MYSTERIOUS LOCATION BASED ENHANCED ROUTING PROTOCOL IN MOBILE AD-HOC NETWORKS

[1]P. Dhivya, Asst.Prof /CSE,[2]B.Sasikala, Asst.Prof /CSE,
[3]P.Vinothini ,Asst.Prof /CSE, [4]T.G Ramya priyatharsini, Asst.Prof /CSE
Bharathiyar Institution of engineering for women,Salem,Tamilnadu
divsri35@gmail.com

Abstract **—** ***MANETs feature of self-organizing and independent infrastructures, which make them an ideal choice for uses such as communication and information sharing. In some protocol are unable to provide anonymity protection using Greedy perimeter stateless routing algorithm (GPSR). To agreement high anonymity protection at a scummy cost, proposed systems use a Mysterious Location-based Enhanced Routing protocol (MLRT) is animatedly partitioned the network field into sectors as intermediary relay nodes and also chooses arbitrarily nodes using Prioritization of Forwarding algorithm, the Time to Live (TTL) algorithm used for non-observable anonymous route. It mainly hides the data creator/receiver between many initiators/receivers to strengthen source and destination anonymity protection. However, anonymity protection for sources, destinations, and itineraries. It also has strategies to effectively counter intersection and timing attacks MLRT routing protocol gives full security for the messages compare to other routing protocol.***

Keywords — Mobile ad hoc networks, anonymity, routing protocol, zone partition

1. INTRODUCTION

A Mobile Ad Hoc Networks (MANET) is an autonomous system of mobile nodes. It consists of mobile platforms, for example a router with multiple hosts and wireless communications devices. Here in simply referred to as 'nodes' which are free to move. Therefore, MANET has been unremarkably deployed in adverse and hostile environments wherever central authority purpose isn't necessary. The critical characteristic of MANET is that the dynamic nature of its constellation which might be often modified attributable to the unpredictable quality of nodes. Furthermore, every mobile node in MANET plays a router role, whereas transmission knowledge over the network. Hence, any compromised nodes beneath an adversary's Management might cause vital injury to the practicality and security of its network from the impact would propagate in acting routing tasks. There is a unit another challenge and complexities:

[1] The scalability is needed in MANET because it is employed in military communications, as a result of the network grows consistent with the necessity, therefore every mobile device should be capable to handle the intensification of network and to accomplish the task.

[2] MANET is infrastructure less networks with no central administration. Every device will communicate with each alternative device. Therefore, it becomes tough to notice and manage the faults. In MANET the mobile devices will move at random. The work of this dynamic topology ends up in route changes, frequent network partitions and probably packet losses.

[3] Every node within the network is autonomous. Therefore have the instrumentality for radio interface with completely different transmission or receiving capabilities in uneven links.

2. EXISTING SYSTEM

Existing anonymity routing protocols in MANETs can be mainly classified into two categories: hop-by-hop encryption and redundant traffic. 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 the aforementioned Anonymity protections.

For example, ALARM (Anonymous Location Aided Routing in Suspicious MANET) cannot protect the location anonymity of the source and destination, SDDR (Secure Dynamic Distributed Routing) algorithm cannot provide route anonymity, and ZAP (Zone Based Anonymous Position) routing protocol only focuses on destination anonymity. Many anonymity routing algorithms are based on the geographic routing protocol and Greedy Perimeter Stateless Routing (GPSR) that greedily forwards a packet to the node closest to the destination.

However, the protocol's strict relay node selection makes it easy to reveal the source and destination and to analyze traffic. On the other hand, limited resource is an inherent problem in MANETs, in which each node labors under an energy constraint. MANETs' complex routing and stringent channel resource constraints impose strict limits on the system capacity.

Disadvantages

In order to provide high anonymity protection (for sources, destination, and route) with low cost. MANETs' complex routing and channel resource constraints impose strict limits

on the system capacity. Unable to give complete protection.

3. PROPOSED SYSTEM

To propose a Mysterious Location- based Enhanced Routing protocol (MLRT). MLRT dynamically partitions a network field into zones and randomly chooses nodes as intermediate relay nodes, which form a non- traceable anonymous route. Specifically, in each routing step, a data sender or forwarder partitions the network domain 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 POF algorithm to send the data to the relay node.

In the last step, the data are broadcast to k nodes in the destination zone, providing k-anonymity to the destination. In addition, MLRT has a strategy to hide the data initiator among a number of initiators to strengthen the anonymity protection of the source. MLRT is also resilient to intersection attacks and timing attacks.

Using the Analyze of MLRT in terms of anonymity and efficiency. To conducted experiments to evaluate the performance of MLRT in comparison with other anonymity and geographic routing protocols.

MLRT Routing Module

MLRT features a dynamic and unpredictable routing path, As shown in Figure 1,which consists of a number of dynamically determined intermediate relay nodes. For example horizontally partition it into two zones A1 and A2. Then vertically partition zone A1to B1 and B2. After that, horizontally partition zone B2 into two zones. Such zone partitioning consecutively splits the smallest zone in an alternating horizontal and vertical manner. To call this partition process hierarchical zone partition. MLRT 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.

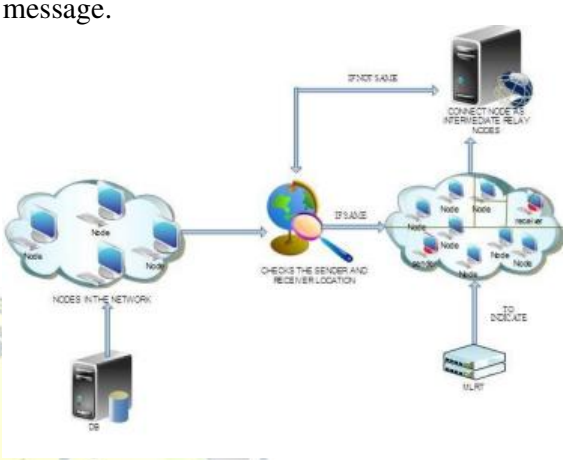


Fig-1: MLRT Protocol

Dynamic Pseudonym Module

A source node S sends a request to a destination node D and the destination responds with data. A transmission session is the time period that S and D interact with each other continuously until they break. Christo Ananth et al. [8] proposed a secure hash message authentication code. A secure hash message authentication code to avoid certificate revocation list checking is proposed for vehicular ad hoc networks (VANETs). The group signature scheme is widely used in VANETs for secure communication, the existing systems based on group signature scheme provides verification delay in certificate revocation list checking. In order to overcome this delay this paper uses a Hash message authentication code (HMAC). It is used to avoid time consuming CRL checking and it also ensures the integrity of messages. The Hash message authentication code and digital signature algorithm are used to make it more secure . In this scheme the group private keys are distributed by the roadside units (RSUs) and it also manages the

vehicles in a localized manner. Finally, cooperative message authentication is used among entities, in which each vehicle only needs to verify a small number of messages, thus greatly alleviating the authentication burden.

Specifically, keep the precision of time stamp to a certain extent, say 1 second, and randomize the digits within 1/10th. Hence, the pseudonyms cannot be easily reproduced.

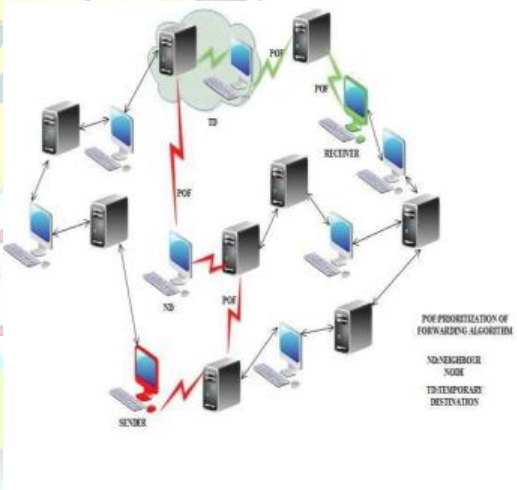
A node's pseudonym expires after a specific time period in order to prevent adversaries from associating the pseudonyms with nodes. If pseudonyms are changed too frequently, the routing may get perturbed; and if pseudonyms are changed too infrequently, the adversaries may associate pseudonyms with nodes across pseudonym changes. Therefore, the pseudonym change frequently should be appropriately determined.

Anonymity Protection Module

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 answered. Though MLRT 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.

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 instance, two nodes A and B communicate with each other at a time 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 the communication nodes is a way to counter timing attacks.



As shown in Figure 2,MLRT, the "notify and go" mechanism and the broadcasting in ZD both put the interaction between S-D into two sets of nodes to obfuscate intruders. More significantly, 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.

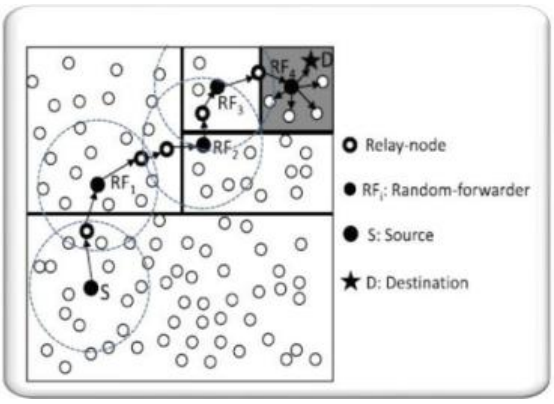
Fig-2: Message Sending and Receiving In Unknown Location

Random Forwarder Module

Given an S-D pair, the partition pattern in MLRT varies depending on the randomly selected TDs and the order of horizontal and vertical division, which provides a better anonymity protection. Figure 3, shows two possible routing paths for a packet packet issued by sender S targeting destination D in MLRT. There are also many other possible paths. In the upper routing flow, data source S first horizontally divides the area into two equal-size zones, A1 and A2, in order to separate S and ZD. S then randomly selects the first temporary destination TD1 in zone A1 where ZD resides. Then, S 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 TD1. This node is considered to be the first random- forwarder RF1. After RF1 receives a packet, it vertically divides the region A1 into regions B1 and B2 so that ZD and itself are separated in two different zones. Then, RF1 randomly selects the next temporary destination TD2 and uses GPSR to send packet to TD2. This procedure is repeated until a packet receiver finds itself residing in ZD, i.e., A partitioned zone is ZD has k nodes. Then, the node broadcasts the packet to the k nodes

4. CONCLUSION

Previous anonymous routing protocols, relying on either hop-by-hop encryption or redundant traffic, generate high cost. Also, some protocols are unable to provide a complete source, destination, and route anonymity protection. MLRT 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 make it difficult for an intruder to detect the two endpoints and nodes en route. A packet in MLRT includes the source and destination zones rather than their positions to provide anonymity protection to the source and the destination. MLRT 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, MLRT has an efficient solution to counter intersection attacks. MLRT's ability to fight against timing attacks is also analyzed.

5. REFERENCES

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

[2] X. Wu, J. Liu, X. Hong, and E. Bertino, "Anonymous Geo- Forwarding in MANETs through Location Cloaking," Oct(2008) IEEE Trans.Parallel and

Distributed Systems, vol. 19, no. 10, pp. 1297-1309.

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

[4] "ARM: Anonymous Routing Protocol for Mobile Ad hoc Networks,'' (2002)Stefaan Seys and Bart Preneel.

[5] Y. Xue, B. Li, and K. Nahrstedt, "A Scalable Location Management Scheme in Mobile Ad-Hoc Networks," (2001) technical report.

[6] K. El-Khatib, L. Korba, R. Song, and G. Yee, "Anonymous Secure Routing in Mobile Ad-Hoc Networks," (2003)Proc. Int'l Conf. Parallel Processing Workshops (ICPPW).

[7] .A. Pfitzmann,M.Hansen, T. Dresden, andU.Kiel,"Anonymity,Unlinkability, Unobservability, Pseudonymity, and Identity Managementa Consolidated Proposal for Terminology, Version 0.31,"technical report, (2005).

[8] Christo Ananth, M.Danya Priyadharshini, "A Secure Hash Message Authentication Code to avoid Certificate Revocation list Checking in Vehicular Adhoc networks", International Journal of Applied Engineering Research (IJAER), Volume 10, Special Issue 2, 2015,(1250-1254)

[9] Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," (2002).

[10] Proc. IEEE Workshop Mobile Computing Systems and Applications(WMCSA), T. Camp, J. Boleng, and V. Davies, "A Survey of Mobility Models for Ad Hoc Network Research," (2002) Wireless Communications and Mobile Computing, vol. 2, pp. 483-502.