Anonymity,Unlinkability,Unobservability for Routing Protocol in MANETs

Ms.Deepika.S, PG Student
M.E – Computer Science And Engineering
M. Kumarasamy College of Engineering
Karur, Tamilnadu, India
deepikame2014@gmail.com

Mrs.B.Padmini Devi, Asst. Professor
Department of CSE
M. Kumarasamy College of Engineering
Karur, Tamilnadu, India
lakshana06@gmail.com

Abstract - *Privacy protection of mobile ad hoc networks is more demanding than that of wired networks due to the open nature and mobility of wireless media. In wired networks, one has to gain access to wired cables so as to eavesdrop communications. Privacy-preserving routing is crucial for some ad hoc networks that require stronger privacy protection. In hostile environments, the enemy can launch traffic analysis against interceptable routing information embedded in routing messages and data packets. Allowing adversaries to trace network routes and infer the motion pattern of nodes at the end of those routes may pose a serious threat to covert operations. A number of schemes have been proposed to protect privacy in ad hoc networks. However, none of these schemes offer complete unlink ability or unobservability property since data packets and control packets are still linkable and distinguishable in these schemes. In this paper, we define stronger privacy requirements regarding privacy-preserving routing in mobile ad hoc networks. Anonymous key establishment process and route discovery process authenticates the routing paths taken by individual messages. Achieving anonymity is a different problem than achieving data confidentiality. While data can be protected by cryptographic means, the recipient node address and maybe the sender node address of a packet cannot be simply encrypted because they are needed by the network to route the packet.*

Keywords: *Mobile Ad hoc Networks, Anonymity, Routing protocol, Geographical routing,*

I. Introduction

A Mobile Ad-hoc NETwork (MANET) is a self-configuring network consisting of mobile hosts equipped with wireless communication devices. The transmission of a mobile host is received by all hosts within its transmission range due to the broadcast nature of wireless communication and Omni-directional antennae. If two wireless hosts are out of their transmission ranges in the ad hoc networks, other mobile hosts located between them can forward their messages, which effectively build connected networks among the mobile hosts in the deployed area. Due to the mobility of wireless hosts, each host needs to be equipped with the capability of an autonomous system, or a routing function without any statically established infrastructure or centralized administration. The mobile hosts can move arbitrarily and can be turned on or off without notifying other hosts. The mobility and autonomy introduces a dynamic topology of the networks.

A Mobile Ad hoc NETwork (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. People and vehicles can thus be internetworked in areas without a preexisting communication infrastructure or when the use of such infrastructure requires wireless extension. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that not in the direct communication range use intermediate node(s) to communicate with each other. In these two situations, all the nodes that have participated in the communication automatically form a wireless network, therefore this kind of wireless network can be viewed as mobile ad hoc network.

The Mobile Ad hoc NETwork has the following typical features like Unreliability of wireless links between nodes. Because of the limited energy supply for the wireless nodes and the mobility of the nodes, the wireless links between mobile nodes in the ad hoc

network are not consistent for the communication participants. Due to the continuous motion of nodes, the topology of the mobile ad hoc network changes constantly: the nodes can continuously move into and out of the radio range of the other nodes in the ad hoc network, and the routing information will be changing all the time because of the movement of the nodes. Lack of incorporation of security features in statically configured wireless routing protocol not meant for ad hoc environments.

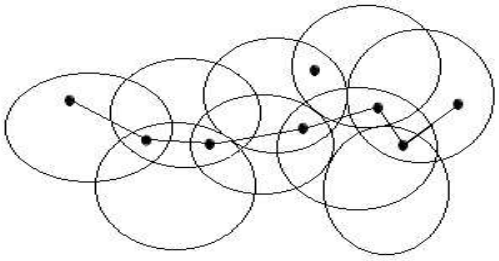

Fig 1.1.Architecture of MANET

The topology may gets changes in the MANETs. Because the topology of the ad hoc networks is changing constantly, it is necessary for each pair of adjacent nodes to incorporate in the routing issue so as to prevent some kind of potential attacks that try to make use of vulnerabilities in the statically configured routing protocol. Because of the features listed above, the mobile ad hoc networks are more prone to suffer from the malicious behaviors than the traditional wired networks. Therefore, we need to pay more attention to the security issues in the mobile ad hoc networks.

II. Related work

Anonymous routing schemes in MANETs includes providing anonymity to the network nodes and identities. By the different usage of topological information, they can be classified into on-demand or reactive routing methods [8], [3], along with geographic hash methods [1],[4], [11], [10], [13], and proactive routing methods [5]. Also there are anonymous middleware working between network layer and application layer[2],[9]. Since topology routing does not need the node location information, location anonymity protection is not necessary.

ALERT provides route anonymity, location anonymity and identity anonymity of source and destination. By using hop by hop encryption and redundant traffic, which offers high cost.But the ALERT protocol has low cost because they need a random forwarder to choose the next node to send the packet.Privacy-Preserving Location-Based On-Demand Routing in MANETs uses PRISM protocol which offers better privacy and security against both insider and outsider adversaries. AODV presents an attractive foundation for PRISM, but does not require mobility to be synchronized. AODV is a on-demand location centric reactive protocol.

To deal with this problem, the authors further proposed Discount-ANODR[19] that constructs onions only on the return routes. Anonymous on Demand routing with untraceable Routes for Mobile Ad-hoc Networks is the first one to provide unlinkability for routing in ad hoc networks. User anonymity is implemented by group signature which can be verified without disclosing one's identity. Group signature is used to establish session keys between neighboring nodes, so that they can authenticate each other anonymously. And subsequent routing discovery procedure is built on top of these session keys. Hence it is easy to see that USOR[18] fulfills the anonymity requirement under both passive and active attacks, as long as the group signature is secure. ANODR[19] uses one-time public/private key pairs to anonymity and unlinkability which may be a drawback for the security purpose like link between source and destination can be breakable.

Hop-by-hop authentication is used to prevent adversaries from participating in the routing to ensure route anonymity [3], [11], [10], [7], along with geographic hash mechanism [4].Including the trapdoor information in the route request, is decrypted and encrypted at each hop. Hence even for a global adversary who can eavesdrop every transmission within the network, it is impossible for him to find linkage between messages without knowing any encryption key. MASK topological routing uses neighborhood authentication in routing path discovery to ensure that the discovered routes consist of legitimate nodes and are anonymous to attackers. The works in [3], [4], [11], [10] are based on geographic routing. In GSPR [3], nodes encrypt their location updates and send location updates to the location server. However, GSPR does not provide route anonymity because packets always follow the shortest paths using geographic routing, and the route can be detected by adversaries in a long communication session. In [4], a mechanism called geographic hash is used for authentication between two hops en route, but the anonymity is compromised because the location of each node is known to nodes in the vicinity.

In the AO2P [10] 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. Since AO2P

does not provide anonymity protection to destinations, the authors further improve it by avoiding the use of destination in deciding the classification of nodes. The improved AO2P selects a position on the line connecting the source and destination that is further to the source node than the destination and replaces the real destination with this position for distance calculation. ASR [11] conducts authentication between the source and the destination before data transmission. The source and each forwarder embed their public keys to the messages and locally broadcast the messages. The destination responds to the source in the same way. In each step, the response is encrypted using the previous node's public key so that only the previous forwarder can decrypt the message and further forward it. However, such public key dissemination in routing makes it possible for attackers to trace source/destination nodes. Ariadne [7] uses TESLA to conduct broadcasting-style authentication between two neighboring hops en route.

Although it uses symmetric key cryptography in the authentication, a high amount of traffic is inevitably incurred in broadcasting. SEAD uses low-cost one-way hash functions rather than asymmetric cryptographic operations in conducting authentication for lower cost. However, all of these hop-by-hop encryption methods generate high cost due to the use of hop-by-hop public-key cryptography or complex symmetric key cryptography. Redundant traffic-based routing uses redundant traffic, such as multicast, local broadcasting, and flooding, to obscure potential attackers. Multicast is used in the Aad[6], [8] topological routing algorithm to construct a multicast tree or forest to hide the destination node. Broadcast is used in MAPCP topological routing [9] and other geographic routing protocols [5], [11]. ASR [11] shuffles packets to prevent traffic analysis in addition to the hop-by-hop authentication mentioned above.

ALARM takes advantage of group signatures to preserve node anonymity while allowing authentication of location updates. There are many group signature schemes in the literature that differ widely in their security properties and efficiency features. ALARM is not restricted to any particular group signature scheme. Any secure group signature scheme can be used as long as attacks are limited to those by active outsiders and passive insiders. ALARM relies on group signatures to construct one-time pseudonyms used to identify nodes at certain locations. The framework works with any group signature scheme and any location-based forwarding protocol can be used to route data between nodes. We have shown through simulation that node privacy under this framework is preserved even if a portion of the nodes are stationary, or if the speed of movement is not very high. It includes developing an analytical model which captures the loss in node privacy due to the dynamics of the speed and the mobility patterns of nodes inside the MANET.

III. Proposed model

As similar to previous approaches [5],[14], this study also concentrated on the anonymity protection on network. In order to increase the higher efficient anonymity the concept unobservability with AODV routing protocol has been implemented. In MANET, any node can be of source or destination because of its mobility. An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks is used to provide the complete unobservability for all types of packets. Unobservability ensures that a user may use a resource or service without others being able to observe that the resource or service is being used. Unobservability requires that users cannot determine whether an operation is being performed.

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. It has the "notify and go" mechanism for source anonymity, and uses local broadcasting for destination anonymity. In addition, ALERT has an efficient solution to counter intersection attacks. ALERT's ability to fight against timing attacks is also analyzed. Experiment results show that ALERT can offer high anonymity protection at a low cost when compared to other anonymity algorithms. It can also achieve comparable routing efficiency to the base-line GPSR algorithm. Like other anonymity routing algorithms, ALERT is not completely bulletproof to all attacks. Future work lies I reinforcing ALERT in an attempt to thwart stronger, active attackers and demonstrating comprehensive theoretical and simulation results.

The above represented square shaped box represents the network, where these networks are dynamically partitioned into various fields. First step takes place by partitioning the whole network into two fields by naming as x1 and x2.Then further the zone x1 gets partitioned into two fields like y1and y2. This process gets continued to form the hierarchial partitioning.

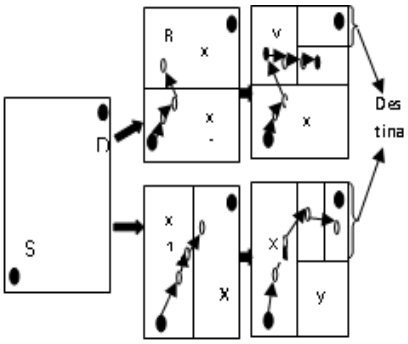

Fig.3.1.Examples of Zone partitioning.

A.The Destination Zone Position

The reason we use Z_D rather than D is to avoid exposure of D. Zone position refers to the upper left and bottom-right coordinates of a zone. One problem is how to find the position of Z_D, which is needed by each packet forwarder to check whether it is separated from the destination after a partition and whether it resides in Z_D. Let H denote the total number of partitions in order to produce Z_D.Using the number of nodes in Z_D (i.e., k), and node density, H is calculated by

$$H = \log_2((\rho \cdot G)/K)$$

where G is the size of the entire network area. Using the calculated H, the size G, the positions (0,0) and (x_G, y_G) of the entire network area, and the position of D, the source S can calculate the zone position of Z_D.

B. Destination Anonymity protection

Destination anonymity is determined by the number of nodes in the destination zone, which is related to node density and the size of the destination zone.

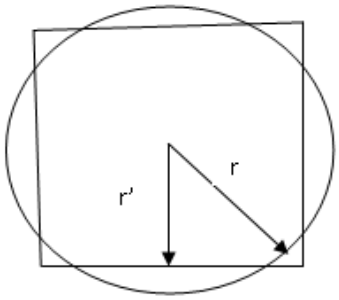

Fig.3.2.Approximating a zone using a circle

Hence, we can calculate the radius of this approximate circle

as below:

$$\pi r^2 = \left(\frac{1}{2}\right)^2 \rightarrow r = \frac{2r'}{\sqrt{\pi}}$$

Thus,

$$\beta(r') = \frac{\sqrt{\pi}r'}{v}$$

IV. Results and Discussion

This division shows the simulation results of the proposed ALERT algorithm. By using NS2 (Network Simulator 2) the simulation analysis was carried out. The proposed part carries several nodes to be partitioned into various zones inorder to choose the random forwarder using AODV Routing Protocol.

The performance analysis which shows that the network may have two to many source and destination.The Relay nodes are selected due to the MAC configuration.The packet may transfer from source to destination in various direction inorder to provide security.

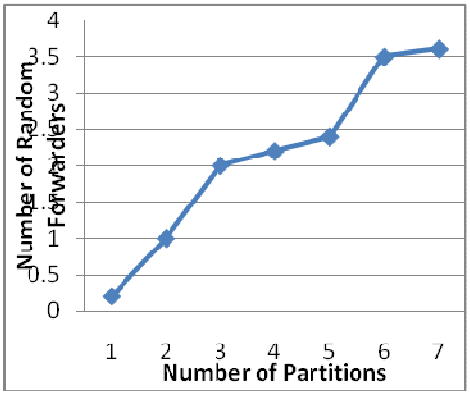

Fig.4.1.The no.of random forwarders versus the no.of partitions

The number of RFs versus the number of partitions in ALERT.We see the average number of RFs follows approximately a linear trend-* as the number of partitions increases. This experimental result is consistent with the analytical results. A higher number of partitions H lead to more RFs, hence high anonymity protection. This is because higher node density leads to more nodes in the destination zone, and more nodes could remain in the destination zone after certain a time than with lower node density. Also, because of node mobility, the number of nodes that have moved out of the destination zone increases as time passes.

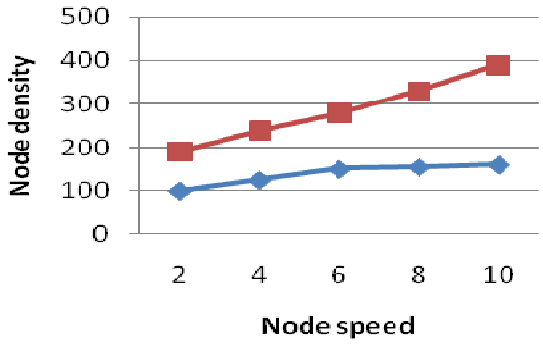

Fig.4.2. Influence of node moving speed and partitions on destination anonymity.

The mobile nodes within the radio range are communicated inside an adhoc infrastructure, where each node is equipped with wireless transmitter and receiver. If they send packets out of radio range they use multi hop communication. In MANET Route Discovery falls in important role. First it searches its route cache for suitable destination. If no such destination, Route discovery is initiated.

V. Conclusions

In this paper we addressed the relying on either hop-by-hop encryption or redundant traffic, generate high cost. Also, some protocols are unable to provide complete source, destination, and route anonymity protection. 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. It can also achieve comparable routing efficiency to the base-line GPSR algorithm. 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. Future work lies in reinforcing ALERT in an attempt to thwart stronger, active attackers and demonstrating comprehensive theoretical and simulation results.

VI. REFERENCES

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

[2]. "KeLiu'sNS2Code,"http://www.cs.binghamton.edu/~kliu/research/ns2code/index.html, 2012.

[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]. "TheNetworkSimulator-ns- 2, http://www.isi.edu/nsnam/ns, 2012.

[5]. 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.

[6]. 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.

[7]. 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.

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

[9]. K.E. Defrawy and G. Tsudik, "PRISM: Privacy-Friendly Routing in Suspicious MANETs (and VANETs)," Proc. IEEE Int'l Conf. Network Protocols (ICNP), 2008.

[10]. 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.

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

[12]. C.-C. Chou, D.S.L. Wei, C.-C. Jay Kuo, and K. Naik, "An Efficient Anonymous Communication Protocol for Peer to-Peer Application over Mobile Ad-Hoc Networks,"IEEE J. Selected Areas in Comm., vol. 25, no. 1, pp. 192-203, Jan. 2007.

[13]. 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.

[14]. 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. 2008.

[15]. Debian Administration, http://www.debian-administration.org/ users/dkg/weblog/48, 2012

[16]. 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.

[17]. X. Wu, "DISPOSER: Distributed Secure Position Service in Mobile Ad Hoc Networks: Research Articles,"Wireless Comm. and Mobile Computing, vol. 6, pp. 357- 373, 2006.

[18]. Zhiguo Wan, Kui Ren, and Ming Gu "USOR: An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks" VOL. 11, NO. 5, MAY 2012.

[19]. L. Yang, M. Jakobsson, and S. Wetzel, "Discount Anonymous On Demand Routing for Mobile Ad Hoc Networks," Proc. Secure comm and Workshops, 2006.