SECURE NEIGHBOUR VERIFICATION AND TRANSMISSION USING RTA ROUTING IN MANET

ANANDHI.A, DHIVYA.G, KALAIVANI.R, KESHAVARTHINI.P

***Abstract*: Anonymous attacks are one of the approaching threats in open source networks. The approaches based on frequency face a storm when the number of data transferred from source to destination is not constant. The TOA (Time of Arrival) fails in examining the exact location of the attacker. The new approach of RADR (Random Distance aware Routing) is a counter measure to the spoofing and a methodology to overcome the drawbacks of the existing frequency based approaches. TESLA broadcast protocol is used to ensure source authentication. Messages generated by the node are signed using its identity key, and it can be verified by any node who knows the user's public key via its certificate.**

In this situation TESLA certificates can be very useful to protect the anonymous user which is computationally much more efficient.

Index terms- Anonymous communication, MANET, RADR, TESLA.

I. INTRODUCTION

The Adhoc network is collection of nodes, devices and forms a temporary network without any centralized administration. The information can be exchanged in a network through mobile and wireless medium, without need of external support. Such a type of network called ad hoc network. The Adhoc network is infrastructures network in which routers and host does have fixed. This network connected by wireless link. The nodes which are present in the network are capable of movement and can be connected dynamically in an arbitrary manner. The Adhoc network is limited transmissions range, limited energy and computing the resources. The ad hoc network function is address allocation; authentication or authorization must be designed with volatile network topology.

The Manet is a type of wireless ad hoc network on top of a link layer network. The mobile ad hoc network is a continuously and self configuring network which can be arrange or ordered as to fit for a detonated task. It is also self-maintained for network flexibility. The routers are freely to move and organize themselves. The mobile ad hoc network may change dynamically and unpredictably. So it may operate in a standalone fashion.

***ANANDHI.A**, Computer science and engineering, Christ college of engineering and technology, Puducherry, India. **DHIVYA.G**, Computer science and engine ering , Chr ist college of engineering and technology, Puducherry, India.*

***KALAIVANI.R**, Computer science and engineering, Christ college of engineering and technology, Puducherry, India.*
***KESHAVARTHINI.P**, Computer science and engineering, Christ college of engineering and technology, Puducherry, India.*

The nodes or device present in Manet can move independently and change its link to so other devices frequently. The node is willing to forward the data to other nodes. The nature of Manet operation is routing the packets and security issues and host configuration. The mobile ad hoc network consists of many nodes, in which the nodes can join or leave the network at anytime and anywhere without the need of permission because it is decentralized architecture. The Manet need efficient distributed algorithm to determine the network organization and its routing. The mobile IP technology is used to support for nomadic host that can be said to be roaming, which may be connected through internet or other fixed address space.

The Manet also performs the switch function such as router. The network can be controlled by distribute among the terminal. The data packets can be delivered from source to destination through 1 or more intermediate nodes. The main aim of Manet is used to provide authentication for anonymous users providing a complete secure routing process. To ensure all suspicious nodes does not infer in the routing process, and to providing lesser false positive rates. Thus we have to provide a complete secure routing process, the rest of the paper is organized as follows; the introduction is followed by the literature survey in section II. Section III describes the existing mechanisms for transmission. Section IV consists of our proposed system with its explanation and advantages followed by conclusion in section V.

II.LITERATURE SURVEY

[1]ALARM allows the node to communicate in a secure path and it provides a safe transmission of data over the node. It also provide the privacy, authentication for each node and it protect form both active and passive attackers. To provide these facilities they handled a method which is a cryptographic technique which is nothing but a group signature. This provides privacy features which can be viewed by a traditional public key signature. This method can be even applicable even in large and in dynamic groups. They can be viewed by a constant-size group public key. It accepts the node into the

ISSN: 2278 – 1323

group only if it is a valid group member. It uses the one time certificate to generate a group signature. [2]In Manet radio communication the traffic analysis is more so we introduce a concept of MASK. It produces an effective communication in traffic analysis even in attacks. It allows the node to communicate by either providing the network layer address or Mac address it node not release its id to communicate. It takes care of routing and packet forwarding. The route for anonymous node is chosen by shared link identifier it was identified by neighborhood authentication. [3]The Manet used in high risk areas whereas in military or law enforcement. Due to this we provide more security to those application areas by providing privacy by constructing on-demand location –based anonymous MANET routing protocol. In this technique it provides the data from attackers and the data transmission between the nodes will be effective. It provides privacy to information rather than to secure them from attack so that the information can't be attacked by any attackers easily. [4]It provides anonymous communication even in the traffic analysis. It is used to establish anonymous communication. It helps to establish connection between the source and destination to be in anonymous. The network connection in onion routing is strongly bounded. It is accessed by a series of proxies. The proxies are used to convert the message format to a generic format it can pass through in onion routing. It is based on connection based services. Onion routers take care of the packet till it being failed or it moves out of the node. Onion proxy itself can accept or reject the request by protocol, destination host, destination port or identify the application proxy. If it reject the request it appropriate error of the application proxy.**[5]** MASK can perform both the Mac layer and network layer communication. It work in dynamic pseudonymous that static Mac and network address. It can able to perform in sender and receiver anonymity as well as sender receiver relationship anonymity. It provides node unlocatability and intractability. It provides high routing efficiency. It network model is to achieve a single hop Mac layer communication. It always choose the short path for packet forwarding rather than the best path.[6]It is an attack in traffic analysis which interrupts the routing messages and data packets. It also trace the node location and attack the packets to overcome these problem ANODR is used. It is used to eject the ad-hoc routing. It prevents from attacks of packets from source and destination for location privacy. It is based on broadcast with trapdoor information. It avoids using public key cryptosystem

III EXISTING WORK

In existing the paper introduce a concept of group signature, whenever the source send packets at that time the node id and its group should to added and send to all corresponding path. They are used on demand ad hoc routing protocol. There are 3 processes to implement that concept. Initially they the source node will broadcast the route request message to all node present in the network.

The second process the source node will send packets to the destination as it predetermined path. The intermediate node check at each packet receiving time whether the node have id and update the information in the forwarding table. This will be continuing until it will reach the destination. The third process the destination after receiving that request then automatically the destination sends the route response message to the source node as it receives the same path.

The source will receive the route response message from destination its starts send the packet. While sending packets each node will be updating the information to the routing and forwarding table

The anonymous communication is mainly introduced for anonymous users. The third party comes to the network means they have a permission to use the resources.

Adversaries and Attack Models

The attack models can be classified into various types. If the attackers present in the network they know all information about the circuit in the private/public key. Suppose if the attacker present in outside the network the does not know the information about the keys.

Passive attack:

The passive attack contains intruder but does not able to modify the original message .it will be monitoring on the transmission. They are types of attack release of message contain that can be view the dat. And traffic analyses based on frequency and length we can detected the data

Active attack:

The active attacks are easily detecting the message and modify the message as our wish and add contents for that old message. We can able to delete that message based on denial of service

Network Assumptions

Public Key Infrastructure

Each node present in the network contains a public/private keys by using the node will provide authority certificate and for secure routing process

Group Signature

Each node contains private or public keys. The group head provide the certificate for those keys. It is dynamic management system so it works under the control of administration. This type of network is suitable for ad hoc networks

Storage model:

Destination Table

The destination table contains all the information about the source ie the node id and its key and other information about the node. Source and destination us the symmetric key that can be securely store the data.

Neighborhood Table

The each node in the network can exchanges the information to its neighbors they can generate pseudonyms for communication purpose with other neighbors

Routing Table

ISSN: 2278 – 1323

The route table maintains the routing information about the source, intermediate, destination. They are route request/respond message. When a node generates or forwards a route request, a new entry will be created in its routing table, which stores the request's pseudonym and the secret verification message in this route discovery. The name for that entry is pending. After it received the entry will updated and is active.

Forwarding Table

The forwarding table records the switching information of an established route. In each entry of the forwarding table, the route pseudonym is generated by the destination node, while the node pseudonyms of the previous and next hop are obtained after processing the related RREQ and RREP packets.

IV OUR PROPOSED CONCEPT

In this project to provide a complete secure routing path that means providing TESLA certificate for each node present in circuit. Each node will communicate with certified node only. So easily we can easily identify the attacker. The TESLA certificate First create an array for storing information about each node, in the routing process the tesla certificate number does not repeat. There are 4 fields we take for each node. The parameters are Node id, Broadcast message count, Request/Reply message, Drop msg. If any nodes have null value means that node can't be added to circuit. For attacker we itself generate NULL value, to check whether it is reject the node or not for checking process. Then start communicating and data transfer (certificate sharing).

The TESLA broadcast authentication protocol represents a fundamental paradigm shift in source authentication in a group setting. TESLA divides the time of transmission by the source into n intervals of equal duration

Point-based methods return an estimated point as a localization result. In RADR, during the off line phase, a mobile transmitter with known position broadcasts beacons periodically, and the RSS readings are measured at a set of landmarks. Collecting together the averaged RSS readings from each of the landmarks for a set of known locations provides a radio map. At runtime the value of source node compared with the radio map.

By using RADR algorithm we can calculate distance from source to all nodes. The communication is done based on distance, if the attacker steal the near node id means the source wrongly send data to that attacker. Based on distance we can identify the fault packets.

Compute the sender node's location with respect to the co-ordinates. Compute the location of the receiver (Self Known).Calculate the distance between source and destination using the co-ordinate positions of both the source and destination. Store the difference in distance of the request packet in a localization table.

For every "i" in "n" cycle of data transfer, check if the data is arriving from the same destination (based on distance).If any of the data is occurring from a different localization value then drop the packet and terminate the connection. There are 4 modules:

PROVIDING TESLA CERTIFICATE

There are 4 fields we take for each node. The parameters are Node id, Broadcast message count, Request/Reply message, Drop message. Components present in tesla. Node id-node id should be mentioned. Number of broadcast-how many nodes will be broadcasted. Request /reply message-if the request is 6 the reply will get at least 5 then it is good node. Drop-the node will be joined another group means, the node drop will be less when compare to the whole group drop. If any nodes have null value means that node can't be added to circuit. For attacker we itself generate NULL value, to check whether it is reject the node or not for checking process. Then start communicating and transferring the data (certificate sharing)

AUTHENTICATIONAND COMMUNICATION

Create another array ie communication array that contains node id, no of certificate share with other node. Intermediate node should maintain how many times the node will hold that certificate. TESLA divides the time of transmission by the source into n intervals of equal duration

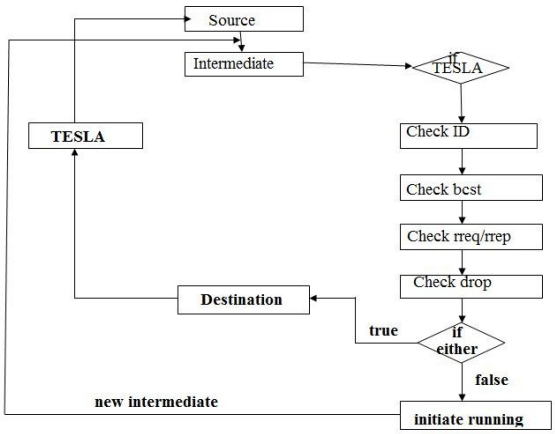

Fig 1.Authenticationand Communication

CALCULATING THE DISTANCE

Initially calculate the distance between sources to all intermediate nodes. By its longitudinal latitudinal positions it will calculate based on that the node will communicate with other node. If the attacker steals that information and its id means the source send wrongly to that attacker, based on distance we will decide that the node is attacker.

DISTANCE BASED COMMUNICATION

Compute the sender node's location with respect to the co-ordinates. Compute the location of the receiver (Self Known).Calculate the distance between source and destination using the co-ordinate positions of both the source and destination. Store the difference in distance of the request packet in a localization table.

For every "i" in "n" cycle of data transfer, check if the data is arriving from the same destination (based on distance).If any of the data is occurring from a

ISSN: 2278 – 1323

different localization value then drop the packet and terminate the connection.

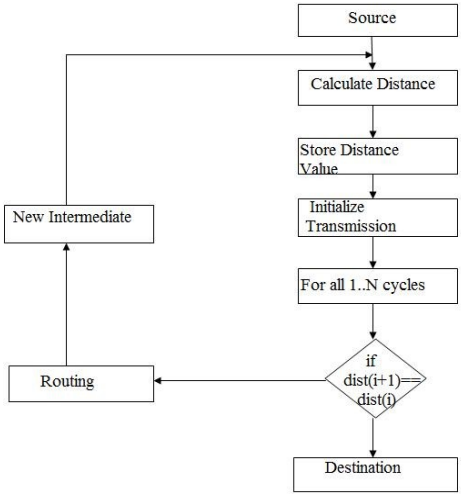

Fig 2. Distance based Communication

ADVANTAGES

To provide authentication for anonyms users
To provide a complete secure routing path To achieve lesser false positive rate (security)

V.CONCLUSION AND FUTURE ENHANCEMENT

In this paper, we design an authenticated and anonymous routing protocol for MANETs in adversarial environments. The route request packets are authenticated by TESLA certificate, which can defend the potential active anonymous attacks without unveiling the node identities AASR provides complete secure routing path and lower packets loss ratio in different mobile scenarios in the presence of adversary attacks. It also provides better support for the secure communications that are sensitive to packet loss ratio. In our future work, we will improve AASR to reduce the packet delay and to maintain security.

REFEERENCE

[1] K. E. Defray and G. Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs," *IEEE Trans. on Mobile Computing*, vol. 10, no. 9, pp. 1345–1358, Sept. 2011.

[2] Y. Zhang, W. Liu, and W. Lou, "Anonymous communications in mobile ad hoc networks," in *Proc. IEEE INFOCOM 2005*, vol. 3, Mar. 2005, pp.1940–1951.

[3] K. E. Defray and G. Tsudik, "Privacy-Preserving Location-Based On- Demand

Routing in MANETs," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 10, pp. 1926–1934, Dec. 2011.

[4] M. G. Reed, P. F. Syverson, and D. M. Goldschlag,

"Anonymous Connections and Onion Routing," *IEEE Journal on Selected Area in Comm.*, vol. 16, no. 4, pp. 482–494, May 1998.

[5] Y. Zhang, W. Liu, W. Lou, and Y. G. Fang, "MASK: Anonymous On-Demand Routing in Mobile Ad hoc Networks,"

IEEE Trans. on Wireless Comms., vol. 5, no. 9, pp. 2376–2386, Sept. 2006.

[6] J. Kong and X. Hong, "ANODR: Anonymous on Demand Routing with Untraceable Routes for Mobile Ad hoc networks," in *Proc. ACM MobiHoc'03*, Jun. 2003, pp. 291–302.

[7] R. Song, L. Korba, and G. Yee, "AnonDSR: efficient anonymous dynamic source routing for mobile ad hoc networks," in *Proc. ACM Workshop Security of Ad Hoc and Sensor Networks (SASN'05)*, Nov. 2005.

[8] Z. Wan, K. Ren, and M. Gu, "USOR: An Unobservable Secure On- Demand Routing Protocol for Mobile Ad Hoc Networks,"

IEEE Trans.on Wireless Communication, vol. 11, no. 5, pp. 1922–1932, May. 2012

[9] X. Hong, J. Kong, Q. Zheng, N. Hu, and P. Bradford, "A Hierarchical Anonymous Routing Scheme for Mobile Ad-Hoc Networks," in *Proc. IEEE MILCOM'06*, Oct. 2006.

[10] J. Paik, B. Kim, and D. Lee, "A3RP: Anonymous and Authenticated Ad hoc Routing protocol," in *Proc. International Conf. on Information Security and Assurance (ISA'08)*, Apr. 2008.

Anandhi. A, Working as an Assistant professor in Christ College of Engineering and Technology, Puducherry, India

Dhivya.G, Perusing B.Tech degree in Christ College of Engineering and Technology, Puducherry, India

Kalaivani.R, perusing B.Tech degree in Christ College of Engineering and Technology, Puducherry, India

Keshavarthini.P perusing B.Tech degree in Christ College of Engineering and Technology, Puducherry, India

ISSN: 2278 – 1323