ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

A Novel Key Distribution Scheme for Efficient Group Communication in MANET

G. Babu[1], R. Balamurugan M.E[2]

M.E Computer Science & Engineering, Adhiparasakthi Engineering College, Melmaruvathur, India[1]

Assistant Professor, Adhiparasakthi Engineering College, Melmaruvathur, India [2]

Abstract— Mobile ad-hoc Network (MANET) is collection of mobile platforms that form a dynamic infrastructure communication network wherever required. Until recently, Mobile nodes formed a group communication, even for communication there is a problem of efficient and securely broadcast from sender to remote cooperative group occurs in many emerging applications. In Existing consider several distributed collaborative group key management had unavailability of a fully trusted key generation procedure. To overcome the problem, this paper proposed a new key management to ensure the safety of group key and to protect the group communication. In propose a tesla based triple key encryption to protect communication group by using a novel key approach, its implementation affability without relying on a fully trusted authority provide our protocol a very promising solution to many applications. Furthermore, our scheme provides basic strategies of member addition/deletion and rekeying operation for cooperative group.

Index Terms— Ad hoc networks, broadcast, co-operative computing, information security, key management.

I. INTRODUCTION

The field of wireless and mobile communications has experienced an unprecedented growth during the past decade. In latest emerging networks, there is a need to broadcast to remote cooperative groups using encrypted transmission. Examples can be found in access control in remote group communication arising in, mobile ad hoc networks (MANETs), vehicular ad hoc networks (VANETs), etc.

A mobile ad hoc network is an autonomous collection of mobile devices (laptops, smart phones, sensors, etc.) that communicate with each other over wireless links and cooperate in a distributed manner in order to provide the necessary network functionality in the absence of a fixed infrastructure. They can also be heterogeneous, which means that all nodes don't have the same capacity in term of resources (power consumptions, storage, computation, etc.) [1]. In

MANETs, it is important to support group-oriented applications, such as audio/video conference and one-to-many data dissemination in battlefield or disaster rescue scenarios.

Until recently, however, the way in which such groups are formed had not drawn much attention. Because communication in wireless networks is broadcast and a certain amount of devices can receive transmitted messages, the risk of unsecured sensitive information being intercepted by unintended recipients is a real concern [2]. For instance, a commander may issue secret commands to soldiers in battlefield via satellite-to-MANET communication. Consequently, efforts to secure group communications in MANETs are essential. From the above MANET group communication, the common difficulty is to allow a sender to securely transmit data to a remote cooperative group from unintended nodes. A resolution to this problem must meet several constraints. The sender is remote and can be dynamic. The transmission may traverse various way including insecure networks before reaching the corresponding group members. Also, the sender may wish to choose only a subset of the group as the receivers. Furthermore, it is hard to resort to a fully trusted third party to secure the transmission. Facilitate remote access control of group-oriented communication without relying on a fully trusted secret key generation center.

1.1 Related Work

The major security concern in group-oriented communications with access control is key management. Existing key management systems in these scenarios are mainly implemented with two approaches referred to or group key exchange by some authors and key distribution systems. Both are active research areas having generated large respective bodies of literature.

Group key agreement allows a group of users to negotiate a common secret key via open insecure networks. Then, any member can encrypt any confidential message with the shared secret key and only the group members can decrypt.

In this way, a confidential intragroup broadcast channel can be established without relying on a centralized key server to generate and distribute secret keys to the potential members. A large number of group key agreement protocols have been proposed [3-5].
The earlier efforts [3], [4] focused on efficient establishment of the initial group key. Broadcast encryption schemes in the literature can be classified in two categories: symmetric-key broadcast encryption and public-key broadcast encryption. In the symmetric-key setting, only the trusted center generates all the secret keys and broadcasts messages to users. Hence, only the key generation center can be the broadcaster or the sender. In the public-key setting, in addition to the secret keys for each user, the trusted center also generates a public key for all the users so that anyone can play the role of a broadcaster or sender.

2. PROPOSED WORK

2.1 Contribution

Our role includes three aspects. 1). The problem of secure transmission to cooperative groups, in which the heart is to establish a broadcast channel securely and efficiently under certain constraints. From existing key management approaches do not provide effective solutions to this problem. On one hand, group key agreement provides an efficient solution to secure intragroup communication, but for a remote sender, it requires the sender to simultaneously stay with the group members for multiple rounds of interactions to agree a common secret session key before transmitting any secret contents [6]. This is impractical for a remote sender who may be in a different location.
2). Broadcast encryption enables senders to broadcast to non-group members of a fixed group without requiring the sender to interact with the receivers before transmitting secret contents, but it relies on a centralized key manager to generate and distribute secret keys for each group member. 3). These imply: a) before a confidential broadcast channel is established, numerous confidential unicast channels from the key server to each potential receiver have to be constructed; and b) the key manager holding the secret key of each receiver can read all the communications and has to be fully trusted by any potential sender and the group members.

2.2 proposed system

A new key management paradigm referred to as group key agreement-based broadcast encryption. The system architecture is illustrated in fig. 1.

The potential receivers are connected together with efficient local connections. Via communication infrastructures, they can also connect to heterogeneous networks.

Each receiver has a public/secret key pair. The public key is certified by a certificate authority, but the secret key is kept only by the receiver.

A remote sender can retrieve the receiver's public key from the certificate authority and validate the authenticity of the public key by checking its certificate, which implies that no direct communication from the receivers to the sender is necessary. Then, the sender can send secret messages to any chosen subset of the receivers.

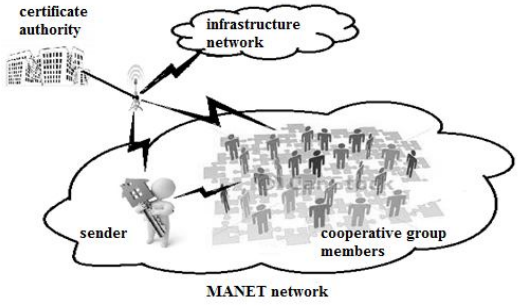

Fig. 1 System design

The proposed research is provide encryption process for sense that the intrusion detection system (IDS) and avoid. New IDS take care of two kinds of attacks, namely, the black hole attack and the Sybil attack. Whereas in proposed approach can be incorporated in any routing protocol. The TESLA (Timed Efficient Stream Loss-tolerant Authentication) broadcast authentication protocol, an efficient protocol with low communication and computation overhead, which scales to large numbers of receivers, and tolerates packet loss.

2.2.1 Key Management to Remote Cooperative Groups

The main theme of key management is to securely distribute a session key to the corresponding receivers, it is sufficient to define the system as a session key encapsulation mechanism.

TABLE 1

NOTATIONS

Notation	Description
N	Total Number Of Users
n	Subset From Users
i	Index
u_i	Any User From Subset
pk_i	Public Key
pr_i	Private Key
sk_i	Secret key(Session key)

The sender can continuously encrypt any message under the session key in single conversations and the corresponding receiver decrypt the message. In key management consists of the following operations: 1). Key Generation, 2). Encryption, 3). Decryption.

- Key Generation: In key generation algorithm is perform in each user $u_{i,}$ where i is belongs to {1,…,N} to generate his public/secret key pair. A sender want to send data to group member's n, where n is subset of N. For any user act as sender, then the sender need key pair of n members. Suppose i is any user, he is in {1,…,n} or any member for his key pair is denoted by (pk_i/sk_i). In this public keys are know by all members in the network. The public/secret keys are maintained by certificate authority.
  - Encryption: It is done by sender, who is may or may not be in the group set i.e. (1, …,n). For encryption sender know the public key of all intended receivers. Sender need the details of all the users public keys from that sender only use potential receivers keys i.e. (1,…n)ϵ (1,…,N). In encryption process get the input as receiver's public key i.e. pk_i where i ϵ (1,…,n) and message or session key. From the encryption process completed got output data as concatenation of encrypted message with hash code.
  - Decryption: This decryption performs by each receiver in subset. The receivers exact the session key or message as output from received encrypt message. Each receiver uses their secret key to decrypt the corresponding received message. Only n member of users perform this operation.

In key management the certificate authority act as a third parity, he knows all users public key information. In previous system model the certificate authority act as fully trusted system, but in this act as partially trusted system. This type of trusted system called as public key infrastructure.

There is a difficult for sender use the fully trusted system. In fully trusted system sender want to connect with receiver for secret key exchange because of trusted system has user's public key and secret key pair. But in the partially trusted system sender no need to connect with receiver because the sender request the certificate authority to get the public key information of users.

From the key management process clearly define the sender and receiver only involved in encryption and decryption process. It does not depend on the size of N users.

2.2.2 Algorithm for Encryption and Decryption

In group communication scheme using ECC Diffie-Hellman (ECDH) exchange algorithm to share the session key between nodes. $E_q(a,b)$ is a equation of elliptic curve with parameter a,b and q, where is a prime. In curve select the base point G whose largest order value is s. Then user selects the private key pr_i from that generate pk_i that will store in certificate authority. Session key can share by using receiver's public key and sender private key. TESLA based triple key encryption is used during data transmission. The sender split the session key into uniform interval.

Proposed key generation: each user i for i=1,…., N randomly chooses x_i. Then generate public key X_i register the public key in certificate authority.

- Encryption: A sender wishes to broadcast data to n users. The sender runs the following algorithm.

1). Randomly select q, drive the G. And compute X_i.

2). Extract the public group encryption key for subset n.

3). Compute the share key i.e share key.

4). Compute the session key k. calculates the hash code.

5). Broadcast the hash code.

- Decryption: From each receiver from the group decrypt their received data in following manner.

1). Compute the secret decryption key

2). Using the secret the receiver extracts the session key $sk_{i.}$

Since the (P,Q)-ECDH assumption is believed to hold, no such polynomial-time algorithm exists, and hence no polynomial time attacker can distinguish the session key to any receiver set from a random string in the session key space . Therefore, our scheme is secure against polynomial time-bounded attackers.

2.2.3 Practical Aspects of Key Management Scheme.

Member organization: Many key management schemes organize the users in a tree-based structure. However, for our scheme, it is preferable to organize them in a chain and then use the sender to close the chain to form a logical ring.

The chain can be formed by ordering the users lexicographically by the least important bits of their unique public keys, and then a ring is formed by closing the chain with the sender, where the public keys {pk_{i1}, …..,pk_{in} } of the receivers and the temporary public key pk_{i0} of the sender appear as the corresponding nodes in the ring, respectively. It represented in fig. 2.

Compared to the tree-based structure, the above structure allows better performance for receiver and sender changes.

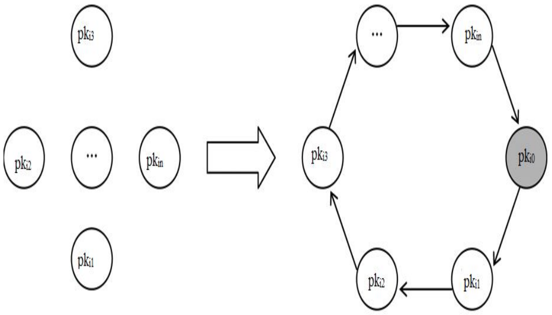

Fig. 2 Member organization

Member addition/deletion: In existing group key agreement-based key management protocols, to exclude a group member or enroll a new member, multiple rounds of communication among the members are required before the sender can securely broadcast to the new receiver set. In our scheme, it is almost free of cost for a sender to exclude a group member by deleting the public key of the member from the public key chain or, similarly, to enroll a user as a new member by inserting that user's public key into the proper position of the public key chain of the receivers. After the deletion/addition of certain member, a new logical public-key ring naturally forms. Hence, a trivial way to enable this change is to run the protocol independently with the new key ring. We illustrate in the following an alternative implementation equivalent to the trivial way, but such that much cost is saved by exploiting the values computed in the last run of the protocol.

Member Deletion: the deletion of member u_i from the receiver group. Then, the sender and the remaining receivers need to apply this change to their subsequent encryption and decryption procedures.

- Encryption: The sender runs this algorithm as follows.

1) Randomly select prime q, secret key and compute the new public key. In this step, the sender indexed by reinserts herself into the ring and connects to receivers.

Hence, the operation is the same as that of the basic protocol, but the sender has to choose new random values.

2) Compute the new public group encryption key.

3) Compute the new secret session key.

4) Broadcast to the receivers the new hash code.

- Decryption: The receivers run this algorithm as follows.

1) According to Step 1 of the decryption procedure of the basic protocol, it is easy to see that only receivers and need to respond to the change in this step.
2) Compute the new group decryption key.
3) Receiver extracts the new session key.

Member Addition: If the sender would like to include a new member, the sender just needs to retrieve the public key of this user and insert it into the public key chain of the current receiver set. Then, the sender and receivers in the new receiver set need to apply this change to their subsequent encryption and decryption procedures.

- Encryption: The sender runs this algorithm as follows.

1) Randomly select prime q, secret key and compute the new public key. In this step, the sender indexed by added new user into the ring and connects to receivers. Hence, the operation is the same as that of the basic protocol, but the sender has to choose new random values.
2) Compute the new public group encryption key.
3) Compute the new secret session key.
4) Broadcast to the receivers the new hash code.

- Decryption: The receivers run this algorithm as follows.

1) The decryption procedure of the basic protocol, it is easy to see that only receivers with the new user need to respond to the changes in the ring.
2) Compute the new group decryption key.
3) Receiver extracts the new session key.

Rekeying: The above refers to the change of members. Even if the receiver group does not change, various scenarios may require key update. This is a complex issue in most key management schemes. On the contrary, our protocol can provide three levels of key update, which facilitates flexible rekeying strategies. There are three strategies:

1. Session Key Update
2. Group Decryption Key Update
3. Long-Term Secret Key Update

Updating the long-term secret key of a member causes more overhead than updating her session key or her group decryption key, although the long-term secret key update process described is still much more efficient than a completely new run of the protocol. This is reasonable because the long-term secret key is the one that should be changed least often; each member should keep its long-term key secure to reduce unwanted burden to other members.

3. PERFORMANCE EVALUATION

This is very desirable in ad hoc networks where members may join and leave, or some member's key might be compromised. Also, one should note that although our protocol needs one round interaction for decryption in the cases of member changes or update of the group decryption key or long-term keys of members, only very few members are involved in the interaction. Our new key management paradigm has also structural advantages over existing paradigms. Compared to group key agreement, our approach does not require a remote sender to simultaneously stay online with the receivers. This makes possible the desirable pattern for the senders. Compared to broadcast encryption, our approach does not require a fully trusted key server and is easy to be deployed.

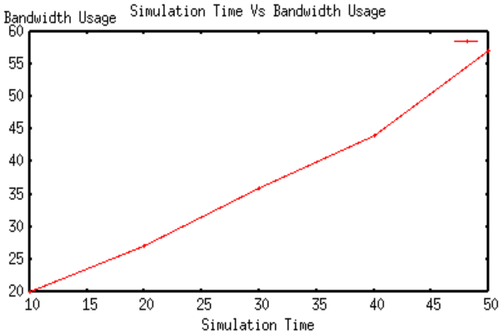

Fig. 2 Simulation time Vs Bandwidth Usage

From the Fig. 2 to known the bandwidth usage in during the transmission can be analyses the experimental result. That the communication between sender and group members needs the expected number of sessions varying from 10 to 50, and size of the bandwidth limited by 60 Hz.

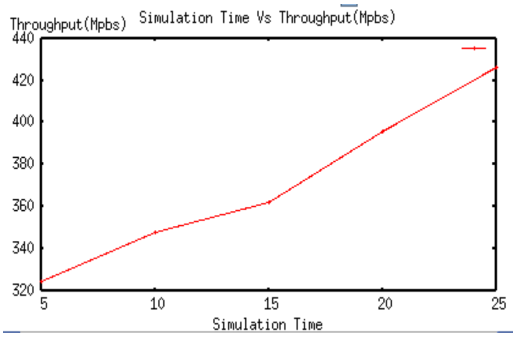

Fig. 3 Simulation time Vs Throughput

From the Fig. 3 to known the bandwidth used transmission can be analyses the experimental result. That the communication between sender and group members needs the expected number of sessions varying from 10 to 50, and duration of throughput varies from 320 to 440 Mbps.

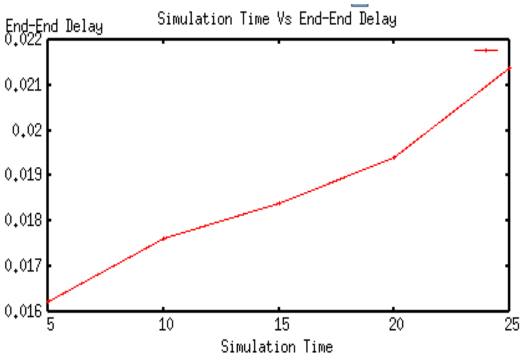

Fig. 4 Simulation time Vs Delay

From the Fig. 4 to known the delay can be analyses the experimental result. That the communication between sender and group members needs the expected number of sessions varying from 10 to 50, and delay between end nodes to reach up to 0.022.

4. CONCLUSION

We have proposed a new key management paradigm to enable sender no need to connect with receiver for broadcasts to remote cooperative groups with only partially trusted third party. Our scheme had proved secure in the standard model. A systematic complexity analysis and extensive experiments show that our proposal is also efficient in terms of computation and communication. These features render our scheme a talented solution to group-oriented communication with access control in various types of ad hoc networks.

REFERENCES

[1] Priyanka Goyal, Vinti Parmar,and Rahul Rishi," MANET: Vulnerabilities, Challenges, Attacks, Application," IJCEM International Journal of Computational Engineering & Management, Vol. 11, pp. 33-35, January 2011.

[2] Y.-M. Huang, C.-H. Yeh, T.-I. Wang, and H.-C. Chao, Constructing secure group communication over wireless ad hoc networks based on a virtual subnet model," IEEE Wireless Commun., vol. 14, no. 5, pp. 71–75, Oct. 2007.

[3] M. Burmester and Y. Desmedt, "A secure and efficient conference key distribution system," Adv. Crypt., vol. 950,UROCRYPT'94, LNCS, pp. 275–286, 1995.

[4] M. Waldvogel, G. Caronni, D. Sun, N. Weiler, and B. Plattner, "The versakey framework: Versatile group key management," IEEE J. Sel. Areas Commun., vol. 17, no. 9, pp. 1614–1631, Sep. 1999.

[5] R. Dutta and R. Barua, "Provably secure constant round contributory group key agreement in dynamic setting," IEEE Trans. Inf. Theory, vol. 54, no. 5, pp. 2007–2025, May 2008.

[6] Lifeng Lai, Yingbin Liang, and Wenliang Du," Cooperative Key Generation in Wireless Networks" IEEE Journal On Selected Areas In Communications, vol. 30, no. 8, pp. 1579-1581, September 2012.