International Journal For Technological Research In Engineering
Volume 1, Issue 10, June-2014 *ISSN (Online): 2347 - 4718*

IDENTITY AND LOCATION HIDING EFFICIENT ROUTING PROTOCOL IN WIRELESS NETWORKS

Sandeep Batageri[1], Mrs. Shruthi T V[2](Assi Prof)
Information Science and Engineering
East West Institute of Technology
Bangalore, India

Abstract- Mobile ad hoc networks are one of the emerging fields for research and development of wireless networks. due to the popularity of mobile device and wireless networks significantly increased over the past years, wireless ad-hoc networks has now become one of the active field of network communication. One of the most important challenge in mobile ad hoc network is providing security to the data. In order to provide security, the location and identity of the nodes are hidden. The existing protocols are based on the hop-by-hop encryption and redundant traffic. These protocols cannot provide full anonymity protection to the source, destinations and also involves more overhead. To overcome these limitations, identity and location hiding routing protocol is proposed. It will provide full anonymity protection to the source, route and destination at a low cost and also involves less overhead. Initially, it will divide the network into zones and selects the intermediate nodes as realy node and random forwarder to send the data to the destination. It uses certain mechanism to hide the source and destination among many nodes in the network. When data reaches to the destination zone, the data is broadcast to the remaining nodes in the destination to protect the destination node. Attacks such as timing attacks and counter inter section attacks can be solved by using this proposed system.

Keywords- Mobile ad hoc networks, pseudonym, GPSR, Location server.

I. INTRODUCTION

Mobile ad hoc networks (MANETs) have received increasing attention in recent years due to their mobility feature, dynamic topology, and ease of deployment. A mobile ad hoc network is a self-organized wireless network which consists of mobile devices, such as laptops, cell phones, and Personal Digital Assistants (PDAs), which can freely move in the network. In addition to mobility, mobile devices cooperate and forward packets for each other to extend the limited wireless transmission range of each node by multi-hop relaying. The purpose of ad-hoc networks is to enable the mobile device users to share resources, provide services to each other or simply establish a network for communication and information exchange. Ad hoc networks have a number of applications where infrastructure free communication is required. These applications include emergency relief, military operations, on-demand conferencing and home networking. Like any communication network, the true potential of wireless ad hoc networks cannot be exploited without considering and adequately addressing the security issues. Security is one crucial requirement for these networks services. Implementing security is therefore of prime importance in such networks. Provisioning protected communications between mobile nodes in a hostile environment, in which an attacker can launch attacks to disrupt network security, is a primary concern. Anonymous routing protocols are important in MANETs to provide security to the data by hiding the node identity and location among the many nodes within the network. Anonymity in MANETs means the identity and location data sources (i.e. senders) and destinations (i.e. recipients), as well as route could not be exposed. "Identity and location hiding of sources and destinations" means it is hard for other nodes to obtain the real identities and exact locations of the sources and destinations. For route anonymity, for each step in routing, the protocol will go to take the different path. So that if one of the node compromises means, it will not going to affect the routing path. Due to the concept of unobservability and unlinkability the nodes in the network only knows its succeeding node and preceding node.

II. LITERATURE SURVEY

The existing protocols are based on the hop-by-encryption and redundant traffic. These protocols could not provide protection to the source and destinations at a low cost and uses public key cryptography. Due to the usage of public key cryptography, each node must know the key to encrypt and decrypt the data as a result delay increases. For example, consider existing protocol ALARM which cannot protect the both source and destination. In hop by hop encryption, the packet sent by the source node is encrypted at each layer in order to protect the data from the attacker. The routing protocols are either proactive or reactive. Some of existing protocols are proactive so that network lifetime also decreases. All these hop by hop encryption methods generate high cost due to the public key cryptography. ALARM is a proactive routing protocol in which each node broadcast its location information to the neighboring authenticated nodes. After that it can build a routing map, this map can leaks the destination node location so that route anonymity can be compromised.Redundant traffic based routing schemes uses the local broadcasting, flooding and multicast. Some of the protocol uses the flooding technique to protect the destination by creating the tree using some of the nodes in the network. Existing protocol such as ZAP uses local broadcasting to protect destination but it does not protect the

source as well as route. One of the main disadvantages of the redundant traffic is that it provides anonymity protection at a high cost.

III. PROPOSED SYSTEM

A. Design Goals

We intend to design a routing protocol which can protect the privacy of source node, destination node and routes. We define the expected goals or properties that we want to achieve are as follows:

1) Ensure Privacy

- Identity of nodes: Identity of nodes consists of the following requirements: (i) The real identities of source node and destination node along with remaining nodes are kept secret in order to provide security (ii) The source and the destination have no information about the real identities of intermediate nodes along the route.
- Location of source and destination: Location Privacy consists of the following requirements: (i) no one knows the exact location of the source or the destination, except themselves.
- Route Anonymity: Route Anonymity can be achieved because each time the chosen path will be different for sending the data from source to destination. Suppose the attacker compromises the particular route then routing path between source node and destination node changes to protect route anonymity.

2) Ensure Security: The protocol can protect the necessary functionalities, such as discover and maintain the route, from various types of attacks.

B. Dynamic Pseudonym and Location server

Position-based routing algorithms for ad hoc networks have been widely used recently. Recently along with node IDs, the additional information such as nodes position is also used for sending the data from source to destination. Suppose two nodes are in the same position then routing is performed based on their nodes IDs. In such cases, the nodes in the same position have the unique IDs and also routing is done based on their IDs, if necessary means position of the node can be revealed. If an adversary cannot match a position to a node ID correctly, node anonymity can be achieved.

The given pseudonym for a particular node for a particular communication session time should be less in order to prevent the attacker to computed the pseudonym. if the communication session time is less. There may also be many nodes for an attacker to listen, so that computing overhead is more and the success rate is low. Each node in the network piggybacks its location and pseudonym information to the neighboring nodes using "HELLO" messages. Each node maintains a routing table which holds the location and pseudonym information about the nodes. Each node has a location server. When a node A wants to know the location information and public key of another node B, it will sign the request containing B‟s identity using its own identity. Then, the location server of A will return an encrypted position of B and its public key, which can be decrypted by A using the pre distributed shared key between A and its location server. When node A moves, it will also periodically update its position to its location server. Sometimes more than one location server is used to increase the reliability. If one of the location servers fails, then nodes can access the data using another location server.

C. Routing Algorithm

The proposed system uses the two important routing algorithms:

- GPSR routing algorithm
- ALERT routing algorithm

Mobile ad hoc networks consist of autonomous mobile nodes. The main routing problem in mobile ad hoc network is finding the efficient path from source to destination. The nodes in the mobile networks are continuously moving so that topology of the network changes. In such a situation finding an efficient path becomes an challenge and to find such efficient route in such networks requires routing algorithm. This algorithm finds the new route from source to destination and breaks existing (old) route as the topology of the network changes.The GPSR algorithm is used for sending the

data from source to destination. The main purpose of using GPSR algorithm is that it will send the data to the node that is nearest to the destination. So that each time when network is divided, the node uses the GPSR algorithm to send data to the next node that is nearest to the destination within that zone.

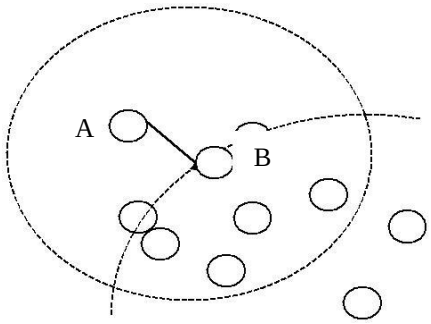


Fig 1 Example for GPSR algorithm

Consider the above figure. In which node „A‟ is called as source node, „B‟ is called neighboring node and „D‟ is called as destination node. Suppose node „A‟ wants to send data to the destination node „D‟. at that time, the node „A‟ send data to the neighboring node „B‟ within their transmission range, Because the node „B‟ is nearest to the destination node „D‟. After that node „B‟ send data to another node within its transmission range. This process continues until the data reaches to the destination node.Anonymous Efficient Routing Protocol uses dynamic Hierarchical Zone Partition. It dynamically partitions a network field into zones either horizontally or vertically and randomly chooses nodes in zone as intermediate relay nodes. This intermediate relay

node forms non traceable anonymous route. Consider the figure 2 which shows the rectangular network area in which S represents the source and D represents the destination. For sending the data from source to destination we have to divide the network in to zones in the following manner.

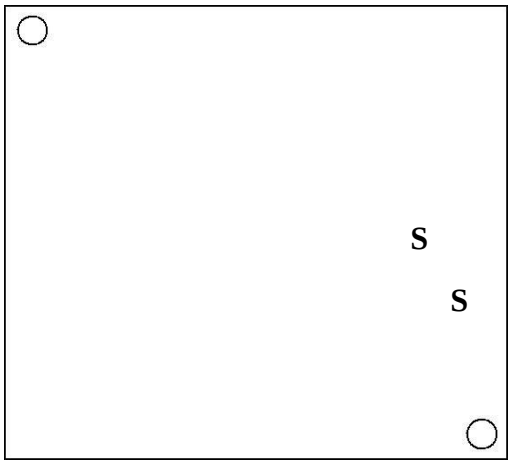


Fig 2 Network with source and destination

According to the GPSR algorithm it chooses the node that is nearest to the destination as shown in Figure 2. The given area is horizontally partitioned into two zones X and Y. We then vertically partition zone X to X1 and X2. After that, we horizontally partition zone X2 into two smaller zones such as X3 and X4. This type of zone partitioning consecutively splits the smallest zone in an alternating vertical and horizontal manner. This partition process is known as hierarchical zone partition. ALERT uses the hierarchical zone partition. In each step, it randomly chooses a node in the partitioned zone as an intermediate relay node which is called data forwarder, thus dynamically generating an unpredictable routing path for a message. The zone with k nodes where D exists is called as the destination zone which is denoted as Z_D. K is used to control the degree of anonymity protection for the destination.

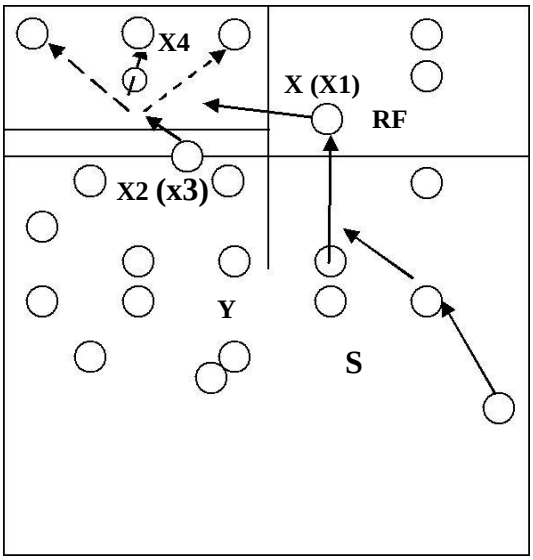


Fig 3 Example for Zone Partition

Considering the figure 3 in which S is denoted as source node and D is denoted as destination. For sending the data from source to destination, the network is initially divided in to two zones. In the diagram, initially the network is divided in to X and Y zones, then source node sends data to the first relay node, then it in turn sends the data to the second relay node. Then it will send the data to the next intermediate node called as random forwarder (RF). Then this random forwarder checks whether itself and destination are in the same zone, it will going to divide the network once again either vertically or horizontally. In this case, the first random forwarder sends the data to the next node, this process continues until the data reaches to the destination zone. When the data reaches to the destination zone, it will broadcast the data to the remaining nodes in the destination zone. When the data reaches to the destination zone x4, it will broadcast the data.

The nodes that are involved during transmission of data from source to destination are:

Source node: The node starts sending the data to the destination

Destination node: The node going to receive the data from the source node.

Relay node: The node that is going to receive the data within the same zone.

Random forward: The node that is going to receive the data in different zone.

Finally data broadcast to the remaining nodes in the destination zone.

D. Destination Position and Anonymity

The node checks itself and destination are in the same zone. if so, it will going to divide the network in to zones. After dividing the network into number of zones, finally the destination zone is created. The zones are created either horizontally or vertically based on the position of the destination node. Once the data reaches to the destination zone, it will broadcast data to that zone. Once the data broadcast to the destination zone, the destination verifies and accepts the data. The number of nodes in the destination zone indicates the degree of anonymity protection. If the attacker wants to know the destination node, it should check all other nodes in the destination zone. to do this one it consumes the time so that it is difficult for an attacker to know the correct destination within a short period of time. As the number of nodes in the destination zone increases the degree of anonymity is also increases.

IV. RESULTS

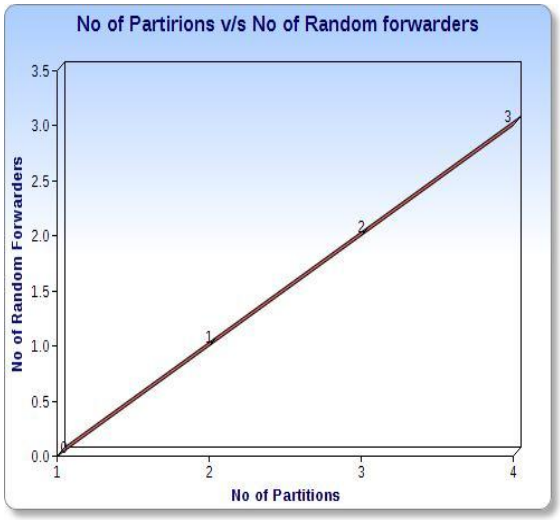
By using the following metrics to evaluate the routing performance in terms of effectiveness on Anonymity protection and efficiency:

A. The number of participating nodes: The total number nodes include during the transmission of data from source node to destination node. They are

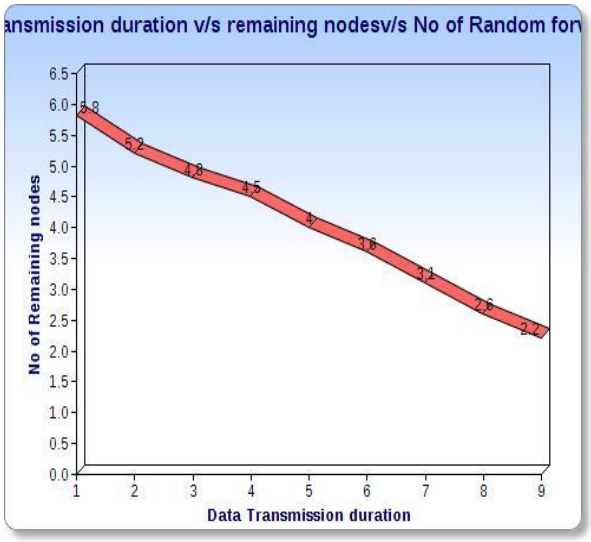
- Source Node
- Destination Node

- Relay Node
- Random Forward

B. The number of random forwarders: The Intermediate nodes are selected as random forwarders, when the data is sending from one zone to another zone. The number of random forwarders increases as the number of partitions increases. Random forwarder is going to select whenever the new partition is created. Suppose two zones are created then only one random forward is selected. Similarly, when three zones are created then two random forwarders are selected.



C. Destination Anonymity Protection: Destination anonymity Protection is depends on the number of nodes remaining in the destination zone. If more number of nodes are present in the destination then anonymity protection is high. Initially the number of nodes in the destination has high density so that they are closely connected so that nodes are normally not moved from that zone. As the time goes density decreases so that nodes moves from that zone as a result destination zone contains less number of nodes so that destination anonymity protection decreases.



D. Network Delay: From the graph, we come to know that ALARM has slightly more delay when compared to the ALERT because In ALARM, Public key cryptography is used so that for sending the data from one node to another node we require to encrypt and decrypt the data using public keys so that the delay increases, in case of ALERT there is no use of public key cryptography so that delay is less when compared to the ALARM even though it is taking longest path during the transmission.

V. CONCLUSION

Existing anonymous routing protocols are based on the either hop by hop encryption or redundant traffic. These protocols cannot provide full protection to the source, destination as well as route and these protocols produces high cost in order to provide anonymity protection. The proposed protocol provides anonymity protection to source, destination as well as to route at a low cost without involving more overhead by dividing the network into zones. After creating the zones, intermediate nodes are selected as relay node and random forwarder. The relay node is selected when the sending node and receiving node are in the same zone. Similarly the random forwarder is selected when sending node and receiving node are in different zone. When data reaches to the destination data will be broadcasted. The number of nodes in destination zone indicated the degree of anonymity protection to the destination node. This protocol is a good solution for the certain types of attack such as timing attacks and counter inters section attacks.

REFERENCES

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

[2] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On Demand Routing Protocol for Ad Hoc Networks," Wireless Networks,vol. 11, pp. 21-38, 2005.

[3] 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.

[4] B. Zhu, Z. Wan, M.S. Kankanhalli, F. Bao, and R.H. Deng, "Anonymous Secure Routing in Mobile Ad-Hoc Networks," Local Computer Networks (LCN),2004.

[5] T. Camp, J. Boleng, and V. Davies, "A Survey of Mobility Models for Ad Hoc Network Research," Wireless Communications and Mobile Computing,vol. 2, pp. 483-502, 2002.

[6] J. Kong, X. Hong, and M. Gerla, "ANODR: Anonymous onDemand Routing Protocol with Untraceable Routes for MobileAd-Hoc Networks,"Proc. ACM MobiHoc,pp. 291-302, 2003.

