Volume 3, Issue 4, April-2016, pp. 199-203 ISSN (O): 2349-7084

International Journal of Computer Engineering In Research Trends

Available online at: www.ijcert.org

Secure Routing for MANET in Adversarial Environment

Nilima N. Patil, Kuldeep K. Vartha, Ashwini W. Wankhade, Sagar A. Patil

Abstract:-Collection of mobile nodes is known as ad-hoc network in which wireless communication is used to connect these mobile nodes. A major requirement on the MANET is to provide unidentifiability and unlinkability for mobile nodes. There are various secure routing protocols have been proposed, but the requirement is not satisfied. The existing protocols are unguarded to the attacks of fake routing packets or denial-of-service broadcasting, even the node identities are protected by pseudonyms. We propose a new secure routing protocol which provides anonymity named as authenticated anonymous secure routing (AASR), to satisfy the requirement of mobile networks and defend the attacks. The route request packets are authenticated by a group signature and public key infrastructure, to defend the potential attacks without exposing the node identities. The cocept of key-encrypted onion routing which provides a route secret verification message, 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 to the existing protocols.

Keywords – Anonymous Routing, Mobile Ad hoc Networks, AASR.

1. INTRODUCTION

Mobile ad hoc networks (MANETs) are unguarded to security threats due to the open wireless medium and dynamic topology. It is difficult to provide trusted and secure communications in adversarial environments. The adversaries outside a network may infer the information about the communicating nodes or traffic flows. Also the nodes inside the network cannot be trusted, since a valid node may be captured by enemies and becomes malicious. Hence, anonymous communications are important for MANETs in adversarial environments.

In Section 1 a brief introduction is given with problem definition. Related work with various secure routing protocols in MANET's technique is illustrated in Section 2. Proposed work with detailing is explained in Section 3. Output Screenshots and simulation results are described in Section 4. Section 5 is all about the conclusion of overall paper.

1.1. MOTIVATION

Motivation for proposed protocol lies in recently growing issue in MANETs which is anonymity with authentication. Already, there are various anonymous routing protocols proposed but those not provide the anonymity. We find that the objectives of unidentifiability and unlinkability are not fully satisfied by the already existing protocols. Anonymity is defined as the state of being unidentifiable within a set of subjects. These protocols are also vulnerable to the denial-of-service (DoS) attacks. Due to the lack of packet authentication, it is difficult for the protocols to check whether a packet has been modified by an attacker node. The key to implementing the anonymous communications is to develop appropriate anonymous secure routing protocols. We propose secure routing protocol based on the key-encrypted onion routing with group signature which is used to authenticate the RREQ packet per hop.

1.2. PROBLEM DEFINITION

In MANETs, the requirements of anonymous communications can be achieved by the combination of unindentifiability and unlinkability. Already there are

so many anonymous routing protocols proposed. Our main aim is the type of topology based on-demand anonymous routing protocols, which are general for MANETs in adversarial environments. The commonly used on-demand ad hoc routing protocols are AODV [2] and DSR . Secure Ad-hoc On-demand Distance Vector RoutingProtocol (SAODV) [4] is advance version of AODV routing protocol. SAODV make use of asymmetric cryptography with the help of group signatures. When a node wants to send a message it digitally signs the RREQ packet and send it to the neighboring nodes.On receiving a RREQ, intermediate nodes verifies the signature before updating or creating a reverse route to the hostwith the help of cryptography. Secure Efficient Ad-hoc Distance Vector Routing (SEAD) [3] protocolis a proactive routingprotocol which maintains fresh lists of destinations and their routes by periodically distributing routing tables throughout the network. This protocol makes use of hash chain method for checking the authenticity of the data packet. This hash chainvalue is used for transmitting a routing update. A node that receives a routing update, verifies theauthentication of eachentry of the message. SEAD make use of destination sequence number in order to remove looping. Both SAODV and SEAD cannot satisfy the requirement of anonymous communications. Now, we focus on the MANETs in adversarial environments, where the public and group key can be initially deployed in the mobile nodes. We propose an authenticated anonymous secure routing (AASR) to overcome the above problems. We use a key-encrypted onion to record a discovered route and design an encrypted secret message to verify the RREQ-RREP. To authenticate the RREQ packet at each hop is necessary which is achieved by group signature.

2. RELATED WORK

G. Anandhi, Dr. S. K. Srivatsa [1], provide a detailed survey of different kind of attacks and proposed solutions for handling those attacks. Their paper also gives a brief comparison of various protocols available for secured routing in MANET like Secure Ad-hoc On-demand Distance Vector Routing Protocol (SAODV), Secure Efficient Ad-hoc Distance Vector Routing (SEAD), and Security-Aware ad hoc Routing (SAR).

Sheng Liu, Yang, Weixing Wang [2], propose the basic characteristic, key techniques of Ad Hoc networks, and compared with other mobile communication systems. Through analyzing and comparing with DSR, TORA, ABR, AODV, it researched on-demand routing protocol for Ad Hoc networks. It introduces AODV routing protocol in details.

Prasuna V G, Dr. S. Madhusudhana Verma [3], propose Secure Efficient Ad hoc Distance Vector with fixed hash chain length in short SEAD-FHC protocol to minimize and stabilize the computational complexity that leads minimization in delay time and maximization in throughput. A series of simulation experiments are conducted to evaluate the performance.

C. Sreedhar, Dr. S. Madhusudhana Verma, Dr. N. Kasiviswanath [4], describes Secure AODV routing protocol which was designed to enhance security services to the original AODV. SAODV protocol was designed with cryptographic techniques such as digital signatures, which can have significant impact on the routing performance of AODV routing protocol.

3. PROPOSED WORK

There are many anonymous on-demand routing protocols. But these protocols arevulnerable to the denial-of-service (DoS) attacks, such as RREQ based broadcasting. Due to thelack of packet authentication, it is difficult for the protocolsto check whether a packet has been modified by a malicious node. So, we proposed the other routing protocol known as authenticated anonymous secure routing (AASR) which is topology-based routing rather than location-based routing. To avoid theinformation leakage during RREQ and RREP processes, AASR uses the nodes pseudonym instead of its real identifier. We choose the onion based routing to record the anonymous routes, because the onion is more scalable than othermechanisms and can be extended, for example to multiple paths.We assume that the nodes are equipped with public and private keys during network initializationphase and can generate the shared symmetric key in an on-demand manner.

3.1. ONION ROUTING

It is a mechanism to provide private communications over a public network. The source nodesets 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 sourceand 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.

3.2. GROUP SIGNATURE

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 (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 signature identity. Only the group trust authority can trace the signature identity and revoke the group keys.

3.3. PROTOCOL DESIGN

Protocol design present the design of AASR protocol. Considering the mobility, we take the on-demand ad-hoc routing as the base of protocol, including the following phases

- Route discovery phase
- Data transmission phase
- Route maintenance phase.

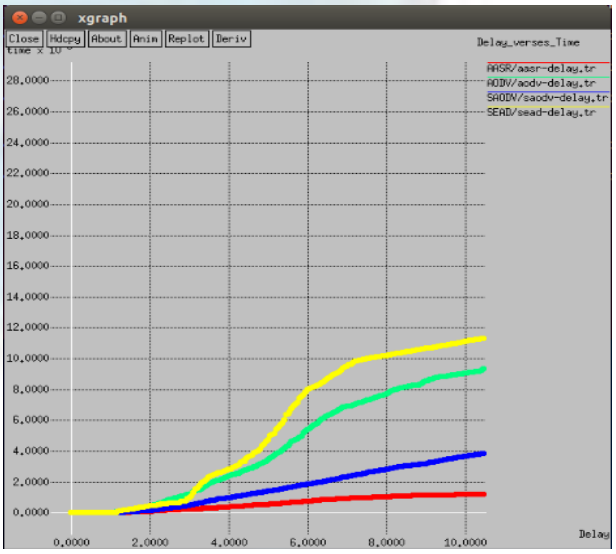
In the first route discovery phase, the source node broadcasts an RREQ packet to every node in the network. If the destination node receives the RREQ to itself, it will reply an RREP packet back along the incoming path of the RREQ. In order to protect the anonymity when exchanging the route information, we redesign the packet formats of the RREQ and RREP, and modify the related processes. After the route is discovered, data can be send over that route.

3.4. ROUTING PROCEDURE

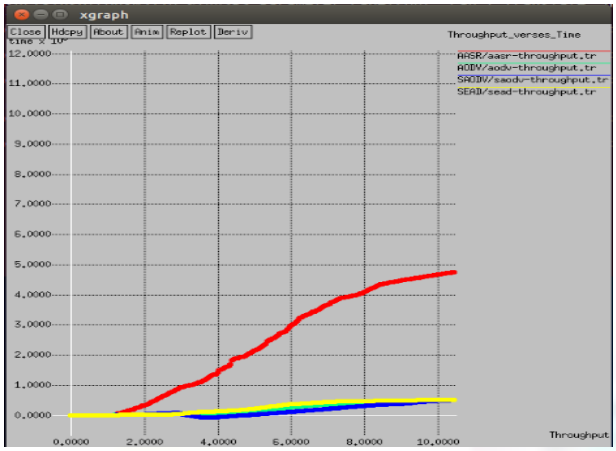
The routing algorithm can be implemented based on the existing on-demand ad hoc routing protocol like AODV or DSR. The main routing procedures can be given as follows:

1) During route discovery, a source node broadcasts an RREQ packet in the format which contains packet type identifier; sequence number randomly generated by source; an encrypted message for the route validation at the intermediate nodes; an encrypted message for the request validation at the destination node; finally whole packet is signed by source group private key.
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. This process is repeated until the RREQ packet reaches the destination or expired.
3) Once the RREQ is received and verified by the destination node, the destination node assembles an RREP packet in the format which contains packet type identifier; route pseudonym generated by destination; original message encrypted by destination shared key, and broadcasts it back to the source node.
4) On the reverse path back to the source, each intermediate node validates the RREP packet 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 packet format .
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 established route in the format of packet which contains packet type; the route pseudonym that can be recognized by intermediate nodes; the data payload which is encrypted by the session key. Every intermediate node forwards the data packets by using the route pseudonym.

4. OUTPUT SCREENSHOTS



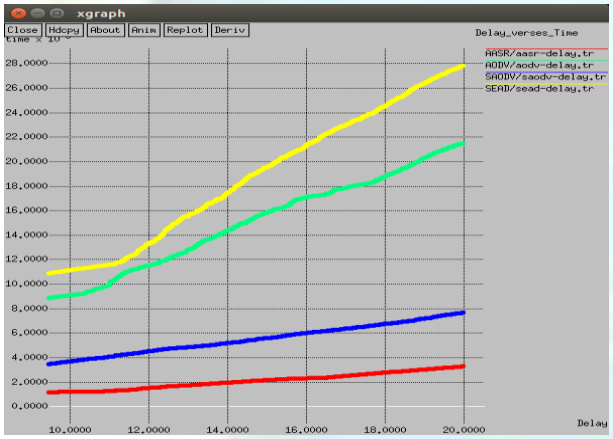
(a)



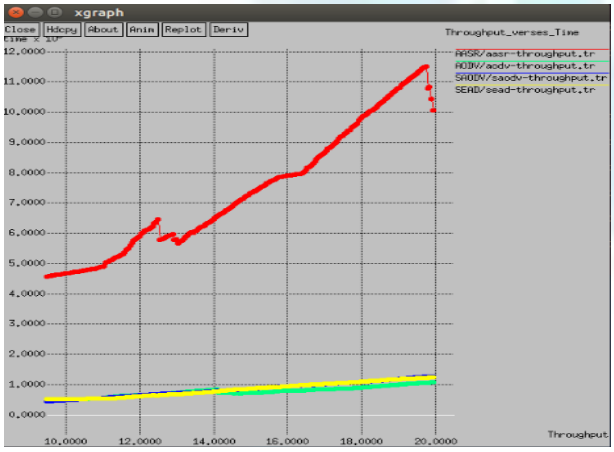
(b)

Fig 1. Performance comparison before attack

(a) Delay. (b) Throughput.



(a)



(b)

Fig 2.Performance comparison after attack (a) Delay,.(b) Throughput.

4.1. SIMULATION RESULT

The proposed approach is implements with NS2 simulator. AODV protocol is used for routing purpose with the support of cryptographic operations. The mobile Ad-hoc network of 30 nodes is created with the boundary area of 1500*1500 meter. We compare the performances of AASR to those of SEAD, SAODV and AODV in various mobility and adversary scenarios. The radio uses the two-ray ground reflection propagation model. The channel capacity is 1Mbps. The transmission range is 150m. The Random Way Point (RWP) model is used to model the nodal mobility. In our simulation, the mobility is controlled in such a way that the speed varies in the range of the minimum and maximum speeds. A total of 15 UDP based CBR sessions are used to generate the network traffic. For each session, the data packets are generated with the size of 1000 byte in the rate of 1Mbps. The source-destination pairs are chosen randomly from all the nodes.

We present two groups of simulation results. The first one is to compare the routing performances of AODV, SAODV, SEAD and AASR under different mobility scenarios before the attacks as shown in Fig. 1. The second one is to compare their behaviors under the packet dropping attacks with different levels as shown in Fig. 2. We perform four simulation runs for each configuration, and record the performances, including throughput and end-to-end delay.

5. CONCLUSION

MANET is a highly dynamic and mobile network and hence more vulnerable to attack. Anonymous communications are important for MANETs in adversarial environments to defend it from various attacks. So, the proposed secure routing protocol for MANETs which is authenticated anonymous secure routing (AASR) provides anonymity. AASR uses the concept of group signature and onion routing. The key-encrypted onion routing with a route secret verification message is designed to record the anonymous as well as to prevent the intermediate nodes from inferring the real destination. Compared to SEAD, SAODV and AODV, AASR provides higher throughput and lower end-to-end delay in different mobile scenarios in the presence of adversary attacks.

REFERENCES

[1] Sneddon, G.Anandhi, Dr.S.K.Srivatsa, "Secured Routing in MANETs", International Journal of Computer Science and Information Technology, Vol. 2, Issue 2, pp.: (311-318), Month: April-June 2014.

[2] Sheng Liu, Yang, Weixing Wang, "Research of AODV Routing Protocol for AdHoc Networks", 2013 AASR, Conference on Parallel and Distributed Computing and Systems.

[3] Prasuna V. G, Dr. S. Madhusudhana Verma, "SEAD-FHC: Secure Efficient Distance Vector Routing with Fixed Hash Chain length", Global Journal of Computer Science and Technology Volume 11 Issue 20 Version 1.0 December 2011

[4] C. Sreedhar, Dr. S. Madhusudhana Verma, Dr. N. Kasiviswanath,"Performance Analysis of Secure Routing Protocols in Mobile Ad-Hoc Networks", International Journal of Computer Science And Technology .

