© 2015 IJIRT | Volume 1 Issue 12 | ISSN: 2349-6002

Providing Security and Energy Management in Location Based Routing of Manet's

Suprita Sambranikar[1], Prathima S D[2]
[1]*Final Year M.Tech Dept. Of ECE, BTL Institute Of Technology And Management, Bangalore, India.*
[2]*Asst. Prof: Dept. Of ECE, BTL Institute Of Technology And Management, Bangalore, India.*

***Abstract*- Mobile Ad Hoc Networks (MANETs) use unknown routing protocols that hide from view node identities and routes from outside observers in order to provide ambiguity protection. As we know existing unknown routing protocols depends on hop-by-hop encryption and redundant traffic. It generates high cost and cannot provide full ambiguity protection to packet sources, destination, and routes. Because of high cost the essential resource restriction problem exists in MANETs mainly in multimedia wireless applications. To provide high ambiguity protection at low cost, we offer an Anonymous Location-based Efficient Routing protocol (ALERT) that provides Security and Energy Management in Location Based Routing of MANETs. ALERT dynamically divides the network area into zones and arbitrarily chooses nodes in zones as intermediary relay nodes, which form non detectable unknown route. It also hides the packet initiator/receiver among many initiators/receivers in order to provide anonymity protection to source and destination. Thus, ALERT provides ambiguity protection to sources, destinations and routes. It as well has strategies to successfully oppose intersection and timing attacks. We theoretically examine ALERT in terms of ambiguity and efficiency. Experimental results illustrate reliability with the theoretical examination, and compared to other anonymous routing protocols ALERT achieves improved route anonymity protection at lower cost. The proposed method is inspired with Network Simulator (NS2) to analyze its performance in terms of network life span, packet delivery ratio, Control overhead and end to end delay than the existing schemes.**

***Index Terms*- Mobile ad hoc networks, ambiguity, routing protocol, geographical routing**

I. INTRODUCTION

Now day's Mobile ad hoc networks are developing in high-speed, it has lots of wireless applications that can be used in large number of areas such as business, emergency services, military, education and activity. Manet is a continuously identity organizing, communications-less network of mobile devices connected without wires. Each device in a Manet is free to move arbitrarily in any direction, and will therefore connect its links to other devices commonly. MANET is more vulnerable than wired network due to mobile nodes, threats from compromised nodes within the network, partial objective security, active topology, scalability and requires centralized management. Because of these vulnerabilities, MANET is more flat to cruel attacks. Although ambiguity may not be a necessary in civil oriented applications, it is risky in military application. Consider a MANET in military applications, through traffic analysis, enemies may destroy transmitted packets by attacking soldiers, commander nodes, and block the data transmission by comprising relay nodes, thus putting us at a dangerous disadvantage.

Unknown routing provides secure communication between two nodes by hiding nodes unique identity and prevents these nodes from traffic analysis attacks of adversaries. In this paper the main goal of unknown routing is to hide identity and location of data sources and route. So attacker cannot easily recognize identity and location in network of nodes.

This paper is organized as follows: In Section 2, we explain methodology. We discuss ALERT protocol in section 3. In section 4, we tentatively examined ALERT in terms of ambiguity and efficiency. In section 5 and 6 we have advantages and simulation results. The conclusion and future work are given in Section 7.

II.METHODOLOGY

The method of providing security and energy management in location based routing of MANETs working will be made in the following steps:

- Unknown routing: ALERT will give identity, location ambiguity of source and destination and route ambiguity.
- Low cost: Rather than depending on hop-by-hop encryption and redundant traffic, ALERT especially uses randomized routing of one communication copy to provide ambiguity protection.

- Resilience to intersection and timing attacks: ALERT will effectively oppose intersection attacks and also avoids timing attacks. Because of it's not fixed routing paths between source destinations.
- Extensive simulation: We conducted simulation results and evaluated ALERT performance with other anonymous routing protocols.

III.ALERT-NETWORK MODELS

ALERT is used in different network models with node group patterns. Such as random way position model and group mobility model.

Consider MANET used effectively in military appliance. Using network model information intruder may try to find out location of nodes. So ambiguity may be at risk. Therefore, an unknown communication protocol is required to provide strict ambiguity to the sender. Also the attacker tries to block the packets by interrupting packets on a routing path. Therefore, route should also be undetectable. And with help of intersection attack on traffic destination node can be detected, so destination node also needs the protection ambiguity.

A. Dynamic Pseudonym and Location of Node

Dynamic pseudonym is another identity specified to node. In ALERT real MAC address can be replaced as pseudonym for the node identifier. Nodes MAC adress can be used to find the nodes presence in the network. Therefore changing MAC address with pseudonym is the main advantage of ALERT protocol. This pseudonym is the mixture of MAC address and Current time crush. But if the attacker knows the information then they can find out the nodes easily. Therefore, to prevent this time crush can be arbitrarily selected. This pseudonym is not permanent it expires after a specific time period so that attacker cannot relate the pseudonym with nodes. One problem with this pseudonym is changing pseudonym frequently create routing anxious. Therefore these pseudonym changes commonly should be suitably determined.

B. The ALERT Routing Algorithm

ALERT provides random and dynamic routing path, which has number of dynamically selected intermediate nodes. Below figure shows the network partition into zones using alert routing algorithm.

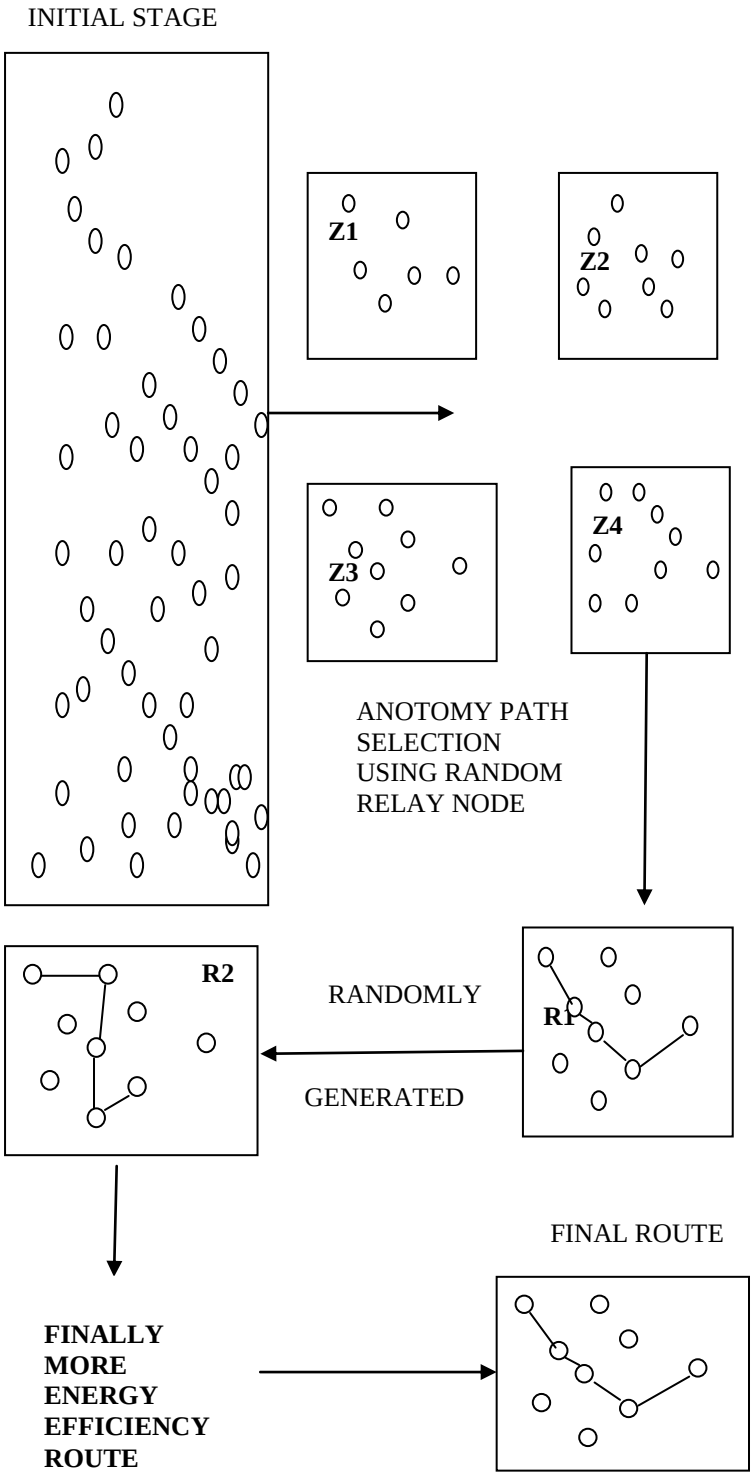

Fig 1.Routing among zones in ALERT

C. Location of Destination Zone

To avoid disclosure of destination we are using destination zone position. The destination zone position

is made from the bottom right and upper left coordinates of the zone. To calculate zone position we have,

$$H = \log2 (\rho.G/k)$$

Where as

H=Total number of partition in order to produce ZD
G=size of entire network area
ρ=Node density

Using H and G the position (0, 0) & (Xg, Yg) of entire network area and position of destination node, the source can calculate the zone position of ZD.

D. Packet Format

Some information is needed, for the successful routing between source and destination, which is embeds in the data by source and each packet forwarder node. For ALERT following packet format is used.

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

Fig.4 ALERT Packet Format

RREQ/RREP/NAK- used to acknowledge the failure of packet.
Ps- Pseudonym of a source.
Pd – pseudonym of a destination.
Lzs & Lzd – are the location of Hth partitioned source zone and destination zone.
h- Number of divisions.
H – Maximum number of division allowed.

IV- ANONYMITY PROTECTION AND STRATEGIES AGAINST ATTACKS

A. Anonymity Protection

The main objective of ALERT is to provide unique name to the nodes, location ambiguity for source, destination and route. For this ALERT dynamically divides the network into zones and selects random forwarders to transfer packet from source to destination. With this the attacker will not detect the packet.

Unknown path between the source and destination node ensures that neighbor nodes on the path do not know where the end points. It provides the ambiguity protection to the source and destination. ALERT has "notify and go" mechanism.

B. Strategy to oppose Intersection Attacks

In intersection attack the attacker can collect the information of the communicating nodes and they can detect the routing path.

To prevent this, ALERT proposes a strategy called counter intersection attack. In this attack the destination is broadcasted into K-anonymity. This broadcasting is done in two steps. In first step packet is broadcasted into K-anonymity but it will not reach the destination node. In second step random forwarders will receive the packet and forwards to the destination node at this point attacker get confused and he will not know which the destination node is.

C. Resilience to Timing Attacks

In timing attacks, during packet departure and appearance times, an attacker can find the data transmitted between source and destination, with this it will identify position of S and D. For example, two nodes X and Y communicate with each other at an interval of 5 seconds. When, the attacker finds that X and Y are sending and receiving the packet at fixed time of six second. Then, the attacker would estimate that X and Y are communicating with each other.

Avoiding the exposure of interaction between communication nodes is a way to oppose timing attacks. In ALERT, the "notify and go" method and the broadcasting in ZD both put the interaction between S-D into two sets of nodes to confuse attackers. Likewise, the routing path between a given S-D pair and the communication delay change constantly, which once more keeps an attacker from finding the S and D.

V. ADVANTAGES

- ALERT provides identity, location ambiguity of source and destination and route ambiguity.
- Rather than depending on hop-by-hop encryption and redundant traffic, ALERT mainly uses randomized routing of one message copy to provide anonymity protection.
- ALERT can also keep away from timing attacks because of its nonfixed routing paths for a source destination pair.
- We conducted inclusive experiments to calculate ALERT's performance in comparison with other unknown protocols

VI. SIMULATION RESULT

The total numbers of sensor nodes are 100 deployed in 1000x1000 areas with static source and sink chosen. Initial simulation run is made to send the "hello" packets, and two random paths are selected between source and destination according to randomly selected relay nodes. Remaining energy calculation is made for two selected to select which one is more energy efficient. The final route will be more protected and also energy resourceful.

The Performance evaluation is made through the xgraph for

- Packet delivery ratio
- Energy
- Control overhead packets
- Throughput

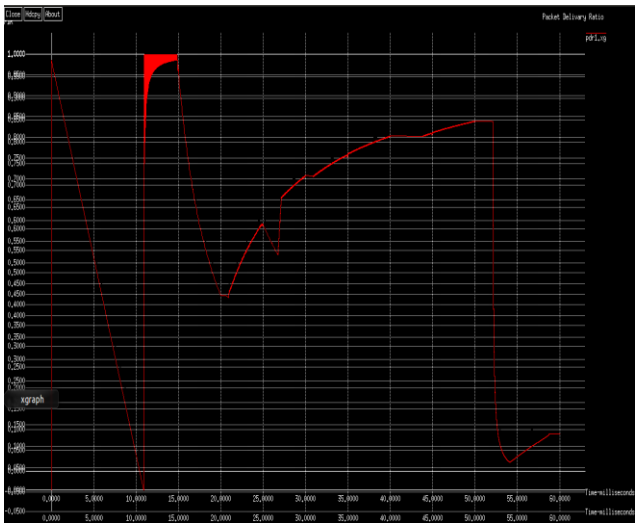

Fig5. Performance of Packet Delivery ratio

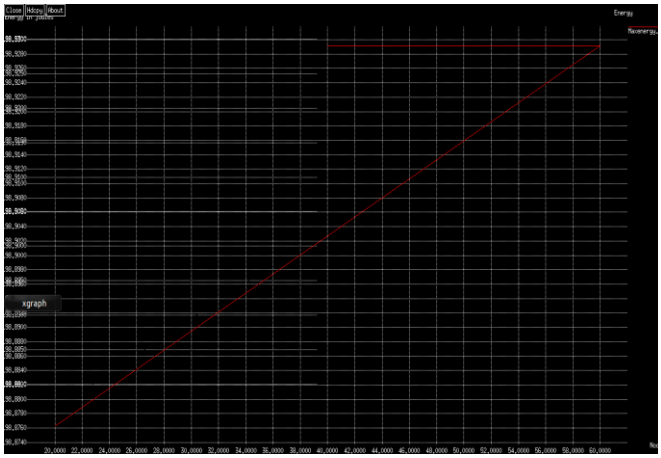

Fig6.Performance of Energy

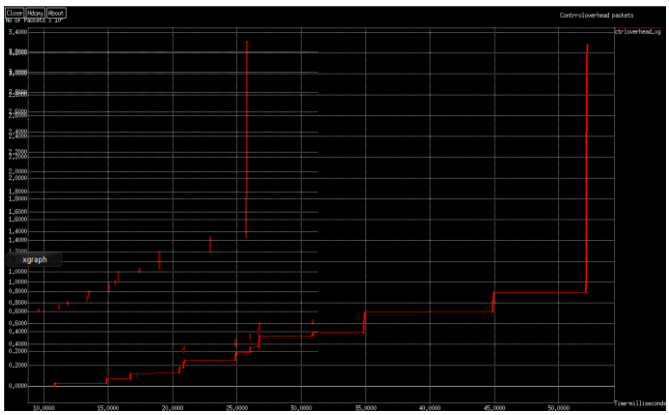

Fig7.Performance of Control overhead Packets

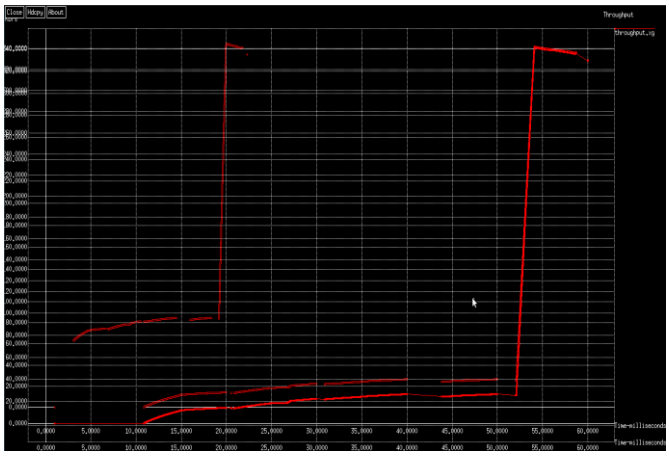

Fig8.Performance of Throughput

VII. CONCLUSION AND FUTURE WORK

Existing anonymous routing protocols depend on either hop-by-hop encryption or redundant traffic and generate high cost. Also, some routing protocols are not able to provide complete route anonymity protection for source and destination. ALERT is prominent by its low down cost and ambiguity security for sources, destinations, and routes. It uses active hierarchical zone divisions and random relay node selections to make it difficult for an intruder to detect the two endpoints and nodes en route. A data in ALERT includes the source and destination zones rather than their positions to provide ambiguity protection to the source and the destination. ALERT further makes the strong ambiguity 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 ambiguity, and uses narrow broadcasting for destination ambiguity. In addition, ALERT has an capable solution to oppose intersection attacks and fight against timing attacks. Experimental outcome shows that

ALERT can provide high ambiguity protection at a low cost when compared to other ambiguity algorithms. It can also accomplish similar routing competence to the base-line GPSR algorithm. Like other ambiguity routing algorithms, ALERT is not totally bulletproof to all attacks.

Future work exists in reinforcing ALERT in an effort to prevent stronger, active attackers and representing complete theoretical and simulation results.

ACKNOWLEDGEMENT

This research was supported in part by my project guide Miss. Prathima S. D. Assistant Professor, Branch of Electronics and Communication Engineering for her exemplary guidance and precious suggestions, which helped me in effectively increasing the part.

REFERENCES

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

[2] 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.

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

[4] A. Pfitzmann, M. Hansen, T. Dresden, and U.Kiel, "Ambiguity, Unlink capacity, Unobservability, Pseudonymity, and Identity Managementa Consolidated Proposal for vocabulary, Version 0.31," technical description, 2005.

[5] T. Camp, J. Boleng, and V. Davies, "A Survey of Mobility Models for Ad Hoc Network investigate," Wireless Communications and Mobile Computing, vol. 2, pp. 483-502, 2002.

[6] Z. Zhi and Y.K. Choong, "Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy," Proc. Third Int'l Workshop Mobile scattered Computing (ICDCSW), 2005.

[7] 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.

[8] I Aad, C. Castelluccia, and J. Hubaux, "Packet Coding for Strong ambiguity in Ad Hoc Networks," Proc. Securecomm and Workshops, 2006.

[9] X. Hong, M. Gerla, G. Pei, and C.C. Chiang, "A Group Mobility Model for Ad Hoc Wireless Networks," Proc. Second ACM Int'l Workshop Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM), 1999.

[10] "The Network Simulator - ns-2," http://www.isi.edu/nsnam/ns, 2012.