International Journal on Applications in Information and Communication Engineering
Volume 1: Issue 7: July 2015, pp 1-3. www.aetsjournal.com ISSN (Online) : 2394-6237

Trust Based Anonymous Authenticated Secured Routing for Manet Adversarial Environments

Manikandan N K , Antony Kumar K , Manivannan D

***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. In this paper, we will improve AASR to reduce the packet delay. A possible method is to combine it with a trust-based routing. With the help of the trust model, the AASR routing protocol will be more effective and delay will be reduced. The nodes in the same network must assist and trust each other in forwarding packets from one node to another. However, this implied trust relationship can be threatened by malicious nodes that may modify or disrupt the orderly exchange of packets. But the use of Onion Routing will address the above mentioned problem.

***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, MANET have its significancy by multi hop and infrastructure less data transmission. High mobility of node make the traditional routing.

In Greedy forwarding,the forwarder node is the node far away from the source.Any of the node is out of the coverage range then the node is not reachable and the are Transmission gets failed.In GPSR, a famous GR protocol MAC failure feedback is send to the to the forwarder node thereby the packet is rerouted and data is received at the destination. General problem in data transmission is that single transmission of packet leads to multiple reception due to interruption, traffic, etc. Location based POR has been proposed now.Itdirectly uses location information for guiding packet forwarding. Like other opportunistic routing protocols, it is designed for static mesh networks and, in which several forwarding candidates cache the packet that has been received using MAC interception. If the best forwarder does not forward the packet in certain time slots, suboptimal candidates will take turn to forward the packet according to a locally formed order. The data transmission will not be interrupted if the candidates succeed in receiving and forwarding the packets. Duplicate relaying is important fact to be considered in forwarding packets in node mobility and in collision. For this certain scenarios are made and explained in the overview.In the case of communication hole, Virtual Destination-based Void Handling scheme in which the advantages of greedy forwarding and opportunistic routing can be achieved incase of handling communication voids. Finally, we evaluate the performance of POR through extensive simulations and verify that POR achieves excellent performance in high node mobility.

Manikandan N K is Assistant Professor, Department of CSE,Vel Tech University (Email: manikandan1488@gmail.com)
Antony Kumar K is Assistant Professor, Department of CSE,Vel Tech University (Email: antonykmr32@gmail.com)
Manivannan D is Assistant Professor, Department of CSE,Vel Tech University (Email:mani02.ceg@gmail.com)

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 packet in current 802.11. In POR we use similar scheme as the MAC multicast mode. The use of RTS/CTS/DATA/ACK significantly reduces the collision 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] propose 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., 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 .

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.

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. bold curve.

IV. PROTOCOL DESIGN

In this section, we present the design of AASR protocol. Considering the nodal mobility, we take the on-demand ad hoc routing as the base of our protocol, including the phases of route discovery, data transmission, and route maintenance. In the route discovery phase, the source node broadcasts an RREQ packet to every node in the network. If the destination node 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.

As an example, we use a five-node network to illustrate the authenticated anonymous routing processes. The network is shown in Fig.1, in which the source node *S* discovers a route to the destination node *D*.

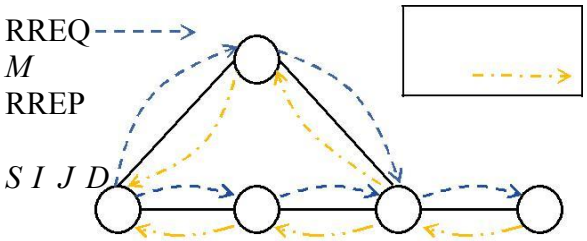

Fig. 1. Network topology

V. PROTOCOL EVALUATION

In this section, we check whether AASR can achieve the anonymity goals and defend the above mentioned attacks.

A. Anonymity Analysis

We check three types of anonymities of AASR, namely identity anonymity, route anonymity, and location anonymity. In the anonymity analysis, we assume that all the nodes, including those on the discovered route, are potential adversaries and interested in the privacy information about the two communication parties that discover the route.

1) *Identity Anonymity:* Our routing protocol can function without using the nodes' identities. All the nodes generate random nonce to indicate themselves. Consequently, any intermediate or adversary nodes cannot acquire the identities of the source and destination nodes. Besides the trapdoor information **dest** in the RREQ packet, there is no identity-related information involved in routing and forwarding processes.

However, in ANODR, *dest* is also used in the RREPs backward forwarding. An intermediate malicious node can use it to infer the destination. In AASR, we adopt an encrypted secret V_{SD} as the verification message in the RREP phase. Although N_v and K_v will be known by the intermediate nodes in route discovery, they are not related to the destination's identity. Thus, AASR provides better unindentifiability and unlinkability than ANODR.

2) Route Anonymity: During the route discovery, the Source, intermediate, and destination nodes only have information about the nodes' pseudonyms of the previous and next hop. Even if a node participates in route discovery, it has

no idea about the entire route, neither an exterior adversary. Since the nonce of destination node is one-time randomly generated and only known by its neighborhood, it is hard for the cooperative and malicious nodes to infer the multi-hop route.

3) Location Anonymity: The packet format of AASR does not include any information related to the network topology and the number of participating nodes (such as TTL and sequence). Thus the inside malicious node cannot infer the network topology.

One potential problem of our protocol is that the size of the key-encrypted onion may increase with the number of hops along the RREQs broadcasting path. By assuming a maximum number of hops, and fixed message size, and random TTL technique [11], [16], such problem can be resolved. Due to the space limit, we do not present the details here. With the deployment of the technique, the external malicious node cannot infer the hop count by observing the packet size.

B. Security Analysis

Passive Attacks: One type of passive attacks is a global eavesdropper. As discussed in the previous section, it is im-possible for an eavesdropper to obtain the identity information about the source or destination node in any communication session in AASR.

Another type of passive attack is the silent dropping, which means the adversaries or selfish nodes silently refuse to perform the requested functions in the protocol. In normal routing protocols, the watchdog model can be used to detect such actions. However, in the anonymous mobile communication, it is hard to recognize the misbehavior of adversaries or selfish nodes. In AASR, this can be improved by introducing a node trust model [24].

Impersonation Attacks: Impersonation attacks can be launched by the inside attackers. For example, the RREQ packets may be read and modified in some anonymous routing protocols. While in AASR, any node without the group key cannot join the communications. Because the forgery of a group signature is computational infeasible, it is impossible for an adversary to modify the packets. Since the group signature is traceable, if a group manager is available in the network, the singer of the fake routing packet can be identified by the group manager with the group's master key.

DoS Attacks: DoS attacks aim to deplete the nodes' resources. If the attacks are launched by the outside adversaries not having the keys, the packets can pass the packet verification. Such DoS attacks have little threat on our protocol. If the attacks are launched by the inside adversaries, more damage will be caused. However, once an inside adversary does so, its behavior of sending a large amount of route requests can be detected by other nodes in its neighborhood. Such abnormal behavior will be reported to the group manager. Then the attacker will be identified by tracing its signature.

VI. CONCLUSION

In this paper, we design an authenticated and anonymous routing protocol and 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

[1] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in Proc. Int. Cryptology Conf. (CRYPTO'04), Aug. 2004.

[2] S. William and W. Stallings, Cryptography and Network Security, 4thEdition. Pearson Education India, 2006.

[3] 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.

[4] 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.

[5] 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.

[6] D. Boneh and M. Franklin, "Identify-based encryption from the weilpairing," inProc. CRYPTO'01, ser. LNCS, vol. 2139. Springer-Verlag, 2001, pp. 213–229.

[7] 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.

[8] 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.

[9] 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.

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

[11] 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.

[12] 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.