Routing Approach to Avoid Attacks Based on Anonymous Location in MANETs

Rekha M
M.Tech, CS&E,
Amc Engineering College, Bangalore-560083,
India. (Rekha.m.2820@gmail.com)

Mrs.Jeevitha R
Asst. professor, CS&E,
Amc Engineering college, Bangalore-560083
,India.(Jeevitha.cute@gmail.com)

***Abstract*—Anonymous routing protocols are used to hide the route between the source and destination, source identity and destination identity. In the existing system, anonymous routing protocols use hop by hop encryption or redundant traffic which may result in high cost and it doesn't provide different anonymity protection to source, destination and route. Because of these disadvantages, propose a protocol called Anonymous Location Based Efficient Routing Protocol (ALERT). The main technique used to provide anonymity is hierarchical partition. ALERT dynamically partition the network into vertical/horizontal zone. Greedy perimeter stateless algorithm (GPSR) is used to transmit the data from one node to another. It also effectively avoids the counter intersection attacks and timing attacks.**

.Keywords—Mobile ad hoc networks, anonymity, routing protocol, intersection attack, timing attack.

I. INTRODUCTION

Ad hoc network is a network where there is no existence of wireless infrastructure for networking, Instead each node communicates with each other using their sole transmitter-receiver only. In this kind of network each and every node does participate voluntarily in transit packet that flow to and from different nodes. Each node do follow same routing algorithm to route different packets. A mobile ad-hoc network(MANET) is a self-configuring network of mobile routers (and associated hosts) connected by wireless links. Mobile ad-hoc network (MANET) consists of collection of movable nodes. Ad-hoc network act as a stand-alone autonomous network. The packet routing is one of the most emerging areas in mobile ad-hoc network.Research in various aspects of mobile ad hoc networks (MANETs) has been very active, motivated mainly by military, disaster relief, and law enforcement scenarios.

More recently, location informationhas become increasingly available through small and inexpensive GPS receivers, partially prompted by the trend of introducing location-sensing capabilities into personal handheld devices.

MANETs feature self-organizing and independent infrastructures, which make them an ideal choice for uses such as communication and information sharing. Nodes in MANETs are vulnerable to malicious entities that aim to tamper and analyze data and traffic analysis by communication eavesdropping or attacking routing protocols. Although anonymity may not be a requirement in civil oriented applications, it is critical in military applications (e.g., soldier communication). Consider a MANET deployed in a battlefield. Through traffic analysis, enemies may intercept transmitted packets, track our soldiers (i.e., nodes), attack the commander nodes, and block the data Transmission by comprising relay nodes (RN), thus putting us at a tactical disadvantage.

Existing anonymity routing protocols in MANETs can be mainly classified into two categories: Hop-by-hop encryption and Redundant traffic that generate a significantly high cost, which exacerbates the resource constraint problem in MANETs. In a MANET employing a high-cost anonymous routing in a low quality of service in voice and video data transmission due to depleted resources may lead to disastrous delay in network operations. Most of the current approaches are limited by focusing on enforcing anonymity at a heavy cost to precious resources because public-key based encryption and high traffic generate significantly high cost. In addition, many approaches cannot provide all of therefore mentioned anonymity protections. Its drawbacks are: current approaches are limited by focusing on enforcing anonymity at a heavy cost to precious resources because public-key-based encryption and high traffic generate significantly high cost, many approaches cannot provide all of the aforementioned anonymity protections, ALARM cannot protect the location anonymity of source and destination, SDDR cannot provide route anonymity, and ZAP only focuses on destination anonymity.

In order to provide high anonymity protection (for sources, destination, and route) with low cost, the propose system as an Anonymous Location-based and Efficient Routing protocol (ALERT). ALERT dynamically partitions a network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non-traceable anonymous route. Specifically, in each routing step, a data sender or forwarder partitions the network field in order to separate itself and the destination into two zones. It then randomly chooses a node in the other zone as the

next relay node and uses the GPSR algorithm to send the data to the relay node. ALERT has a strategy to hide the data initiator among a number of initiators to strengthen the anonymity protection of the source. ALERT is also resilient to intersection attacks [9] and timing attacks.

In summary, the contribution of this work includes:

1. Anonymous routing. ALERT provides route anonymity, identity, and location anonymity of source and destination.
2. Low cost. Rather than relying on hop-by-hop encryption and redundant traffic, ALERT mainly uses randomized routing of one message copy to provide anonymity protection.
3. Resilience to intersection attacks and timing attacks. ALERT has a strategy to effectively counter intersection attacks, which have proved to be a tough open issue [9]. ALERT can also avoid timing attacks because of its non-fixed routing paths for a source-destination pair.

II. DETAIL STUDY

A. Routing In MANETs

Routing is the process of information exchange from one host to the other host in a network. Routing is the mechanism of forwarding packet towards its destination using most efficient path. Efficiency of the path is measured in various metrics like, Number of hops, traffic, security, etc. In Ad-hoc network each host node acts as specialized router itself. Routing protocol for ad-hoc network can be categorized in three strategies.

- Pro- active Vs Re- active routing protocol.
- Hybrid protocols.

1) Pro-active Vs Re-active routing protocol

In proactive routing scheme every node continuously maintains complete routing information of the network. This is achieved by flooding network periodically with network status information to find out any possible change in network topology. Current routing protocol like Link State Routing (LSR) protocol (open shortest path first) and the Distance Vector Routing Protocol (Bellman-Ford algorithm) are not suitable to be used in mobile environment. Destination Sequenced Distance Vector routing protocol (DSDV) and Wireless routing protocols were proposed to eliminate counting to infinity and looping problems of the distributed Bellman-Ford Algorithm. Examples of Proactive Routing Protocols are: Global State Routing (GSR), Hierarchical State Routing (HSR), and Destination Sequenced Distance Vector Routing (DSDV).

Every node in Re-active routing protocol maintains information of only active paths to the destination nodes. A route search is needed for every new destination therefore the communication overhead is reduced at the expense of delay to search the route. Rapidly changing wireless network topology may break active route and cause subsequent route search. Examples of reactive protocols are: Ad hoc On-demand Distance Vector Routing (AODV), Dynamic Source Routing (DSR), Location Aided Routing (LAR), Temporally Ordered Routing Algorithm (TORA).

2) Hybrid routing protocols.

There exist a number of routing protocols of globally reactive and locally proactive states. Hybrid routing algorithm is ideal for Zone Based Routing Protocol (ZRP).One of the major challenges in designing a routing protocol for ad hoc networks systems from the fact that, on one hand, a node needs to know at least the reachability information to its neighbors for determining a packet route and, on the other hand, the network topology can change quite often in an ad hoc network.

B. Anonymity In MANETs

Anonymous routing protocols are crucial in MANETs to provide secure communications by hiding node identities and preventing traffic analysis attacks from outside observers. Anonymity in MANETs includes identity and location anonymity of data sources (i.e., senders) and destinations (i.e., recipients), as well as route anonymity. "Identity and location anonymity of sources and destinations" means it is hard if possible for other nodes to obtain the real identities and exact locations of the sources and destinations.

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 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.

Many anonymity routing algorithms [1],[6],[4],[5] are based on the geographic routing protocol (e.g., Greedy Perimeter Stateless Routing (GPSR) that greedily forwards apacket to the node closest to the destination. However, the protocol's strict relay node selection makes it easy to revealthe source and destination and to analyze traffic. Anonymous routing protocols are essential in MANET to provide anonymity to source destination and route.

For Source Anonymity, ALERT contributes to the achievement of anonymity by restricting a node's view only to its neighbors and constructing the same initial and forwarded messages. This makes it difficult for an intruder to tell if a node is a source or a forwarding node.

For Destination Anonymity, the data is broadcasted to k nodes in the destination zone, providing k-anonymity to the destination.

C. Timing Attack

In timing attacks through packet departure and arrival times, an intruder can identify the packets transmitted between S and D, from which it can finally detect S and D. For example, two nodes A and B communicate with each other at an interval of 5 seconds. After a long observation time, the intruder finds that A's packet sending time and B's packet receiving time have a fixed five second difference such as (19:00:55, 19:01:00) and (20:01:33, 20:01:38). Then, the intruder would suspect that A and B are communicating with each other.

Avoiding the exhibition of interaction between communication nodes is a way to counter timing attacks. More importantly, the routing path between a given S-D and the communication delay (i.e., time stamp) change constantly, which again keeps an intruder from identifying the S and D.

D. Intersection Attack

In an intersection attack, an attacker with information about active users at a given time can determine the sources and destinations that communicate with each other through repeated observations. Intersection attacks are a well-known problem and have not been well resolved [9]. Though ALERT offers k-anonymity to D, an intersection attacker can still identify D from repeated observations of node movement and communication if D always stays in ZD during a transmission session. This is because as long as D is conducting communication, the attacker can monitor the change of the members in the destination zone containing D. As time elapses and nodes move, all other members may move out of the destination zone except D. As a result, D is identified as the destination because it always appears in the destination zone.

III. Related Work

Anonymous routing schemes in MANETs have been studied in recent years.

[1] Y. Zhang et.al Hop-by-hop authentication is used to prevent adversaries from participating in the routing to ensure route anonymity. MASK topological routing uses neighborhood authentication inrouting path discovery to ensure that the discovered routes consist of legitimate nodes and are anonymous to attackers. Y. Zhang et.al says that anonymous authentication with low cryptographic overhead and high routing efficiency can be obtained by using proactive neighbor detection. It is resistance to a wide range of adversarial attacks. MASK relies on a proactive neighbor detection protocol to constantly see the snapshot of its one-hop mobile neighborhood. MASK's neighbor detection protocol is identity-free.

[2] B. Zhu et.al ASR 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.

[3] X. Wu et.al ZAP uses a destination zone, and locally broadcasts to a destination zone in order to reach the destination without leaking the destination identity or position. A disadvantage of redundant traffic-based methods is the very high overhead incurred by the redundant operations or packets, leading to high cost. Although some methods such as ZAP only perform local broadcast in a destination zone, these methods cannot provide source or routing anonymity.

[4] K.E. Defrawy et.al ALARM uses proactive routing, where each node broadcasts its location information to its authenticated neighbors so that each node can build a map for later anonymous route discovery. However, this map construction leaks destination node locations and compromises the route anonymity.

[5] X. Wu 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 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.

[6] J. Li et.al GLS are zone-based location services and also uses hierarchical zone partitioning, its use is for location service, GLS divides the entire square area into four sub squares and then recursively divides these into smaller squares the zone division and hierarchies in GLS are configured in advance and the location servers are selected based on the different hierarchies.

IV. System Model

System architecture is the conceptual design that defines the structure and behavior of a system. An architecture description is a formal description of a system, organized in a way that supports reasoning about the structural properties of the system. It defines the system components or building blocks and provides a plan from which products can be procured, and systems developed, that will work together to implement the overall system. The System architecture is shown below in fig 1.

User configures the sensor nodes and sends the packets to the sensor nodes. Sensor nodes either encrypt or decrypt the packet, those encrypted or decrypted packets are forwarded

by forwarder chooser that act as a temporary destination, this process continues until it reach to the destination, the sender is used to send the packet to scheduler.

Finally measuring the latency, packet delivery ratio, security, and Energy consumption is done.

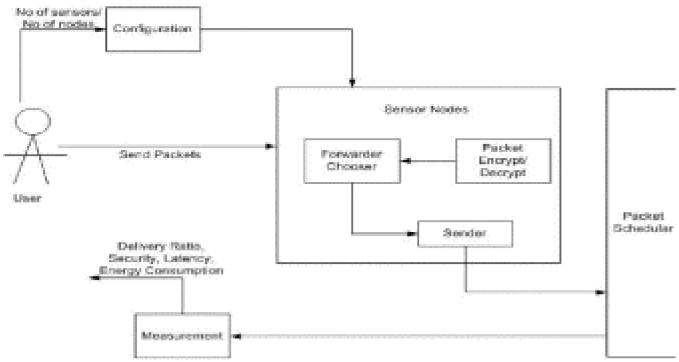

Fig:1 system architecture

A. The ALERT Routing Algorithm

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 Z_d 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). ALERT aims at achieving k-anonymity for destination node D, where k is a predefined integer. Thus, in the last step, the data are broadcasted to k nodes in Z_d, providing k-anonymity to the destination.

V. CONCLUSION AND FUTURE ENHANCEMENT

In this paper, proposed system 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 and dynamically partitions a network field into zones and randomly chooses nodes in zones as intermediate relay nodes

REFERENCES

[1] Y. Zhang, W. Liu, and W. Luo, "Anonymous Communications in Mobile Ad Hoc Networks," Proc. IEEE INFOCOM, 2005.

[2] 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.

[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.2008.

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

[5] 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.

[6] J. Li, J. Jannotti, D.S.J. De, C. David, R. Karger, and R. Morris, "A Scalable Location Service for Geographic Ad Hoc Routing," Proc. ACM MobiCom, 2010.

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

[8] J. Raymond, "Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems," Proc. Int'l Workshop Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobservability (WDIAU), pp. 10-29, 2001.

[9] 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.

[10] 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.

[11] Mobile Ad hoc Networking Carlos de MoraisCordeiro and Dharma P. Agrawal BR Research Center for Distributed and Mobile Computing, ECECS University of Cincinnati, Cincinnati, OH 45221-0030 – USA.

[12] 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.

[13] An Overview of Mobile Ad Hoc Networks: Applications and Challenges JeroenHoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester.