Trust Based Anonymous Authenticated Secure Routing for MANETs

M.Narmatha Priyaa, G. Ravi

Abstract

Secure communication is important in mobile ad hoc networks. The mobile ad hoc network is a continuously self-configuring network. It is also an infrastructure-less network. The main need in the network is to provide secure communication. There are some nodes in the network which reveal the secret information. These nodes are termed as the untrusted nodes. There are some particular nodes which do not reveal the secret message to the other malicious nodes. These nodes are termed as the trusted nodes. These trusted nodes are used for routing. There are many protocols in the network which are used for secure routing. But these protocols are not successful in providing the security of the network. In this paper, the proposal of a new routing protocol named as trust based routing protocol is employed which provides security in the network.

Keywords

Anonymous, Authenticated, Group signature, Mobile Ad hoc networks, Onion Routing, QOS Routing Protocol, Trapdoor, Trust Based and Trustworthiness.

1 INTRODUCTION

MOBILE ad hoc networks are not secure due to the threats.To provide secure communication the nodes inside the network must to be trusted nodes. There are many untrusted nodes present in the network. These nodes reveal the secret message to the malicious nodes. On other situation the communication between the nodes must be anonymous. Anonymous communications are mainly used for protection purpose. In anonymous communications the node identifications and routes are replaced by random numbers or pseudonyms for protection purpose. The definition of anonymity is the state of being unidentifiable within a set of subjects. The combination of unidentifiability and unlinkability is the requirements of anonymous communications in MANETS [2]. Generally for MANETS the topology based on – demand anonymous routing protocols are used. The on- demand ad-hoc routing protocols such as AODV and DSR are anonymized directly to develop the anonymous protocols. After using the protocols such as AASR, ANODR, SDAR, Anon DSR, MASK and Discount ANODR the requirement of unidentifiability and unlinkability is not fully satisfied. The main function of ANODR
focuses on protecting the node on route identities during a route discovery process, especially on the routing packets. For example, ANODR we may consider the Route request (RREQ) and Route reply (RREP). In ANODR, during the RREQ it adopts a global trapdoor message, instead of using the ID of the destination node. In backward RREP forwarding the intermediate nodes release the disclosed trapdoor message from which the route can be identified. In SDAR, during routing procedures the nodes are its one- hop neighbours and are made to know each other ID. The intermediate nodes in route may be revealed to the destination node in Anon DSR. A clear node ID is used in the route discovery in the MASK and Discount- ANODR. The AAS adopts a Key- encrypted onion to record a discovered route and design an encrypted secret message to verify the RREQ- RREP linkage. It is assumed here that there are no secure nodes used in communication. To overcome this adaptation of TAASR is done to eliminate the pre- mentioned problems. Extensive simulations are used to compare TAASR with that of AASR. The results show that it provides less delay than AASR. In future work, the throughput can be increased.

The remainder of this paper is organized as follows. The background and related work of ad hoc anonymous routing and AASR and TAASR (Trust Based Routing) are introduced in section II. The network scenario is discussed in Section III. The design of TAASR protocol is presented in section IV. The evaluation of TAASR is in section V. The simulation results are provided in section VI. Section VII concludes this paper.

2 BACKGROUND AND RELATED WORK

In the following section, this paper introduces the basic concepts in trust routing, and provide a short survey on the existing routing protocols, along with the routing of the trusted nodes. The routing between the nodes is done by using trusted nodes. The trust nodes are mainly used in providing secure communication. The trust nodes do not reveal the transmitted packets to the untrusted nodes.

2.1Anonymity and security primitives

The unlinkability is done by using the anonymous communication. The unidentifiability is employed by using this anonymous communication. Thus the following are the common mechanisms that are widely used in anonymous secure routing. Trapdoor is a common concept which create anonymous key between the source and the destination [13]. Using secret key the source and destination can open elements and node ID. In this concept the intermediate node can include elements along with the existing elements. In trapdoor the name itself implies that it does not allow others to trap the packets. Onion Routing is a mechanism to provide private communication over a public network [14]. The source node forms a specific route message with a core of onion. Core of

onion is nothing but layer of messages. The layer of messages gets added by an encrypted layer during the route request message. The ID of the forwarding node is not known to the source and the destination. Group signature [15] scheme does not disturb the anonymity but provide authentications. The group trust authority is known as group manager. This group trust authority issues a pair of group public and private keys for every member in a group. Private key generates its own signature for the member. The other member in a group verifies this signature. During this verification the signer's identity is not revealed. Tracing of the signer's identity is done by the group trust authority. Group keys are also revoked by the group keys.

2.2. Anonymous on- demand routing protocols

The anonymous on-demand routing protocols are more. There are two categories in anonymous – on- demand routing protocols namely topology based and location based [2]. The topology based is known as location –centric [16]. There are some protocols which are designed for location-based or location – aided anonymous communications. These location based protocols used for design are as follows: AO2P, PRISM, ALERT. These location aided anonymous communications require localization services. For MANETs, the focus is mainly on topology – based routing.

The problems in meeting the unidentifiability and unlinkability occurs in SDAR, Anon DSR, MASK and D-ANODR. In SDAR and Anon DSR the neighbour node ID's across the route are possible to expose. The MASK and D-ANODR uses plain node ID's in the route request. The information leakage can be prevented during the RREQ and RPEP process by using the pseudonym instead of its real ID.

The protocols A3RP, RAODR [18], USOR [19] and PRISM [22] use additional authentication schemes for signing the routing packets. The neighborhood authentication is provided by MASK. But the signing of the routing packets couldn't be done by MASK. The master key mechanism is deployed by RADOR but the anonymity, traceability and enforceability which are supported by a group signature is not provided by RADOR. Since onion is more scalable than other mechanism which can be extended for example for multiple paths this onion based routing is used.

2.3. AASR

This AASR (Authenticated Anonymous Secure Routing) provides Route Request and Route reply mechanism. This Route Request is sent to the neighbour nodes. The neighbor nodes send the route reply to the existing nodes. The route reply is sent to the node which sends the Route Request. The Route reply verifies the path. The source node sends an ID to the neighbouring node. The neighbouring node receives the ID and forwards the packet to the next neighbouring node. This node Id provides secure communication. There are secret keys used to unlock the packets. They are known only to the source and the destination.

2.4.Trustworthiness – based QOS Routing Protocol for wireless Ad Hoc Networks:

Trustworthiness – based Quality of service (TQOS) routing is the combination of a new secure routing protocol (SRP) with quality of service (QOS) support – secure route discovery, secure route setup, and trustworthiness – based QOS routing metricies are the functions of TQOS routing public and shared keys and are used for the security of the routing control messages. The generation of the public key and shared keys are done by on demand. The maintenance of shared keys is done dynamically. The most difficult internal attacks are detected by the message exchanging mechanism. The QOS of the links along a route is combined with the requirements on the trustworthiness of the nodes in the network to obtain the routing metrics. The implementation procedure for each node, the maintenance of a local certificate repository, the building up of trust among a node and its neighbors, and establishment of a self- organized PKI are need to be investigated.

3. PROPOSED METHOD:

In this section the presentation of the adversaries and attack models, the network assumptions and the node model along with the authentication and the confidentiality are discussed. The network assumptions include the key server, attacker, trust nodes, untrusted nodes. Node model includes the transmission of the packets, route request, route reply, identification of the trust nodes. The differentiation is identified among the trust and the untrusted nodes. Packet transmission takes place between the trusted nodes and eliminates the transmission of the packets along the untrusted nodes.

3.1. Confidentiality

Confidentiality ensures that the information transmitted across the network is accessible only by the intended recipients. The following information ensures the confidentiality of the information. The device A encrypts the message using the public key of device B. Device B can decrypt the message successfully since the private key is known to the device and hence ensures the message confidentiality.

3.2. Adversaries and Attack Models

The attackers inside the network poses chances of knowing the secret keys based on the behaviour of the attacks and are classified as follows.

The active and the passive are the behaviours of the locations which are either inside the network or outside the network. Based on their behaviours and locations the classification of the attacks are Passive outside attack, Active outside attack, Passive inside attack and Active inside attack.

Passive outside attack: This passive outside attacks is done by an external global passive adversary. This tries to reveal the identities of the source, destination and en-routes of a particular flow. The observation of the wireless communication is done by passive outside attack. The recording of all wireless communication in the network is kept within it.

Active outside attack: This attack moves randomly from one place to another. These attacks are visible. The routing is mainly breaked due to this attack. This may launch a DOS

attack. The actions are revealed to others in this mechanism. The active outside attack does not have any restrictions as possessed by the passive outside attack.

Passive inside attack: This attack is caused by the nodes in MANETS. They know the traffic pattern and node mobility information since they have a capacity to learn them. The legitimate MANET nodes are the attackers and it possesses the similarity in passive outside attackers by trying to infer the identities of the source and destination. The nodes do not expose themselves but it performs enrooting of the nodes.

Active inside attack: The active inside attack changes the messages sent to the receiver. The packets are totally changed. They act as a valid node and send messages. The modification, injection and replaying of genuine messages is done by this active inside attack. The impersonation attacks are launched by them and the nodes perform masquerading as other nodes.

3.3. Network Assumptions:

Let the MANET is denoted as T and make the following assumptions. The assumptions include Public key infrastructure, Group signature and neighbourhood symmetric key. The network assumptions provide the group manager for group signature, certificate authority, for public key infrastructure, and route discovery for neighbourhood detection in neighbourhood symmetric key.

1) Public Key infrastructure: The public key infrastructure has node T. This node T has a pair of public/ private keys. This pair of public and the private keys is issued by the public key infrastructure. The certificate authority also issues this pair of the public and the private keys. For example consider a node A which is an element of T. (A ∈ T) the KA+ denotes the public key for (A ∈ T) and KA- denotes the private key for (A ∈ T). This dynamic key management scheme is as same as the secure routing [23] which already exists. The network runs without online PKI or CA services by using the dynamic key management scheme.

2) Group Signature: A pair of group public and private keys is issued by a group manager to each node in the network which is assumed as T. Let GT+ denotes the group public key. GA- (for A ∈ T) denotes the group private key. The group public key remains the same for all the nodes in T, while the group private key GA- (A ∈ T) is different for each node. The group signature mechanism runs properly by allowing the working of the dynamic key management scheme along with the admission control function of the network. Military ad hoc network adopts this group signature mechanism.

3) Neighbourhood Symmetric Key: Security can be established between any two neighbour nodes. The symmetric key is created with their public/ private keys by the neighbour nodes. The routing discovery RREQ on HELLO messages are used for this neighbourhood symmetric key. Let the assump
tion made as KAB is the shared symmetric key for two nodes A and B (A, B ∈ T). This assumption is issued for the data transmissions between them. MASK, RAODR and USOR are used in the establishment of one- hop shared key.

Let us summarize the approaches in table.

Table II
Notations for security Primitives

Notations	Descriptions
KA+	Public key of node A
KA	Public key of node B
GT+	Group public key of the network T
GA-	Group private key of node A
KAB	Symmetric key shared by nodes A and B
{d} KA+	Data d is encrypted by key KA+
[d] KA-	Data d is signed by node A
<d> KAB	Data d is encrypted by shared key KAB
(d) KA	Data d is encrypted by one symmetric key of A
OK (m)	Encrypted onion for message m with key K
N NA	One- time Nym – generated by A to indicate itself
Debt	A special lit – string tag denoting the destination

3.4. Node model

1) Destination Table: All the possible destination nodes are assumed to be known by the source node. The destination table stores the pre- determined trapdoor string destination information including one of the destination's pseudonym and public key. The shared symmetric key is generated which is required for data encryptions in the session. After the session to the destination is employed the symmetric key requirement is needed. The symmetric key generated by the source node is stored in the destination table before sending the route requests and after receiving the route reply. (Dest–Nym, Dest-string, Dest- public – Key, session- key) is a sample entry of the destination table.

2) Neighbourhood Table: The local information exchange between the neighbours is done by each and every node. There are different pseudonyms generated for the communication between the neighbours. The shared symmetric keys are established along with the neighbours security association. The neighbourhood stores the information.

3) Routing Table:A new entry is created every time in the routing table when a node is generated or when the route request is forwarded by a node. The secret verification message and the requests pseudonym are stored in the route discovery."Pending" is the status marked for such entry.

4) Forwarding Table: Switching information is recorded in the forwarding table like VCI (Virtual Channel Identifier) the per hop pseudonym acts as an identifier for packet switching.

The design of TAASR protocol is presented in this section. The TAASR identifies the source and destination. A particular node acts as a key server. This key server node is used for key transferring. The keys are transferred from one node to its neighbour nodes. The neighbour nodes receive the keys and transfers the keys to its neighbouring nodes. The ROUTE REQUEST is first sent to all the nodes. The nodes receive the ROUTE REQUEST and return the ROUTE REPLY to the nodes. The ROUTE REPLY is received by the source node.

The source node sends the packet to the neighbouring node. The nodes are differentiated as trusted nodes and untrusted nodes. The trusted nodes are used for transmitting the packets. The untrusted nodes are not involved in packet transmission.

The protocol evaluation is done by the following: Anonymity Analysis: Identity Anonymity, Route Anonymity and location Anonymity are 3 anonymities.

1) Identity Anonymity: Random none is generated by identity Anonymity.

2) Route Anonymity: The source, intermediate and destination node have information about the nodes pseudonyms of the previous and next hop.

3) Location Anonymity: The malicious nodes couldn't infer the information about the secret path in location anonymity.

Security Analysis: Security Analysis includes Passive Attacks, impersonation Attacks and DOS Attacks.

Passive Attacks: This passive attack is of two types. One type of attack is global eavesdropper. Another type of attack is silent dropping.

Cryptographic overhead Analysis: Cryptographic overhead analysis uses the keys of encryption, decryption, verification, symmetric and onion.

4. PERFORMANCE SIMULATION

The simulation TAASR protocol is done.

A. Network Configurations

1) Topology and Traffic

In the simulations the area of the network is 1200m x 300m with 60 nodes initially and uniformly distributed. A total of 15UDP based CBR sessions are used for the generation of traffic.

2) Attack Models

The function of the malicious mode is to drop the packets randomly. The probability of packet dropping is varied from 0.1 to 0.5.

B. Simulation Results

The presentation of simulation results with the comparisons of AASR and TAASR.

AASR with TAASR

The delay of AASR is compared with TAASR. On observing the graph the TAASR produces less delay when compared with AASR.

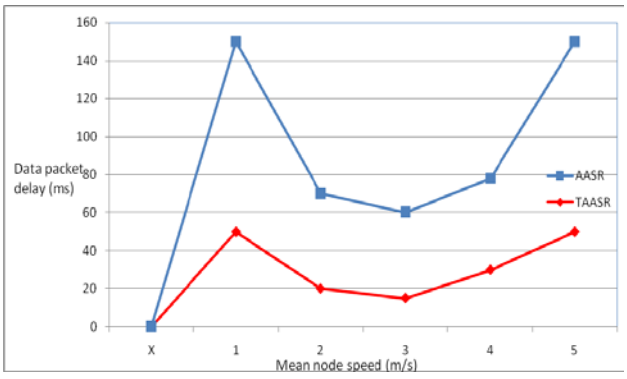

Figure: 4.1 End-To-End Delay of AASR compared with TAASR

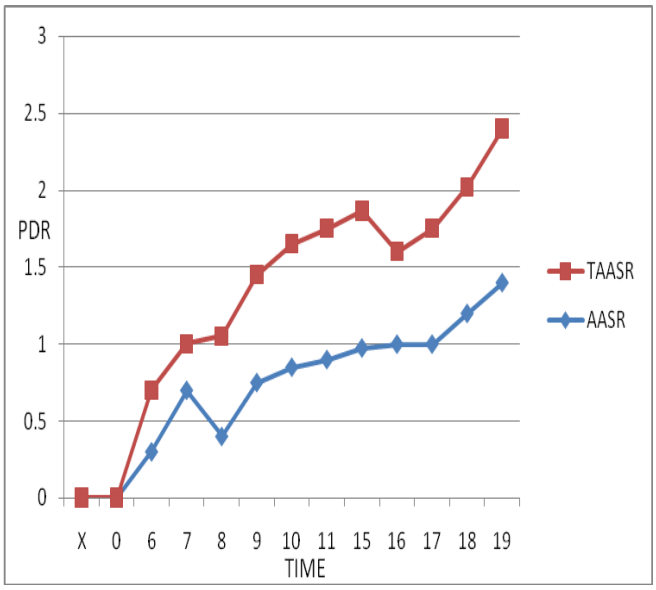

Figure:4.2. Packet delivery ratio

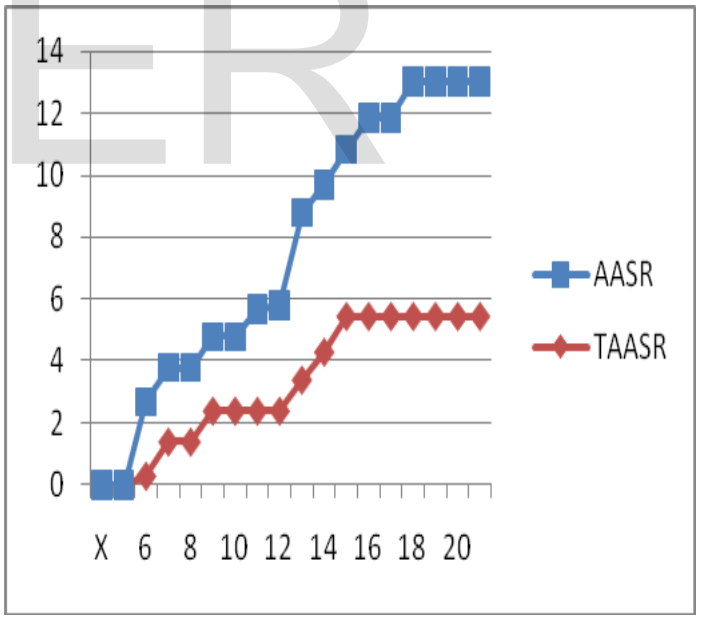

Figure:4.3. Throughput

5. RESULTS AND DISCUSSION

The delay of AASR is compared with TAASR. The TAASR has minimum delay when compared with the AASR. The security is enhanced by using the trust based routing protocol. Since the transmission occurs quickly through the trusted nodes the network security is increased.

6 CONCLUSION

In this paper, the proposal of the Trust Based anonymous authenticated secure routing protocol is done. Group signature is used for defending the potential active anonymous attacks. The key- encrypted onion routing with the message which has to be kept secret is designed to provide anonymous secure communication on comparing TAASR with AASR TAASR produces faster transmission of the packets.

REFERENCES

[1]Wei Liu and Ming Yu," AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments," in IEEE transactions on Vehicular Technology, No. Y, March 2014

[2] D. Kelly, R. Raines, R. Baldwin, B. Mullins, and M. Grimaila, "Towards a taxonomy of wired and wireless anonymous Networks," in Proc. IEEE WCNC'09, Apr. 2009.

[3] C. Perkins, E. Belding-Royer, S. Das, et al., "RFC 3561 - Ad hoc On- Demand Distance Vector (AODV) Routing," Internet RFCs, 2003.

[4] D. Johnson, Y. Hu, and D. Maltz, "RFC 4728 - The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4," Internet RFCs, 2007.

[5] 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.

[6] J. Kong, X. Hong, and M. Gerla, "ANODR: An identity-free and ondemand routing scheme against anonymity threats in mobile ad hoc networks," IEEE Trans. on Mobile Computing, vol. 6, no. 8, pp. 888– 902, Aug. 2007.

[7] 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'l Conf. Local Computer Networks (LCN'04), Nov. 2004, pp. 618–624.

[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.

[9] Y. Zhang, W. Liu, and W. Lou, "Anonymous communications in mobile ad hoc networks," in Proc. IEEE INFOCOM 2005, vol. 3, Mar. 2005, pp. 1940–1951.

[10] Y. Zhang, W. Liu, W. Lou, and Y. G. Fang, "MASK: Anonymous On- Demand Routing in Mobile Ad hoc Networks," IEEE Trans. on Wireless Comms., vol. 5, no. 9, pp. 2376–2386, Sept. 2006.

[11] L. Yang, M. Jakobsson, and S. Wetzel, "Discount anonymous on demand routing for mobile ad hoc networks," in Proc. Int. Conf. on SECURECOMM'06, Aug. 2006.

[12] J. Paik, B. Kim, and D. Lee, "A3RP: Anonymous and Authenticated Ad hoc Routing protocol," in Proc. International Conf. on Information Security and Assurance (ISA'08), Apr. 2008.

[13] S. William and W. Stallings, Cryptography and Network Security, 4th Edition. Pearson Education India, 2006.

[14] M. G. Reed, P. F. Syverson, and D. M. Goldschlag, "Anonymous Connections and Onion Routing," IEEE Journal on Selcted Area in Comm., vol. 16, no. 4, pp. 482–494, May 1998.

[15] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in Proc. Int. Cryptology Conf. (CRYPTO'04), Aug. 2004.

[16] K. E. 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.

[17] 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.

[19] R. Song and L. Korba, "A robust anonymous ad hoc ondemand routing," in Proc. IEEE MILCOM'09, Oct. 2009.

[20] Z. Wan, K. Ren, and M. Gu, "USOR: An Unobservable Secure On- Demand Routing Protocol for Mobile Ad Hoc Networks," IEEE Trans. on Wireless Communication, vol. 11, no. 5, pp. 1922–1932, May. 2012.

[21] X. Wu and B. Bhargava, "AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol," IEEE Trans. Mobile Computing, vol. 4, no. 4, pp. 335–348, July/Aug. 2005.

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

[23] H. Shen and L. Zhao, "ALERT: An Anonymous Location-based Efficient Routing Protocol in MANETs," IEEE Trans. on Mobile Computing, vol. 12, no. 6, pp. 1079–1093, 2013.

[24] M. Yu, M. C. Zhou, and W. Su, "A secure routing protocol against Byzantine attacks for MANETs in adversarial environment," IEEE Trans. on Vehicular Tech., vol. 58, no. 1, pp. 4459–460, Jan. 2009.

[25] X. 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.

[26] M. Yu and K. Leung, "A Trustworthiness-based QoS routing protocol for ad hoc networks," IEEE Trans. on Wireless Comms., vol. 8, no. 4, pp. 1888–1898, Apr. 2009.

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