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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

An Secure Anonymous Group Communication in Mobile Ad-Hoc Networks

K.Vinoth Kumar[1] , N.Senthil Kumaresan[2]

Assistant Professor , M.A.R College of Engineering and Technology ,Tamil Nadu , India[1]

PG Scholar, J.J College of Engineering and Technology ,Tamil Nadu , India[2]

Abstract — Secure group communication with efficient self-organizing key agreement and key establishment is essential to distributed applications in mobile ad-hoc networks (MANETs). In this paper, we propose a Secure Anonymous Routing Protocol (SARP) which is able to provide confidentiality service and non-repudiation service simultaneously. SARP based on Group signature and ID-based cryptosystem for ad hoc networks. The design of SARP offers strong privacy protection completes unlinkability and content unobservability for ad hoc networks. In the proposed scheme, all group members contribute their own public keys to negotiate a shared encryption public key, which corresponds to all different decryption keys. By using the shared public key and the respective secret key, confidentiality and non-repudiation can be obtained, respectively. Both are essential to secure group communication in MANETs. Compared with the exiting anonymous routing schemes for multiple recipients. Accordingly, it is quite suitable to secure group communication in self-organizing, distributed and resource-constrained MANETs.

Keywords — Anonymous routing, key establishment, non-ruputation, group communication, MANET.

I. INTRODUCTION

Secure group communication is of great importance for many collaborative and distributed applications, such as video conferencing, collaborative computation and secure replicated database. To design secure group communication for MANETs is both critical and challenging because of their unique distributed nature. The MANETs differentiate themselves from others by the following facts. Firstly, they are self-organizing and relies on no fixed infrastructure (no base stations, access points, remote servers etc.). All network functions are performed by the nodes forming the network, and each node performs the functionality of host and router, relaying data to establish connectivity between source and destination nodes not directly within each other's transmission range. Secondly, MANETs are peer systems with distributed control and without central nodes. Last but not least, MANETs have constrained resource, such as communication resource, computation resource and energy. These features can be seen as constraints faced by researchers when designing secure group communication mechanism for MANETs. To begin with, secure mechanisms for group communication have to be self-organizing without being dictated by a policy we cannot find a control centre for secure group communication in MANETs. Moreover, the secure mechanisms for group communication must be inexpensive in communication and efficient in computation for the reason that MANETs are resource-constrained networks. Accordingly, schemes and protocols from conventional wire line networks are not suitable or adaptable to this kind of networks. To achieve secure group communications in MANETs, a group key for fast encryption and decryption must be shared only by group members. Then, group communication messages are encrypted by the group key.

Privacy protection of mobile ad hoc networks is more demanding than that of wired networks due to the open nature and mobility of wireless media. In wired networks, devices like desktops are always static and do not move from one place to another. Hence in wired networks there is no need to protect users' mobility behavior or movement pattern, while this sensitive information should be kept private from adversaries in wireless environments. To achieve unobservability, a routing scheme should provide unobservability for both content and traffic pattern. Hence we further refine unobservability into two types one is content Unobservability, referring to no useful information can be extracted from content of any message and another one is Traffic Pattern Unobservability, referring to no useful information can be obtained from frequency, length, and source-destination patterns of message traffic.

The contributions of this paper include:

1) We provide a thorough analysis of existing anonymous routing schemes and demonstrates their vulnerabilities.

2) We propose SARP, to our best knowledge, the first unobservable routing protocol for ad hoc networks, which achieves stronger privacy protection over network communications.

3) Detailed security analysis and comparison between SARP and other related schemes are presented in the paper.

4) We implemented SARP on ns2 and evaluated its performance by comparing it with the standard implementation of AODV in ns2. In next section, we discuss related work on anonymous routing schemes for ad hoc networks. After that we analyze the proposed scheme against various attacks. We also compare it with other anonymous routing schemes.

II. SARP: SECURE ANONYMOUS ROUTING PROTOCOL

In this section we present a Secure Anonymous Routing Scheme SARP for ad hoc networks. In this protocol, both control packets and data packets look random and indistinguishable from dummy packets for outside adversaries. Only valid nodes can distinguish routing packets and data packets from dummy traffic with inexpensive symmetric decryption. The intuition behind the proposed scheme is that if a node can establish a key with each of its neighbors, then it can use such a key to encrypt the whole packet for a corresponding neighbor. The receiving neighbor can distinguish whether the encrypted packet is intended for itself by trial decryption. In order to support both broadcast and unicast, a group key and a pair wise key are needed. As a result, SARP comprises two phases: anonymous trust establishment and unobservable route discovery. The unobservable routing scheme SARP aims to offer the following privacy properties.

1) Anonymity: the senders, receivers, and intermediate nodes are not identifiable within the whole network, the largest anonymity set.

2) Unlinkability: the linkage between any two or more IOIs from the senders, the receivers, the intermediate nodes, and the messages is protected from outsiders. Note linkages between any two messages, e.g., whether they are from the same source node, are also protected.

3) Unobservability: any meaningful packet in the routing scheme is indistinguishable from other packets to an outside Attacker. Not only are the content of the packet but also the packet header like packet type protected from eavesdroppers. And any node involved in route discovery or packet forwarding, including the source node, destination node, and any intermediate node, is not aware of the identity of other involved nodes (also including the source node, the destination node, or any other intermediate nodes).

A. Key Establishment Phase

Here, each and every node in the network communicates with its direct neighbors within its radio range for key establishment. The source node generates a random number and then computes a signature using its private signing key any one can verify this using group public key and after which broadcast to its neighborhood. Once the neighbor receives it, it checks for the signature and if successful then the neighborhood node computes the signature using its own signing key and computes the session key and reply to the source node. A pair wise key is constructed anonymously, as a result of which the messages exchanged are not observable.

B. Route Discovery Phase

Depending on the keys established on the previous phase, route discovery process is initiated. This phase consist of route request, route reply and data transmission. Route request (RREQ): Let the transmission between two nodes say, S and B. The node S chooses a random number and uses the identity of node B to encrypt the trapdoor information that can be opened only by private ID-based key of B. Fig.1shows the Route Discovery of SARP.

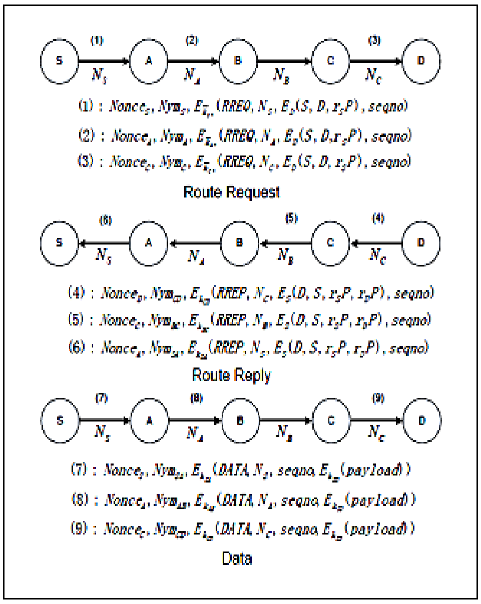

S
A
B
C
D
(1)
(2)
(3)
N_S
N_A
N_B
N_C
(1) : $Nonce_S, Nym_S, E_{k_{SA}}(RREQ, N_S, E_B(S, D, r_S P), seqno)$
(2) : $Nonce_A, Nym_A, E_{k_{AB}}(RREQ, N_A, E_B(S, D, r_S P), seqno)$
(3) : $Nonce_C, Nym_C, E_{k_{CD}}(RREQ, N_C, E_D(S, D, r_S P), seqno)$
Route Request
(6)
(5)
(4)
(4) : $Nonce_D, Nym_{CD}, E_{k_{CD}}(RREP, N_C, E_S(D, S, r_S P, r_D P), seqno)$
(5) : $Nonce_C, Nym_{BC}, E_{k_{BC}}(RREP, N_B, E_S(D, S, r_S P, r_D P), seqno)$
(6) : $Nonce_A, Nym_{SA}, E_{k_{SA}}(RREP, N_S, E_S(D, S, r_S P, r_D P), seqno)$
Route Reply
(7)
(8)
(9)
(7) : $Nonce_S, Nym_{SA}, E_{k_{SA}}(DATA, N_S, seqno, E_{k_{SD}}(payload))$
(8) : $Nonce_A, Nym_{AB}, E_{k_{AB}}(DATA, N_A, seqno, E_{k_{SD}}(payload))$
(9) : $Nonce_C, Nym_{CD}, E_{k_{CD}}(DATA, N_C, seqno, E_{k_{SD}}(payload))$
Data

Fig.1 Route Discovery of SARP

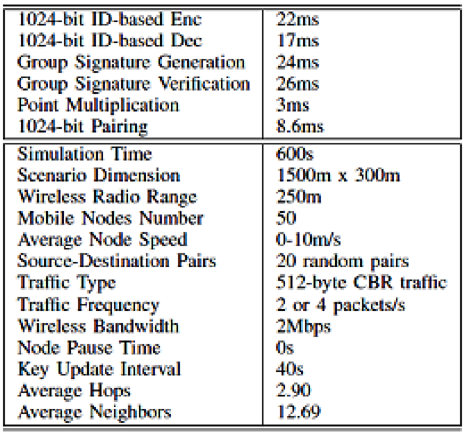
Route Reply (RREP): Once the node B realizes it is the destination node, B starts to make the RREP message to the source node S. Broadcast technique is used for route reply messages. The node B chooses a random number and computes a cipher text to make aware that it is the valid destination capable of opening the information. Once route reply is carried out, before the data transmission, the node checks for load that is being transferred. In this case a intrusion detecting node is placed in between the other nodes. If the load is greater than the threshold, attack is detected and a secure data transmission is carried out. If the load is less than the maximum limit and if the new profile is less than the maximum threshold, then there is no attack.

C. Unobservable Data Transmission

Once the source node S finds out its successful destination to be B, it can start data transmission using pseudonyms and keys that is generated in earlier phases to achieve unobservability. On receiving the message from S, the intermediate node will know that the message is for them. After the decryption by the right key, it will know to whom the data packet must be sent next. Thus the data packet must be forwarded by the intermediate nodes until it reaches the destination node B.

III. SIMULATION AND PERFORMANCE EVALUATION

The proposed routing scenario is implemented using NS2. Under the topology formation, 50 nodes are randomly distributed within a network field of 1680×970 meter such as a rectangle field. The traffic type is 512-byte CBR traffic. The node receives necessary cryptographic data to participate in the network. Each node stores a unique identity and public/private key pair with a certificate, the public key of the key server, and the required cryptographic data for the key exchange protocol. The IDS node checks for the load to detect attacks if any. The implementation result gives acceptable performance in terms of packet delivery ratio, packet delivery latency. But this protocol achieves anonymity, complete unlinkabilty, unobservability in terms of content and traffic and more over resists completely can achieve unobservability without too much computation cost. Table.1 shows the simulation parameters.



1024-bit ID-based Enc	22ms
1024-bit ID-based Dec	17ms
Group Signature Generation	24ms
Group Signature Verification	26ms
Point Multiplication	3ms
1024-bit Pairing	8.6ms
Simulation Time	600s
Scenario Dimension	1500m x 300m
Wireless Radio Range	250m
Mobile Nodes Number	50
Average Node Speed	0-10m/s
Source-Destination Pairs	20 random pairs
Traffic Type	512-byte CBR traffic
Traffic Frequency	2 or 4 packets/s
Wireless Bandwidth	2Mbps
Node Pause Time	0s
Key Update Interval	40s
Average Hops	2.90
Average Neighbors	12.69

Table.1 Simulation Parameters

As a result SARP comprises two phases: Fig 2.a shows the packet delivery ratio of SARP.

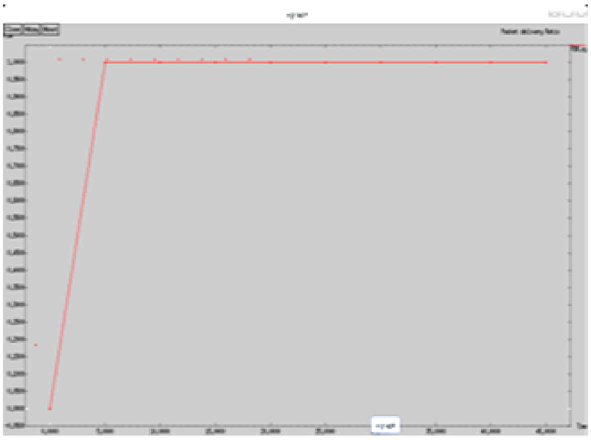


Fig.2.a Packet delivery ratio of SARP

Fig 2.b shows the packet delivery ratio of SARP. In AODV, only three types of routing control packets, namely routing request packet, routing reply packet, and routing error packet.

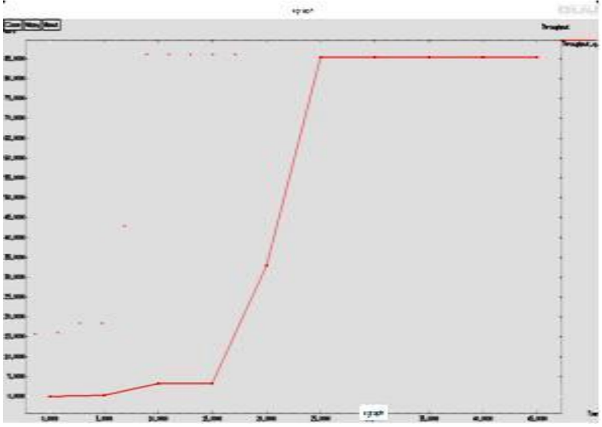


Fig.2.b Throughput of SARP

Fig 2.c Show that packet drop of SARP. In SARP only trusted neighbors will forward route packets for each other, otherwise packets are simply dropped.

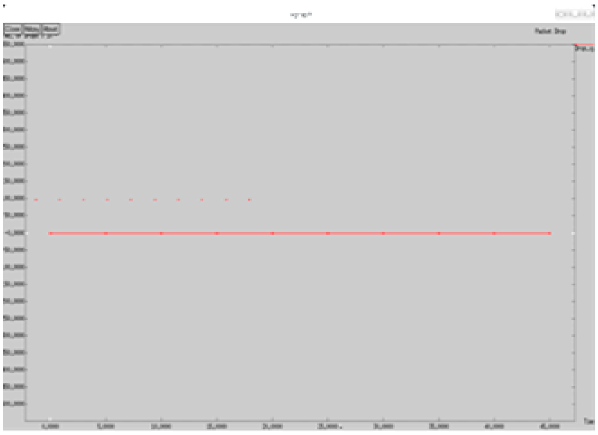


Fig.2.c Packet drop of SARP

IV. CONCLUSION

To achieve secure group communications with both confidentiality and non-repudiation in MANETs, we design a secure anonymous routing protocol scheme, which encrypts once with one key establishment produced for all group members. SARP based on Group signature and ID-based cryptosystem for ad hoc networks. The design of SARP offers strong privacy protection completes unlinkability and content unobservability for ad hoc networks. The security analysis demonstrates that SARP not only provides strong privacy protection, it is also more resistant against attacks due to node compromise. The proposed scheme is self-organizing rather than dictated by a policy administrator. It will be able to provide some technology support for secure group communication in MANETs. Actually, our scheme is also suitable to other network models and scenarios, such as peer-to-peer systems and cloud computing systems since both of them are dynamic peer systems in common with MANETs.

REFERENCES

[1] L. Song, L. Korba, and G. Yee, "AnonDSR: efficient anonymous dynamic source routing for mobile ad-hoc networks," in Proc. 2005 ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 33–42.
[2] J. Kong and X. Hong, "ANODR: aonymous on demand routing with untraceable routes for mobile ad-hoc networks," in Proc. ACM MOBIHOC' 03, pp. 291–302.
[3] Sy, R. Chen, and L. Bao, "ODAR: on-demand anonymous routing in ad hoc networks," in 2006 IEEE Conference on Mobile Ad-hoc and Sensor Systems..
[4] 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. 2004 IEEE LCN, pp. 618–624.
[5]Y.Zhang,W.Liu,andW. Lou, "Anonymous communications in mobile ad hoc networks," in 2005 IEEE INFOCOM.
[6] 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, 2011
[7] A. Pfitzmann and M. Hansen, "Anonymity, unobservability, and pseudonymity: a consolidated proposal for terminology," draft, July 2000.
[8] Y. Zhu, X. Fu, B. Graham, R. Bettati, and W. Zhao, "On flow correlation attacks and countermeasures in mix networks," in PET04, LNCS 3424, 2004, pp. 207–225.
[9] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," Commun. of the ACM, vol. 4, no. 2, Feb. 1981.
[10] S. Capkun, L. Buttyan, and J. Hubaux, "Self-organized public-key management for mobile ad hoc networks," IEEE Trans. Mobile Comput., vol. 2, no. 1, pp. 52–64, Jan.-Mar. 2003.
[11]Zheng, X., Huang, C.T., Matthews, M.: 'Chinese remainder theorem based group key management'. Proc. 45th ACM Southeast Regional Conf., Winston-Salem, North Carolina, USA, 2007, pp. 266–271.
[12] Chiou, G.H., Chen, W.T.: 'Secure broadcasting using the secure lock', IEEE Trans. Softw. Eng., 1989, 15, (8), pp. 929–934.
[13]Qianhong, W., Yi, M., Willy, S., Bo, Q., Josep, D.F.: 'Asymmetric group key agreement'. Proc. EUROCRYPT, Cologne, Germany, 2009,(LNCS, 5479), pp. 153–170.
[14] Han, Y., Gui, X.: 'Multi-recipient signcryption for secure group communication'. Proc. ICIEA2009, Xi'an, China, 2009, pp. 161–165.
[15] Han, Y., Gui, X., Wang, X.: 'Multi-recipient signcryption for secure wireless group communication', available at http://www.eprint.iacr.org/2008/253.

BIOGRAPHIES

K.Vinoth Kumar received the **B.E.** degree in Electronics and Communication Engineering from the Kurinji College of engineering and technology, Manapparai, Anna University, Chennai, India, in 2009. He received the **M.E.** degree in Applied Electronics from the J.J College of engineering and technology, Trichirappalli, India, in 2011. Currently doing **Ph.D.** in Communication and Networking in Karpagam University Coimbatore. He is a member in Universal Association of Computer and Electronics Engineer (UACEE) and member in International Association of Engineer (IAENG). He published six international journals. His research interest includes wireless communication, Mobile Ad hoc networks, Sensor Networks, Communication networks.

N.Senthil Kumaresan received the B.E. degree in Computer Science Engineering from the P.T.R College of engineering and technology, Madurai, Anna University, Chennai, India, in 2011.Currently doing M.E. Computer Science Engineering in J.J College of engineering and technology, Trichirappalli, India. His research interest includes Cloud Computing, wireless communication, Mobile Ad hoc networks, and Data Mining and Web services.