Enhanced Perimeter Routing Protocol in Mobile Ad-Hoc Networks

Dhivya. T, Sumathy. S, Chinnadurai. S
M.E CSE II Year, M.E CSE II Year, Assistant Professor/CSE,
Srinivasan Engineering College, Tamilnadu, India.

***Abstract*-MANETs use anonymous routing protocols that hide node locations from outside attackers. This routing protocol mainly relies on hop-by-hop encryption mode. In order to transfer the messages from sender to receiver in a secured manner, a mysterious location based enhanced routing protocol for mobile ad-hoc networks is proposed. It splits the network into horizontal and vertical zones till the sender and the receiver are in different zones. The main aim is to hide the sender, receiver and their locations and transmit the message. The nodes in the zones are connected as intermediate relay nodes, in which each node maintains a location server. Then randomly selects a temporary destination in the zone and transmit the message to the node that is closer to the temporary destination. Second temporary destination is selected till the message resides in the receiver zone. There is a time limit in the message transaction from sender to receiver. Within the time limit the message should reside in the Receiver zone. Else the message will expire due to security and to control the time delay. Here the routing protocol mainly works on Greedy Perimeter Stateless Routing algorithm. This protocol gives full security for the messages compare to other routing protocol.**

***Key words*- anonymity protection, routing protocol, encryption.**

I. INTRODUCTION

RAPID application development of Mobile Ad Hoc Networks (MANETs) has imitated huge wireless applications that are used in vast areas such as, emergency services, military, education, and entertainment. MANET is an infrastructure less network, which makes a perfect choice for some important uses such as communication and information sharing. Nodes in MANETs are dangerous to malicious entities that aim to tamper and analyze data. Although anonymity protection may not be a requirement in civil related applications, it is vital in military applications for example communication between soldiers and commanders.

Anonymous routing protocols are essential thing in MANETs to provide insure communications by hiding the node identities and precluding traffic analysis attacks from attackers [2] [3]. Anonymity protection in MANETs involves identity and location anonymity of senders and receivers, also route anonymity. For route anonymity, resisters, either en route or out of the route, cannot trace a packet flow back to its source or destination, and no node has the information about real identities and locations of intermediate nodes. In order to separate the relationship between source and destination, it is important to form an anonymous pathway between the two endpoints and guarantee that nodes en route don't know where the endpoints are, especially in MANETs where Location devices may be outfitted.

In order to transfer messages from source to destination in secured manner and low cost, An Enhanced Perimeter Routing Protocol (EPRP) is proposed for MANETs. Hierarchical zone partition [5] is done in the network and nodes in the network zones are chosen as intermediate relay nodes, which forms non-traceable anonymous route. In each routing step, a data sender or receiver partitions the network field into number of sub zones in order to separate itself and the receiver node should be in two different zones. It then randomly chooses a node in the other zone as the next relay node. By using the [9] GPSR algorithm the shortest path between the sender and receiver node should be calculated.

II. METHODOLOGIES USED FOR ANONYMITY PROTECTION

A. GPSR PROTOCOL (Greedy Perimeter Stateless Routing):

```
N is the number of nodes.
U and v is the Sender and the Receiver
W is the midpoint between the Sender and the receiver
Step 1: for all v 2 N do
Step 2: for all w 2 N do
Step 3: if w == v then
continue
Step 4: else if d [(u;v)> max[d(ump,)d(vow)] then
Step 5 :( eliminate edge (u;v))
break
end if
end for
end for
```

Explanation

GPSR Algorithm is used to select the shortest way to the destination. For example node S send message to the node which nearer to the destination distance which act as the intermediate relay nodes. And it forward to the next node which is nearer to the destination which has higher priority based on its distance from the destination and finally the message transmitted the destination node D. This is process provides full security and no one can stole the data.

B. *TIME TO LIVE ALGORITHM:*

- Perform 30/α random walks of TTL value log (N).
- Perform pings to sampled peers and sort the latencies. Calculate latency threshold x which excludes 1 – α latencies.
- Locate and connect to any 1 / α peer with latency below the threshold (short links).
- Locate and connect to any 1 / α peer with latency over the threshold (long links).

Explanation

Assigning the [12] TTL value log (N) like 30/0.1 = 300. Let’s assume that parameter α is set to 0.1. Pings is a computer network administration utility used to test the reach ability of a host on an Internet Protocol (IP) network. Perform pings to sort the latencies, latencies means measure of time delay experienced in a system and limits the maximum rate that information can be transmitted. It connects randomly to 1 / α peer, all of which belong to Source peer. These links are called short links. It also connects randomly to 1 / α other peers, which do not belong to C. These are called long links.

III. RELATED WORK

In an existing system, the routing protocols in MANETs are mainly depends upon two methods: hop-by-hop encryption and redundant traffic. The hop-by-hop encryption technique uses public-key-based encryption. This encryption technique works on the principle of sending message from one hop to another hop through some routing devices like switches; routers etc. during the message transformation between each and every device a key will be generated, which is hidden to unauthorized user. In this encryption method there will be a possibility of high traffic generation which is drastically high cost.

Existing routing protocols in MANETs contain many approaches that fail to provide full anonymity protection. For instance, some protocol cannot protect the location anonymity of source and destination and few protocols cannot provide route anonymity [1], and only focuses on destination anonymity [2].

Limited resource is an inbuilt problem in MANETs, in which each node efforts under an energy constraint. The recent increasing growth of multimedia application imposes higher requirement of routing efficiency. Significantly it is high cost to implement. The protocols used in this system fails to provide complete security to the nodes. It is more complex work when compared to all other techniques.

IV. SYSTEM ARCHITECTURE

The system architecture of EPRP is shown in the following diagram. All the possible nodes should be registered with proper ip address.

Hierarchical zone partition is done. Then the source, destination and intermediate nodes are selected. All these nodes maintain the database which holds details of the nodes in network.

There are many ways to send the packet. The shortest path is calculated by using GPSR algorithm and then the message should be transferred the temporary destination first and then forward to the destination node through the random forwarder. Time to Leave algorithm is used to fix the time limit for the message which are going to be transferred.

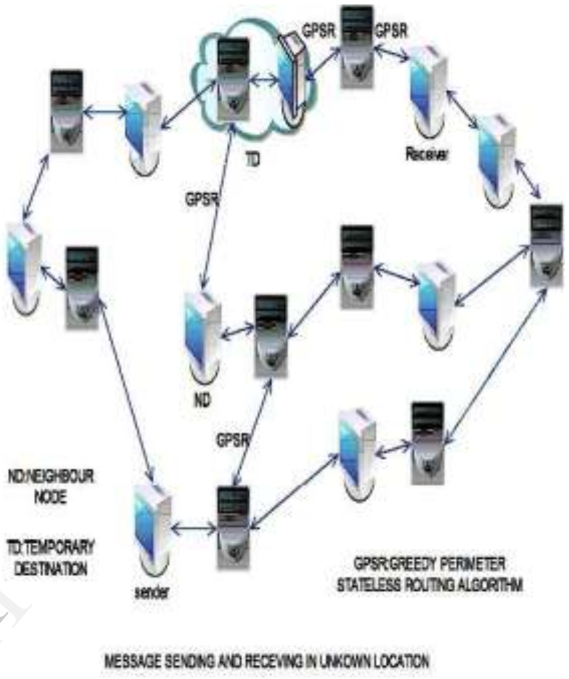
GPSR
GPSR
TD
Receiver
GPSR
ND
GPSR
ND:NEIGHBOUR NODE
TD:TEMPORARY DESTINATION
sender
GPSR:GREEDY PERIMETER STATELESS ROUTING ALGORITHM
MESSAGE SENDING AND RECEVING IN UNKOWN LOCATION

Fig. 1. System architecture

The above diagram shows that the message sending and receiving in the unknown location.

V. PROPOSED SYSTEM

The main aim EPRP is to send the data from source node to destination node through the intermediate relay node. The source and destination should be in different zones. First the data is forwarded to the nearest intermediate node and so on; then the data is broadcasted to k nodes in the receiver zone, providing k-anonymity to the destination. The EPRP protocol has a strategy to hide the data initiator among a number of initiators and also reinforce the anonymity protection of the source node.

A. *Contribution*

In this paper GPSR algorithm [9] is inured to find the shortest path between the source and destination node.

The two dominant factors in the scaling of a routing algorithm are:

- The rate of change of the topology.
- The number of routers in the routing domain.

The Time to leave algorithm [12] is used to set the expiration time for the message. If it crosses the time limit the message content also will be expired or discarded.

B. *Node Registration*

All nodes are registered in the database with particular ip address and the database should be maintained in secured manner. This process is used to identify all the correct users in the database. The communication path should be enabled between the sender and the receiver. It gives more security to the data and used to protect the data transmission between the sender and the receiver.

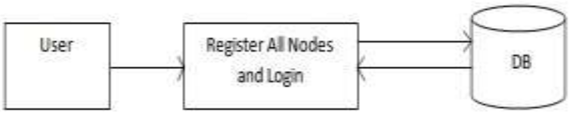

Fig. 2. Node registration

This diagram shows that the user has to register all the possible nodes with particular ip address. A mesh topology is created and weight is allotted for each and every path.

C. *The EPRP Routing*

The EPRP routing, if the source node and destination are in the same zone, divides the particular zone into subzone (hierarchical zone partition). This zone [3] partition is used to protect the node from the malicious users. In this module the nodes in the network checks for the location of sender and receiver. If the location is same, it divides the networks into horizontal and vertical zones. If not connect intermediate relay node is connected and then message is forwarded to the destination node.

Temporary relay node is selected. Through that temporary relay node the message is transferred to the destination node. In order to maintain security for the messages, it should be encrypted. Hence the attackers could not hack the messages which are going to send.

D. *Dynamic Pseudonym*

A source node S sends a request to a destination node D and the destination responds with data. In which, each node uses a dynamic pseudonym as its node identifier rather than using its valid MAC address [10], which can be used to mark out the node's existence in the network. Time stamp should be precise enough to prevent an attacker from recomputing the pseudonym.

In this module, the sender and receiver maintain the location severs. It stores the details of the node i.e. location address, port number and ip address of the node which are invisible to hackers. Timestamps are used to calculate the complexity. [11] If the pseudonyms are changed frequently, the routing may get disconcerted. Therefore, the frequent changes of the pseudonym should be determined appropriately.

E. *Anonymity Protection*

In this module intersection attack and timing attack are resolved. In an intersection attack, an attacker can determine the sources and destinations nodes which are communicate with each other. Intersection attacks are a familiar problem that has not been well resolved yet. Though offers k-anonymity to the destination D, an intersection attacker can identify D from frequent observations of node movement and communication.

In anonymity protection, the neighbour node checks for the expiration time of the message by using the TTL algorithm [10] [13]. If the current time of the message is lesser than the expiration time, the message is forwarded to the random forwarder. If not the particular message will be expired.

Avoiding the exhibition of interaction between communication nodes is a way to counter timing attacks. In EPRP, the "notify and go" mechanism put the interaction between S-D into two sets of nodes to obfuscate intruders.

F. *Random Forwarder*

Given an S-D pair, the partition pattern in varies depending on the randomly selected temporary destination (TDs). It shows that two possible routing paths for a packet issued by sender S targeting destination D in EPRP.

In this module the neighbour node checks for the shortest distance by using GPSR algorithm [9]. The node which has shortest distance will have higher priority. Then the packet is forwarded to the selected destination via temporary relay node.

VI. CONCLUSION

In this paper Time to leave algorithm [12] and GPSR protocol [9] is used to provide anonymity protection for the source, destination and route nodes in the MANET network. The EPRP protocol provides better anonymity protection for the nodes in the network when compared to all other protocols which are used. It reduces traffic and avoids collision between the nodes. Hence it resolves the timing attack and intersection attacks which are used in the previous works. The GPSR algorithm is used to find the shortest path between the source and destination nodes among various paths. It generates low cost due to the presence of hierarchical zone partition. Like other anonymity routing algorithms, EPRP is completely bulletproof to all attacks. The main work lies in reinforce EPRP in an attempt to stop the strong attackers and demonstrating comprehensive theoretical and simulation results.

ACKNOWLEDGMENTS

We would like to thank our college Srinivasan Engineering College, principal Dr.B.Karthikeyan, our HOD Mrs.S.Jayanthi, my guide Mr. S.Chinnadurai and other staff for their continuous support and for their helpful comments on the earlier drafts of this paper.

REFERENCES

1. A.R. Beresford and F. Stajano, "Mix Zones: User Privacy in Location-Aware Services," 2004.
2. K.E. Defrawy and G. Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs," 2007.
3. H. Frey and I. Stojmenovic, "On Delivery Guarantees of Face and Combined Greedy-Face Routing in Ad Hoc and Sensor Networks," Proc. ACM MobiCom, 2006.
4. Haiying Shen and Lianyu Zhao, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs", June 2013.
5. Y.C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," 2002.

6. M.F. Mokbel, C.-Y. Chow, and W.G. Aref, “The New Casper: Query Processing for Location Services without Compromising Privacy,” 2006.
7. N.R.Potlapally, S. Ravi, A. Raghunathan, and N.K. Jha, “Analyzing the Energy Consumption of Security Protocols,” 2003.
8. Sk.Md.M. Rahman, M. Mambo, A. Inomata, and E. Okamoto, “An Anonymous On-Demand Position-Based Routing in Mobile Ad Hoc Networks,” 2006.
9. [9]S. Ratnasamy, B. Karp, S. Shenker, D. strin, R. Govindan, L. Yin,and F. Yu, “Data- Centric Storage in Sensornets with GHT, a Geographic Hash Table,” Mobile Network Applications, 2003.
10. L. Sweeney, “k-Anonymity: A Model for Protecting Privacy,” Int’l J. Uncertainty Fuzziness Knowledge-Based Systems, 2002.
11. X. Wu, “AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol,” July/Aug. 2005.
12. X. Wu, J. Liu, X. Hong, and E. Bertino, “Anonymous Geo-Forwarding in MANETs through Location Cloaking,” Oct.2008.
13. Y. Xue, B. Li, and K. Nahrstedt, “A Scalable Location Management Scheme in Mobile Ad-Hoc Networks,” technical report, 2001.