International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Enhanced Onion Routing Framework for MANETs

Karumuri. Ashok Kumar[1], B. Neelima[2]

[1]Computer Science Engineering, Vignan's Lara Institute Of Technology, Guntur, India

Abstract: ***The mobile ad hoc networks (MANETs) is wireless and dynamic topology network medium, which may suffer from many open security criticism. The major issue of mobile ad hoc networks (MANETs) is to send the data in secure manner from source to destination node in adversarial (opponent) environment such wireless node communication issues are node traffic, node attack and data accessing of intermediate nodes. Many of us has to develop the routing protocol for security enhancement in adversarial environment, but this protocols are not that much secure routing in MANETs. The existing protocol works on the basis of authentication group signature, and onion routing protocol. In this paper proposal routing protocol method is Authenticated Anonymous Secure Routing with Trust based model. AASR protocol concept is to defend the neighbour nodes attack by the way of key encryption and decryption in route-request and route-reply. The calculating trust value of the intermediate node in MANET routing can helps to avoid the end to end packet transfer delay between nodes.***

Keywords: Trust Model, Authenticated Routing, Group Signature, Onion Routing, Mobile Ad hoc Networks

1. Introduction

In Ad hoc on-demand trend, routing information is created to requested destination. On-demand strategy causes less overhead and easier to scalability. Ad hoc on demand distance vector routing (AODV) is the combination of DSDV and DSR. TORA (Temporary Ordered Routing Algorithm) is based on link reversal algorithm. Each node in TORA maintains a table with the distance and status of all the available links. A mobile ad hoc network (MANET) is a wireless and easily configures for transfer the data to all active destination node of the network [1]. In the ad-hoc network, there is no fixed infrastructure such as base stations or mobile switching centres.

Mobile nodes that are within each other's radio range communicate directly via Wireless links, while those that are far apart rely on other nodes to relay messages as routers. Node mobility in an ad hoc network causes frequent changes of the network topology. Mobile ad hoc networks are finding ever increasing applications in both military and civilian scenarios due to their self-organizing, self-configuring capabilities [2].

An ad hoc network can be attacked from any direction at any node which is different from the fixed hardwired networks with physical protection at firewall and gateways. Altogether it denotes that every node should be equipped to meet, both inside or outside attacker directly or indirectly.

This paper is topology based MANETs, it has chance to get attack in its routing path for this consideration need authenticated based topology routing. Our anonymous communications in MANETs has unidentifiability and unlinkability. Unindentifiability means the source and destination node cannot be identify by the other nodes. Unlinkability means that the route between the source and destination node cannot be linked directly together [3].

In this paper, totally based on topology- based on- demand routing protocols for MANETs in adversarial environment.
The existing protocols are not that much sufficient to anonymous secure delay reduce scheme during packet transmission, such protocols are ANODR, Anon DSR, and Discount-ANONR [4]. After examining these protocols, we find that the objectives for secure routing with reduce delay by Authenticated Anonymous Secure Routing (AASR) with Trust based model. MANETs with Group Signature have both public and private key to select the authenticated mobile nodes in adversarial environment [5] – [6]. The key encrypted onion to record a discovered route and design an encrypted secret message to verify the RREQ-RREP linkage. The proposing an authenticated anonymous secure routing (AASR) with calculating Trust value to avoid the delay in anonymous routing path. The following part will present AODV, DSR, TORA and ABR as characteristic protocols of on-demand trend.

2. Methodology

2.1 Group Signature

Group Signature is a method for allowing members of a group to sign anonymously in a MANET routing protocol. Group Signatures can be viewed as traditional public key signatures with additional privacy features. This approach is to run a group key agreement protocol at the beginning of every time slot and use the resulting group key as the common parameter and scalable. The more efficient approach is to use a group key agreement protocol in order to agree on the common parameter and group manager to generate and distribute this starting value. Group Signature scheme has group manager, who is response for adding new members and revoking signature of individual nodes in anonymity are given to a group manager.

***Public Key*:** key this is common to all the members of a group.

***Private Key*:** key which gives privacy for the data of individual members in a group.

2.2 Onion Routing

Onion routing protocol is a technique for connection establishment and keying for anonymous communication.

Licensed Under Creative Commons Attribution CC BY

Messages are repeatedly encrypted the information when sent source to destination nodes in Route-Request of onion routers [7]. In Route-Request has each onion router nodes removes a layer of encryption and uncover routing information when sends the message from destination node to the source node.This prevents these intermediary nodes from knowing the origin, destination and contents of the message.

A routing onion is a data structure formed hide layer (encrypted) for forwarding a text message with successive layers of encryption. In such a way each node formed unhide layer (decrypted) for back warding a text message with successive layer of decryption, the original plaintext message only being viewable to sender and recipient. It is end to end encryption and decryption process between the source and the destination in adversarial environment.

2.3 Trapdoor

Trapdoor is widely used in cryptography and gives a one-way communication and difficult to use in the opposite direction without special information between two sets. A padlock and its key , it is trivial to change the padlock from open to closed without using the key, by pushing the shackle into the lock mechanism. Opening the padlock easily to source – destination by accessing pre- established key to be used [8]. A trapdoor in cryptography has the very specific aforementioned meaning and it is not to be confused with a backdoor.

2.4 Trust Based

The trust is the authenticated as the degree of subjective belief about the behaviors of a sufficient entity. Trust node is the probability by which an individual node performance of anonymous routing in adversarial environment. Trust node is related to performances of nodes in the data reputation and recommendation. In trust node of anonymous routing in adversarial environment response for reducing delay in data transmission [9] [10].

Trust in MANETs is a degree of the belief that a node in a network or an agent in a distributed system will carry out tasks. In direction observation trust, an observer estimates the trust of his one-hop neighbor based on its own opinion. Therefore, the trust value (T) is the expectation of a subjective probability that a trust or uses to decide whether or not a trustee is reliable.

In the direct observation, we assume that each observer can overhear packets forward by an observed node and compare them with original packets, so that the observer can identify the malicious behaviors of the observed node. Therefore, the observer node can calculate trust values of its neighbors. In order to obtain less biased trust value (T), we also consider other observers opinions in our project. If the trust value (T) is less than the threshold value (λ), the node will be fixed as untrusted node and will not be considered for further transmission

3. Objectives and Overview of The Protocol

3.1 Objectives

In this paper, we propose to design a trust-based security protocol approach which attains confidentiality and authentication of packets in routing of MANETs having following objectives:

***Privacy*:** No public factor identities the node privacy. Each node is anonymous and occurs at different locations with private identity.

***Network security*:** Facility to resist the active and passive attack, the network itself detecting and eliminating the source of attacks.

***Trust based*:** Authenticated node involves in data transmission, so it provide high security.

***Performance*:** Privacy and network security is goal, which cannot reduce the performance of MANET.

3.2 Overview of Protocol

In this paper a proposed Authorized node packet forward scheme in MANETs has centralized infrastructure by location based routing protocol. It uses trust values for forwarding packets to authorized node [11]. By group signature and onion routing each intermediate nodes make increase the data packet security using hash value and forward the packets towards the destination node fig.1. The destination node verifies the hash value and access the data packet using trapdoor mechanism.

This routing protocol dynamically calculating the nodes trust value, the source node can select the intermediate for transmitting the packet to the destination node. The source node can be able to select the more trusted routes than selecting the shorter routes. In authorized routing, trusted value of the nodes can help to reduce the end to end packet transfer delay and energy consumption.

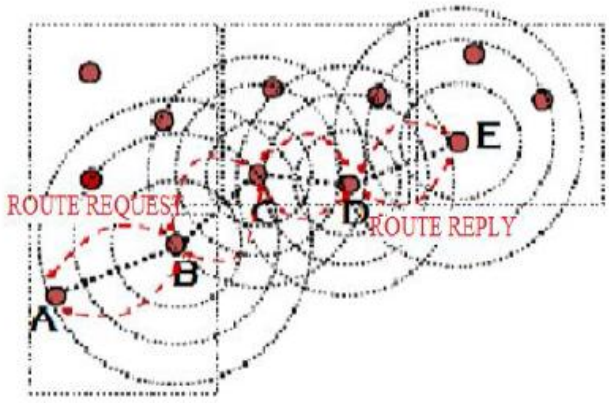

Figure 1: Trust based MANET Routing

4. Attacker in Adversarial Environment

In adversarial environment, an ad hoc network can be attacked from any direction at any node which is different from the fixed hardwired networks with physical protection

Licensed Under Creative Commons Attribution CC BY

at firewall and gateways. Altogether it denotes that every node should be equipped to meet a directly or indirectly. Malicious attack can be initiated from both inside and outside of the network. A specific node is difficult in large ad hoc networks; it is more dangerous and much difficult to detect the attacks from an affected node. It denotes that every node should be prepared to work in a way that it should not trust on nay node immediately.

Adversarial environment affected by both active and passive attack in both insider and outsider manner [12]. Attack can be performed either from outside of the group entity is outside attack and from within the group by an insider that already has certain access to the network is inside attack.

***Active attacker*:** The attacker tries to bypass or break into secured systems. Active attacks include attempts to circumvent or break protection features, to introduce malicious code, and to modify information. These attacks are mounted against a network backbone, exploit information in transit, electronically penetrate an enclave and attack an authorized remote user during an attempt to connect to an enclave. Active attacks result in the disclosure or dissemination of data files, Denial of Service (DoS), and modification of data.

***Passive attacker*:** Monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks. Passive attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information such as passwords. Passive interception of network operations enables adversaries to see upcoming actions. Passive attacks result in the disclosure of information or data files to an attacker without the consent or knowledge of the user.

5. Routing Design

The design of Trust based Authenticated anonymous secure routing protocol [13] is shown in Fig.2.

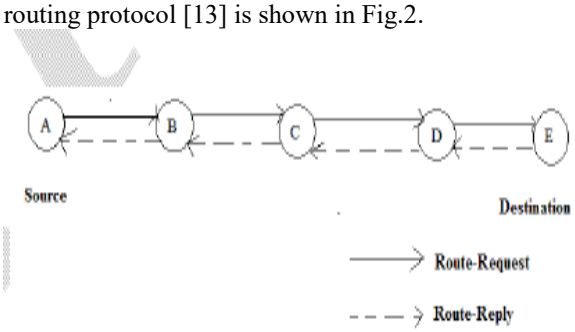

Figure 2: Secure Routing

The trust value in the anonymous node gives the authentication for individual nodes to participate in packet transfer. Routing process has key agreement and its security notation of packet transfer between source A and destination E by Route-Request and Route-Reply is given in Table.1.

Table 1: Notation Table

Notation	Description
P^+	Public key of node
P^-	Private key of node
G^+	Group public key of node
G^-	Group private key of node
K_{AE}	Shared key between A and E
O^+	Encrypted onion message with key of node
O^-	Decrypted onion message with key of node
T	Trust value of individual node in a group
A	Trusted value

5.1. Route-Request

The source node determines its path to send the packet to the destination node. It checks the communication path and make clear by way of sending request to the destination.

***Source node*:** Source node A initially sends the packet to the destination node E with session key K and make encryption when the message is transmit (1).

$$s \rightarrow [P_A^-, G_A^+, K_{AE}, O_A^- \cdots \quad (1)$$

***Intermediate node*:** Intermediate nodes which receives the message from source node A and the further encryption, before send the message to the destination node E (2).

$$I \rightarrow [P_B^-, G_B^-, O_B^- \cdots \quad (2)$$

***Destination node*:** Destination node E receives the message from intermediate node, which uses shared key to access the secret message. The node E ready to route reply after receive the packet and reply to node A.

5.2. Route-Reply

The destination node make sure to the source node the route is clear for transferring packet.

***Destination node*:** Destination node E can send the route reply to the source node A in its original path (3).

$$D \rightarrow [P_E^-, G_E^+ \cdots \quad (3)$$

***Intermediate node*:** Intermediate node which receives the reply from destination node E and make decrypt the message to another neighbor intermediate node (4).

$$I \rightarrow [P_B^-, G_B^+, O^+ \cdots \quad (4)$$

***Source node*:** Source node receives the route reply from intermediate node for successfully packet transmission and ready to discover new packet in same path. This packet transfer is updated in routing table.

6. Conclusion

In this paper, we design trust based authenticated anonymous routing protocol design for MANETs in adversarial environment. It uses trust values to favor packet forwarding by maintaining a trust counter for each node. If the trust counter value falls below a threshold, the corresponding intermediate node is malicious node. In this proposed

Licensed Under Creative Commons Attribution CC BY

scheme, authorized node has high throughput and packet delivery ratio can be improved significantly with decreasing average end to end delay by increasing trust value.

References

[1] Wei Liu and Ming Yu, "AASR:Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments," *IEEE Transaction On Vehicular Technology.*, vol. X, no. Y, May 2014.
[2] H.Shen and L.Zhao, " ALERT:An Anonymous Location-based Efficient Routing Protocol in MANETs, " *IEEE Trans. on Mobile Computing*, vol. 12, no. 10, pp. 1079-1093, 2013.
[3] Zheiong Wei, Helen Tang, F.Richard Yu, Maoyu Wang and Peter Mason, " Security Enhancements for Mobile Ad hoc Networks with Trust Management Using Uncertain Reasoning, " *IEEE Transaction On Vehicular Technology*, vol. X, no. Y pp. 1-12, 2013.
[4] K.E.Defraway and G.Tsudik, " Privacy-Preserving Location-based On- Demand Routing in MANETs, " *IEEE Journal on Selecting Areas in Communications*, vol. 29, no. 10, pp. 1926-1934, Dec.2011.
[5] K.E.Defraway 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.
[6] Michael G.Reed and Paul F.Syverson and David M.Goldschlag, " Anonymous Connection and Onion Routing, " *IEEE Journal on Selecting Areas in Communications*, vol. 16, no. 4, pp. 482-494, May.1998.
[7] Yanchao Zhang, Wei Liu, Wenjing Lou and Yuguang Fang, " MASK:Anonymous On-Demand Routing in Mobile Ad hoc Networks, " *IEEE Journal on Wireless Communications*, vol. 5, no. 9, pp. 2376-2385, Sep.2006.
[8] C.Perkins, E.Belding-Royer, S.Das, et al, " RFC 3561 – Ad hoc On- Demand Distance Vector (AODV) Routing, " *Internet RFCs*, 2003.
[9] J.Kong and X.Hong, " ANonymous On-Demand Routing with Umtraceable Routes for Mobile Ad hoc Networks, " in *proc. ACM MobiHoc'03,* pp. 291-302, Jun.2003.
[10] Yanchao Zhang, Wei Liu, and Wenjing Lou, " Anonymous Communications in Mobile Ad hoc Networks, " in *Proc. IEEE INFOCOM* 2005, vol. 3, pp. 1940-1951, Mar.2005.
[11] J.Paik, B.Kim, D.Lee, " A3RP:Anonymous and Authenticated in Ad hoc Routing Protocol, " in *Proc.International Conf. on Information Security and Assurance (ISA'08)*, Apr.2008.
[12] X.Wu and B.Bhargava, " AO2P:Ad Hoc On-Demand Position-Based Private Routing Protocol, " *IEEE Trans. on Mobile Computing*, vol. 4, no. 4, pp. 335-348, July/Aug.2005.
[13] X.Kong, J.Hong, Q.Zheng, N.Hu and P.Bradford, " A Hierarchical Anonymous Routing Scheme for Mobile Ad-Hoc Networks, " in *proc. IEEE MILCOM'06,* Oct.2006.

Author Profile

Karumuri. Ashok Kumar Obtained the B.Tech. degree in Computer Science and Engineering(CSE) from St.mary's Engineering College, chebrole. At present pursuing M.Tech in Computer Science and Engineering(CSE) Department at Vignan's Lara Institute Of Technology, Vadlamudi, Guntur.

B. Neelima obtained the B.Tech Degree in Computer Technology from PVPSIT, Vijayawada, in 2012 and M.Tech from PVPSIT Vijayawada in 2014.She has 1 year of teaching experience and working in Computer Science and Engineering (CSE) Department at Vignan's Lara Institute Of Technology, Vadlamudi, Guntur.

Licensed Under Creative Commons Attribution CC BY