Advances in Computer Science and Information Technology (ACSIT)
Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 2, Number 11; April-June, 2015 pp. 69-73
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/acsit.html

An Efficient Anonymous Secure Routing(EASR) Protocol for MANETs in Adversial Environment

Manjesh Patel[1], Sangeetha Rao[2] and Rashmi Mothkur[3]

[1,2]B.E, M.Tech ISE Dept, Jain University
[3]B.E, M.Tech CSE Dept, UBDTCE
E-mail: [1]manjeshpatel3@gmail.com, [2]raoksangeetha@gmail.com, [3]rashmimothkur@gmail.com

Abstract—*Anonymous communications are important for many applications of the mobile ad hoc networks (MANETs) deployed in adversary environments. A major requirement on the network is to provide unidentifiability and unlink ability for mobile nodes and their traffics. 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 (DoS) broad-casting, even the node identities are protected by pseudonyms. In this paper, we propose a new routing protocol, i.e., Efficient anonymous secure routing (EASR), to satisfy the requirement and defend the attacks. More specifically, the route request packets are authenticated by a group signature, to defend the 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 EASR protocol with improved performance as compared to the existing protocols.*

1. INTRODUCTION

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 nodes identifications and routes are replaced by random numbers or pseudonyms for protection purpose.

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 combination of unindentifiability and unlinkability [1]. 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.

There are many anonymous routing protocols proposed in the past decade. Our focus is the type of 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 [2] and DSR [3]. For this purpose, the anonymous security associations have to be established among the source, destination, and every intermediate node along a route. The resulting protocols include ANODR [4], [5], SDAR [6], AnonDSR [7], MASK [8], [9], and Discount-ANODR [10].

After examining these protocols, we find that the objectives of unindentifiability and unlinkability are not fully satisfied. For example, ANODR focuses on protecting the node or route identities during a route discovery process, especially on the routing packets, e.g., Route REQuest (RREQ) and Route REPly (RREP). ANODR adopts a global trapdoor message in RREQ, instead of using the ID of the destination node. However, the route can be identified by a disclosed trapdoor message, which may be released to the intermediate nodes in backward RREP forwarding. The other protocols rely on the neighborhood detection and authentication, but may partially violate the anonymity requirements for performance considerations. For example, in SDAR, the node and its one hop neighbors are made to know each other's ID during the routing procedures. In AnonDSR, the intermediate nodes en route may be revealed to the destination node. In MASK and Discount-ANODR, a clear node ID is used in the route discovery.

These protocols are also vulnerable to the denial-of-service (DoS) attacks, such as RREQ based broadcasting. Due to the lack of packet authentication, it is difficult for the protocols to check whether a packet has been modified by a malicious node. Recently, group signature is introduced to anonymous

routing. In A3RP [11], 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.

In this work, we focus on the MANETs in adversarial environments, where the public and group key can be initially deployed in the mobile nodes. We assume that there is no online security or localization service available when the network is deployed. We propose an Efficient anonymous secure routing (EASR) 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. The results show that, it provides more throughput than ANODR under the packet-dropping attacks, although AASR experiences more cryptographic operation delay.

The remainder of this paper is organized as follows. The network scenario is discussed in Section II. The design of EASR protocol is presented in Section III. We evaluate EASR in Section IV and provide the performance results in Section V. Section VI concludes this paper.

2. NETWORK SCENARIO

We denote a MANET by **T** and make the following assumptions.

2.1 Public Key Infrastructure*:* Each node **T** initially has a pair of public/private keys issued by a public key infrastructure (PKI) or other certificate authority (CA). For node A ($A \in \mathbf{T}$), its public/private keys are denoted by $KA+$ and $KA-$.

2.2 Group Signature: We consider the entire network **T** as a group and each node has a pair of group public/private keys issued by the group manager. The group public key, denoted by $GT+$, is the same for all the nodes in **T**, whiles the group private key, denoted by $GA-$ (for $A \in \mathbf{T}$), is different for each node. Node A may sign a message with its private key $GA-$,and this message can be decrypted via the public key $GT+$ by the other nodes in **T**, which keeps the anonymity of A .

2.3 Neighborhood Symmetric Key: Any two nodes in a neighborhood can establish a security association and create a symmetric key with their public/private keys. This association can be triggered either by a periodical HELLO messages or by the routing discovery RREQ messages. For two nodes A and B ($A;B \in$ T), the shared symmetric key is denoted by K_{AB} and used for the data transmissions between them.

2.4 Node Table: contains information of Node ID, corresponding Group to which it belongs, group signature, status of data, and various attack information.

2.5 Routing Table: When a node generates or forwards a route request, a new entry will be created in its routing table, which stores the request's pseudonym and the secret verification message in this route discovery. Such an entry will be marked in the status of "pending". If an RREP packet is received and verified, the corresponding entry in the routing table will be updated with the anonymous next hop and the status of "active".

2.6 Destination Table: We assume that a source node knows all its possible destination nodes. The destination information, including one of destination's pseudonym, public key, and the pre-determined trapdoor string *dest* will be stored in the destination table. Once a session to the destination is established, the shared symmetric key is required for data encryptions in the session. Such symmetric key is generated by the source node before sending the route requests, and stored in the destination table after receiving the route reply.

2.7 Kalman Filtering Method

In this system, the system follows an integration of system monitoring modules and intrusion detection modules in the context of Ad hoc Networks. The system emphasis an extended Kalman filter (EKF) based mechanism to detect false injected data. Specifically, by monitoring behaviors of its neighbors and using EKF to predict their future states (actual in-network aggregated values), each node aims at setting up a normal range of the neighbors' future transmitted aggregated values.

2.8 Algorithm

Advanced Encryption Standard algorithm is used for encryption and decryption. Secure hash algorithm SHA1 is used for group signatures.

3. EASR PROTOCOL

The Problem of the system is to avoid the vulnerable to the attacks of fake routing packets or denial-of-service (DoS) broadcasting; even the node identities are protected by pseudonyms and have to provide an Efficient anonymous secure routing (EASR), to satisfy the requirement and defend the attacks.

A new routing protocol, i.e., Efficient anonymous secure routing (EASR) is proposed. 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.

3.1 System Architecture

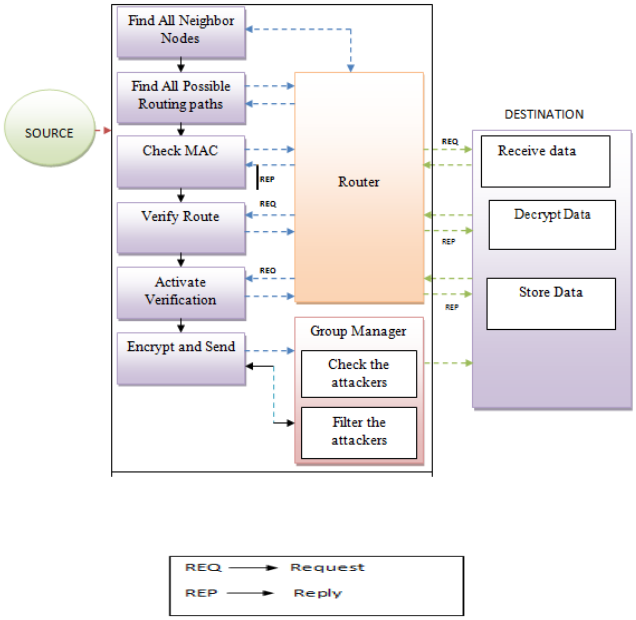

Fig. 1: System Architecture.

3.2 Modules

3.2.1 Service Provider

In this module, the Service Provider will browse an file, assign signature to all nodes, assign group key to all groups (group1, group2 and group3) and then send to particular user (A, B, C, D and F). After receiving the file he will get response from the receiver. The Service Provider can have capable of manipulating the data file.

3.2.2 Router

The Router manages a multiple Groups (Group1, Group2, Group3, and Group4) to provide data storage service. In Group n-number of nodes (n1, n2, n3, n4…) are present, and in a Router energy will be generated and it will select the smallest energy path, the sensor node which have more energy will communicate first and connect to another groups and send to the particular receiver. In a router service provider can view the node information details and view the routing table details. If any attacker is found in a node, then it will select another path.

3.2.3 Group Manager

In this module, the group manager can distribute key for each and every group (Group1, Group2 and Group3) and a group each node has a pair of group public/private keys issued by the group manager. Group signature scheme 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 (Group Manager). Only the group trust authority (Group Manager) can trace the signer's identity and revoke the group keys. If any attacker will found in a node then the group manager will identify and then send to the particular users.

3.2.4 Receiver (End User / Group Member)

In this module, there are an n-numbers of receivers are present (A, B, C, D and F). All the receivers can receive the data file from the service provider. The service provider will send data file to router and router will connect to all groups and send to the particular receiver, without changing any file contents. The user can only access the data file. For the user level, all the privileges are given by the GM authority and the Data users are controlled by the GM Authority only. Users may try to access data files within the router.

3.2.5 Attacker

In this module, the attacker can attack the node in three ways Passive attack, DOS attack and Impression attack. Dos attack means he will inject fake Group to the particular node, Passive attack means he will change the IP address of the particular node and Impression attack means he will inject malicious data to the particular node.

3.3 Anonymous Route Request

3.3.1 Source Node: We assume that S initially knows the information about D, public key, and destination IP.

$$S \rightarrow *: [RREQ;\ V_D;\ V_{SD};Onion(S)]\ G_{S\text{-}}$$

where *RREQ* is the packet type identifier; *Nsq* is a sequence number randomly generated by *S* for this route request; V_D is an encrypted message for the request validation at the destination node; V_{SD} 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 $G_{S\text{-}}$.

3.3.2 Intermediate Node: The RREQ packet from S is flooded in **T**. Now we focus on an intermediate node I, 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 neighborhood table:

Once *I* receives the RREQ packet, it will verify the packet with its group public key $G_{T+.}$ As long as the packet is signed by a valid node, *I* can obtain the packet information. Otherwise, such an RREQ packet will be marked as malicious and dropped.

Then *I* tries to decrypt the part of V_D with its own privatekey. In case of decryption failure, *I* understands that it is not the destination of the RREQ. *I* will assemble and broadcast another RREQ packet in the following format:

$$I \rightarrow *: [RREQ;\ V_D;\ V_{SD};Onion(I)]G_{I\text{-}}$$

where V_D, and V_{SD} are kept the same as the received

RREQ packet; the key-encrypted onion part is updated to

Onion(*I*). The complete packet is signed by *I* with its group private key *GI*-.

I updates the onion in the following way:

$Onion(I) = O_{KSI}\ (Onion(S))$

Onion(*S*) is obtained from the received RREQ packet; this layer of onion is encrypted with the symmetric key K_{SI} .When *I*'s RREQ reaches the next hop *J*, *J* will perform the same procedures and update the onion in the RREQ with one more layer, which is:

$$Onion(J) = O_{KIJ}\ (N_J\ ;Onion(I))$$

3.3.3 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 VD, it understands that it is the destination of the RREQ. D can obtain the session key K_{SD}, and the validation key Kv. Then D is ready to assemble an RREP packet to reply the S's route request.

3.4. Anonymous Route Reply

3.4.1 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 follow:

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

where RREP is the packet type identifier; Nrt is the route pseudonym generated by D; Kv and Onion(J) are obtained from the original RREQ and encrypted by the shared key KJD. The intended receiver of the RREP is J.

3.4.2 Intermediate Node: We assume that J has already established a neighbor relationship with I, D, and M. The following entries are already in J's neighborhood table. If J receives the RREP from D, J will navigate the shared

keys in its neighborhood table, and try to use them to decrypt $\langle Kv;Onion(J)\rangle K_{JD}$. In case of a successful decryption, J knows the R_{REP} is valid and from N_D, and J also obtains the validation key Kv. Then J continues to decrypt the onion part. J knows the next hop for the RREP is N_I

The format of J's RREP towards the previous hop I is defined as:

$$J \rightarrow * : (R_{REP};N_{rt};\ \langle Kv;Onion(I)\rangle K_{IJ}\ )$$

where Nrt and Kv are obtained from the received RREP; Onion(I) is obtained by from the decrypted Onion(J); the shared key KIJ is obtained from J's neighborhood table. The intended receiver of the RREP is I.

When the RREP packet travels according to the layers on the onion, it will start at the destination node and move back to its previous node. Each time the intermediate node can associate a value with the underlying wireless link on which the RREP travels, until the RREP packet reaches the source. In our protocol, every node records the one-time link pseudonyms announced by its neighbor node. Then the intermediate nodes' forwarding tables can be established after the RREP's trip.

3.4.3 Source Node: When the RREP packet reaches S, S validates the packet in a similar process to the intermediate nodes.

4. EVALUATION OF EASR

4.1 Security Analysis

4.1.1 Passive Attacks: One type of passive attacks is a global eavesdropper. As discussed in the previous section, it is impossible 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.

4.1.2 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.

4.1.3 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.

5. PERFORMANCE EVALUATION

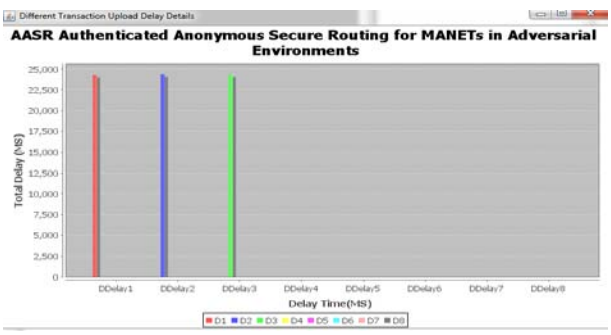

Fig 2: Transaction Upload Delay Details

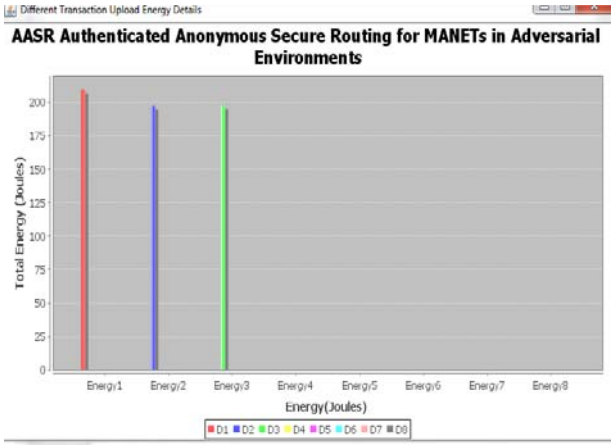

Fig 3: Transaction Upload Energy Details

6. CONCLUSION

In this paper, we design an authenticated and anonymous routing protocol for MANETs in adversarial environments. The route request packets are authenticated by group signatures, which can defend the potential active anonymous attackswithout 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.

In our future work, 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.

REFERENCES

[1] 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.

[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] R. Song and L. Korba, "A robust anonymous ad hoc on-demand routing," in *Proc. IEEE MILCOM'09*, Oct. 2009.

[4] 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.

[5] S. Seys and B. Preneel, "ARM: Anonymous Routing protocol for mobile ad hoc networks," *Int. Journal of Wireless and Mobile Computing*, vol. 3, no. 3, pp. 145–155, Oct. 2009.

[6] 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.

[7] D. Johnson, Y. Hu, and D. Maltz, "RFC 4728 - The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4," *Internet RFCs*, 2007.

[8] 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. on Mobile Computing*, vol. 6, no. 8, pp. 888– 902, Aug. 2007.

[9] 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.

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