Secure Routing Using ASOR Protocol for MANETs

KALAIMANI A[1], AMBIKA B[2], KOUSALYA S[3], SUBATHRA S R[4]

[1] PG Scholar, ECE Department, Hindusthan college of engineering and Technology, Coimbatore, Tamil Nadu, India

[2]Assistant professor, ECE Department, Hindusthan college of engineering and Technology, Coimbatore, Tamil Nadu, India

[3]PG Scholar, CSE Department, Hindusthan Institute of Technology, Coimbatore, Tamil Nadu, India

[4]PG Scholar, ECE Department, Hindusthan college of engineering and Technology, Coimbatore, Tamil Nadu, India

Abstract--Privacy protection is one of the critical issues in Mobile Adhoc Networks. To provide unobservability and unlinkability on the network was the major requirements. Although ,there was number of secure protocols available previously, still the mobile nodes are insecure and the requirements on the network was not completely satisfied. The risk of security attacks increases, if the distance between the node increases. In order to provide security, the QOS requirements have to be met. Onion routing and group signature are used in this paper to provide secure routing and broadcasting to find secure route for data transmission. Onion routing is used to record a discovered route and to provide intermediate node to modify the routing packets. Without disturbing the anonymity, Group signature is used for authentication.ASOR provides security regarding both inside and outside attacks.

Keywords -- Mobile Ad hoc Networks, Onion Routing, Group Signature**.**

I. INTRODUCTION

Mobile Adhoc networks is a self aligning network formed by mobile nodes interconnected by numerous hop communication paths and free to move in any direction and order themselves randomly. MANET has a active network topology and there is no federal controller and substructure, it is a self-governing network and there is a incomplete security. The two requirements on the network are need to be satisfied , i.e., the intermediate node may not be revealed to other nodes and gives more security and does not show what type of message or data are transferred between two nodes. MANETs are much more disposed to attack than wired network, because of the forthcoming reasons:

- Mansard dropping – By using different protocol analyzers, Hacker snips the data by overlooking into the packets.
- Animatedly Changing The Network Topology – Mobile nodes comes into the network may allow any malicious node to join the network without identified.
- Mutual Algorithms – Joint trust between the mobile nodes is required for the Manet's routing algorithm which violates the principles of network security.
- Lack of Federal Monitoring.
- Lack of Clear Line of guard – Need to organize layered security mechanism, for that need two line of defense –recognition and rejoinder.

MANET security involves confirmation, key organization and sharing and encryption. Routing protocols had a prepresence and predistributing of public and secret keys for all members. These protocols ignore key exchange and confirmation. MANET has a some disadvantages, they are:

- Lack of authorization
- Limited security

In this work we initially organize public and group key in mobile nodes to provide security, we propose an anonymous secure onion routing (ASOR) to overcome the security problems. Onion routing is used to record a discovered route because onion routing is more scalable and can be extended to multiple paths. The group signature is used for authentication purpose and to prevent the intermediate node to modifying the routing packet. There are numerous routing protocol available for MANET ,still the mobile networks are vulnerable to many attacks.

The remainder of this paper is as follows. The related work of adhoc routing protocol, the network scenario and the design are discussed in forthcoming section.

II. BACKGROUND AND ASSOCIATED WORK

In this section, we introduce some usual mechanisms which are widely used in routing protocols, and provide a survey on existing routing protocols.

A. *Mechanisms*

Mechanisms used in routing protocols are explained below.

- Trapdoor: In cryptographic functions, a trapdoor is a usual notion that defines a one-way event between two sets. A global trapdoor is an information collection process in which intermediary nodes may add information. Only assured nodes, such as source and sink nodes can unlock and recover the elements using pre-recognized secret keys. The usage of trapdoor requires an unidentified end-to-end key contract between the source and destination.
- Onion Routing: It is a procedure to grant private transmission over a public network. The source node fits up the core of an onion with a particular route message. During a route request phase, each sending on node adds an encrypted layer to the route request message. The source and destination nodes do not essentially know the ID of the sending on node. After receives the onion, the destination node delivers it along the route rear to source. The intermediary node can authenticate its role by decrypting and deleting the onion's external layer. Finally an anonymous route can be recognized.
- Group Signature: Group signature method can grant authentications without troubling the secrecy. Single member in the group may have a set of group public and private key released by group manager. The member can produce its own signature by its individual private key, and such signature can be certified by other members in the group without telling the signer's identity. Merely the group manager can track the signer's identity and cancel the group keys.

B. *Anonymous Routing Protocols*

There are many anonymous routing protocols. There are two categories: topology based and location based routing. Some of the location based routing protocols are AO2P, PRISM, and ALERT and these protocol requires localization services. Our paper is for general MANETs. So we concentrate only on the topology- based routing instead of location-based routing.

Unlinkability and unobservability are not fully satisfied in SDAR, AnonDSR, MASK, and D-ANODR.For the route request of MASK and D-ANODR,plain node ID is used and for SDAR and AnonDSR, node IDs in the neighborhood and along the route is used. Instead of its real ID, node's pseudonym is used to avoid info leakage during RREQ-RREP processes.

Some protocols are used for additional authentication which includes A3RP, RAODR, USOR, and PRISM. Neighborhood authentication is provided by MASK. but, it can't sign the routing packets. RAODR cannot provide traceability, anonymity, and enforceability. In this project, onion routing is used to record a discovered route because onion routing is more scalable and can be extended to multiple paths.

Eventually, key distribution and node anonymity assumptions in route discovery are need to be rethinking.

III. NETWORK ATTACK MODELS

In this section, we discuss about the attack models. Without loss of broad view, we assume that all the network protocols and functions are known by an adversary. The attackers beyond the network don't know the secret keys, but those interior the network may know the keys. We categorize the attacks according to their performances and positions.

- Passive outside attack: There may be an exterior global passive enemy, who can detect and to note down all the wireless communications in the network. It will try to show the individualities of the source, destination, and deduce the traffic flows by joining the packets to the source or sink nodes.
- Active outside attack: The passive attackers avoid any attack that shows their attacks meanwhile they attempt to be hidden, nevertheless the active outside attackers do not have such limits. They may target to distract the routing or propel a DOS attack. They can transfer from here to here and propel attacks arbitrarily.
- Passive inside attack: Like the passive outside attackers, the identities of source, destination, or en-route nodes are infer by the attackers. Meanwhile they can read the legal packets, the traffic prototype or node mobility information may be erudite by them.
- Active inside attack: They can alter, insert, and replay unpretentious messages. They can imitate as other nodes and launch the impersonation attacks and also creates one or more spook nodes by generating valid routing packets.

IV. ANONYMOUS ROUTING SCHEME

Here we consider six nodes for anonymous routing scheme. This is illustrated in Figure.1. A is the source node, F is the destination node and B, C, D, E are intermediary nodes. The source node A discovers the route to the node F which is the destination node.

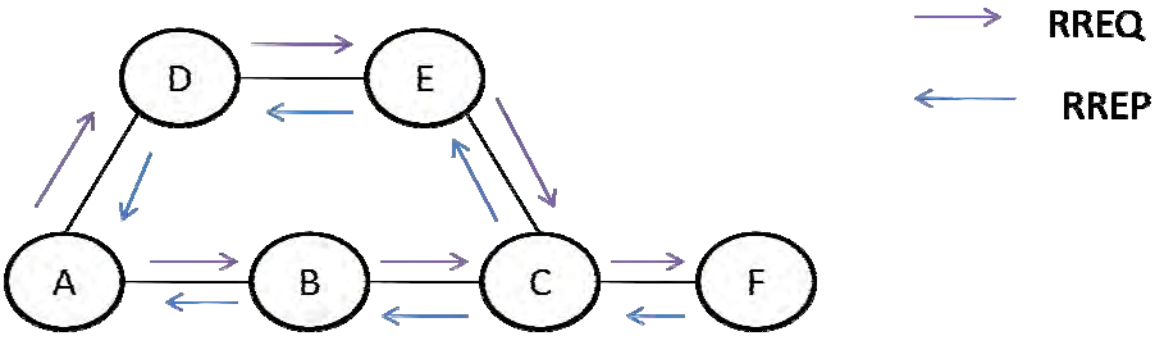

Figure.1.Network topology

Initially route request is send to discover the path in which the destination node is reached. After receiving the route request, the destination node send the acknowledge route reply along the path from which it receives the route request.

A. Anonymous key establishment

Node Authentication and session key generation are the two parts of Anonymous key establishment. Each node uses this to anonymously construct the session key with everyone of its neighbors.

1) Node Authentication

Each node has its public and private key issued by the group manager and the signature is send to its neighbour node. The neighbour node checks whether the key is a valid one. If it is a valid one, then it produce the session key and its own signing key and send it for reply. By using Diffie Hellman algorithm, group signature and the session key both are generated. Consider an example, if the node A wants to communicate with the node B, then the signature of A is send to node B.B checks, whether the key is a valid one and produce its own signing key and send it to A for reply.

2) Session Key Generation

If the keys are valid, node B creates its own session key and send to the node A and the node A verify the key. If both the keys are same, then data transfer has take place. If the session keys are not matched, then we identify that there is a attacker.

B. Routing

Here Onion routing mechanism is used. The source node fits up the core of an onion with a particular route message. During a route request phase, each sending on node adds an encrypted layer to the route request message. The source and destination nodes do not essentially know the ID of the sending on node. After receives the onion, the destination node delivers it along the route rear to source. The intermediary node can authenticate its role by decrypting and deleting the onion's external layer. Finally an anonymous route can be recognized.

The routing procedure can be explained as follows:

- During route discovery phase, Route request (RREQ) packet is broadcast by the source node.
- If the intermediary node receives the route request packet, by using group public key, it verifies the RREQ packet and adds one layer exterior to the key encrypted onion. and this process is repeated till it reaches the destination node.
- After the Route request is received and checked by the sink node. It sends the route reply (RREP) packet rear to the source node.
- During this phase, each intermediary node verifies the route reply packet and its routing and forwarding tables was updated. Then the exterior layer of the key encrypted onion is removed and it continues its broadcasting and updates the RREP packet.
- The source node, after receiving the RREP packet, it checks the packet, and updates the routing and forwarding tables. The route discovery phase is over.
- Now, the source node starts the data transmission.

V. CONCLUSION

Authentication and anonymity have many hypothetically attention grapping applications in adhoc networks, nevertheless foregoing protocol do not contemplate both of them into a single paper. In this paper, we projected Anonymous Secure Onion Routing Protocol (ASOR), with a group signature and onion routing mechanisms for MANETs. The major aspect is to deliver end-to-end anonymity and security. Contrasted to different secure routing protocols, it delivers higher throughput and also deliver better support for the secure communications, that are precise to packet loss ratio. In our future work, we will improve ASOR to improve the route efficiency.

REFERENCES

[1] D. Kelly. R. Raines, R. Baldwin, B. Mullins, and M. Grimaila, "Towards a taxonomy of wired and wireless anonymous networks", in Proc. IEEE WCNC '09, Apr, 2009.

[2] J. Kong and X. Hong, "ANODR: An Identity free and on demanding routing with untraceable routes for mobile ad hoc networks', in Proc. ACM MobiHoc'03, Jun, 2003,pp, 291-302.

[3] Y. Zhang, W. Liu, W. Xu, 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.

[4] M. G .Reed, P.F. Syverson, and D.M. Goldschalg,"Anonymous Connections and Onion Routing," IEEE Journal on Selected Area in comm.., vol. 16, no,4,482-494, May 1998.

[5] Z. Wan, K. Ren, and M. Gu, "USOR: An 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.

[6] K.E Defrawy and G. Tsudik, "Privacy- Preserving Location – Based On – demand routing in MANETs,' IEEE Journal on Selected Areas in Communications, vol. 29, no10, pp, 1926-1934, Dec, 2011.

[7] H. Shen and L. Zhao,"ALERT: An anonymous Location –based Efficient Routing Protocol in MANETs" IEEE Trans. On Mobile Computing, vol. 12, no. 6, pp, 1079-1093,2013.

[8] M. Yu and K. Leung,"A Trustworthiness-based QoS routing protocol for ad hoc networks," IEEE Tans. On Wireless Comms., vol. 8, no. 4, pp 1888-1898, Apr. 2009.