International Journal of Latest Engineering Research and Applications (IJLERA) ISSN: 2455-7137

Volume – 02, Issue – 05, May – 2017, PP – 41-46

Trust Based Authenticated Anonymous Secure Routing For MANET

Smriti Jain, N. Marline Joys Kumari, Ramakrishnan V
Department of Information Technology
VIT University, Vellore
Tamilnadu -632014

Abstract: Mobile ad-hoc networks are wireless and dynamic topology networks. The main purpose of using MANET is to send the data securely between source and destination in a public channel. Due to the advancement of a technology, the need of wireless networks is increasing day by day. Hence, MANET adds upon its usage over wired communication, especially wireless networks are ideally suited for use in rescue and emergency operations because of their advanced applications in situations like crisis management, military and health care. So, message security plays predominant importance in mobile ad-hoc networks but wireless networks are vulnerable to many attacks that are not secured and less-worthy.

The existing protocols works on the basis of authentication, group signature, and onion routing. Here, we proposed TRUST BASED ANONYMOUS SECURE ROUTING (TBASR) for MANET in adverse environment. This protocol defends the neighbor nodes attacks by the way of key encryption and decryption through route-request and reply. The node trust is achieved through group signature and trust of the path is achieved by asymmetric key encryption. By using this it detects intruders in the networks and avoids packet delay between opponent nodes. Onion routing is used for obtaining anonymity during packet transmission.

Keywords: MANET, Group Signature, Onion Routing, Asymmetric key cryptography, Anonymous Routing.

I. INTRODUCTION

Mobile ad-hoc network is a wireless setup and can be easily configured to transfer data among all destination nodes.

Mobile nodes which are within the radio range will communicate directly through wireless links, while other nodes which are far apart will communicate through routers. Mobile ad hoc network is vulnerable to security threats. It deals with Anonymcity which means communication in MANET which leads to Unidentifiability and Unlinkability. Unidentifiability means that source and destination are transparent to other nodes i.e. they cannot identify other nodes. Unlinkability means that there should not be any direct link between source and destination.

The two-phase of communication in Mobile –Ad hoc network are: Route discovery and data transmission. In adverse environment, both phases are prone to variety of attacks. First, misbehaving node will disrupt the route discovery by pretending itself as destination by responding with corrupted information. In this way, the attacks can obstruct the flow of traffic by authenticated user and influences the knowledge of legitimate nodes. Misbehaving nodes can also leads to the interruption of data transmission phase by data loss.

AASR[1] does not provide trusted communication between the nodes, which causes more packet delay and link failure in the networks. The attackers can get access to the whole data easily when confidential information is routed through single path whereas when the information is fragmented and send with different disjoint routes it increases confidentiality and robustness, so that it will be difficult for the intruder to get access over the information.

The proposed work for secure routing will reduce delay by Trust based Anonymous secure routing. We will use a key-encrypted onion to record the discovered route and will make a encrypted secret message to verify the RREQ- RREP link. RREQ packets are checked per hop by Group Signature so to prevent intermediate node from modifying it. It has both node identity and public key to select the authenticated mobile node. Asymmetric key encryption is used to obtain path trust.

II. RELATED WORK

In adverse environment the attack can be from any direction at any node. Every node should be equipped to meet an attack directly or indirectly. An attack can be internal or external. The attack performed from the outside of the group entity is termed as outside attack and that from if the attack is within the group by an insider who is legitimate to access the network is termed as internal attack. A node should work anonymously so that it should not trust the neighboring nodes.

Passive Attacks

Passive attacks break the system based upon observed data. It does not attempt to alter the content of the data. It monitors unencrypted traffic and looks at the clear-text passwords for sensitive information that can be used in other types of attacks. Passive attack attempts to capture authenticated information, and will attack weakly decrypted packets. Passive attacks result in the leakage of information or data files by an attacker. Therefore privacy of the data is compromised. Even though a passive attack is less harmful, it becomes dangerous to fetch information.

Active Attacks

An active attack is characterized by the attacker attempting to break into the system. The intruder may introduce a new data into the system and potentially change data within the system. The attacker is to bypass or break into secured systems resulting in the introduction of malicious code and modification of information. An active attack causes damage to the system resources or affects their operation. In active attacks Integrity or Availability of data is compromised. Example of active attacks is Denial of Service (DoS) and modification of data.

AASR protocol [1] has features to provide anonymous communication in an adversarial environment. Packets are authenticated by the group signature. The attackers will not able to identify, the identity of the node. Onion routing is used to prevent the secret message from intermediate nodes to reveal the information. But there is a lack of trust between nodes in the network. Many security protocols were proposed but all those do not meet trust factors. Trust based management framework [10], discusses about trust factor in MANET. It is used for selecting most efficient path in the network and the route is updated during route exchange process.

DSR [9] proposes two mechanisms, Watchdog and Path rater. Watchdog maintains buffer of a transmitted packets and overhears of the other node which helps in the detection of misbehaving nodes. Here the packets are in the buffer and the overhead packets will be compared. If there is a match, the packet is successfully forwarded, and it will be removed from the buffer. Path rater detects the malicious nodes with a link metric, which is estimated with respect to reliability of the links and knowledge of the misbehaving nodes. The drawbacks of these methods are that misbehaving nodes cannot be distinguished from the failed nodes. A trusted node can easily be rated as malicious, if the transmission breaks.

III. PROPOSED WORK

The proposed protocol provides secured trust-based routing in adversary MANET environment by detecting link failure and packet loss. Mobile ad hoc networks (MANETs) are wireless and dynamic topology network medium, which may suffer from many open security criticism. Anonymous communication is more important for Mobile Ad hoc networks. Wireless network is vulnerable to many attacks, less-trustworthiness and has many security issues. In proposed work, we present a new routing protocol termed as Trust-based Anonymous Secure Routing for MANET in Adversarial Environment which includes secure routing between Source and Destination, with secure route discovery and setup. The following methodologies are used to ensure the trusted communication in the network.

Two trust models are proposed, Node trust and Path trust. Node trust is achieved by Group signature in which group manager ensures that only authenticated and trusted nodes are present in the particular network. Then path trust is obtained during route discovery, in which trust values are calculated and compared to discover a trusted path. Once the trust is accomplished, messages will be transmitted using Onion routing. These approaches ensure that the routing protocol will be more active to detect link failures, caused either by the mobility or adversary attacks. Trust-based secured protocol approaches tend to authenticate packets through the routing scenario of MANETs.

A. GROUP SIGNATURE

Group Signature is used for node's authentication and verifying trust-worthiness of a node in a particular network. In this method group manager compares the id of the nodes in its database with those present in the network and if the id is match then the certificate will be provided.

The certificate **(C)** contains public key (**Nk)**, node's identity (**Nid)** and timestamp **(T)** signed by the group manager. If the public key is compromised Group manager announces to the group members that the certificate is no longer valid, revocation of certificate takes place and new certificate will be provided. Revocation of the certificate takes even if the timestamp **(T)** expires. After issuing the certificate, public keys of all nodes will be shared between each node.

C= Ek (Nid || Nk || T)

After trusted nodes are selected in the network, the trusted path for packet transmission is discovered during route discovery phase.

B.ROUTE DISCOVERY AND SHORTEST PATH CALCULATION

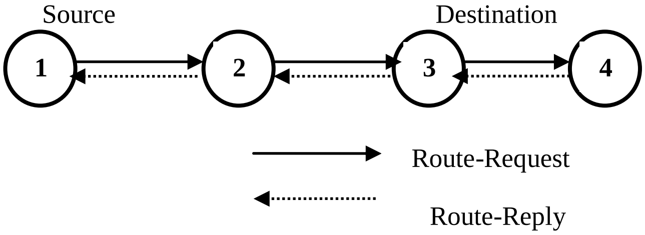


Fig.3. 1 Route Discovery

In Route discovery phase, the source node sends the RREQ message to destination node through all possible paths. For both the RREQ and RREP packet Asymmetric key Cryptographic method is used. Destination node sends back the encrypted RREP packet to the source node through the shortest path. RREQ packet is encrypted using next node's public key and it contains identity of source (SID) and destination node (DID), RREQ message, hop count, Transmission time (rate at which the packet is forwarded from source to destination and vice versa), trust value of all nodes between the source and destination. Initially trust value is assigned to all the trusted nodes.

S = Ek (SID || DID|| RREQ || STRUST || SPC)
STRUST = (Trust_value || Hop_count || Transmission_time)

--------------- [Equation **(1)**]

Once the intermediate node receives the RREQ packet from the source node, it will decrypt it with its own private key, it checks for destination node; if it is destination node then it finds the shortest path and sends the RREP message back to the source node. If not, the node will decrypt the packet and adds its identity (IID) and forwards to the next node. Trusted value will get added till it reaches destination node. Each time when the packet moves from one node to another, the hop count will get incremented by 1. Fig.3.1. Shows how RREQ, RREP packet moves between source and destination.

I = Dk (SID || DID ||RREQ || STRUST || SPC)
I = Ep (IID || SID ||DID ||RREQ || STRUST || SPC)

After the destination node receives the RREQ packets from all the possible paths, it will find the shortest path among those paths and sends the RREP packet back to the source node. It adds a new field named as DTRUST which contains hop count, Transmission time, and Trust value.

D= Ep (SID || DID ||RREP || STRUST || DTRUST || SPC)
DTRUST=(Trust_value||Hop_count||Transmission_time) ----- [Equation **(2)]**

On receiving the RREP packet, the source node checks for the STRUST and DTRUST values (Equation 1 and Equation2). The path is considered as trusted, if the Trust value and Hop count matches and also if there is no delay in the Transmission time. Once the trusted path is selected the message is transmitted securely through the trusted path. Since, Asymmetric key cryptography method is used for both request and reply messages. Only trusted nodes which are identified during group signature will only be able to open the request or reply packets. By this even if an intruder tries to open the packet without knowing the public key the message cannot be hacked. In this method the complete path is made trusted and secured for transmission.

C. SHORTEST PATH CALCULATION (SPC)

The shortest path for forwarding the reply packet is chosen using Dijkstra method.

Algorithm:

1. The source node is initialized with starting value as 0.
2. The distance of the source node is marked as permanent, all other distances are temporary.
3. Source node is made as active.
4. Temporary distance is calculated with number of hops present between the source and destination node through all possible paths.
5. Among the calculated distances, shortest value is selected and that distance is marked as permanent.

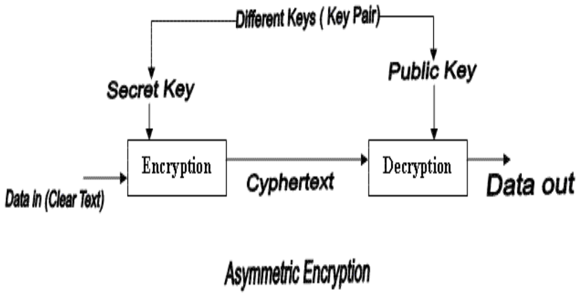
If there is any link failure in the path due to mobility, then the next shortest path is marked as permanent. Once the trusted and shortest path is discovered the message is transmitted using onion routing method.

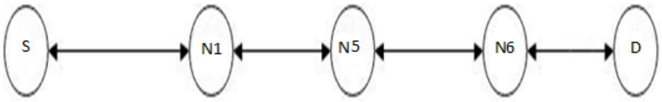
D. ONION ROUTING

Onion routing protocol is a layered encryption technique used for anonymous communication. It uses Diffie-Hellman Asymmetric key encryption algorithm. This method ensures that same set of parameters are used by the sender and the receiver. Diffie-hellman is used for secure key exchange and is used to obtain anonymity.

Asymmetric encryption algorithm or public key algorithm uses different keys for encryption and decryption .This public key method is used for transmitting encryption keys and data securely when the sender and receiver have no opportunity to agree on a secret private key.

Diffie-Hellman key agreement algorithm is not for encryption or decryption but it enables two parties which are involved in communication to generate a shared secret key. This let them to exchange information confidentially.





Transmission path

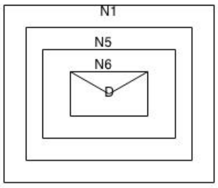


Fig 3.2 Onion Routing-Encryption

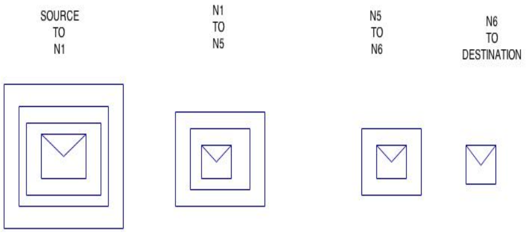


Fig 3.3 Onion Routing-Decryption

For example, Fig 3.2 and 3.3 shows the encryption and decryption in onion routing. The source node encrypts the message using node public keys of all nodes in the chosen trusted path between source and destination node. A layered encryption is done over the message with public keys of Destination node D, and then subsequently with N6, N5, and N1. The source node forwards the packet to node N1. After receiving the packet N1 decrypts its layer with its private key and forwards the packet to N5. Node N5 decrypts its layer and forwards to N6. Node N6 again decrypts its layer and forwards to destination. Once the destination node receives the packet it decrypts and looks for the message. The received message contains only information about source node. Only the recipient will be able to see the message. Onion routing checks Location and Route Anonymity. Location Anonymity- Topology of the network is hidden Route Anonymity- Intermediate only knows about previous and next hop identity

IV. PERFORMANCE FACTORS

The three algorithms Diffie-Hellman algorithm, RSA algorithm, elliptic curve cryptography algorithm are public key algorithms and are based on number theoretic functions. This requires arithmetic with very long operands and keys, longer the operand and keys more secure the algorithm becomes. To compare algorithms we consider security level the best known attack requires 2^n steps. Thus, an algorithm is said to have a secure level of n bit. The following criteria are used for performance

1. Computational speed up
   It is important that the encryption and decryption algorithm should be fast enough to meet the requirement.
2. Key length value
   This shows how the data is encrypted.
3. Encryption ratio
   Measurement of the amount of data that should be encrypted.
4. Security issues
   This defines how secure the encryption technique is.
5. Time
   The total number of operations depends on the processor speed and complexity of the algorithm, lesser the time of algorithm more the number of operations improve.
6. Throughput
   As the throughput increases the power consumption decreases.

V. RESULT AND DISCUSSIONS

This table presents performance and comparison with respective to the following parameters:

Table1. Comparison of Asymmetric Encryption Algorithms

Parameter	RSA	Diffie Hellman
Key Used	Different keys	Share Keys
Throughput	Low	Lower than RSA
Encryption ratio	High	High
Power consumption	High	Lower than RSA
Key Length	>1024 bits	Key exchange management
Security issues	Timing Attack	Eavesdropping

We are improving AASR to reduce packet delay by combining it with trust based routing. With the help of this routing protocol we can detect link failure caused due to adverse affects. This also minimizes the denial of services attack.

VI.CONCLUSION

The proposed work is to create a Trust based Anonymous Secure Routing protocol design for MANET in adversarial environment (TBASR). The combination of above three methods ensures that no intruder can attack the packet. Group signature is used for node’s trust, Asymmetric key Cryptography for path trust and Onion routing for anonymous transmission in the network. With the help of the trust model, the routing protocols will be more active in detecting link failures, caused either by the mobility or adversarial attacks. This method ensures the secure and trusted communication.

References

[1]. Wei Liu and Ming Yu, "AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments", *IEEE transaction on Vehicular Technology*, Vol.63, No.9, 2014.

[2]. Poonam Gera, Kumkum Garg, and Manoj Misra, "Trust-based Multi-Path Routing for Enhancing Data Security in MANETs", Inter*national Journal of Network Security, Vol.16, No.2, PP.102-111, Mar. 2014*

[3]. Sanzgiri K., B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks," in *Proceedings of the 10th IEEE International Conference on Network Protocols*: IEEE Computer Society, 2002.

[4]. J. Kong and X. Hong, "ANODR: ANonymous on demand routing with untraceable routes for mobile ad hoc networks," in *Proc. ACM MobiHoc*, pp. 291–302, Jun. 2003.

[5]. A.Boukerche, K. El-Khatib, L. Xu, and L. Korba, "SDAR: A secure distributed anonymous routing protocol for wireless and mobile ad hoc networks," in *Proc. IEEE Int. Conf. LCN*, pp. 618–624, Nov. 2004