EFFICIENT AND AUTHENTICATED SECRET ROUTING PROTOCOL TO PROTECT AGAINST ATTACKS IN MANETS

[1]Uma s, [2]Dr. Poornima A S
[1]Student M.Tech CSE SIT Tumkur, [2]Associate Professor SIT Tumkur
Email:[1]umaasha92@gmail.com, [2]aspoornima@sit.ac.in

Abstract— MANETS are the wireless networks without any fixed infrastructure and they have dynamic topology. Due to these characteristics Manets are at a risk of variety of attacks. So providing trusted & secure communications for MANETS is an important aspect. Adversaries always aim to learn the identities of communicating nodes, the route through which the data flows as well as the network traffic pattern. Allowing Adversaries for tracing the routes and inferring the motion pattern of the communicating nodes may pose a serious threat to the applications include covert operations. So it is necessary to provide Anonymous communications for MANETS that achieves the objective of Unidentifiability & Unlinkabilty. A number of Anonymous secure routing protocols have been proposed recently, but the objective is not fully satisfied. The proposed protocol provides packet authentication using group signature and provides desirable anonymous communications using key-encrypted onion & secret verification message, which is more advantageous as compare to the existing protocols .The proposed protocol provides very high throughput and less the end-to-end delay of the system compare to other anonymous protocols.

Index Terms— MANETs, Anonymous communications , Group Signature, Onion routing.

I. INTRODUCTION

Mobile ad-hoc networks consisting of wireless mobile nodes in which every node in the network capable of communicating with each other without use of any centralised authority or the fixed infrastructure, for this reason MANETS are called as Infrastructure less network. Each node in MANET work as a router, forwards the packets from one node to another within the network for the purpose of communication. The Fig.1 represents the example for MANET containing mobile nodes. These MANETS dynamic topology because any mobile node can join or leaves the network at any point of time within the transmission range due to the reasons such as nodes mobility, node failure and loss of energy in the nodes. Other characteristics of MANETS are self-configurable, self-organisable, fast and & easily deployable and provide connectivity irrespective of the users Geographical position. Due to those desirable characteristics that are mentioned above MANETs have become increasingly popular and have wide varieties of applications in various fields such as Military applications, Natural disaster(earth quakes or floods),vehicular computing ,mobile office, personal networking (notepads, PDAs, cell phones) etc. Because of the wider applications of MANETs a lot of research has been conducted on various aspects such as routing, Security, QoS, management of network etc. But MANETs are they are vulnerable to many security threats due their inherent characteristics such as open wireless medium and frequently changing topology.

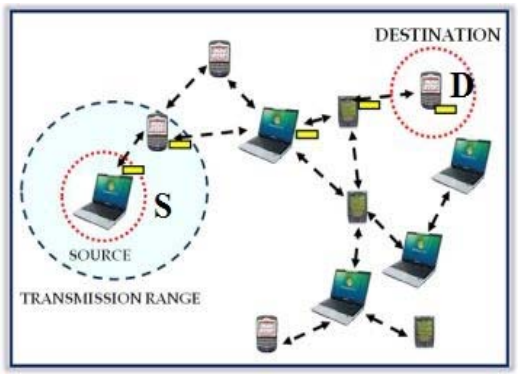

Fig.1 Infrastructure less Network

Providing privacy and security to the network under the presence of adversaries is a critical task because adversaries outside the network may infer the about the communicating nodes by passive traffic observation. And the nodes inside the network cannot be always trusted since any valid node may be captured by enemies and may become malicious. By considering all these issues providing anonymous communications[4] for MANETs is the best way to give high level security. Anonymous communications means the identification of nodes and the route through which data flows are replaced by some random numbers. The proposed protocol achieves anonymity by providing Unlinkabilty and Unidentifiabilty[1]. Unidentifiabilty means that the source and destination node identities cannot be revealed to other nodes in the network. Unlinkabilty can be defined as the traffic flows from the source node to the destination node cannot be revealed and recognised by other nodes in the network. One major key for implementing this anonymous communications is developing appropriate anonymous secure routing protocols by anonymizing the commonly used on-demand routing protocol, such as AODV[2] and DSR[3].

II. RELATED WORK

A number of anonymous routing schemes have been proposed in the past decade and they provide different level of security and privacy protection at different cost. Some schemes are more scalable to size but they require more computation effort. Let's have a brief study of existing Anonymous routing protocols.

A. ANODR

It is the protocol that focuses on only protecting the node or route identities during route discovery process, especially on the routing packets.it uses the global trapdoor message in RREQ and the route can only be identified by the disclosed trapdoor message, that may release to the intermediate nodes in the backward RREP forwarding and in Discount-ANODR a clear node id's used in the process route discovery so the objective of anonymity is not fully satisfied. Another disadvantage of ANODR is that is suitable only for small network and the efficiency is less.

B. MASK

The entire protocol relies upon the master key for the security of the network and this system cannot expel a node that is considered as an adversary from its group. The intruder can use different pseudonym to access the network even it is identified as an intruder so this protocol is highly vulnerable security threats and it also clear node id's used in the route discovery process that is not efficient. And it consumes lot power compare to other existing protocols.

C. Covert operations in MANETS: A Survey

Mobile ad-hoc networks are a rapidly rising area for research and commercial development. MANETs are very useful for military, ecological, and technical applications to name a few. One of the most active areas of explore in ad-hoc networks is that of Military communication and operations. Suppose when a covert mission is launched, that includes group of reconnaissance, attack task forces and surveillance then the ad-hoc network must provide reliable routes between command post and the groups for reliable delivery of commands/controls and for transmitting situation data as well as the video reporting. Providing location privacy protection and anonymity is a critical task and once the attacker's gains access then entire mission may be compromised. For example, unexpected change in the traffic pattern of a military network may indicate a upcoming action, a series of commands or a state change of network alertness [5]. That may also reveal the identities and locations of command centres and even the goals of covert missions.

III. PROPOSED SYSTEM

The EASR protocol is proposed in order to overcome the above mentioned drawbacks and

the protocol is designed based on the concept of standard routing protocol such as AODV[2].So our protocol also includes the phases such as route discovery phase, route maintenance as well as the data transmission. But according our protocol each of these phases are anonimyzed for the security purpose where the nodes id's are replaced by some random numbers and the protocol considers the entire MANET as a group with efficient group managers.
The EASR protocol uses the three techniques mentioned below.

Trapdoor :It uses symmetric key cryptography and secret sharing to protect the source and destination nodes from identifying the shared communications[7].
Onion routing: It combines symmetric & asymmetric public key cryptography to provide secure and anonymous protection for the routing packets[6] & communication data between source and destination.
Group signature: Without disturbing the anonymity group signature provides packet authentication. Each member in the group consists of a pair of group private key and the group public key.
Table maintainance: The protocol maintains 4 different tables such as destination table, routing table, neighborhood table, intermediate table for secure route discovery and as well as the route maintenance.

The following are the overall steps that are included in the proposed protocol.

I. Node anonymity is done by computing some random numbers for each and every node in the network.
II. To construct secret session keys an anonymous key establishment process is performed.
III. To find the best and secret path to the destination an anonymous route discovery process is initiated.

A. PROTOCOL DESIGN

Let us consider the below diagram that represents the working flow of the proposed EASR protocol in that we are concentrating on the route discovery process.

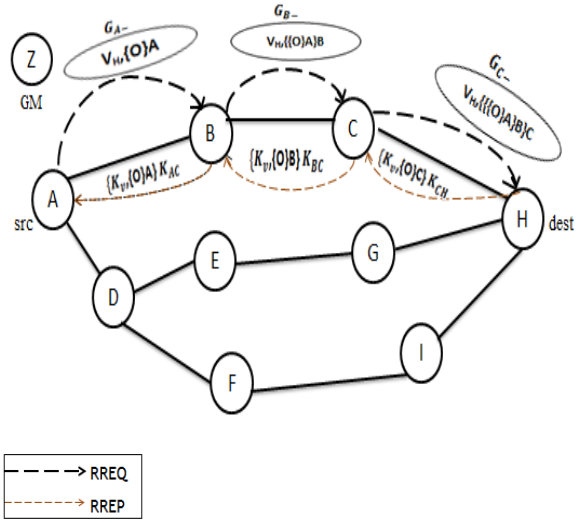

Fig.2.Network topology

Consider network shown in fig.2 in which node A discovers the route to the destination node H. Source Node A initiate the route discovery process by constructing the RREQ packet in the below format[8] and if there is no session key it will generate the session key between itself and the destination node H i,e. K_{AH} and then it will update is destination table.

Dest.Nym	Dest.Str	Dest.Pub_key	Session_key
N_H	Dest	K_{H+}	K_{AH}

$$A \rightarrow * : [RREQ, N_{sq}, V_H, V_{AH}, Onion(A)]G_{A-} \quad (1)$$

$$V_D = \{N_V, K_V, dest\}K_{AH}, \{K_{AH}\}K_{H-} \quad (2)$$

Where,
RREQ→packet type identifier
N_{sq}→pseudonym of S for the current RREQ
V_H &V_{AH}→encrypted secret message for the request validation at the destination node and the only the destination node can be able to decrypt this messages[9].
Onion(A)→key-encrypted onion created by A[Onion(A)]=$\sigma_{K_{gr}}(N_A)$
G_{S-}→ whole RREQ is signed by the A with its private key G_{S-}
N_V→one time nonce for route discovery
K_v→symmetric key

Consider the equation (2),if H is the receiver if the message H can decrypt the 2nd part by its private key K_{H-} then decrypt the 1st part by its

private key K_{AH}, otherwise it is not able to decrypt the received message. After sending the RREQ it will update its routing table as shown below.

Req_Nym	Dest_Nym	Ver_Msg	Status
N_{sq}	N_H	V_H	Pending

The node B receives the RREQ and decrypt it using its group public key, then it tries to decrypt the V_H part since it is not the destination it cannot be able to decrypt. So it reconstructs RREQ by copying the onion part of the route request and then applies its onion layer to the received onion. And then it will update its neighborhood table as below and forwards the reconstructed RREQ to its neighbor nodes.

Neighbour_Nym	Session_Key
N_A	K_{AB}
N_C	K_{BC}

After that node C receives the RREQ and it will repeat the same operation as the node B, since it is not the destination it cannot decrypt the whole message so it will reconstruct the RREQ by adding one more onion layer and forward that RREQ to its neighbor nodes and updates its intermediate table shown below.

Rt_Nym	Prev_hop_Nym	Next_hop_Nym
N_{rt}	N_B	N_H

This process repeats until RREQ is received by the valid destination. The node H receives the RREQ which is the destination.it will unlock the secret message V_H and then obtain symmetric key K_V and copies that key K_{CH} and generates the route pseudonym then constructs the RREP and sends back to the node c. The format of the RREP[8] packet is

$H \rightarrow * : (RREP, N_{rt}, \{K_V, Onion(C)\}K_{CH})$

Where,

RREP→packet type identifier
N_{rt}→route pseudonym generated by H
K_{JD}→shared key between source and destination

The intermediate node c receives the RREQ packet and decrypt using its shared key. After that it will obtain the validation key & then it will decrypt the onion layer as shown in fig.2. it came to know that it is not the intended receiver and then knows its assigned task ,forwards the RREP to node B. Node B performs as similar to C forwards that packet to source. source node A verifies the received RREP.If the secret message obtained after decrypting the final layer of the onion as well the message that is sent by the source are the same then it will treat that route as a valid secret route and establishes the route along that path and updates its routing table. The format of the data that is transmitted on the established path is

$$S \rightarrow D : (DATA, N_{rt}, \{P_{data}\}K_{AH})$$

Where,
DATA→packet type
P_{data}→data payload

Upon receiving a data packet, each node along the path will look into its forwarding table. The node will only forward the packet to its anonymous next hop only when the N_{rt} in the data packet matches the entry in the forwarding table.

B. ROUTING PROCEDURE

1. SN broadcasts RREQ to all Nodes

2. IN receives RREQ, verifies using its public key & add one layer on the top of key encrypted onion and forwards until reach DN

3. DN receives RREQ from SN or IN

4. DN verifies RREQ and assembles an RREP and then broadcasts back to SN

5. Each IN validates the RREP and updates its routing & forwarding tables and removes one layer on the top of the key encrypted onion and continuous broadcasting the updated RREP

6. SN receives RREP, verifies the packet

7. If the decrypted onion core equals to one of SN's issued nonce then updates its routing & forwarding tables

8. Route is established

9. SN starts the data transmissions in the established route

10. Every IN forwards the data until it reaches DN by using route pseudonym

C. APPROACH

The Proposed protocol has more advantages compare to the many existing anonymous routing protocols since it provides packet authentication without violating anonymity and uses the technique onion routing which is more scalable compare to the other cryptographic techniques such hash functions. The objective of anonymity is fully satisfied there is no possibility of information leakage during communication. But it is difficult for the single group manager to maintain the entire MANET if once the group manager is hacked by malicious node or attacked the entire communication will be compromised and also for large-scale network cryptographic overhead will be more and single manager can't alone manage such a large network so it is better have two or more group manager for the security purpose.

The advantages of having multiple group managers are

1. There will be co-ordination between the all group manager so the entire task can be divided by all the group managers
2. If one of the group manager become malicious, other group manager can verify and avoid the unexpected risk.

IV. CONCLUSION

In this paper security vulnerabilities are identified and can be avoided successfully by using both trapdoor and the onion routing concept. Group signatures play an important role for providing packet authentication.by using multiple group managers the will be more secure and confidentiality is achieved. We can also avoid the intermediate nodes by modifying the packets by using onion routing and the anonymous route also discovered using the same. Compared to the existing protocol ANODR the proposed protocol provides high throughput and lesser packet loss ratio.

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 ICC, Jun. 2009, pp. 1–8.

[2] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," IETF RFC 3561, Jul. 2003. [Online]. Available:www.ietf.org/rfc/rfc3561.txt

[3]. D. Johnson, Y. Hu, and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for MobileAdHocNetworks for IPv4," IETFRFC4728, Feb. 2007. [Online]. Available: www.ietf.org/rfc/rfc4728.txt

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

[5].DARPA.Research Challenges in High Confidence Networking,july1998

[6]. M. G. Reed, P. F. Syverson, and D. M. Goldschlag, "Anonymous connections and onion routing," IEEE J. Sel. Areas Commun., vol. 16, no. 4, pp. 482–494, May 1998.

[7]. S. William and W. Stallings, Cryptography and Network Security, 4th ed. Delhi, India: Pearson Education India, 2006.

[8]. Wei Liu, Member, IEEE, and Ming Yu, Senior Member, Authenticated Anonymous Secure Routing for MANETs in Adversarial EnvironmentsIEEE,2014

[9]. J. Kong, X. Hong, and M. Gerla, "ANODR: An identity-free and ondemand routing scheme against anonymity threats in mobile ad hoc networks," IEEE Trans. Mobile Comput., vol. 6, no. 8, pp. 888–902,Aug. 2007