ISSN:0975-9646

An Overview of Anonymous Routing ALERT Protocol

Snehlata Handrale, Prof. S. K. Pathan

*Department of Computer Engineering,University of Pune,
Pune , India*

***Abstract*— In Mobile Ad-Hoc Network (MANET) ,for security purpose anonymous routing protocol used. This protocol hides nodes original identity from outsider, so that observer cannot threaten the security of network. There are few existing anonymous routing protocol available for MANET. From thse some are relying on hop-by-hop encryption or redundant traffic, but they are having high cost and provide low anonymity. Therefore to provide high anonymity protection with low cost, propose an Anonymous Location Based Efficient Routing Protocol. In this protocol, given network dynamically partition into zones. Every zone having nodes which are act as intermediate nodes.These nodes get randomly selected for routing so that observer cannot indentify route.For anonymity ALERT hides mainly source and destination identity using pseudonym which changes frequently. And ALERT also hide route between source and destination. With this ALERT also having stratergy against intersection attacks.**

***Keywords*— Mobile Ad-Hoc Network, Anonymity, Intersection attack etc.Introduction**

I. INTRODUCTION

Now a days using mobile Ad-hoc Network , numerous wireless application can be developed and these are used in many number of areas like mainly in military ,education ,commerce ,entertainment.

MANET- MANET’s basic features are self organizing and independent infrastructure. All the nodes in the network are mobile and uses wireless communications to communicate with other nodes.But as perspective of security of MANET ,these network get easily broken their security. Mainly data get lost or stolen by tampering and analyzing data and traffic analysis eavesdropping method or attacking routing protocol.For this security issue one solution is to use anonymous routing in the network that can not be identified by any other nodes or attacker or observer. Although this anonymous routing is not required in general application .but it is very essentitial in Military ,Banking like application, where security of communication is main purpose.

Anonymous routing provides secure communication between two nodes by hiding nodes original identity and prevent these nodes from traffic analysis attacks of advresaries.In this paper the main task of anonymous routing is to hide identity and location of data sources (i.e sender,receipent)and route.so attacker can not easily identify identity and location in network of nodes.

This paper is organized as follows: InSection 3, describe existing anonymous routing protocol. Section 4 describe ALERT protocol. In Section 4, we theoretically analyzed ALERT in terms of anonymity and efficiency. The conclusion and future work are given in Section 5.And References in section 6.

II. EXISTING ANONYMOUS ROUTING PROTOCOL

A. ALARM

Anonymous Location Aided Routing in Suspicious MANETs is one of the anonymous routing protocol in MANET. ALARM find out problems in MANET. And also provide secure anonymous routing in network. For this it uses link state routing protocol. Takes nodes current position to broadcast and construct topology snapshots and forward data. For security purpose ALARM uses advanced cryptographic techniques as well as it provides node authentication, non- traceability, privacy features, data integrity. It also provide security against active and passive attacks. But problem with ALARM is it cannot protect location anonymity of source and destination node.

B. ASR

Another anonymous routing protocol is Anonymous Secure Routing (ASR) protocol. This protocol provide additionnal properties on anonymity, i.e. Identity Anonymity and Strong Location Privacy. As well as at the same time ensure the security of discovered routes against various passive and active attacks. But ASR protocol having route anonymity problem.

C. AO2P

AO2P is one of the important anonymous routing protocol, It is An ad hoc on-demand position-based private routing algorithm. This protocol is mainly proposed for communication anonymity. In this instead of node identity ,nodes position is used for route discovery.

III.ALERT-ANONYMOUS LOCATION BASED EFFICIENT ROUTING PROTOCOL

ALERT can be used in different network models with node movement patterns. Such as random way point model and group mobility model.

Using network model information attacker may find out location of nodes. So anonymity may get threaten. Therefore, an anonymous communication protocol is needed which can provide untraceability to strictly ensure the anonymity of sender. As well as attacker try to block the data packets by injecting 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 anonymity.

A. *Pseudonym and Location of Node*

Dynamic pseudonym is another name or identity given to node. In ALERT pseudonym used as node identifier with replacement of its real MAC address. Nodes 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 is easily find out the node. Therefore, to prevent this time stamp can be randomly selected. This pseudonym is not permanent ,it expires after a specific time period so that attacker can not associate the pseudonym with nodes.With this pseudonym there is one problem is changing pseudonym frequently create routing uneasy. Therefore these pseudonym change frequently should be appropriately determined.

B. *The ALERT Routing*

Generally ALERT provides unpredictable and dynamic routing path,which having no.of dynamically selected intermediate nodes.

1. First ALERT partitions given network area into two zones as horizontally (or vertically).

2. Then again split every partitions into two zones as vertically (or horizontally). This process called as hierarchical zone partition.

3. After partitioning ALERT randomly select a node in each zone at each step as an intermediate relay node ,in this way ALERT provide dynamically creating an unpredictable routing path.

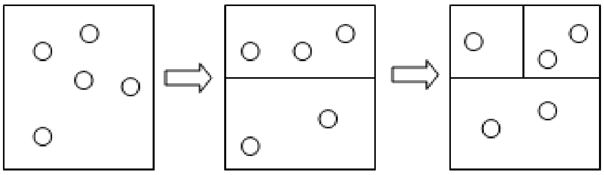


Fig. 1 Horizontal Partitioning

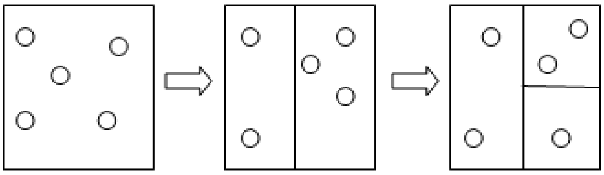


Fig. 2 Vertical Partitioning

Above figs shows both partitioning, here we generally network considered in rectangle form. In this rectangle circle consider as nodes. Consider one example of routing in ALERT .Following fig shows this

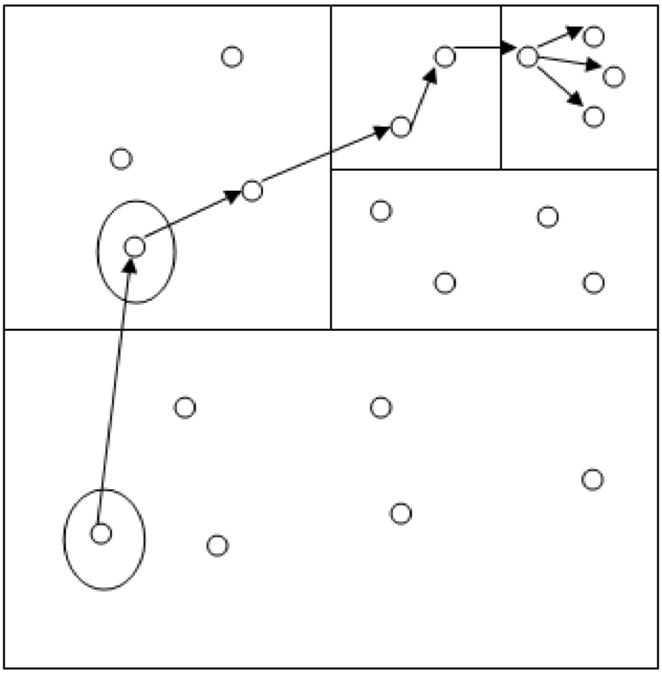


Fig 3. Zonal Routing of Nodes

In this example we first horizontally partition network then vertically and so on. While this partitioning each data source of forwarder node checks whether itself and destination node are not in same zone. If it is not then partitioning continues. In above fig where the destination node locate that zone is called as destination zone denoted as ZD and that zone having k nodes ,which is used to control the degree of anonymity.

While in routing first source node randomly chooses a node in other zone known as temporary destination (TD) and then uses GPSR routing algorithm to send the data to node close to TD. This process continues to reach data to destination node. A node closer to TD known as Random Forwarder (RF) .But in destination zone data is broadcasted in ZD to k nodes which provides k anonymity i.e attacker or observer does not known at destination node.

Here one assumption is taken that destination node with not leave the destination zone during the data transmission to it. So it can successfully receive the full data without any loss. For successful completion of data transmission destination node send a confirmation to source node. If source node not receive to confirm during predefined time period, it will resend packets. As a large no.of hierarchies generated they create more routing hops which increses anonymity degree but also increase the delay.

C. *Location of Destination Zone*

Zone position is made from the upper left and bottom right coordinates of a zone. It is used by each packet forwarder to check wheather it is separated from destination zone or not, To calculate zone position we have H denotes total no.of partitions in order to produce ZD and no.of nodes i.e k and node density ρ ,

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

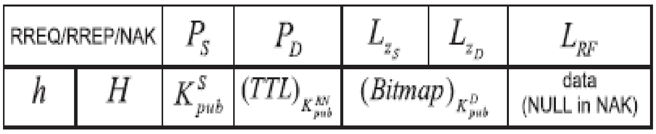
Where as

G=size of entire network area

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

D. *Packet Format*

For successful routing netween source and destination some information is needed, which is embeds in the packet by source and each packet forwarder node. For ALERT following packet format is use.



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

Fig.4 ALERT Packet Format

RREQ/RREP/NAK- use to acknowledge the loss of packet.

Ps- Pseudonym of a source.

Pd – pseudonym of a destination.

Lzs & Lzd – are the position of Hth partitioned source zone and destination zone.

h- number of divisions.

H – maximium number of division allowed.

IV - How Achieve Anonymity Protection And Strategies Uses Against Attacks

A. *Anonymity Protection*

The main goal of ALERT is to provide identity and location anonymity of source and destination in MANET. For this ALERT dynamically and randomly chooses relay node for forming route between source and destination. So due to this intruder cannot observe a stastical pattern of transmission.

Anonymous path between source and destination ensures that nodes on the path does not know where the end points are. Unlinkability is major strength of privacy protection i.e source and destination cannot be associated with the packets in their communication by adversaries.

B. *Strategy against Intersection Attacks*

Intersection attack ,in which an attacker can determine communicating nodes using observation of routing between them and collecting information about them.

Active Users To counter intersection attack ALERT proposes a strategy. In this it broadcasted the packets in destination zone ZD. So that attacker confuse who is destination .This broadcasting is done in two steps. In first step packet is broadcasted but not reach to destination node. In second step nodes who receive the packets then forward packets to remaining node who yet not receive in this destination node is present so it receive the packet. In this situation attacker get confused and can't concentrate in their observation.

V. Conclusion

Existing anonymous routing protocols, depend on either hop-by-hop encryption or redundant traffic which generate high cost. And some protocols are not provide complete source, destination, and route anonymity protection. 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. A packet in ALERT includes the source and destination zones rather than their positions to provide anonymity protection to the source and the destination. ALERT further strengthens the anonymity protection of source and destination by hiding the data initiator/receiver among a number of data initiators/ receivers. In addition, ALERT has an efficient solution to counter intersection attacks.

References

[1] L. Zhao and H. Shen, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs," IEEE TRANSACTIONS ON MOBILE COMPUTING, JUNE 2013.

[2] A. Pfitzmann, M. Hansen, T. Dresden, and U.Kiel, "Anonymity ,Unlinkability, Unobservability, Pseudonymity, and Identity Managementa Consolidated Proposal for Terminology, Version 0.31," technical report, 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] 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.

[5] 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.

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

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

[8] 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.

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

[10] 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.