Secure Routing and Data Transmission in MANETs using Digital Signature

Sreelekshmi. S
PG Scholar, Applied Electronics, Dept. of Electronics and Communication
Immanuel Arasar J.J. College of Engineering
Marthandam

***Abstract*—Anonymous communications are vital for many applications of Mobile ad hoc Networks (MANETs) deployed in adversary environments. The various anonymous secure routing protocols proposed so far, are vulnerable to passive attacks that affect the confidentiality of the routing operation. The network is vulnerable to security threats due to its inherent dynamic topology. AASR experiences more cryptographic packet delay. So, an improved secure routing protocol design, Authenticated Anonymous Secure Routing (AASR) protocol integrated with digital signature is proposed to implement anonymous secure routing with enhanced data security features. The new protocol design provides integrity, confidentiality, non repudiation and authentication. The node authentication is achieved by key encrypted onion routing with a route secret verification message. Digital signature formed with the help of RSA and Hash Function Message Digest MD5. AASR with digital signature provides higher throughput and lower packet loss ratio in different mobile scenarios in presence of adversary attacks. Simulation results demonstrate that the proposed protocol is efficient with improved performance.**

***Keywords*—Anonymous Secure Routing, Digital Signature, Hash Function, Mobile Ad hoc Networks**

I. INTRODUCTION

Mobile Ad hoc Networks (MANETs) are dynamic self configuring networks which consists of wireless mobile devices as nodes. They find ever increasing applications in both military and civilian systems. They are vulnerable to security threats due to their inherent characteristics such as open nature and dynamic topology. Adversaries induce selfish behavior in the network that disrupts the routing mechanism. Passive attacks create serious security concerns to mobile nodes and their traffics. It is difficult to provide trusted secure communication in critical situations, like battlefield.

Anonymous communications are vital for MANETs in adversarial environments. Anonymity is defined as the state of being unidentifiable within a set of subjects. It is described as a combination of unidentifiability and unlinkability. Anonymous secure routing protocols make use of random numbers or pseudonyms for representing the node identities.

The various anonymous routing protocols proposed so far do not satisfy complete anonymity. The existing protocols partially violate anonymity requirements for performance considerations. Information about the route or the node identities are disclosed by malevolent nodes during the routing procedure. Also, they are highly susceptible to Denial-of-Service (DoS) attacks, like RREQ based broadcasting attacks. The lack of packet authentication is another issue. Group signature scheme is not much scalable in the existing secure routing protocols. So it is difficult for the protocols to check whether a packet has been modified by a malicious node. The anonymous route calculation by secure hash function mechanism is not as scalable as the encrypted onion mechanism.

Authentication is essential to verify the true identity of the participating node and to protect the data integrity. Malicious nodes degrade the routing performance and consume the network resources. They inject false routing information in the network, intercept or modify the packets. Passive attacks, if not prevented, paves way to active attacks that destroy the whole network. Hence robust security mechanisms are necessary to mitigate against these eventualities.

Authenticated Anonymous Secure Routing (AASR) protocol is proposed to implement reliable and secure routing in presence of adversaries. Here, the focus is on topology based on-demand anonymous routing protocols which are general for MANETs in adversarial environments. The public and group key are initially deployed in the mobile nodes. A redesign of the control packets, Route REQuest (RREQ) and Route REPly (RREP) aims to preserve all kinds of privacy. Key encrypted onion routing is used 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. Pseudonyms are used to hide the node identities.

Extensive simulations are used to compare the performance of AASR to that of ANODR, a representative on-demand anonymous routing protocol. The results indicate that, it provides much lower packet loss ratio and lower end-to-end delay than ANODR under varying proportions of malicious nodes.

AASR experiences a cryptographic operation delay, due to its role in security processing. More robust operation can be achieved by integrating digital signature techniques to the protocol framework. Cryptographic solutions prevent the impact of attackers by enhanced authentication of the participating nodes through digital signature schemes. This results in enhanced reliability and secure routing operation with reduced cryptographic overhead.

The digital signature can be formed with the help of RSA algorithm and hash function MD-5. Thus AASR combined with digital signature technique enables to obtain lower packet loss ratio in adverse scenarios and provide secure anonymous data transmission. The new design can achieve all kinds of information security goals like confidentiality, integrity, availability and authentication.

II. RELATED WORK

Jiejun Kong and Xiaoyan Hong in 2003 proposed the Anonymous On Demand Routing Protocol (ANODR) with untraceable routes for MANETs. On-demand routing schemes are more “covert” in nature in that they do not advertise in advance; they just set up routes as needed. Here, the security concept called broadcast with trapdoor information is used. ANODR ensures that adversaries cannot discover the real identities of local transmitters. But it is unable to withstand the passive attacks that lead to high packet loss.

Karim El Defrawy and Gene Tsudik in 2011 conducted a study on the Anonymous Location Aided Routing in suspicious MANETs, the ALARM framework which supports anonymous location-based routing. The protocol demonstrates the feasibility of obtaining, at the same time, strong privacy and strong security properties. It uses the nodes’ current location to construct a secure MANET map. The loss in node privacy due to the dynamics of speed is a serious concern.

K.E.Defrawy and G.Tsudik in 2011 studied about the Privacy-friendly Routing in Suspicious MANETs (PRISM). It is an anonymous location centric on-demand routing protocol based on three building blocks; AODV, group signature and location information. The AODV protocol is used for route discovery. Group signatures, are used to ensure the conditional privacy property. Finally, location information is available to each node via GPS. This modular approach is computationally more efficient than ALARM. The security features provided by PRISM ensures safe operation in adverse scenarios, but suffers from packet delay.

Y.Zhang, W.Lou, and Y.G.Fang in 2013 conducted a study on a novel Anonymous Location-based Efficient Routing protocol (ALERT) in MANETs. It uses the hierarchical zone partition technique that dynamically partitions the network field into zones and randomly chooses nodes in those zones to serve as intermediate relay nodes. ALERT achieves better route anonymity protection and better routing efficiency. The inability of the protocol to adapt to the fast changing topology and number of participant nodes launch insecurity problems.

Z.Wan, K.Ren and M.Gu, in 2012 proposed an Unobservable Secure on-demand Routing scheme termed as USOR. This offers complete unlinkability and content unobservability for all types of packets. USOR is efficient as it uses a novel combination of group signature and ID based encryption for route discovery. It can well protect user privacy against both inside and outside attackers. The drawback is that every node maintains topology information, which is not a secure technique. The protocol cannot resist blackhole and wormhole attacks which may tamper with its performance.

III. NETWORK STRUCTURE

Here, an analysis of the adversaries, attack models and key establishment is done.

A. *Adversarial Environment*

Adversaries modify, fabricate or drop the packets to create an artificial delay. External adversaries try to destroy the network and acts as wireless link intruders. Internal adversaries are node intruders that capture and tamper the nodes. They aim to violate the availability of MANET and try to prevent the network from providing timely services.

B. *Attack Model*

The goal of a secure MANET system is to prevent routing protocol attacks. Passive attacks like eavesdropping and traffic monitoring are launched by internal adversaries. They are harmful to the network characteristics like availability and integrity. The invisible passive intruders aim to infer the traffic pattern and the identities of the source, destination or the en route nodes. This kind of misbehavior in the network leads to inefficient power management and security.

C. *Trapdoor*

The trapdoor concept is a one-way function between two sets. A global trapdoor is an information collection mechanism in which intermediate nodes may add various information elements. Only source and destination nodes can unlock and retrieve the elements. This is possible with the help of secret keys that establishes an anonymous end-to-end agreement.

D. *Key Establishment*

Consider the entire MANET as a group, denoted as T. Each node has public or private keys issued by a public key infrastructure (PKI). Besides, each node consists of a pair of group public or private keys issued by a group manager. The group public key, denoted by G_{T+}, is the same for all nodes in T while the group private key denoted by G_{A-} is different for each node. Any two nodes in a neighborhood can establish a security association and create a symmetric key that can be used for data transmission between them.

The notations can be summarized as in the table I.

TABLE I. SECURITY PRIMITIVES

Notations	*Descriptions*
K_{A+}	Public key of node A
K_{A-}	Private key of node A
G_{T+}	Group public key of network T
G_{A-}	Group private key of node A
K_{AB}	Symmetric key shared by nodes A and B

E. *Node Model*

1) Destination Table: The destination information, including destination’s pseudonym, public key, and pre-determined trapdoor string dest will be stored in destination table. For a particular session, the shared symmetric key is required for data encryption in that session. A sample entry of the destination table consists of destination pseudonym, trapdoor string, public key and session key.

2) Neighborhood Table: Every node locally exchanges information with its neighbors. It can generate different pseudonyms to communicate with different neighbors. This information is stored in the neighborhood table. A sample entry of the neighborhood table is neighborhood pseudonym and session key.

3) Routing Table: When a node generates or forwards a route request, a new entry will be created in the routing table. If a RREP packet is received and verified, the routing table will be updated. The fields of the routing table are request pseudonym, destination pseudonym, verification message, next hop pseudonym and status.

4) Forwarding Table: The forwarding table records the switching information of an established route. A sample entry of the forwarding table consists of the route pseudonym, previous hop pseudonym and next hop pseudonym. The route pseudonym is generated by the destination node, while the node pseudonyms of the previous and next hops are obtained after processing the related RREQ and RREP packets.

IV. SYSTEM DESIGN

The on-demand ad hoc routing is the base of the AASR protocol design. The packet formats of RREQ, RREP and the related processes are modified in order to protect anonymity while exchanging route information. The protocol building blocks are as follows:

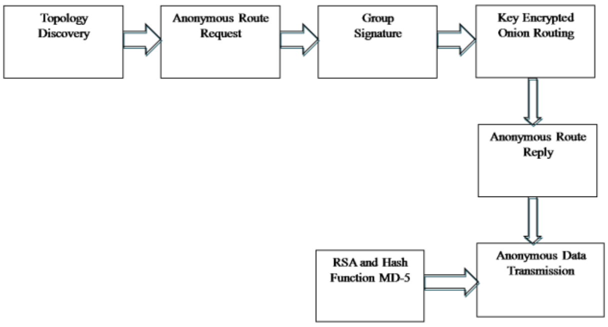

Topology Discovery
Anonymous Route Request
Group Signature
Key Encrypted Onion Routing
Anonymous Route Reply
RSA and Hash Function MD-5
Anonymous Data Transmission

Fig. 1. System Model

A. *Topology Discovery*

This section deals with the process of node creation. Several nodes are arranged in a random fashion in a specified area. Coverage range and connectivity are two important characteristics of the mobile nodes. A node can directly communicate with another which is within its communication range. Otherwise multiple hops are necessary to establish a communication link. Each node establishes a neighborhood relationship with the other nodes.

B. *Anonymous Route Request*

The anonymous routing procedures can be summarized as follows:

1) Source route request: Source node(S) generates a new session key KSD for association between source and detination. It acts as an initiator and broadcasts a route request packet to its neighboring nodes. The RREQ packet is of the format as follows:

$$[\text{RREQ}, N_{sq}, V_D, V_{SD}, \text{Onion}(S)]G_{S-} \qquad (1)$$

Here, RREQ is the packet type identifier; N_{sq} is the sequence number randomly generated by S; V_D is an encrypted message for request validation at the destination node; V_{SD} is an encrypted message for route validation at the intermediate nodes; Onion(S) is the key encrypted onion created by *S*. The whole RREQ packet is finally signed by *S* with its group private key G_{S-}.The combination of V_D and V_{SD} works as follows:

$$V_{SD} = (N_V)K_V \qquad (2)$$

In the route verification message, N_V is the one time nonce created by source for the particular route discovery process and K_V is the symmetric key. The secret message can be defined in the following format:

$$V_D = [N_V, K_V, \text{dest}]K_{SD}, (K_{SD})K_{D+} \qquad (3)$$

Only destination can decrypt the part of VD with its private key and obtain the corresponding information. The source creates the onion core in the following format:

$$\text{Onion}(S) = OK_V(N_S) \qquad (4)$$

In the core, Ns is the one time nonce generated by the source. It is then encrypted using the symmetric key K_V.

2) Intermediate node validation: The intermediate node(I) has already established neighbor relationships with the other nodes. Once I receives the RREQ packet it validates the packet with the group public key G_{T+}. Then it tries to decrypt the part of V_D with its own private key. In case of decryption failure, I understands that it is not the destination of RREQ. Now, the intermediate node modifies the packet and adds another encrypted layer on top of the key encrypted onion. This process is repeated until the RREQ packet reaches the destination or expired. I assembles and broadcasts the modified RREQ packet in the following format:

$$[\text{RREQ}, N_{sq}, V_D, V_{SD}, \text{Onion}(I)]\ G_{I-} \qquad (5)$$

The whole RREQ packet is finally signed by I with its group private key, G_{I-}. I updates onion in the following format:

$$\text{Onion}(I) = OK_{SI}(N_I,\text{Onion}(S)) \qquad (6)$$

Onion(I) is the updated onion part where K_{SI} is the symmetric shared key and N_I is the nonce generated by I. Onion(S) is obtained from the received RREQ packet.

3) Destination node: The destination node(D) is the intended receiver of the RREQ packet. Only D can decrypt the part of V_D. Then it obtains the session key K_{SD}, validation nonce N_V and validation key K_V.

C. *Group Signature*

The group signature is a special kind of signature scheme that is used to ensure privacy and protection. Any member of a group can sign on behalf of the group. The Group Manager controls the whole mechanism and issues certificates to the group members. This prevents any intermediate node from modifying the packet information. A node can generate its own signature by using its private key and such signature verified by other nodes using the group public key. The group public key is the same for all nodes in MANET while the group private key is different for each node.

Any node can enter and leave the group at any time. Both the new node and group manager must authenticate each other mutually at the time of network joining. Group signatures are unlinkable which makes it computationally hard to establish whether or not multiple signatures are produced by the same group member. Thus, it preserves the anonymity of the signers.

D. Key encrypted Onion Routing

The anonymous key encrypted onion routing serves as the backbone of route discovery process that implement secure and reliable communication. The source node creates the onion core. The one-time nonce is encrypted using the symmetric key and can only be decrypted by destination. Each intermediate node updates the onion part by adding another encrypted layer on top of it. This process continues until the packet reaches destination. Thus the information travels according to the layers on the onion and eventually an anonymous route can be established.

The onion routing procedures protects communication against traffic analysis attacks. Onion routers exhibit private communication over a public network. Each node has information of only the previous hop and next hop. No outside or inside observer would be able to alter the onion.

E. Anonymous Route Reply

1) Destination Node Reply: When destination receives the RREQ from its neighbor, it assembles a RREP packet and send it back to its previous hop. The intended receiver of the packet is I. The RREP packet format is as follows:

$$[\text{RREP}, N_{rt}, (K_V, \text{Onion(I)})\ K_{ID}] \qquad (7)$$

Here, RREP is the packet type identifier; N_{rt} is the route pseudonym generated by D; K_v and Onion(I) are obtained from the original RREQ and encrypted by the shared key K_{ID}.

2) Intermediate node verification: When RREP packet reaches the intermediate node, route verification takes place with the help of shared key K_{ID}. Decryption of onion layer indicates the next hop.Thus, on the reverse path back to the source, it removes one layer on top of the key encrypted onion and continues broadcasting the updated RREP.

3) Source node verification: Similar validation process takes place at the source node. If the decrypted onion core equals S's issued nonce, then S is the original RREQ source.Then the route discovery process ends successfully and the source updates its routing table. Now S is ready to transmit data along the route indicated by the route pseudonym.

F. Anonymous Data Transmission

After successful route discovery, the source is ready to transmit data to the destination. The format of the data packet is as follows:

$$[\text{DATA}, N_{rt}, (P_{data})\ K_{SD}] \qquad (8)$$

where DATA is the packet type, N_{rt} is the route pseudonym, P_{data} is the data payload which is encrypted by the session key K_{SD}. If N_{rt} in data packet matches an entry in the forwarding table then node will forward the data packet. Otherwise the packet will be discarded. The data packet switches along the discovered anonymous route until it arrives at the destination.

G. RSA Algorithm

The RSA algorithm is one of the most common public key cryptosystems which is widely used in digital signature technology. It is used for secure data transmission and is based on factorization of very large numbers. The algorithm is named after its designers, Rivest, Shamir and Adleman. It can be used to encrypt a message without the need to exchange a secret key separately.

They are extensively used in digital signature technology. In such a cryptosystem, the encryption key is kept public and differs from the decryption key which is kept secret. The algorithm is also known as the asymmetric algorithmic technique. It uses a variable size key and variable size encryption block. The algorithm is highly reliable and used in extensive applications. It is computationally efficient and highly improbable for any adversary to crack it. It ensures better privacy and security and resistant to attacks.

H. Hash Function

A hash function is a special type of function used to map digital data of arbitrary size to digital data of fixed size. An important application of secure hashes is verification of message integrity. These functions are widely known as digital fingerprints of data. They are non-invertible and provide faster and secure data transmission.

Cryptographic hash functions find extensive use in digital signature schemes. Here, MD5 is used for computations. The type of algorithmic function produces a 128 bit hash value. This offers digital security and preserves the data integrity. This applies to a block of data of any size and maps the message block to a fixed size hash value, which serves as the authenticator. It can be implemented faster and can withstand all forms of attacks.

I. Digital Signature

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message. The technology makes use of RSA algorithm and hash function MD-5. The digital signature based crypto techniques protects data from unauthorized access or alteration, and can also be used for authentication purposes. The hash values are shorter than the messages, and helps for easier analysis. It also includes measures to counter repudiation either by source or destination.

V. PERFORMANCE ANALYSIS

AASR can achieve the following anonymity and security goals to defend the various attacks, so as to maintain secure communication.

A. Anonymity analysis

There are three important anonymities of AASR, namely identity anonymity, route anonymity, and location anonymity. Here, it is assumed that all the nodes, including those on the discovered route, are potential adversaries that are interested in privacy information.

1) Identity Anonymity: All nodes generate random nonce to indicate themselves. Consequently, the adversaries cannot acquire the identities of source, destination and intermediate nodes. There is no identity-related information in the entire routing process.

2) Route Anonymity: During the route discovery, each node has information of only about the previous and next hop. Even if a node participates in route discovery, it has no idea about the route involved.

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

B. Security Analysis

It is impossible for an eavesdropper to obtain the identity or location information of any participating node, in any communication session in AASR. Here, any node without the group key cannot join the communications. Fake routing packet and routing misbehaviors can be identified with the help of group manager. DoS attacks aim to deplete the nodes' resources and degrade the performance of the network. Any such abnormal behavior is reported to the group manager and can be tracked accordingly.

C. Secure Data Transmission

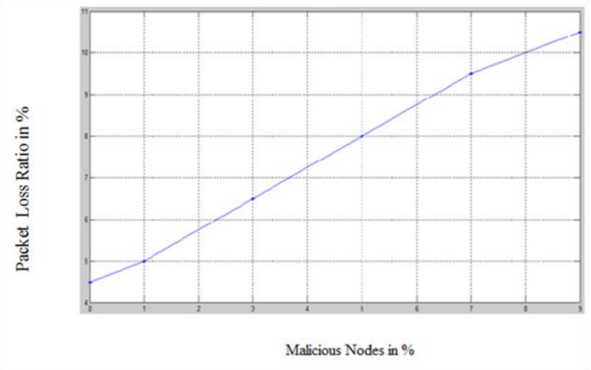
Secure routing and data transmission is an important issue in MANETs. For fast data transmission, the routing protocol must adapt quickly to the topology changes. It should work in a distributed self organizing manner. Cryptographic solutions prevent the impact of attackers by mutual authentication of the participating nodes through digital signature schemes. Advanced cryptographic techniques based on digital signature can ensure secure and reliable routing in presence of adversaries. This makes the network fault tolerant and secure.

VI. SIMULATION RESULTS

The proposed AASR protocol integrated with digital signature technology is simulated using MATLAB software. The simulation procedures analyses the performance of the protocol under various adverse scenarios.

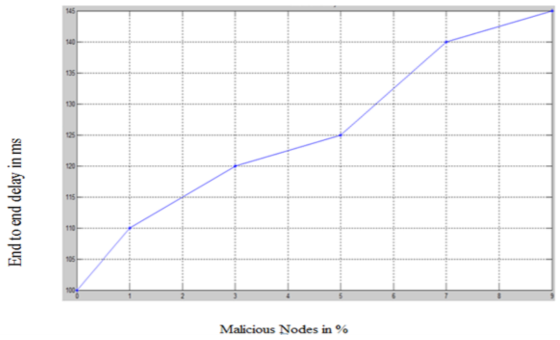
A. Packet Loss Ratio

The ratio of the number of packets lost to the number of packets sent by the source node is termed as the packet loss ratio. It is expressed in percentage. When there is an increase in the number of malicious nodes the PLR gradually increases. The simulation results show that the AASR protocol provides a 2% less packet loss ratio on an average.



B. End-to-end Delay

The average time a packet takes to travel from source to destination is termed as the end-to-end delay. The system counts only the data packets that are successfully delivered to destination. Compared to ANODR, the protocol provides a 30 ms less of delay in average.



VII. APPLICATIONS

With the increasing use of portable communication devices ad hoc networking has widespread applications. The proposed system finds wide use in military battlefields where there is an urgent need for collaborative communication with high degree of security and privacy. It also finds application in natural disasters like earthquakes and floods where emergency rescue operations are to be carried out in a disruption tolerant manner. The system can quickly replace the destroyed communication infrastructure, enabling better coordinated efforts.

VIII. CONCLUSION

The AASR protocol with digital signature offers improved security features that can defend the potential attacks without unveiling the node identities. Compared to AASR, the protocol provides higher throughput and lower packet loss ratio in presence of adversary attacks. It provides better support for secure communications that are sensitive to packet loss ratio.

ACKNOWLEDGMENT

I would like to thank Mr. M. Jeba Vins, M.E., Head of the Department, for his help and support for the work. Also I would like to thank my project guide Mr. P. Vinod, M.E., Assistant Professor, for his guidance throughout the work. I would like to express my deepest thanks to all those people who have influenced the work.

REFERENCES

[1] Boneh, X. Boyen, and H. Shacham, “Short group signatures,” in Proc. Int. Cryptology Conf. (CRYPTO’04), Aug. 2006.

[2] Brown, D. Hankerson, J. L´opez, and A. Menezes, Software ed., implementation of the NIST elliptic curves over prime fields. Springer, 2001.

[3] 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] Defrawy and G. Tsudik, “Privacy-Preserving Location-Based On-Demand Routing in MANETs,” IEEE Journal on Selected Areas Communications, vol. 29, no. 10, pp. 1926–1934, Dec. 2011.

[5] Hong, J. Kong, Q. Zheng, N. Hu, and P. Bradford, “A Hierarchical Anonymous Routing Scheme for Mobile Ad-Hoc Networks,” in Proc. IEEE MILCOM’06, Oct. 2006.

[6] Hu, D.B. Johnson, and A. Perrig, “Ariadne: A Secure On- Demand Routing Protocol for Ad Hoc Networks,” Proc. MobiCom, 2002.

[7] Johnson, D.A. Maltz, and J. Broch, “DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks,” Ad Hoc Networking, Addison-Wesley, 2001.