Secure Neighbor Discovery System for ad-hoc through AASR Protocol

S.Arun Karthick
PG Scholar, Department of Computer Science and Engineering
Hindusthan College of Engineering and Technology
Coimbatore,Tamilnadu-India

K.Sudhakar
Assistant Professor, Department of Computer Science and Engineering
Hindusthan College of Engineering and Technology
Coimbatore,Tamilnadu-India

***Abstract*— Unknown accessing is important for many applications in MANET in adversary environments. The main aim of network is to provide unidentifiability and unlinkability for mobile nodes. In this proposed system a new routing protocol, i.e., authenticated anonymous secure routing (AASR), to satisfy the requirement and defend the attacks has been used. More specifically, the route request packets are authenticated by a group signature, to defend the potential active attacks without unveiling the node identities. By improving AASR, the packet delay can be reduced. A possible method is to combine it with a trust based routing. With the help of the trust model, the routing protocols will be more active in detecting link failures, caused either by the mobility or adversary attacks. By gathering the link quality of each and every node within the path between source to destination in network will be helpful for increasing the energy of the network and to achieve the energy efficient network.**

Keywords- AASR Protocol, Group Signature, Onion Routing, Mobile Ad Hoc Networks, Secure Routing Protocol (SRP), Trust based Quality of Service (TQoS), Anonymous Routing.

I. INTRODUCTION

Mobile Ad-hoc Networks are finding ever increasing applications in both military and civilian systems due to their self-configuration and self-maintenance capabilities. In Ad-hoc environment, wireless transmission are locally broadcasted in the region of the transmitting nodes. Ad-hoc network is used to minimize the energy efficiency, improves the battery lifetime, inherent, scalability. Network security is needed for the protection of data from breaches, and also protection of the computer from hackers. Generally open networks have generated an increased need for network security and dynamic security policies. Anonymous communications are important for MANETs in adversarial environments, in which the nodes identifications and routes are replaced by random numbers or pseudonyms for protection purpose. In MANETs, the requirements of anonymous communications can be described as a combination of unindentifiability and unlinkability. unindentifiability means that the identities of the source and destination nodes cannot be revealed to other nodes. Unlinkability means that the route and traffic flows between the source and destination nodes cannot be recognized or the two nodes cannot be linked. The key to implementing the anonymous communications is to develop appropriate anonymous secure routing protocols. Group signature is used to authenticate the RREQ packet per hop, to prevent intermediate nodes from modifying the routing packet. The anonymous route is calculated by a secure hash function, which is not as scalable as the encrypted onion mechanism. Anonymous routing protocols are crucial in MANETs to provide secure communications by hiding node identities and preventing traffic analysis attacks from outside observers.

II. RELATED WORK

D. Boneh, X. Boyen, and H. Shacham proposes Group signature scheme [1] can provide authentications without disturbing the anonymity. Every member in a group may have a pair of group public and private keys issued by the group trust authority (i.e., group manager). The member can generate its own signature by its own private key, and such signature can be verified by other members in the group without revealing the signer's identity. Only the group trust authority can trace the signer's identity and revoke the group keys.

S. William and W. Stallings [2] proposes a Trapdoor concept in Cryptography functions, that defines a one-way function between two sets. A global trapdoor is an information collection mechanism in which intermediate nodes may add information elements, such as node IDs, into the trapdoor. Only certain nodes, such as the source and destination nodes can unlock and retrieve the elements using pre-established secret keys. The usage of trapdoor requires an anonymous end-to-end key agreement between the source and destination.

Kong and Hong proposed an solution, named ANODR, for anonymous on demand routing in mobile ad hoc networks[10]. Our approach is the onion construction of ANODR, but is different in the following ways. First, ANODR uses public cryptography to exchange the pseudonym for each hop en route, but our approach only employs symmetric building block. Second, each route discovery in ANODR causes a global onion-construction flooding in the networks, and each node receiving the route request tries to open a trap-door function by performing a symmetric decryption and a comparison operation. If a node is not the destination, it will add another layer to the received onion by performing a symmetric encryption, and then broadcast the updated onion. Third, the trap-door design in ANODR requires a key distribution process, and each sender must know the trap-door key of the recipient in order to start a route request. Our approach does not require any key distribution. Finally, a potential drawback of ANODR is lack of terminating condition, i.e., large amount of requests will be propagated in the network for a long time.

D. Boneh, Weil [6] and H. Kim [7] proposes pairings concepts are examples of such bilinear maps, for which the Bilinear Diffie-Hellman Problem (BDHP) is believed to be hard6. It is also worth mentioning that ˆe is symmetric, i.e., ˆe(P,Q) = ˆe(Q, P) for ∀ P,Q ∈ G1, which follows immediately from the bilinearity and the fact that G1 is a cyclic group. We refer to [6], [7] for a more comprehensive description of how the pairing parameters should be chosen in practice for both efficiency and security.

M. G. Reed, P. F. Syverson, and D. M. Goldschlag, proposes Trapdoor mechanism to provide private communications over a public network [8]. The source node sets up the core of an onion with a specific route message. During a route request phase, each forwarding node adds an encrypted layer to the route request message. The source and destination nodes do not necessarily know the ID of a forwarding node. The destination node receives the onion and delivers it along the route back to the source. The intermediate node can verify its role by decrypting and deleting the outer layer of the onion. Eventually an anonymous route can be established.

III. PROPOSED WORK

Anonymous communications are important for MANETs in adversarial environments, in which the nodes identifications and routes are replaced by random numbers or pseudonyms for protection purpose. In a proposed scheme, we use a Authenticated Anonymous Secure Routing Protocol. The on-demand ad-hoc routing as the base of our protocol, including the phases of route discovery, data transmission, and route maintenance the phases of route discovery, data transmission, and route maintenance. In the route discovery phase, Number of nodes are created and routing configuration are established in the network environment.

In a Proposed method uses enhanced AASR protocol for to reduce the packet delay. A possible method is to combine it with a trust based routing concept and Link State method. With the help of the Link State model, the routing protocols will be more active in detecting link failures, caused either by the mobility or adversary attacks. The trust based concept provide the Quality of Service (Qos) to the routing communication process. The wireless links in an ad-hoc network are susceptible to attacks and the nodal mobility renders the network to have a highly dynamic topology, it becomes critical to detect major attacks against the routing protocols of such networks and also provide some extent of QoS to the network traffic. In this paper, we present a new secure routing protocol (SRP) with quality of service (QoS) support, called Trust based Quality Of Service (TQOS) routing, which includes secure route discovery, secure route setup, and trust based QoS routing metrics. The routing control messages are secured by using both public and shared keys, which can be generated on-demand and maintained dynamically. The message exchanging mechanism also provides a way to detect attacks against routing protocols, particularly the most difficult internal attacks. The routing metrics are obtained by combing the requirements on the trustworthiness of the nodes in the network and the QoS of the links along a route. The simulation results have demonstrated the effectiveness of the proposed secure QoS routing protocol in both security and performance.

A. *Anonymous Route Discovery:*

In the route discovery phase Fig:1 shows, the source node broadcasts an RREQ packet to every node in the network. If the destinationnode receives the RREQ to itself, it will reply an RREP packet back along the incoming path of the RREQ. In order to protect the anonymity when exchanging the route information, we re-design the packet formats of the RREQ and RREP, and modify the related processes.

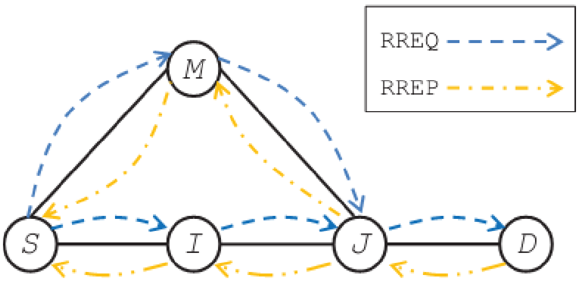
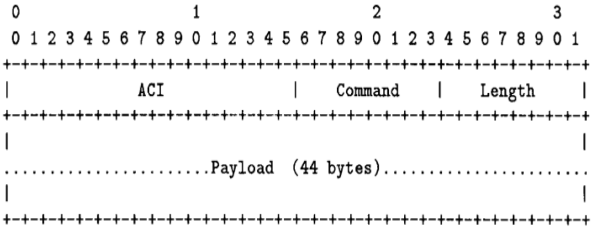


Fig:1 Structure of Network.

B. *Anonymous Connection Identifier (ACI):*

The Anonymous Connection Identifier(ACI) and Command fields are always encrypted using the link encryption between neighboring nodes. Additionally, the Length and Payload fields are encrypted using the link encryption between neigh-boring nodes if the command is either PADDING (0) or DESTROY (3). For CREATE (1) commands, the length is link encrypted, but the payload is already encrypted because it carries the onion. For DATA (2) commands, the length and en-tire payload are encrypted using the anonymous connection’s forward or backward cryptographic operations.



```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              ACI              |    Command    |    Length     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
.......................Payload  (44 bytes).......................
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Fig 2 Generic Cell Structure.

C. *Anonymous Routing Configuration:*

The needed number of nodes is generated by using the node command in NS2. The nodes are disseminating in a wireless environment. The random motion is set as true. So, the nodes are moving in a random direction. Each node is considered as an autonomous node. The nodes are configured as to process in MANET environment. The node configuration is done by using node-config command. We have to specify the Channel used by the node, Radio propagation model, Link layer type, Physical layer type, Type of interface queue and the protocol used to route the packets dynamically.

a) Route Request: Source node will generate a new session key for the association between Source and Destination.

$$S \rightarrow *: [RREQ, Nsq , VD, VSD, Onion(S)]GS-$$

Where RREQ is the packet type identifier; Nsq is a sequence number randomly generated by S for this route request; VD is an encrypted message for the request validation at the destination node; VSD is an encrypted message for the route validation at the intermediate nodes; Onion(S) is a key encrypted onion created by S. The whole RREQ packet is finally signed by S with its group private key GS−.

b) Route Intermediate process: Inter mediate node checks the Nsq and the timestamp in order to determine whether the packet has been processed before or not. Then Inter mediate node tries to decrypt the part of VD with its own private key. In case of decryption failure, Inter mediate node understands that it is not the destination of the RREQ. Inter mediate node will assemble and broadcast another RREQ packet.

$$I \rightarrow * : [RREQ;Nsq;VD;VSD;Onion(I)]GI$$

Destination can decrypt the part of VD; it understands that it is the destination of the RREQ. Destination can obtain the session key and verify all values.

c) Route Reply: When Destination receives the RREQ from its neighbor, it will assemble an RREP packet and send it back to neighbor. The format of the RREP packet is defined as follow:

$$D \rightarrow *: (RREP, Nrt, \langle Kv , Onion(J)\rangle KJD)$$

Intermediate nodes are decrypting the reply message if successfully decrypt it identified its valid after it remove the onion layer and send message to next hop.

When the RREP packet reaches Source, Source validates the packet in a similar process to the intermediate nodes. If the decrypted onion core NS equals to one of Source issued nonce, Source is the original RREQ source. Then the route discovery process ends successfully. Source is ready to transmit a data along the route indicated.

D. *Data Transmission:*

After finish the route discovers the source node encrypt the message and send to the destination node this data transmission is secure between source to destination. This module find out the correct destination because of security purpose, It transfer the data after the secure route to be founded.

E. *Anonymous Onion Routing:*

Once the anonymous connection is established, it can carry data. Before sending data over an anonymous connection, the onion proxy adds a layer of encryption for each onion router in the route. As data move through the anonymous connection, each onion router removes one layer of encryption, so it arrives at the responder as plaintext. This layering occurs in the reverse order for data moving back to the initiator. Therefore data that have passed backward through the anonymous connection must be repeatedly post-crypted to obtain the plaintext.

IV. CONCLUSION

In this paper, we design an authenticated and anonymous routing protocol and Trust based Quality of Service (TQoS) for MANETs in adversarial environments. The route request packets are authenticated by group signatures, which can defend the potential active anonymous attacks without unveiling the node identities. By combining the security mechanism with QoS requirements, we present a secure QoS routing protocol that achieves better performance. In this paper, we proposes Trust based Quality of Service (TQoS) provides secure communication and to reduce the packet loss ratio. The key-encrypted onion routing with a route secret verification message is designed to not only record the anonymous routes but also prevent the intermediate nodes from inferring the real destination. The Link State Model is used to detecting the link failures in the adversary environment.

In our future work, we will use enhanced AASR protocol to reduce traffic. A possible methods is to combine ALARM [3] protocol used to eliminate the malicious node in the adversary environment.

REFERENCES

D. Boneh, X. Boyen, and H. Shacham, “Short group signatures,” in Proc. Int. Cryptology Conf. (CRYPTO’04), Aug. 2004.

[1] S. William and W. Stallings, Cryptography and Network Security, 4th

Edition. Pearson Education India, 2006.

[2] K. E. Defrawy 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.

[3] 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.

[4] M. Yu and K. Leung, “A Trustworthiness-based QoS routing protocol

for ad hoc networks,” IEEE Trans. on Wireless Comms., vol. 8, no. 4, pp. 1888–1898, Apr. 2009.

[5] D. Boneh and M. Franklin, “Identify-based encryption from the weil

pairing,” inProc. CRYPTO’01, ser. LNCS, vol. 2139. Springer-Verlag, 2001, pp. 213–229.

[6] P. Barreto, H. Kim, B. Bynn, and M. Scott, “Efficient algorithms for

pairing-based cryptosystems,” inProc. CRYPTO’02,ser. LNCS, vol. 2442. Springer-Verlag, 2002, pp. 354–368.

[7] M. G. Reed, P. F. Syverson, and D. M. Goldschlag, “Anonymous

Connections and Onion Routing,” IEEE Journal on Selcted Area in Comm., vol. 16, no. 4, pp. 482–494, May 1998.

[8] K. E. Defrawy 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.

[9] J. Kong and X. Hong. ANODR: ANonymous On Demand Routing with untraceable routes for mobile ad-hoc networks. InACM MOBIHOC’03, 2003.

[10] Wei Liu and Ming Yu, “AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments” IEEE transactions on vehicular technology, vol. x, no. y, march 2014.

[11] M. Yu, M. C. Zhou, and W. Su, “A secure routing protocol against

Byzantine attacks for MANETs in adversarial environment,” IEEE Trans.on Vehicular Tech., vol. 58, no. 1, pp. 449–460, Jan. 2009.

[12] L. Yang, M. Jakobsson, and S. Wetzel, “Discount anonymous on

demand routing for mobile ad hoc networks,” in Proc. Int. Conf. on

SECURECOMM’06, Aug. 2006.

[13] X. Wu and B. Bhargava, “Ao2p: ad hoc on-demand position-based

private routing protocol,”IEEE Trans. Mobile Computing, vol.4,no.4,

pp. 335–348, July-Aug. 2005.

[14] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. Belding-Royer, “Authenticated routing for ad hoc networks,"IEEE J. Select. Areas Commun., vol. 2, no. 1, Mar. 2005.

[15] R. Song and L. Korba, “A robust anonymous ad hoc on-demand routing,” in Proc. IEEE MILCOM’09, Oct. 2009.

[16] 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.

[17] S. Seys and B. Preneel, “ARM: Anonymous Routing protocol for mobilead hoc networks,” Int. Journal of Wireless and Mobile Computing, vol. 3,no. 3, pp. 145–155, Oct. 2009.

[18] 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.

[19] 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.