Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments

Prof. Uttara Gogatte[#1] Shivajirao S. Jondhale college of Engg. Dombivali Mumbai, Maharashtra, India.
Ravi Pawar[#2] PG Student, YTCEM Karjat, Mumbai, Maharashtra, India.
1.uttaragogate@yahoo.co.in
2. ravipawar48@gmail.com

Abstract: Anonymous communications are important for many of the applications of mobile ad hoc networks (MANETs) deployed in adversary environments. A major requirement on the network is the ability to provide unidentifiability and unlinkability for mobile nodes and their traffic. Although a number of anonymous secure routing protocols have been proposed, the requirement is not fully satisfied. The existing protocols are vulnerable to the attacks of fake routing packets or denial-of-service broadcasting; even the node identities are protected by pseudonyms. In this paper, we propose a new routing protocol, i.e., authenticated anonymous secure routing (AASR), to satisfy the requirement and defend against the attacks. More specifically, the route request packets are authenticated by a group signature, to defend against potential active attacks without unveiling the node identities. The key-encrypted onion routing with a route secret verification message is designed to prevent intermediate nodes from inferring a real destination. Simulation results have demonstrated the effectiveness of the proposed AASR protocol with improved performance as compared with the existing protocols.

Keywords – MANET, Security, Anonymous, routing, active attacks, Authentication.

1. Introduction

MANET can be defined as a network that contains self-configurable mobile nodes that are connected by wireless links with no access point. In MANETs, each mobile node functions as a router and forwards the routing packet from one node to another for the purpose of communication. Every mobile node is autonomous in nature and they have the ability to move from here to there within the communicating network. So, MANETs have frequently changing dynamic topology and the breaking of communication link is common in the network. MANETs have wide varieties of applications, namely Wireless Sensor Network, Military Battlefields [3], Device Networks, Tactical networks and many. Some challenges as well as the design issues are there to overcome regardless of attractive applications of MANETs. Here exist many security vulnerabilities that are related to security in MANETs.

The example for MANETs that consists of wireless mobile nodes can be seen through an example shown in the below Figure 1.1.Whenever a sender node wants to transmit the information to receiver node which is not reachable from its transmission range[2], then the sender node will initiate the routing process. The Route discovery process identifies the optimum route from sender to the receiver node. Here the intermediate nodes play an important role and they have the responsibility to forward the packets from one node to another node within communication range.

MOBILE ad hoc networks (MANETs) are vulnerable to security threats due to the inherent characteristics of such networks, such as the open wireless medium and dynamic topology. It is difficult to provide trusted and secure communications in adversarial environments, such as battlefields. On one hand, the adversaries outside a network may infer the information about the communicating nodes or traffic flows by passive traffic observation, even if the communications are encrypted. On the other hand, the nodes inside the network cannot be always trusted, since a valid node may be captured by enemies and becomes malicious. As a result, anonymous communications are important for MANETs in adversarial environments, in which the node identifications and routes are replaced by random numbers or pseudonyms for protection purposes.

Anonymity is defined as the state of being unidentifiable within a set of subjects. In MANETs, the requirements of anonymous communications can be described as a combina- tion of unidentifiability and unlinkability [1]. Unidentifiability 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 that the two nodes cannot be linked. The key to implementing the anonymous communica- tions is development of appropriate anonymous secure routing protocols.

Figure 1.1: Infrastructure less network

2. Review of Literature

We introduce the basic concepts in anonymous routing and provide a short survey on the existing routing protocols.

A. Anonymity and Security Primitives

We introduce some common mechanisms that are widely used in anonymous secure routing.

1) Trapdoor: In cryptographic functions, a trapdoor is a common concept that defines a oneway function between two sets [12]. 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 the destination.

2) Onion Routing: It is a mechanism to provide private communications over a public network [13]. 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.

3) Group Signature: The group signature scheme [14] 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.

B. Anonymous On-Demand Routing Protocols

There are many anonymous on-demand routing protocols. Similar to ad hoc routing, there are two categories: topology based and location based [1] or, in other words, node identity centric and location centric [15]. We compare the protocols in Table I, in terms of the key distribution assumption, node anonymity in route discovery, and packet authentication. Our observations are summarized as follows.

First, the routing protocols are designed to work in different scenarios. AO2P, PRISM, and ALERT are designed for location-based or location-aided anonymous communications, which require localization services. Since ours is for general MANETs, we focus on topology-based routing rather than location-based routing.

DISADVANTAGES OF EXISTING SYSTEM:

- The existing protocols are also vulnerable to the denial-of-service (DoS) attacks, such as RREQ based broadcasting.
- The objectives of unindentifiability and unlinkability are not fully satisfied.
- Lack of packet authentication.
- Difficult for the protocols to check whether a packet has been modified by a malicious node.

3. Problem Statement:

In this System to implementing the anonymous communications is to develop appropriate anonymous secure routing protocols. Topology-based on-demand anonymous routing protocols, which are general for MANETs in adversarial environments. To develop the anonymous protocols, a direct method is to anonymize the commonly used on-demand ad hoc routing protocols, such as AODV and DSR . For this purpose, the anonymous security associations have to be established among the source, destination, and every intermediate node along a route. So group signature is introduced to anonymous routing. In A3RP , the routing and data packets are protected by a group signature. However, the anonymous route is calculated by a secure hash function, which is not as scalable as the encrypted onion mechanism.

4. Proposed System:

AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments

We propose a new routing protocol, i.e., authenticated anonymous secure routing (AASR) to overcome the pre-mentioned problems. We adopt a key-encrypted onion to record a discovered route and design an encrypted secret message to verify the RREQ-RREP linkage. Group signature is used to authenticate the RREQ packet per hop, to prevent intermediate nodes from modifying the routing packet. Extensive simulations are used to compare the performance of AASR to that of ANODR, a representative on-demand anonymous routing protocol and our proposed system provides more throughput than ANODR under the packet-dropping attacks, although AASR experiences more cryptographic operation delay.

ADVANTAGES OF PROPOSED SYSTEM:

- Group signature is used to authenticate the RREQ packet per hop, to prevent intermediate nodes from modifying the routing packet.
- Improved performance as compared to the existing protocols

5. Phases of the proposed System

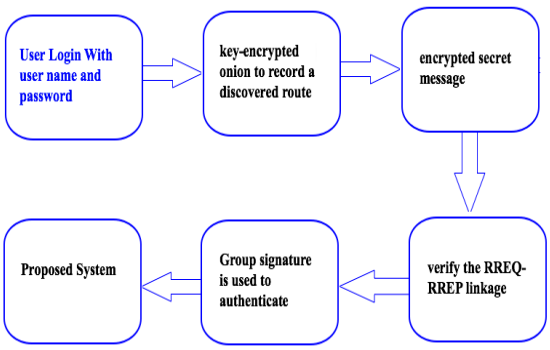

Fig. 1 Proposed system

A. Anonymous Route Request

1) Source Node: We assume that S initially knows the in- formation about D, including its pseudonym, public key, and destination string. The destination string dest is a binary string, which means "You are the destination" and can be recognized by D. If there is no session key, S will generate a new session key K_{SD} for the association between S and D. The following entry will be updated in S's destination table:

Dest.Nym.	Dest.Str	Dest. Pub_Key	Session_Key
N_D	dest	K_{D+}	K_{SD}

2) Intermediate Node: The RREQ packet from S is flooded in T. Now, we focus on an intermediate node I, as shown in Fig. 1. We assume that I has already established the neighbor relationship with S and J. I knows where the RREQ packet comes from. The following entries are stored in I's neighbor-hood table:

Neigh. Nym.	Session_Key
N_S	K_{SI}
N_J	K_{IJ}

3) Destination Node: When the RREQ packet reaches D, D validates it similarly to the intermediate nodes I or J. Since D can decrypt the part of V_D, it understands that it is the destination of the RREQ. D can obtain the session key K_{SD}, the validation nonce N_V , and the validation key K_V .

Then, D is ready to assemble an RREP packet to reply to the S's route request.

B. Anonymous Route Reply

1) Destination Node: When D receives the RREQ from its neighbor J, it will assemble an RREP packet and send it back to J. The format of the RREP packet is defined as follows:

$$D \rightarrow * : (RREP, N_{rt}, \langle K_V, Onion(J)\rangle \; K_{JD}) \quad (9)$$

where RREP is the packet-type identifier, N_{rt} is the route pseudonym generated by D, and K_V and Onion(J) are ob- tained from the original RREQ and encrypted by the shared key K_{JD}. The intended receiver of the RREP is J.

2) Intermediate Node: We assume that J has already estab- lished a neighbor relationship with I, D, and M. The following entries are already in J's neighborhood table:

Neigh. Nym.	Session_Key
N_D	K_{JD}
N_I	K_{IJ}
N_M	K_{MJ}

3) Source Node: When the RREP packet reaches S, S vali- dates the packet in a similar process to the intermediate nodes. If the decrypted onion core N_S is equal to one of S's issued nonce, S is the original RREQ source. S will update its routing table as follows:

Req.Nym.	Dest.Nym.	Ver.Msg.	Next_hop	Status
N_{sq}	N_D	V_{SD}	N_I	Active

C. Anonymous Data Transmission

Now, S can transmit the data to D. The format of the data packet is defined as follows:

$$S \rightarrow D : (DATA, N_{rt}, \langle P_{data}\rangle \; K_{SD}) \quad (11)$$

where DATA is the packet type, N_{rt} is the route pseudonym that can be recognized by downstream nodes, and the data payload is denoted by P_{data}, which is encrypted by the session key K_{SD}.

D. Routing Procedure

The routing algorithm can be implemented based on the existing on-demand ad hoc routing protocol such as AODV or DSR. The main routing procedures can be summarized as follows.

1) During route discovery, a source node broadcasts an RREQ packet in the format of (1).

2) If an intermediate node receives the RREQ packet, it verifies the RREQ by using its group public key and adds one layer on top of the key-encrypted onion, as (7). This process is repeated until the RREQ packet reaches the destination or expires.

3) Once the RREQ is received and verified by the destination node, the destination node assembles an RREP packet in the format of (9) and broadcasts it back to the source node.

4) On the reverse path back to the source, each intermediate node validates the RREP packet of (2) and updates its routing and forwarding tables. Then, it removes one layer on the top of the key-encrypted onion and continues broadcasting the updated RREP in the format of (10).

5) When the source node receives the RREP packet, it verifies the packet and updates its routing and forwarding tables. The route discovery phase is completed.

6) The source node starts data transmissions in the es- tablished route in the format of (11). Every intermedi- ate node forwards the data packets by using the route pseudonym.

6. Conclusion

In this paper, we have designed an authenticated and anonymous routing protocol for MANETs in adversarial environments. The route request packets are authenticated by group signatures, which can defend against potential active anonymous attacks without unveiling the node identities. 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. Compared with ANODR, AASR provides higher throughput and lower packet loss ratio in different mobile scenarios in the presence of adversarial 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 by reducing packet delay. A possible method is to combine it with trust- based routing [24]. With the help of the trust model, the routing protocols will be more active in detecting link failures, caused either by the mobility or adversarial attacks.

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,andD.Maltz,"TheDynamicSource RoutingProtocol (DSR) for Mobile Ad Hoc Networks for IPv4," IETF RFC 4728, Feb. 2007. [Online]. Available: www.ietf.org/rfc/rfc4728.txt

[4] J. Kong and X. Hong, "ANODR: ANonymous on demand routing with untraceable routes for mobile ad hoc networks," in *Proc. ACM MobiHoc*, Jun. 2003, pp. 291–302.

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

[6] A. Boukerche, K. El-Khatib, L. Xu, and L. Korba, "SDAR: A secure distributed anonymous routing protocol for wireless and mobile ad hoc networks," in *Proc. IEEE Int. Conf. LCN*, Nov. 2004, pp. 618–624.

[7] R. Song, L. Korba, and G. Yee, "AnonDSR: Efficient anonymous dynamic source routing for mobile ad hoc networks," in *Proc. ACM Workshop SASN* , Nov. 2005, pp. 33–42.

[8] 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.

[9] Y. Zhang, W. Liu, W. Lou, and Y. G. Fang, "MASK: Anonymous on-demand routing in mobile ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 5, no. 9, pp. 2376–2386, Sep. 2006.

[10] L. Yang, M. Jakobsson, and S. Wetzel, "Discount anonymous on demand routing for mobile ad hoc networks," in *Proc. Int. Conf. SECURECOMM*, Aug. 2006, pp. 1–10.

[11] J. Paik, B. Kim, and D. Lee, "A3RP: Anonymous and authenticated ad hoc routing protocol," in *Proc. Int. Conf. ISA*, Apr. 2008, pp. 67–72.

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

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

[14] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in *Proc. CRYPTO*, Aug. 2004, pp. 41–55.

[15] K. E. Defrawy and G. Tsudik, "ALARM: Anonymous location-aided routing in suspicious MANETs," *IEEE Trans. Mobile Comput.*, vol. 10, no. 9, pp. 1345–1358, Sep. 2011.

[16] S. Seys and B. Preneel, "ARM: Anonymous routing protocol for mobile ad hoc networks," *Int. J. Wireless Mobile Comput.*, vol. 3, no. 3, pp. 145–155, Oct. 2009.

[17] R. Song and L. Korba, "A robust anonymous ad hoc on-demand routing," in *Proc. IEEE MILCOM*, Oct. 2009, pp. 1–7.

[18] Z. Wan, K. Ren, and M. Gu, "USOR: An unobservable secure on-demand routing protocol for mobile ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 5, pp. 1922–1932, May 2012.

[19] X. Wu and B. Bhargava, "AO2P: Ad hoc on-demand position-based private routing protocol," *IEEE Trans. Mobile Comput.*, vol. 4, no. 4, pp. 335–348, Jul./Aug. 2005.

[20] K. E. Defrawy and G. Tsudik, "Privacy-preserving location-based on- demand routing in MANETs," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 10, pp. 1926–1934, Dec. 2011.