International Journal of Engineering Research and General Science Volume 3, Issue 4, Part-2, July-August, 2015
ISSN 2091-2730

Authenticated Anonymous Secure Routing Using Trust Model Technique

Aswathi Rajan, Kiran Krishnan

PG Scholar, Department of ECE, CAARMEL Engineering College, Pathanamthitta, Kerala
Assistant Professor, Department of ECE, CAARMEL Engineering College, Pathanamthitta, Kerala

Email:aswathirajan03@gmail.com

Abstract:Anonymous communications are vital for several applications of the mobile unplanned networks (MANETs) deployed in someone environments. A significant demand on the network is to produce unidentifiability and unlinkability for mobile nodes and their traffics. Though variety of anonymous secure routing protocols is projected, the necessity isn't absolutely glad. The present protocols are susceptible to the attacks of pretend routing packets or denial-of-service (DoS) broadcasting, even the node identities are protected by pseudonyms. A brand new routing protocol is projected, i.e., documented anonymous secure routing (AASR), to satisfy the necessity and defend the attacks. Additional specifically, the route request packets are documented by a gaggle signature, to defend the potential active attacks while not unveiling the node identities.

Keywords: Anonymous Routing, Authenticated Routing,Mobile Adhoc Network,Trust Management.

INTRODUCTION

MANETS rely on wireless transmission, a secured way of message transmission is important to protect the privacy of the data. An insecure ad-hoc network at the edge of communication infrastructure may potentially cause the entire network to become vulnerable to security breaches. There is no central administration to take care of detection and prevention of anomalies in Mobile ad hoc networks. Mobile devices identities or their intentions cannot be predetermined or verified. Therefore nodes have to cooperate for the integrity of the operation of the network. However, nodes may refuse to cooperate by not forwarding packets for others for selfish reasons and not want to exhaust their resources. Various other factors make the task of secure communication in ad hoc wireless networks difficult include the mobility of the nodes, a promiscuous mode of operation, limited processing power, and limited availability of resources such as battery power, bandwidth and memory. Therefore nodes have to cooperate for the integrity of the operation of the network. Nodes may refuse to cooperate by not forwarding packets for others for selfish reasons and not want to exhaust their resources. A community of ad-hoc network researchers has proposed, implemented, and measured a variety of routing algorithms for such mobile, wireless networks. While these ad-hoc routing algorithms are designed to generate less routing protocol traffic than the above-mentioned shortest-path routing protocols in the face of a changing topology, they nevertheless compute shortest-path routes using either topological information concerning the entire network, or topological information concerning the entire set of currently used paths between sources and destinations. Thus, their ability to find routes depends similarly on describing the current wide-area topology of the network to routers.

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 or localization service available when the network is deployed. We propose an authenticated anonymous secure routing (AASR) to overcome the pre-mentioned problems. The primary challenge in building a Manet is mobilisation every device to ceaselessly maintain the knowledge needed to properly route traffic. Such networks could operate by themselves or is also connected to the larger web [3]. They will contain one or multiple and totally different transceivers between nodes. This leads to an extremely dynamic, autonomous topology.

RELATED WORK

The main focus is to discuss the anonymous communication protocols that have been proposed already for MANETs. Most of the works are based on onion routing protocol in which data is enclosed in a series of encrypted layers to form an onion by a series of proxies communicating over encrypted channels.

Kong and Hong [2] proposed Anonymous On-Demand Routing (ANODR) Protocol is the first one to provide anonymity and unlinkability for routing in MANET. ANODR uses one-time public or private key pairs to attain anonymity and unlinkability but fails to assure content unobservability. An efficient anonymous routing for MANET which provides advantages for ANODR protocol is

that routing performance changes notably when different cryptosystems are used to implement the same function. Seys and Preneel [4] proposed Anonymous Routing (ARM) Protocol uses one-time public or private key pairs and go behind only anonymity in route discovery and data forwarding. Yang [5] proposed Discount ANODR performs lower computation and communication complexities at the cost of a small reduction of privacy but provides only source anonymity and routing privacy. Qin [6] proposed On-Demand Lightweight Anonymous Routing (OLAR) scheme which involves the secret sharing scheme which is based on the properties of polynomial interpolation mechanism to reach anonymous message transfer without per-hop encryptions and decryptions. The only job for a forwarder is to perform additions and multiplications which is less expensive than traditional cryptographic operations. Pan and Li [7] proposed Efficient Strong Anonymous Routing (MASR) Protocol which uses onion routing scheme to achieve anonymity but leads to routing overhead and high computational cost. Efficient Anonymous Routing Protocol for Mobile Ad Hoc Networks adapts onion routing algorithm to achieve anonymity. In this the node that participates in the protocol, encrypts the whole message with a trust key and says Hello to its preceding nodes within the expiration time. This approach detects the malicious nodes and isolates the node from the network. V-routing based on proactive routing protocol which hides the location and identity of the communication parties but it provides less security for the data. Zhang [9] proposed Anonymous On-Demand Routing (MASK) enables anonymous on-demand routing protocols with high routing efficiency by comparing with ANODR which is very much sensitive to node mobility that may lower routing efficiency. Dong [10] proposed Anonymous routing protocol with multiple routes (ARMR) communications in mobile ad hoc networks and anonymous and secure reporting (ASR) of traffic forwarding activity in mobile ad hoc networks which makes use of one-time public or private key pairs which achieve anonymity and unlinkability. ARMR uses one-time public-keys and bloom filter to find out multiple routes for mobile ad hoc networks and ASR is designed to achieve stronger location privacy, which ensures nodes on route does not have any information on their distance to the source or destination node. Anonymous Location-Aided Routing in Suspicious MANETs uses group signature but this protocols are not suitable for practical approach to routing in mission-critical location-based environment because there is no analysis on protocols performance for privacy and security.

AASR NODE MODEL

In order to design the routing algorithm the following node models are considered.

Destination Table: we tend to assume that a supply node is aware of all its attainable destination nodes. The destination info, together with one in all destinations' name, public key, and therefore the pre-determined trapdoor string destination are going to be keeping within the destination table. Once a session to the destination is established, the shared radially symmetrical key's needed for information encryptions within the session. Such radially symmetrical keys generated by the supply node before causing the route requests, and keep within the destination table when receiving the route reply. As an example sample entry of the destination table is (DestNym, Dest String, Dest Public Key, Session Key).

Neighbourhood Table: We assume that each node domestically exchanges info with its neighbours. It will generate completely different| pseudonyms to speak with different neighbours. The neighbours security associations are established likewise because the shared regular keys. The data is kept in a very neighbourhood table. For instance, a sample entry of the neighbourhood table is (Neighbour Nym, Session Key).

Routing Table: When a node generates or forwards a route request, a replacement entry are created in its routing table that stores the request's anonym and also the secret verification message during this route discovery. Such associate entry is marked within the standing of "pending". If associate RREP packet is received and verified, the corresponding entry within the routing table are updated with the anonymous next hop and also the standing of "active". Meanwhile, a replacement entry is created within the node's forwarding table. As an example, a sample entry of the routing table is (ReqNym, DestNym, VerMsg, Next hop Nym, Status). Note that, to modify the notation, we have a tendency to ignore the timestamp data of the entry within the table. 4) Forwarding Table: The forwarding table records the switch data of a long time route. We have a tendency to adopt the per hop name because the symbol for packet switch, just like the VCI (virtual channel identifier) in ATM networks. In every entry of the forwarding table, the route name is generated by the destination node, whereas the node pseudonyms of the previous and next hop square measure obtained when process the connected RREQ and RREP packets. For instance, a sample entry of the forwarding table is (RtNym, Prev hop Nym,Next hop Nym).

AASR PROTOCOL DESIGN

The In this section, we present the design of AASR protocol. Considering the nodal mobility, we take the on-demand adhoc 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 redesign the packet formats of the RREQ and RREP, and modify the related processes. 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.

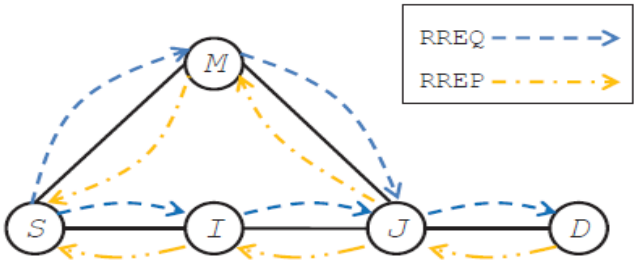

Fig 1: Network topology

Anonymous Route Request

1) Source Node: We assume that S initially knows the information about D, including its pseudonym, public key, and destination string. The destination string dest is a binarystring, which means "You are the destination" and can be recognized by D. If there is no session key, *S* will generate anew session key Ksdfor the association between Sand D.Then, Swill assemble and broadcast an RREQ packet in the format.

$S \rightarrow *$: [RREQ; Nsq; V_D; V_{SD}; Onion(S)] GS

whereRREQis the packet type identifier; Nsqis a sequence number randomly generated by *S* for this route request; $V_D$is an encrypted message for the request validation at thedestination node; $V_{SD}$is an encrypted message for the routevalidation at the intermediate nodes; Onion(S) is a keyencryptedonion created by S. The whole RREQ packet isfinally signed by Swith its group private key GS.

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 neighbour relationship with S and J.I knows where the RREQ packet comes from.I checks the Nsq and the timestamp in order to determine whether the packet has been processed before or not. If the Nsqis not known in the routing table, it is a new RREQ request; if the Nsq exists in the table but with an old timestamp, it has been processed before and will be ignored; if the Nsq exists with a fresh timestamp, then the RREQ is a repeated request and will be recognized as an attack.

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 the S's route request.

B. Anonymous Route Reply

1) Destination Node: When D receives the RREQ from its neighbour 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; Nrt;⟨Kv;Onion (J)⟩KJD)

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 K_{JD}. The intended receiver of the RREP is J.

2) Intermediate Node: We assume that J has already established a neighbour relationship with I, D, and M.If Jreceives the RREP from D, Jwill navigate the shared keys in its neighbourhood table, and try to use them to decryptIn case of a successful decryption, Jknows the RREP 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.

3) Source Node: When the RREP packet reaches S, S validates the packet in a similar process to the intermediate nodes. If the decrypted onion core NS equals to one of S's issued nonce, S is the original RREQ source.Then the route discovery process ends successfully. S is ready to transmit a data along the route indicated by Nrt.

C. Anonymous Data Transmission

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

S → D: (DATA; Nrt; ⟨Pdata⟩KSD)

where DATA is the packet type; Nrt is the route pseudonym that can be recognized by downstream nodes; the data payload is denoted by Pdata, which is encrypted by the session key KSD.

D. 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 summarized as follows:

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

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 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 and updates its routing and forwarding tables. Then it removes one layeron the top of the key-encrypted onion, and continues broadcasting the updated RREP in the format.

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

6) The source node starts data transmissions in the established route in the format. Every intermediatenode forwards the data packets by using the routepseudonym.

SIMULATION RESULTS

We implement the proposed AASR protocol in ns-2 by extending the AODV module to support the cryptographic operations.

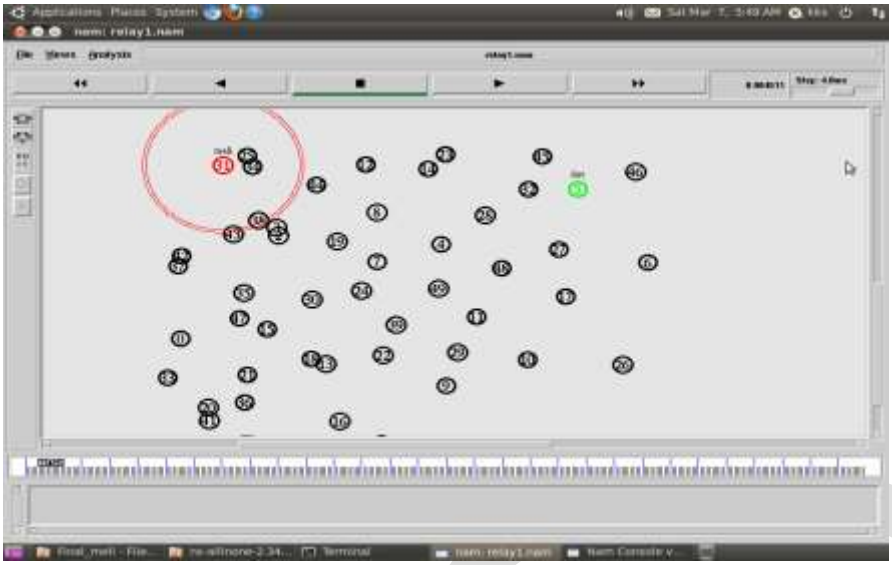

Fig 2: Entering of malicious node into the network.

Entering of malicious node to the network is shown in the figure 2. While entering the network all the normal nodes will send the fake request to the malicious node. Normally the fake node will reply but some cases it will not reply to this request. To avoid this all the nodes will send the fake request to the malicious node. If any of the node receives a reply from the malicious node, it will broadcast to all the nodes in the network.

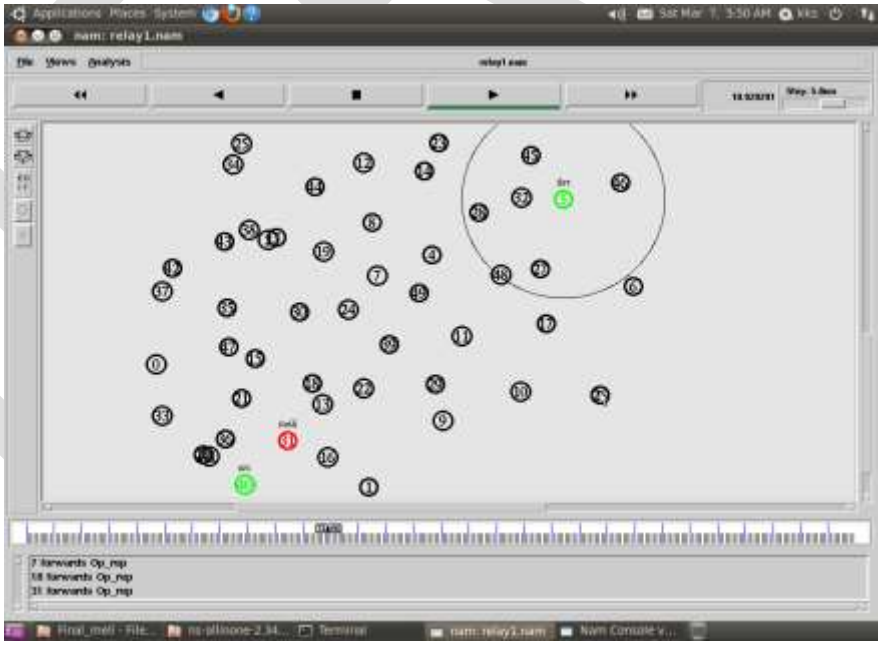

Fig 3: Malicious node entered in the network

In figure 3 the malicious node entered the network and all other nodes are checking and sending the fake request to the malicious node .

.

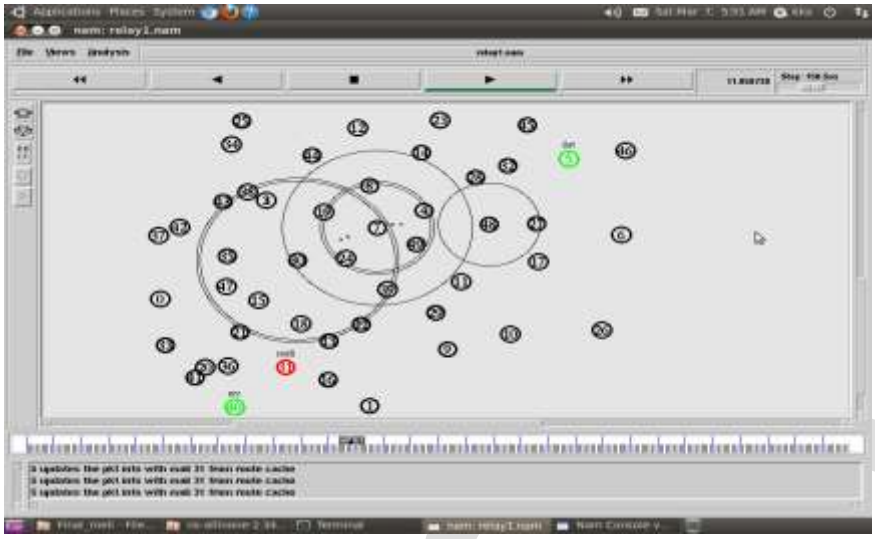

Fig 4: Malicious node identification

In figure 4 the malicious node is identified by all nodes because of the broadcast message. Now all the nodes will eliminate the malicious node from their route. And it will eliminate the path with the malicious node. Data is transmitted to the destination without any failure by avoiding the malicious node in the network.

CONCLUSION

In this paper, we tend to style associate genuine and anonymous routing protocol for MANETs in adversarial environments. The route request packets are genuine by cluster signatures, which might defend the potential active anonymous attacks while not unveiling the node identities. The key-encrypted onion routing with a route secret verification message is intended to not solely record the anonymous routes however conjointly forestall the intermediate nodes from inferring the important destination. This paper gives the information about AASR in network. Which provide different information that useful for achieving propose work with respect to scenario.

REFERENCES:

[1] 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.

[2] J.Kong and X. Hong, "ANODR: Anonymous On Demand Routing with Untraceable Routes for Mobile Ad hoc networks," in Proc. ACM MobiHoc'03, Jun. 2003, pp. 291–302.

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

[4] 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.

[5] Y. Liu, J. Markus, and W. Susanne, "Discount Anonymous On Demand Routing for Mobile Ad hoc Networks," in Proc. 2nd International Conference on Security and Privacy in Communication Networks,Baltimore, 2006, pp. 1-10.

[6] Q. Yang, H. Dijiang, and K. Vinayak, "OLAR: On-demand Lightweight Anonymous Routing in MANETs," in Proc. 4th International Conference on Mobile Computing and Ubiquitous Networking, Tokyo, 2008, pp. 72-79.

[7] P. Jun, and L. Jianhua, "MASR: An Efficient Strong Anonymous Routing Protocol for Mobile Ad Hoc Network," in Proc. International Conference on Management and Service Science, Wuhan, 2009, pp. 1-6.

[8] R. Song, L. Korba, and G. Yee, "AnonDSR: efficient anonymous dynamic source routing for mobile ad hoc networks," in Proc. ACM Workshop Security of Ad Hoc and Sensor Networks (SASN'05), Nov. 2005