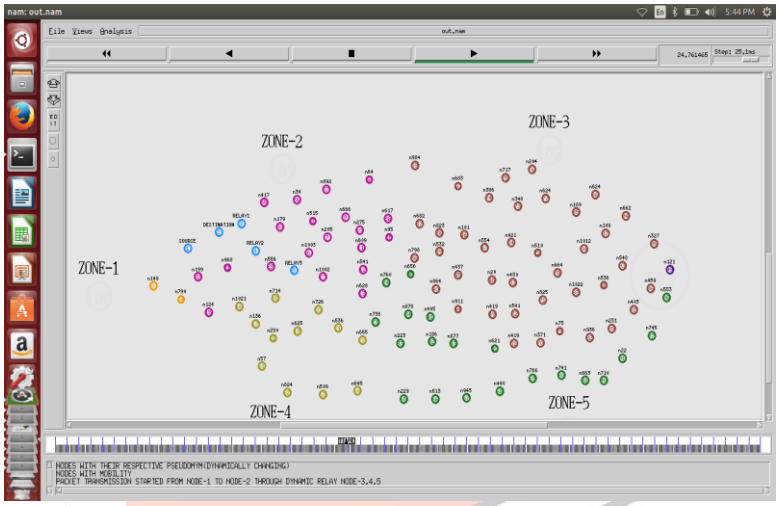
Flooding based anonymity routing which usually uses ACK's, while NAKs are often adopted in geographic routing based approaches to reduce traffic cost. For the same purpose, we choose to use NAKs. In the packet, Ps is the Pseudonym of a source, Pd is the Pseudonym of the destination , h is the number of divisions, H is the maximum allowed number of divisions and Bitmap is used for solving intersection attacks when node A wants to know the location and public key of another node B, it will contact its location server thus there is no need to exchange shared keys between nodes.

IV. SIMULATION RESULTS

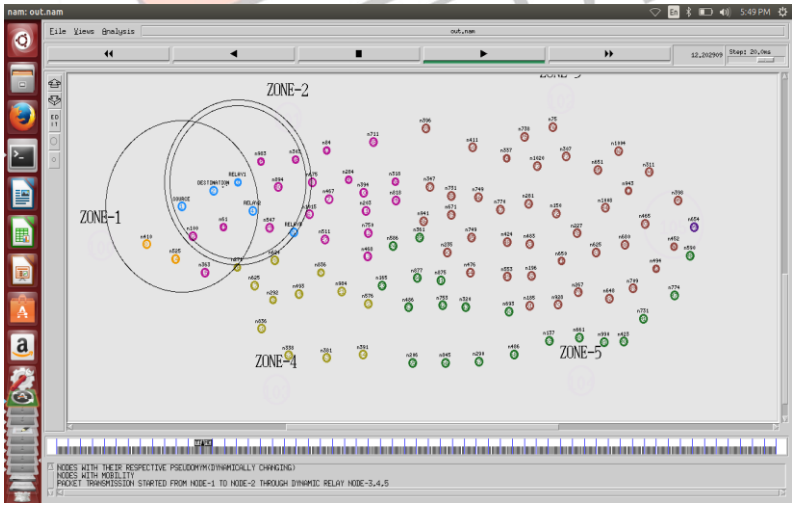
1) Screenshot showing the pseudonyms associated for each node in order to provide security.



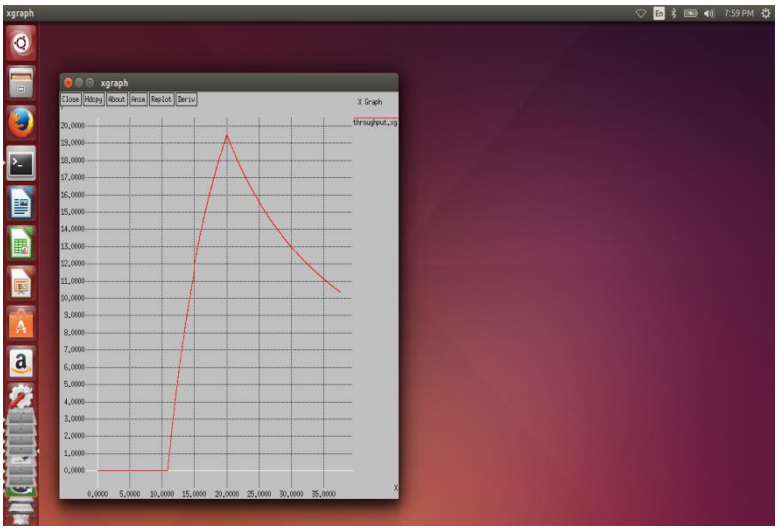
2) Screenshot showing the area is partitioning into five zones in order to provide security.



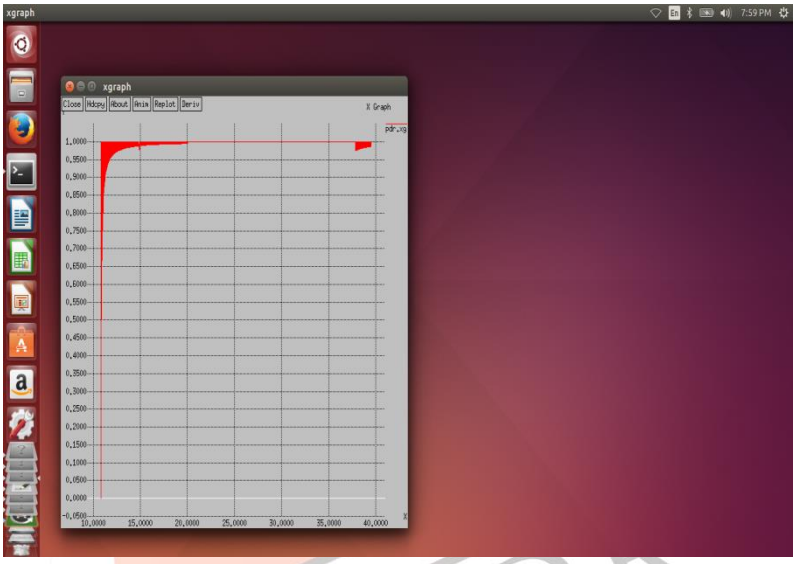
3) Screenshot showing that the packets are transmitting between source and destination through intermediate nodes.



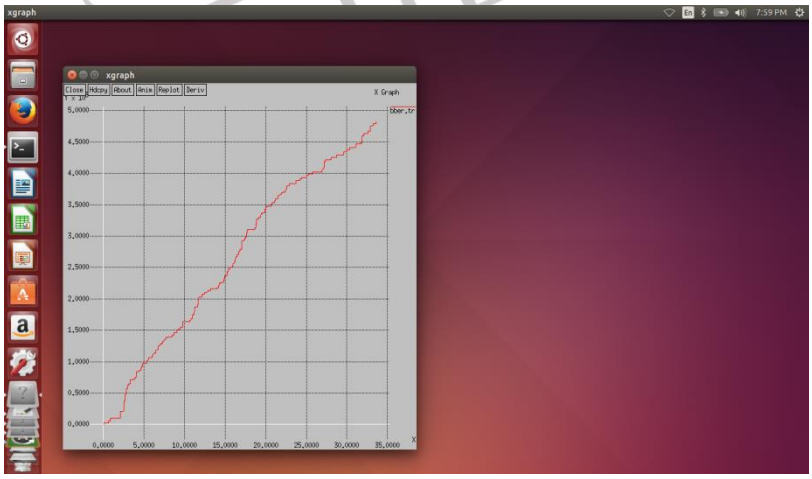
4) Throughput : The average number of packets successfully delivered per unit time.



5) Packet Delivery Ratio: The ratio of data packets received by the destination to those are generated by the source .



6) Control Overhead: The number of packets generated by routing protocol during simulation. The generation of overhead will decrease the protocol performance.



V.CONCLUSION

In this project, proposed ALERT is distinguished by its low cost and anonymity protection for sources, destinations and routes. It uses dynamic hierarchical zone partitions and random relay node selections to make it difficult for an intruder to detect the two endpoints and nodes en route. In the future work, To examine the performance of more comprehensive solutions by using to

provide high anonymity protection it dynamically partitions a network field into many zones and randomly chooses nodes in zones as intermediate relay nodes.

VI.REFERENCES

[1] A. Pfitzmann, M. Hansen, T. Dresden, and U. Kiel,"Anonymity, Unlinkability, Unobservability, Pseudon-ymity, and Identity Management a Consolidated Proposal for Terminology, Version 0.31,"technical report, 2005 .

[2] 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.

[3] L.Zhao and H. Shen,"ALERT: An Anonymous Location- Based Efficient Routing Protocol in MANETs," *Proc. Int'l Conf. Parallel Processing (ICPP), 2011.*

[4] J.Kong, X. Hong, and M. Gerla," ANODR: Anonymous On Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks," *Proc. ACM MobiHoc, pp. 291-302, 2003.*