MLRT: AN MYSTERIOUS LOCATION BASED EFFICIENT ROUTING PROTOCOL IN MANETS

Helensupriya M[1], Sebastin Christhu Raj A[2], Sharmila R[3]

[1] PG Scholar, Dept of CSE, SJCET, Tamilnadu, India
[2] PG Scholar, Dept of CSE, SJCET, Tamilnadu, India
[3] Assistant Professor, Dept of CSE, SJCET, Tamilnadu, India

Abstract

Mysterious Location-based Efficient Routing Protocol (MLRT) is an anonymous routing protocol its play a vital role in Mobile Ad hoc Networks (MANETs). MLRT provide a secure communication by hiding the node identities and preventing the traffic analysis attacks from outside observers in order to provide a mysterious protection. It dynamically partition the network into subzones till the sender and receiver are in different zones and the nodes in the zones are connected as intermediate relay nodes. It uses random relay node selection is difficult for intruder detection and dynamically generating an unpredictable routing path for a message. It maintains a time limit for message transmission due to security and control the time delay. MLRT offers mysterious protection to sources, destinations and routes. It achieves better route anonymity protection and lower cost compared to other anonymous routing protocols. It has a strategy to effectively solve the intersection attacks and avoid timing attacks because of its non-fixed routing paths for a source and destination pair. Also MLRT mainly works on Greedy Perimeter Stateless Routing (GPSR) algorithm.

.***Key Words:*** *Mysterious, routing protocol, mobile ad hoc networks, GPSR.*

---***---

1. INTRODUCTION

Rapid development of MANET can be used in a wide number of areas such as commerce, emergency services, military, education, and entertainment. MANET is a self-configuring network of mobile wireless devices. Devices in a MANET can move either independently or as groups in different directions. Therefore, network topology and links between devices change frequently. Each device may function as a relay and forward traffic destined for other devices. MANETs may operate autonomously or may be connected to other networks.

The existing anonymous routing protocols in MANETs can be mainly classified into two categories: hop-by-hop encryption [1] and redundant traffic [2] .Both the two techniques are generate high cost and cannot provide a mysterious protection to sources , destinations and routes. Hop-by-Hop encryption technique is based on public key for data encryption and decryption. Due to this redundant traffic technique heavy traffic will be occurred in large data transmission. Effects of the two techniques are no security, high cost and heavy traffic. In addition, many approaches cannot provide anonymity protections. For example ALARM [3] cannot protect the location anonymity of source and destination, SDDR [1] cannot provide route anonymity, and ZAP [4] only focuses on destination anonymity. To transfer the message from sender to receiver in a security way and offer a mysterious protection at a low cost propose a Mysterious Location-Based Efficient Routing Protocol (MLRT).

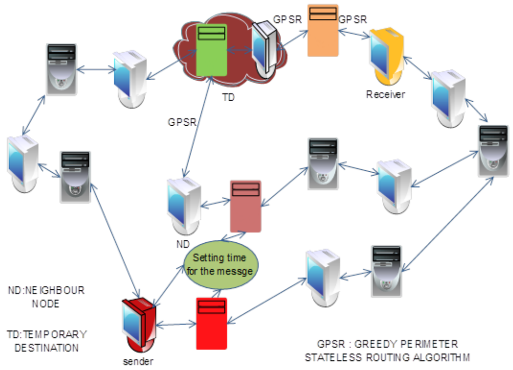
GPSR
GPSR
TD
Receiver
GPSR
ND
Setting time for the messge
ND:NEIGHBOUR NODE
TD:TEMPORARY DESTINATION
sender
GPSR : GREEDY PERIMETER STATELESS ROUTING ALGORITHM

Fig -1: System Architecture Design

The scope of the MLRT is that hide the node identities and routes from outside observers in order to provide the mysterious protection. It split the network into sub zones till the sender and the receiver are in different zones and nodes in the zones are connected as intermediate relay nodes which form a non-traceable anonymous route. Each node itself maintains a location server and randomly selects a node in the zones as temporary destination and transmits the message to a temporary destination that is closer to the destination achieved by GPSR algorithm. There is a time limit in the message transaction. The time limit will exceed message will expire due to security and control the time delay. MLRT offers full mysterious protection to sources, destinations and routes. It achieves better route mysterious protection and lower cost compared to other anonymous routing protocols. Also MLRT mainly works on Greedy Perimeter Stateless Routing (GPSR) [5] algorithm. MLRT is comparison with other anonymity and geographic routing protocols. In summary the contribution of this paper includes:

1. Mysterious routing. MLRT provide a route anonymity, identity, and location anonymity of source and destination.
2. Low cost, Instead of hop-by-hop encryption and redundant traffic, MLRT mainly uses randomized routing of one message copy to provide mysterious protection.
3. Resilience to intersection attacks and timing attacks. MLRT has a strategy to effectively solve counter inter-section attacks. MLRT can also avoid timing attacks because of its non-fixed routing paths for a source-destination pair.

2. METHODOLOGY

2.1 MLRT Routing Algorithm

All the nodes register in the database with particular IP address and registered successfully. The node registration is for to identify all the correct users in the database, and for the communication between the sender and the receiver, and also give the security to data and protect to the data transmission between the sender and the receiver. Node registration is using the node name, internet protocol address, port number and the node range for the security purpose. Above process is for unique identify and the malicious node should not attack the data in the source node. The registered nodes are shall with a range of 1 to 500 because in that range it divide the whole network into zones. And when the user enters the range according to the range the zone folder is created and inside the zone folder the nodes have been placed for the routing. Due to the process it can provide full security to the message and the message transmission between the nodes are safe and secure.

The MLRT routing in this paper it checks the sender and receiver location. If the sender and receiver are in the same zone means it will divide the zone into subzone due to protection from the malicious users. If not same means connected as an intermediate relay nodes. MLRT aim is sender and receiver should be in the different zone. If the zone of the sender and the receiver is zone2 means it will divide the zone into zone2.1 likewise it divide the zone into subzone.

2.2 Dynamic Pseudo Name

In MLRT pseudo name is generated in each node location server. The pseudonym is generated randomly in each node. Each node uses the dynamic pseudo name for node identification. To prevent an attacker from re-computing the pseudo name, the timestamp should be exact(e.g. nanoseconds).Considering the network delay, the attacker needs to compute, e.g.,10^5,times for one packet per node. There may also be many nodes for an attacker to listen, so the computing overhead is not acceptable, and the success rate is low. To further make it more difficult for an attacker to compute the timestamp, increase the computation complexity by using randomization for the timestamps. Specifically, keep the precise of timestamp to a certain extent, say 1 second, and randomize, The digits within 1/10th. Thus, the pseudonyms cannot be easily reproduced. Also, every node maintains a routing table that keeps it's neighbor's pseudonyms associated with their locations. Source node signs to intermediate node by the port number. If the IP address and the port number of the sending node are correct means the location server generate the pseudonym and send the pseudonym to the particular address of the sender. And the sender again resends the message with the pseudonym to the intermediate node and the intermediate node not able to see the data. And it acts as the random forwarder and sends the data to the temporary destination. The pseudonym is stored in the database and when the intermediate node send the pseudonym to the source node means the sent pseudonym is deleted in the database. And again that pseudonym will not be generated. The above process is for security and the malicious node cannot predict through which pseudonym the message is transmitted that's why it randomly generate the pseudonym that process is to enhance more security to the project and secure the data from the malicious attackers.

2.3 Location Server

In MLRT location servers play a significant role. Each node itself handles a location server. When a node moves it will periodically update its position to location server in the range of 1to500. Location servers maintain routing information and generate a dynamic pseudo name. In location server contains information about random forwarder and temporary destination zone.

2.4 Random Forwarder

The source node signs in the intermediate node by the port number and if the port number is correct the intermediate node sends the pseudonym name to the source node and the source node again signs in with the message with the pseudonym and select the random forwarder or the intermediate node through greedy perimeter stateless routing algorithm and selects the intermediate node through the distance and intermediate node acts as the random forwarder and repeat the same process and selects the temporary destination through greedy perimeter stateless routing algorithm and sends the message from the intermediate node to the temporary destination. In the temporary destination it selects the random forwarder through the greedy perimeter algorithm, which give high priority to the node which is nearer to the destination and the message is transmitted to that node and give high priority to node the process continues until the message reach the destination. Random forwarder node should be hiding from malicious attackers to achieve a security. The number of random forwarders determines the length of the routing path in MLRT.

3. SYSTEM IMPLEMENTATION

3.1 Mysterious Protection and Strategies against Attacks

3.1.1 Mysterious Protection

It tells about the mysterious protection from the malicious users and to protect the message from the attackers. In the Intersection attack the registered nodes for a node registered with IP address and its name and the port number that node is a valid node. The network node can be identified through the port number. Any unwanted malicious node with the different node name and the different IP address can be easily identified and it can prevent the message from the malicious users. In timing attacks going to set the time to the message source node set the message time for example say 1 second. It could get reply from its destination stating that received the message successfully. If the reply has not yet come after 1 second means it states that any malicious nodes attacks the message the message will automatically expire after 1 second to avoid the above type of attacks. If the malicious node attacks the message with the particular time means also the message should be drop that states that the malicious node attacking the message. In the case also the message should be dropped. It gives full security to the message.

4. PERFORMANCE AND OUTPUT

The Previous work was long time process. In this work developed using Java Swing. The Previous work caused long time transmission process but the system developed now has a very good user-friendly tool, which has a menu-based interface, graphical interface for the end user. In previous work every node separately maintains a location server. So the cost will be high. In propose every node itself maintain a location server. So the cost will be reduced.

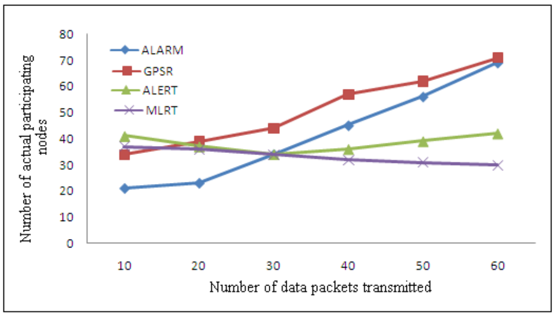

Fig -2: Different Types of Packets Transmitted

5. CONCLUSION

MLRT is distinguished by its low cost and mysterious protection for sources, destinations, and routes. It uses dynamic zone partitions and random relay node selections to make it difficult for an intruder to detect the two endpoints and nodes en route. In addition, MLRT has an efficient solution to counter intersection attacks and fight against with timing attacks. It includes implementing a Time to live (TTL) algorithm for security and control the time delay.

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,” Proc. Int’l Symp. Applications on Internet (SAINT), 2006.

[2]. J.Raymond, “Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems, ”Proc.Int’lWorkshop Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Un-Observability (WDIAU),pp.10-29,2001.

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

[4]. 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.

[5]. Ratnasamy, B. Karp, R.Govindan, D.Estrin, L.Yin, F.Yu and S.Shenker, “Data – Centric Storagein Sensor nets with GHT, a Geographic Hash Table, ”Mobile Network Applications, vol.8, no.4, pp.427-442,2003.

BIOGRAPHIES

Helensupriya M received the B.E degree in CSE stream at Parisutham Institute of Technology & Science in 2012. And pursuing M.E degree in CSE stream at St.Joseph’s College of Engg & tech, Thanjavur..Area of Interest is Mobile Computing.

Sebastin Christhu Raj A received the M.Sc degree in CS stream at Bharathidasan University in 2010. And pursuing M.E degree in CSE stream at St.Joseph’s College of Engg & tech, Thanjavur. He worked as a Production Engineer in OKAY SOFT & Devolepers Pvt.Ltd. Area of Interest is Mobile Computing.

Sharmla R received B.E. Degree in CSE stream at PREC, Thanjavur in 2006, and Done her M.E. Degree in Prist University in 2009, She is working as a Asst Prof in SJCET, Thanjavur. She Presented papers in National & International Conferences, and also Published some books.