ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)

On 21st & 22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

Zone Partition Based Routing Protocol In MANET

M.Priya, S.Vasantmohan

PG Scholar, Department of Communication Systems, Mount Zion College of Engineering and technology, Pudukkottai Tamil Nadu, India

Department of Electronics and Communication Engineering, Mount Zion College of Engineering and technology, Pudukkottai, Tamil Nadu, India

ABSTRACT – Mobile ad hoc networks use anonymous routing protocol that hide sender receiver location and routes from outside attackers and also gives anonymity protection of wireless network. However, existing anonymous routing protocols mainly based on hop-by-hop encryption or redundant traffic, but it's generate high cost and cannot provide full anonymity protection. To offer high anonymity protection, we propose a zone partition based routing protocol. Zone partition based routing protocol dynamically partitions the entire network field into zones and randomly select nodes in zone as intermediate relay nodes, it's form a no traceable anonymous route. Zones contain nodes varies during packet transmissions, so outside observers cannot find packet transmission path. Unfortunately sometime outside observer find sender, receiver locations and route, so this project also proposed neighbor coverage based probabilistic rebroadcast protocol. This protocol correctly indentify attacker's node and preventing from outside attackers. These protocols offer high anonymity protection of entire wireless network. It also effectively prevents the intersection and timing attacks.

KEYWORDS- mobile ad hoc networks, anonymity routing protocol.

I.INTRODUCTION

Rapid development of Mobile Ad Hoc Networks (MANETs) has stimulated numerous wireless applications that can be used in a wide number of areas such as commerce, emergency services, military, education, and entertainment. 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. Anonymous routing protocols are crucial in MANETs to provide secure communications by hiding node identities and preventing traffic analysis attacks from outside observers. There exist hundreds of routing protocols for many different purposes. Mobile ad hoc routing protocols are very specialized in their task. There are two main characteristics to distinguish them. The first characteristic is when they gather their routing information. On one hand we have the proactive (table driven) protocols, which always try to have complete, up-to-date routing information. On the other hand we have the group of reactive (on demand) protocols, which only try to gather routing information when it is needed.

In November 2001 the MANET Working Group for routing of the Internet Engineering Task Force (IEFT) community published the first version of the AODV routing protocol (Ad hoc on demand Distance Vector).
Existing anonymity routing protocol in MANETs cannot protect source, destination location (2) and route from outside attackers. For example, ALARM [2] cannot protect the location anonymity of source and destination, ARM [5] addresses the problem of route anonymity, and ZAP [7] only focuses on destination anonymity.
In order to provide high anonymity protection (for sources, destination, and route) with low cost, we

proposed a zone partition based Routing protocol. Zone partition based routing protocol also protect the timing attacks and intersection attacks.

II.ZONE PARTITION BASED ROUTING ALGORITHM

Zone partition based routing protocol features a dynamic and unpredictable routing path, which consists of a number of dynamically determine intermediate relay nodes. The partition process is called the hierarchical zone partition.

Zone partition based routing protocol 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.

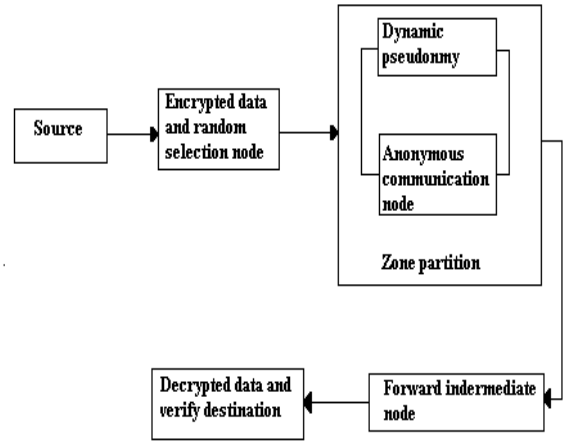

Figure .1 Block diagram

Zone partition based routing protocol offers identity and location anonymity of the source and destination, as well as route anonymity. Zone partition based routing protocol makes the route between an S-D pair difficult to discover by randomly and dynamically selecting the relay nodes.

The resultant different routes fort transmissions between a given S-D pair make it difficult for an intruder to observe a statistical pattern of transmission. This is because the RF set changes due to the random selection of RFs during the transmission of each packet. Even if an adversary detects all the nodes along a route once, this detection does not help it in finding the routes for subsequent transmissions between the same S-D pair.

PROJECT MODULES

1. Zone partition
2. Source node encryption
3. Attackers node identification
4. Packet transmission
5. Destination node decryption and verification

III.ZONE PARTITIONING

Zone partition based routing protocol features a dynamic and unpredictable routing path, which consists of a number of dynamically determined intermediate relay nodes. This protocol divided the whole network into number of zones. The zones contain number of nodes. The nodes vary different zones during data transmission. So the outside observer cannot easily identify the destination and source location. During packet transmission, any zone having attacker's node, that zone also divide the number of zones.

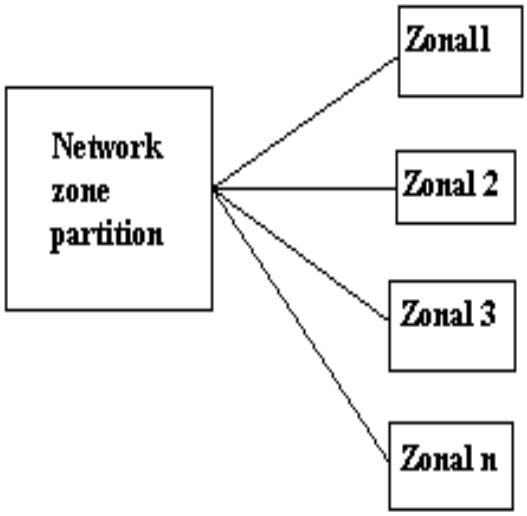

Figure.2 Zone partition

IV. TIMING ATTACKS:

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. 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.

V. NEIGHBOR COVERAGE BASED PROTOCOL

This protocol used to location verification of network. Neighbor coverage based protocol verifies the neighbor knowledge methods perform better than the area based ones. This protocol identifies the attacker's node and prevent from the outside attackers. First each node collects the information about neighbor nodes. The neighbor node estimate how many its neighbors have not been covered by the RREQ packet from source. And add the list. The every node sends the RREP to the source.

The attacker's nodes don't send the RREP packet to the source node. So the source node identified the attacker's node and also transmits the data packets very securely. This neighbor coverage knowledge based mechanism provides the high anonymity protection of sender, receiver location and packet transmitting route.

VI. PERFORMANCE ANALYSIS

This project has been a simulation using NS2 simulator version 2.34 to give anonymity protection of sender, receiver location and create non traceable anonymous route by using the zone partition based Routing protocol. These concepts implement the AODV routing protocol. This project also proposed the neighbor coverage based probabilistic rebroadcast protocol, this protocol improve the routing performance.

TABLE .1

Simulation Parameter	Value
Simulator	NS-2 (V2.34)
Linux os	Ubuntu 10.04
Number of nodes	100
Channel type	Wireless
Packet size	512 bytes

VII. SIMULATION RESULTS

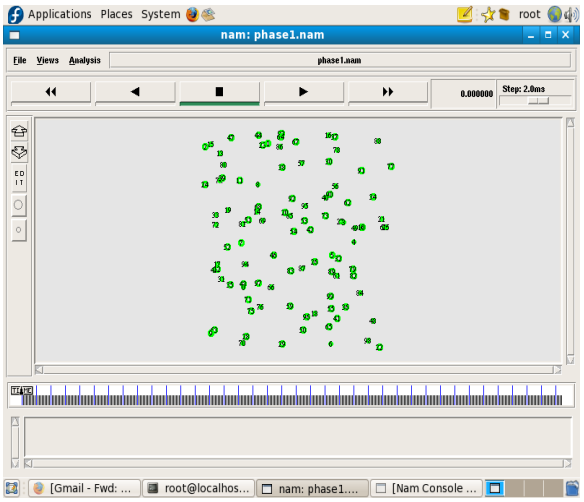

Figure.3 Topology creation

The 100 nodes present in the network. The 100 nodes have a location server. The location server gives the information of sender and receiver location.

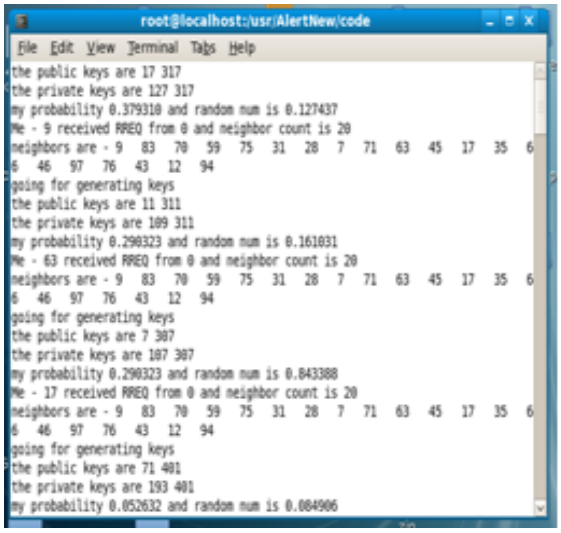

Figure.4 Zone partition

Zone partition based routing protocol consider the entire network field and divide the whole network into number of zones. The zone contain node numbers varies each packed transmission, so outside observers cannot easily identified the packet transmission path.

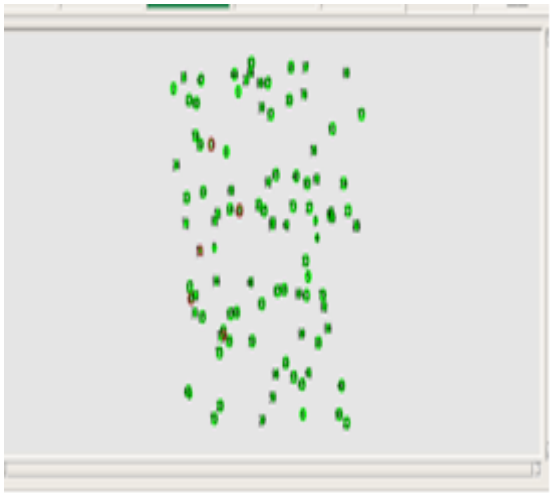

Figure.5 data forward node

The intermediate data forward node is called the random forward node or data forwarder node. The data forward node receive the route request from sender and route request send till the request reach receiver location .The receiver receive the route request and send the route reply to the sender.

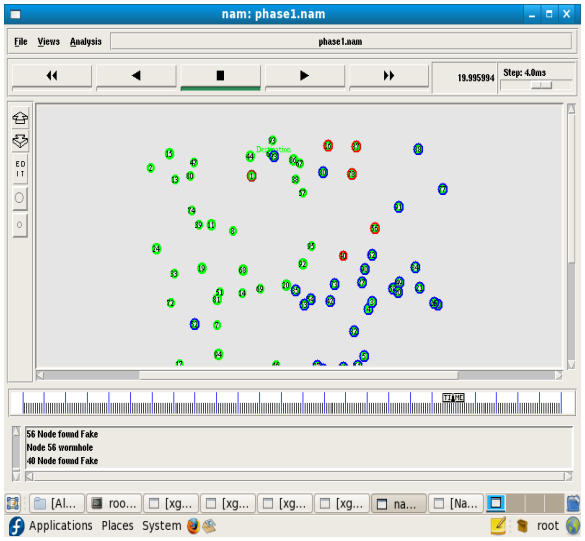

Figure.6 Attackers node identification

Neighbor coverage based routing protocol used to identify the attacker's node. The sender identify attackers node and safely transmit the data packets to the receiver. Blue circle represent the zone partition of nodes. Red circle represent the attackers node.

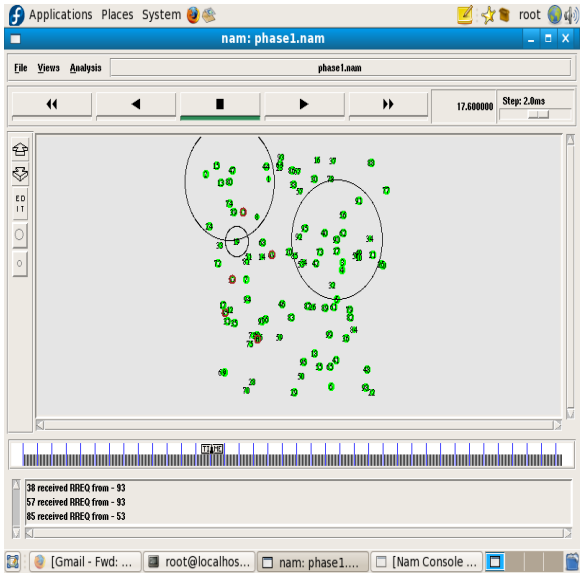

Figure.7 Packet transmission

The sender and receiver location correctly identified and the sender successfully sends data packets to the receiver.

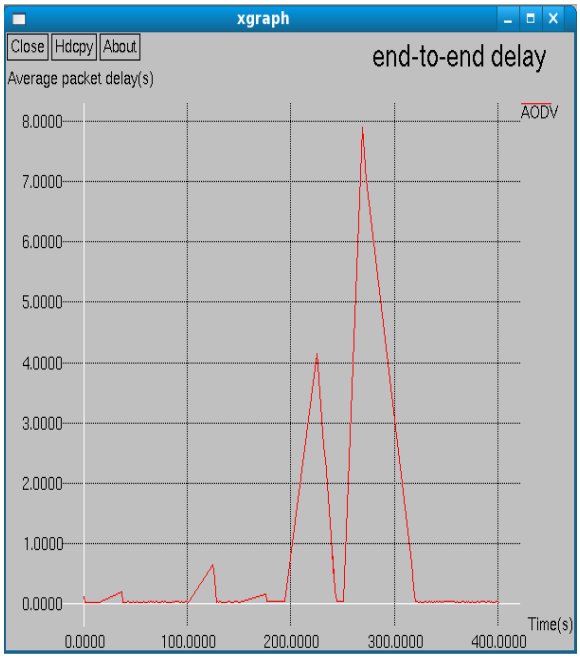

Figure.8 packet delay

The end –to-end average packet delay means the time taken by packets to be transmitted across a network from sender node to receiver node.

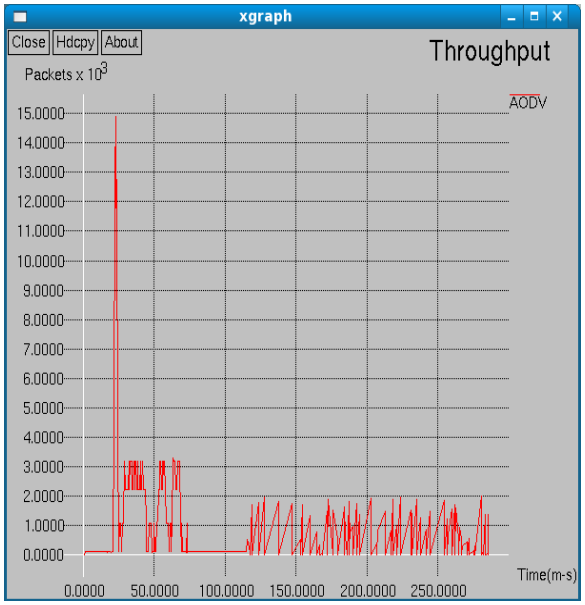

Figure.9 Throughput

Throughput means number of packets received per seconds.

VIII. CONCLUSION

Normally anonymous routing protocols, used 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. Proposed Zone partition based routing protocol gives anonymity protection for sources, destinations, and routes at low cost. The random relay node selections to make it difficult for an attacker to detect the routes. This routing protocol effectively prevent from timing attacks and intersection attacks. The proposed Neighbor coverage based protocol identified attackers node and safely send the packets. The neighbor coverage based protocol reduces the average end-to-end delay and reduce the traffic overhead. These protocols provide maximum protection of data transmitting path and sender, receiver location.

REFERENCES

[1] *.Ei Defrawy. K, Tsudik. G (2008) 'PRISM: Privacy- Friendly Routing in Suspicious MANETs', IEEE international networks protocols Conference*.

[2]. Karim El Defrawy and Gene Tsudik (2007) 'ALARM: Anonymous Location-Aided Routing in Suspicious MANETs', Published by School of Information and Computer Science University of California.

[3].Mizanur Rahman. MD, Atsuo Inomata.(2006) 'Anonymous On-Demand Position-based Routing in Mobile Ad-Hoc Networks', IPSJ Digital Courier, Regular paper, Vol. 2.

[4].Neerja Khatre and Arvind kumar (1012), 'Analysing Performance of AODV Routing Protocol in MANET Networks:A survey' International Journal of Engineering Research and Technology,Vol-3,pp.1-5

[5] Stefaan Seys and Bart Preneel, Leuven. K (2005) 'Anonymous Routing Protocol for Mobile Ad Hoc Networks', Interdisciplinary institute for Broadband Technology.

[6].*Wysocki.T,Abolhasan.M and Alamri.H (2009) 'On Optimising Route Discovery in Absence of Previous Route information in MANET' Proceeding of IEEE VTC Spring pp. 1-5*.

[7] *Xiaoxin Wu, Jun Liu. (2008) 'Anonymous Geo- forwarding in MANETs through Location Cloaking', IEEE transactions on parallel and distributed systems, Vol. 19, no.4, pp. 335-348*.

[8]. Zhi.Z and Choong.Y (2005) 'Anonymous geographic ad hoc routing', Proceedings third workshop mobile distributed computing.

[9].*Zhang.X.M, Wang.E.B and Xia.J.J (2011) 'An Estimated Distance Based Routing Protocol for MANET' IEEE transaction on vehicular technology, vol. 60, no -7, pp: 3473-3844*

[10].*Zhang.X.M, Wang.E.B and Sung.D.K (2013) 'Neighbor Coverage Based Probabilistic Rebroadcast for Reducing Routing overhead in MANET', IEEE transactions on mobile computing, vol.12, no.3.*