ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

IJARCCE

nCORETech

LBS College of Engineering, Kasaragod

Vol. 5, Special Issue 1, Feburary 2016

ASMR: Anonymous Secure Multicast Routing

Sudhesh K M[1], Kiran V K[2]

P G Student, Computer Science & Engineering, NSS College of Engineering, Palakkad, India [1]

Assistant Professor, Computer Science & Engineering, NSS College of Engineering, Palakkad, India [2]

Abstract: Dynamic topology of MANETs make very challenging issue for providing anonymity. There have been many anonymous routing protocols available for providing anonymity and location privacy. Such as AASR satisfy the requirement but packet delay is higher. Multicast routing is essential for ad hoc applications when they operating as groups, privacy preservation is a critical issue in such scenarios. In this paper, we propose an Anonymous Secure Multicast Routing (ASMR) for manet. In this approach, the route request (RREQ) packets are authenticated by a group signature, to protect against active attacks without showing the node identities and for reducing the overhead of packet delay, trust based routing is used there by less trusted nodes are given lesser number of self encrypted parts of a message. This makes it very difficult for malicious nodes to attain the minimum information to break through the encryption strategy. Our protocol extends anonymous routing from unicast communication to multicast and also provides additional security properties.

Keywords: Anonymous routing, Multicasting, Header selection, mobile ad hoc networks (MANETs).

I. INTRODUCTION

Communication privacy is an important issue especially with the Internet becoming an unavoidable daily interaction. However, it is useful in networking in civilian and military environments. The need of anonymous routing leads to the use of public network environment such as Tor and I2P. In the case of normal routing such as wired lan, security is provided to data by tunnelling and encryption. But the node identity is revealed to all nodes there by anyone can understand that who is communicating to whom.

Anonymous routing help users to keep their activities private via unlinkability and unidentifiability. Researchers design anonymity networks that build an overlay network among volunteer systems on the Internet. By using anonymous routing, users can communicate with one another without revealing their identities or locations. The term Anonymity is referred as the state of being unidentifiable within a set of subjects. Because of the characteristics of MANETs, that infrastructure-less network where the nodes are connected without wire the probability of attacking and knowing the path is more than the fixed wired network. To achieve the global requirements for such network security and privacy, anonymous communication systems have been investigated and the existing protocols are studied.
Multicasting is essential in application such as video conferencing, auto-configuration, group communication in conference rooms, multi-player gaming, etc. security in such scenarios is also important because when the communication is carried in military environment, law enforcement. The benefits of multicast communication are reduced network overhead and bandwidth.

There have been numbers of protocols available in this domain. Each protocols are good in specific area only that the objectives are not fully satisfied. For example, ALARM [3**]** provides both security and privacy features, like authentication, data integrity and anonymity. It also offers protection against passive and active insider and outsider attacks. But ALARM is a location-based instead of identity-based communication and ANODR [2] is another protocol is focuses on protecting the node or path information during a route establishment process, particularly on the routing packets, e.g., Route Request (RREQ) and Route Reply (RREP). ANODR use a global trapdoor message in RREQ, rather than using the ID of the destination node. However, the route can be identified by a disclosed trapdoor message, which may be send back to the intermediate hops in backward RREP forwarding. The other protocols are partially violating the security requirements for performance considerations.

AASR [7] use a key-encrypted onion to record a discovered route and design an encrypted secret message to verify the RREQ–RREP linkage. The group signature is used to authenticate the RREQ packet per hop, to provide data integrity. In this paper, focus on the multicast routing in MANETs for adversarial environments where the proposed algorithm is used to find the number of cluster and cluster head. We propose an anonymous secure multicast routing (ASMR) to overcome the aforementioned problems and also for operating as groups, we ignored some of the security primitives

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

IJARCCE

nCORETech

LBS College of Engineering, Kasaragod

Vol. 5, Special Issue 1, Feburary 2016

used by AASR to reduce the packet delay introduced by cryptographic operation delay. But the concept of group signature and key-encrypted onion are kept same. Simulations are used to compare the performance of ASMR with that of other multicast anonymous routing protocol. The results show that it provides more throughput than others under the packet-dropping attacks.

The remainder of this paper is organized as follows. The background and other related work of anonymous routing are introduced in Section II. The underlying protocol is discussed in section III. The proposed concept is discussed in Section and the design of the algorithm for head selection is presented in Section IV. Concludes this paper in Section VI.

II. BACKGROUND AND RELATED WORK

A. Onion Routing

In past decade there have been many anonymous routing protocols was proposed all are based on onion routing[1]. In onion routing, the applications proxy makes connections through a sequence of node called onion routers. The onion cloud allows the connection between the application proxy and onion node is remain anonymous. This makes the system private by hide who is connected to whom, and the route of the connection, from both outside eavesdroppers and other normal routers.

The concept of onion routing is hiding the source and destination from the intermediate router by showing only the next hop address as the destination and previous node and the source. There by the nodes in the network only knows the neighbourhood nodes which makes the routing path hidden from the insider. Data passed along the network connection appear different at each router, so data cannot be reviled.

B. Group Signature

In group signature scheme [4] members of a group may have a group public key used as a common key for encryption and private key given by the group head who is trusted node. The member can send a “join” message to the head for getting its private key. After getting the private key the node can generate its own signature, and such signature then verified by other members in the group. This verification scheme is not reveal the signer’s identity. Only the group head can trace the signer’s identity.

C. Routing Protocols

There are two types routing protocols for Manet Proactive (table driven) Reactive (on demand). In the case of proactive routing each node in the network has routing table which shows distance to all its neighbour node. This can be used for broadcast of the data packets. Proactive routing is not suited for the anonymous communication because it make the system more vulnerable to attack.
Where Reactive Protocol such as AODV has lower overhead since routes are determined on demand by broadcasting RREQ message to all nodes this is done by the source. Such protocol constantly update the route tables. Reactive protocol find the route in an on-demand manner and set the route in order to send out and accept the packet from a source node to destination node.

D. Anonymous Routing Protocols

There are many anonymous on-demand routing protocols. Similar to ad hoc routing are topology based and location based [1] or, in other words, node identity centric and location centric. AO2P, PRISM, and ALERT are designed for location-based or location-aided anonymous communications, which require localization services.
For MANET more attention is for topology-based routing rather than location-based routing. Where AnonDSR and ANODR are based on public key and trapdoor functions. These protocols are not completely meeting the unlinkability because the node IDs in a neighbourhood and along a route are possibly exposed in SDAR and AnonDSR, respectively.

E. Trust Based Routing

Recent studies shown that establishing trust relationship between two nodes will improve the security relationship between them. This concept is very useful for the case of manet. Velloso et al. have proposed a model which creates a trust relationship between nodes in ad hoc network. There the global trust knowledge is not needed in such scenarios and also it is useful for large network. In [6], Lindsay et al. for model trust propagation in ad hoc networks they have developed an information theoretic framework which quantitatively measure trust values. In [5], a secure routing protocol with better quality of service support has been proposed. The nodes in the same network must verify and trust before forwarding packets from one node to another.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

IJARCCE

nCORETech

LBS College of Engineering, Kasaragod

Vol. 5, Special Issue 1, Feburary 2016

F. Multicasting in MANET

For the multicast communication normally tree-based or mesh-based protocols are used. In this tree-based protocol is more efficient in case of routing overhead and scalability. The routing protocol MAODV is used for multicasting in Manet which is multicast version of AODV. Anonymous multicast routing protocols proposed in past years are EEAMA (Kao and Marculescu, 2007), in which receiver establishes a unicast route to the source.

By this route EEAMA builds the multicast tree, with the guaranty that Security level is achieved for the multicast network by providing the security for unicast. But EEAMA has few disadvantages like not stable enough in dynamic scenarios because of using tree structure and also Location privacy is not concerned in this work.

III.UNDERLYING ANONYMOUS PROTOCOL: AASR

ASMR extends the anonymous routing of AASR from unicast to anonymous multicast routing. It uses the basic anonymous RREQ of AASR for finding route to the group head. After the successful route discovery, the encrypted data packet is send to the group head as the multicast address. Head then peals the onion from the encrypted message data is send to all its members.

A. Anonymous Route Request

AASR uses the on-demand ad hoc routing protocol AODV as the base routing protocol. Five-node network to illustrate the authenticated anonymous routing processes. The network is shown in Fig.1 in which the node S discovers a route to the node D. where each RREQ packet will be encrypted by node S will contains destination pseudonym, public key, destination string, and session key.

Table. 1. Security primitives.

Dest.Nym.	Dest.Str	Dest. Pub_Key	Session_Key
N_D	dest	K_{D+}	K_{SD}

Then the source broadcast the RREQ packet in the below format

$S \rightarrow: [RREQ, N_{sq.}, V_D, V_{SD}, Onion(S)]\ G_{S-}$ (1)

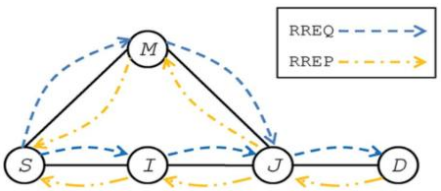

Fig. 1. Network topology.

B. Anonymous Route Reply

When D receives the RREQ from its neighbor J, it will assemble an RREP packet and send it back to J. The format of the RREP packet is defined as follows:

$D \rightarrow: (RREP, Nrt, \langle Kv, Onion\ (J) \rangle\ KJD)$ (2)

Where RREP is the packet type identifier, Nrt is the route pseudonym generated by D, and Kv and Onion (J) are obtained from the original RREQ and encrypted by the shared key KJD. The intended receiver of the RREP is J.

C. Anonymous Data Transmission

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

$S \rightarrow D: (DATA, Nrt, \langle Pdata \rangle\ KSD)$

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.

Upon receiving a data packet, every node will look into its forwarding table. If Nrt in the data packet matches one entry in forwarding table, the node will forward the packet to the anonymous next hop. Otherwise, the data packet will be discarded.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

IJARCCE

nCORETech

LBS College of Engineering, Kasaragod

Vol. 5, Special Issue 1, Feburary 2016

IV. ASMR OVERVIEW

Our proposed protocol ASMR achieves anonymous multicasting based on clustering. The first step of our protocol is the cluster formation. There are different methods for doing this like mobility based clustering, energy based, connectivity based, weighted clustering etc. All of this rely on time complexity. That the time required to establish the cluster is high. Here we give more attention to anonymity so we are using K-Means clustering in which network area is divided into fixed-size square zones. The centroid for the K-Means is selected via cluster head selection rather than random.

Inside the cluster, the nodes that coordinates the cluster activities are called Cluster Head (CH). CH provides all the services to the other nodes. Other nodes are known as ordinary nodes or cluster member. Each member node has direct access to the cluster head.

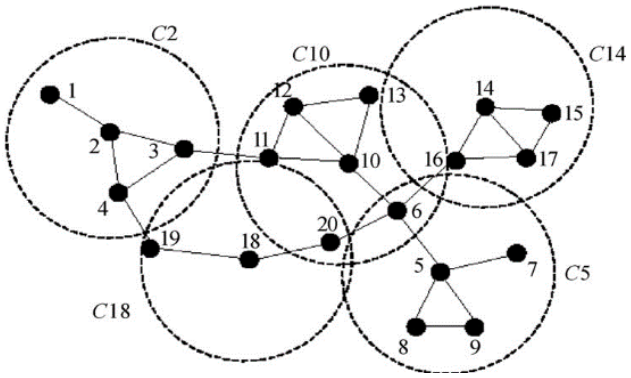

Fig. 2. Network with clusters

A. Cluster head selection

CH is elected by calculating delay of a randomly selected node. Scheme. Each cluster is made by separate geographic area and this area should be same. The cluster head algorithm work as follows

- A random value X is selected; then mod operation is done to get a node from the set of nodes in cluster.
- Then the selected node will send hello packets to its entire neighbor. This is to get the delay takes when multicasting is done.
- This delay is compared with the threshold value of delay, if the value is in the acceptable range this node marked as cluster head otherwise the procedure will repeat to get a head.

This method of head selection gives a cluster head without considering the mobility, energy etc. Here we consider that the node can transmit the packet with an acceptable delay. We are also considering that the cases like

➢ If the CH leaves the network after some time.

This problem will solve if we perform CH selection process at particular time interval.

➢ If any member wants to leave the network

The member must send the leave message to the CH. Upon receiving the Leave message, the CH will remove the node from its table.

Proposed algorithm

Table: Algorithm.

N: Total number of nodes in the cluster.
ch: Cluster Head
Tr: Average delay threshold of Manet
Ps: Acceptable delay variation

1. X □ Select Random
2. J = X mod N
3. For all i □ N: send hello message to neighbors(hello,J)
4. delay = (Trep - Ttr): Trep is the time at the last reply receive
5. if (delay <= (Tr + Ps))

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

IJARCCE

nCORETech

LBS College of Engineering, Kasaragod

Vol. 5, Special Issue 1, Feburary 2016

6. ch = J
7. return ch
8. else go to step 1
9. stop

After successful cluster formation the next step is the verification of trust relationship. The nodes between the cluster head and source node must verify and trust before forwarding packets from one node to another. Inside the cluster each and every node must join the zone by secure join and leave mechanism so security for this nodes is the responsibility of the cluster head and there is no trust relationship between the head and its leaf nodes.

V. NETWORK MODEL

Each node should send "join" message to the head for getting the membership. This is happening after successful classification of the network in to cluster. For security this join message should contain the security parameters. The JREQ message format is as follows.
JREQ = < KD+, KSD >
For simplicity we avoid the destination string and destination pseudonym from RREQ of AASR.
These parameters make the system complex. Then each node then sends the JREQ packet as

N= <JREQ, Nsq, KD+, KSD> GS−

Where KD+, KSD are the public key of head and session key respectively. Nsq is a sequence number randomly generated by N for this route request, the whole RREQ packet is finally signed by N with its group private key GS−.

After successful cluster formation the actual anonymous multicasting process are

A. Data forwarding
Before data forwarding the authentication is done between the source and the group head is same as the AASR. These are mentioned in equation 1 and 2. Now, S can transmit the data to CH. The format of the data packet 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, and the data payload is denoted by Pdata, which is encrypted by the session key KSD.
Upon receiving a data packet, every node will look into its forwarding table. If Nrt in the data packet matches one entry in forwarding table, the node will forward the packet to the anonymous next hop. Otherwise, the data packet will be discarded. The data packet can be switched along the route until it arrives at the cluster head.
When the CH is received the data packet, it first decrypts it and broadcast the data to all its group members. CH is act as the multicast address and anonymity is achieved for the sender to CH by underlying AASR and for broadcasting to group is trusted by group signature.

B. Security Analysis
There may be an external global passive adversary who can observe and record all the wireless communications in the network and also there may be some active adversary they may aim to disrupt the routing or launch a DoS attack. They can move from here to there and launch attacks randomly.
One type of passive attack is a global eavesdropper.it is complex for an eavesdropper to obtain the identity information about the source or destination node in any communication session in ASMR. Only the head can understand the traffic and he is the destination. The RREQ packets cannot be read and modified by attacker because it is secured with group signature and signature is computationally infeasible to decrypt.

VI. CONCLUSION

In this paper, we designed an anonymous multicast routing protocol for MANETs. We extended the authenticated anonymous routing procedure of AASR protocol from unicast to multicast. Here the clusters are formed based on area and cluster head are selected by calculating delay, there by reduces the time complexity and overhead. The use of group

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

IJARCCE

nCORETech

LBS College of Engineering, Kasaragod

Vol. 5, Special Issue 1, Feburary 2016

signature provides authentication anonymity which is capable for avoiding the active attacks without unveiling the node identities. Trust based routing provides secure communication and to reduce the packet loss ratio. Here ASMR is zone based multicast protocol in which location privacy for the cluster head is fully satisfied.

For future work could be concerning data transmission to the set of nodes inside the cluster and the possibility of multiple heads for the cluster.

REFERENCES

[1] J. Kong and X. Hong, "ANODR: ANonymous on demand routing with untraceable routes for mobile ad hoc networks," in Proc. ACM MobiHoc, Jun. 2003, pp. 291–302.
[2] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in Proc. CRYPTO, Aug. 2004, pp. 41–55.
[3] Bao L. "A new approach to anonymous multicast routing in ad hoc networks". In: Proceedings of the Second International Conference on Communications and Networking in China (CHINACOM); 2007.
[4] Kao JC, Marculescu R. "Energy-efficient anonymous multicast in mobile ad-hoc networks". In: Proceedings of ICPADS 2007.
[5] 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.
[6] S. Lindsay, Y. Wei, H. Zhu, and K. Liu, "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 305- 317, Feb. 2006.
[7] D. Kelly, R. Raines, R. Baldwin, B. Mullins, and M. Grimaila, "Towards a taxonomy of wired and wireless anonymous networks," in Proc. IEEE ICC, Jun. 2009, pp. 1–8.
[8] K. E. Defrawy and G. Tsudik, "ALARM: Anonymous location-aided routing in suspicious MANETs," IEEE Trans. Mobile Comput., vol. 10, no. 9, pp. 1345–1358, Sep. 2011.
[9] H. Shen and L. Zhao, "ALERT: An anonymous location-based efficient routing protocol in MANETs," IEEE Trans. Mobile Comput., vol. 12, no. 6, pp. 1079–1093, Jun. 2013.
[10] Wei Liu, Member, IEEE, and Ming Yu, "Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments," IEEE trans. on Vehicular Technology, vol. 63, no. 9, november 2014.
[11] Somayeh Taheri, Salke Hartung," Anonymous group-based routing in MANETs", journal of information security and applications 22 (2015) 87e98.
[12] Mirjeta Alinci, Evjola Spaho, Algenti Lala and Vladi Kolici "Clustering Algorithms in MANETs: A review", 2015 Ninth International Conference on Complex,Inteligent,and Software Intensive Systems.