RESEARCH ARTICLE OPEN ACCESS

Key Management and Group Key Agreement For Fast Transmission To Remote Groups

T.Suruthi, PG Scholar
Department of Information Technology
Francis Xavier Engineering College
Vannarpettai, Tirunelveli.
tsuruthi@gmail.com

T.Anto Theepak, Assistant Professor
Department of Information Technology
Francis Xavier Engineering College
Vannarpettai, Tirunelveli.
theepak_a@yahoo.com

Abstract --
In newly emerging networks, securely and efficiently broadcasting to a remote cooperative group is a major problem. In this paper, a novel key management approach is proposed to solve this problem. The new approach is a cross of existing broadcast encryption and group key agreement. In this approach, each node maintains a public/secret key pair. By seeing the public/secret key of the node, a sender can securely broadcast to any group. The proposed method is to enable send and leave broadcast to remote cooperative groups. If the non intended members collude, they cannot extract any information from the transmitted messages. The proposed approach provides efficient member deletion/addition, flexible rekeying strategies and is also efficient in terms of communication.

Keywords — Access control, ad hoc networks, cooperative computing, Information security, key management, remote group.

I. INTRODUCTION

In newly emerging networks, there is a need to broadcast to remote cooperative groups using encrypted transmission. Examples can be found in remote group communication arising in wireless mesh networks (WMNs), mobile ad hoc networks (MANETs), vehicular ad hoc networks (VANETs), etc. Wireless mesh networks (WMNs) are vigorously self-organized with the nodes in the network automatically establishing an ad hoc network and maintaining the mesh connectivity. It is a multihop layered wireless network. WMN consists of two different types of nodes: mesh routers and mesh clients. Other than the routing capability for gateway/bridge functions a mesh router contains additional routing functions to support mesh networking. Through the multi-hop communications, the same coverage can be achieved by a mesh router with much lower transmission power.

To improve the flexibility of mesh networking, a mesh router is usually equipped with multiple wireless interfaces built on either the same or different wireless access technologies.

MANET is a system, which is made up of wireless mobile nodes. These nodes have wireless transmission and networking characteristics. MANETs are proposed to serve as an effective networking system facilitating data trade between mobile devices even without fixed infrastructures. The MANETs applications include audio/video conference and one-to-many data dissemination in battlefield or disaster rescue scenarios [1].

VANETs are deployed in the near future. A VANET consists of on-board units (OBUs) fixed in vehicles serving as mobile computing nodes and roadside units (RSUs) working as the information infrastructure located in the critical points on the road. Mobile vehicles form many groups in their wireless communication range in the roads, and through roadside infrastructures, vehicles can access other networks such as Internet communication. VANETs are designed for the primary goal of improving traffic safety and the secondary goal of providing value-added services to vehicles [5].

In the group communication scenario, the common problem is to enable a sender to securely transmit messages to a remote cooperative group. A solution to the above problem must meet several constraints. First, the sender is located in a remote place and can be dynamic. Second, the transmission may hybrid various networks including open insecure networks before reaching the intended recipients. Third, the communication from the group nodes to the sender may be limited. The sender will choose only a subset of the group as the intended recipients. Furthermore, it is hard to resort to a fully trusted third party for securing the communication. In the above constraints, mitigating features are, that the group nodes are cooperative and the communication among them is local and efficient. This paper exploits these mitigating features to facilitate remote access control of group-oriented communications without relying on a fully trusted third party.

A. Contribution

In this paper it includes three aspects. First, the problem of securing transmission to remote cooperative groups is formalized, in which the core is to establish a one-to-many channel securely and efficiently under certain constraints. Group key agreement provides an efficient solution to secure intragroup communication, but for a remote sender, it requires the sender to stay online with the group members simultaneously for multiple rounds of interactions to negotiate a common secret session key before transmitting any secret contents. This is impossible for a remote sender who may be in a different time zone. This is further deteriorated if the sender is mobile or otherwise dynamic. Broadcast encryption enables external senders to broadcast to non cooperative members of a preset group without requiring the sender to interact with the receivers before transmitting secret contents, but it relies on a centralized key server to generate and distribute secret keys for each group node. This shows that: 1) before a confidential broadcast channel is established, confidential unicast channels from the key server to each potential receiver have to be constructed; and 2) the key server holding the secret key of each receiver can read all the messages and has to be fully trusted by any potential sender and the group members.

B. Paper Organization

The rest of the paper is organized as follows. In Section II the system architecture is shown. Section III describes the proposed approach for key management. Section IV, V and VI describe the modules, results and finally concludes the paper.

II. SYSTEM ARCHITECTURE

The system architecture is shown in Fig. 1. The potential receivers are connected together with well-organized local connections. Via communication infrastructures, they can also connect to the heterogeneous network. Each receiver node has a public/secret key pair. The public key is only certified by a certificate authority, but the secret key is kept only by the receiver not known to the certificate authority.

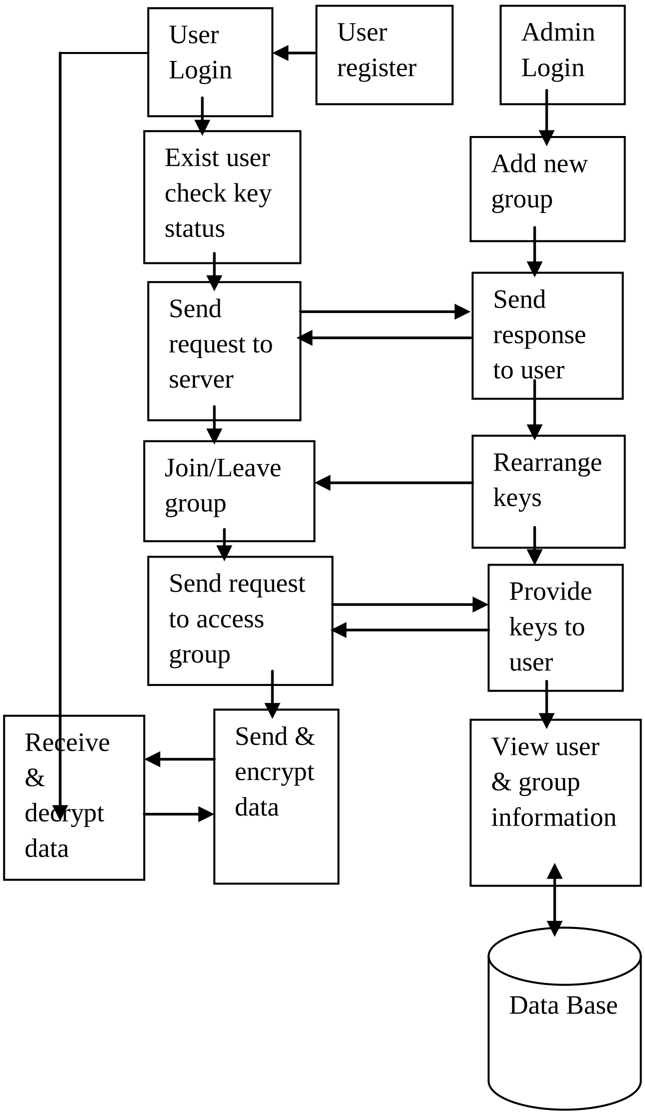

Fig .1.System Architecture

The sender will 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 any secret messages to any chosen subset of the receivers.

III. KEY MANAGEMENT AND KEY DISTRIBUTION

A. Proposed Approach

The proposed key management system includes both the broadcast encryption systems [2] and group key management systems [1].

Key Generation: The key generation parameters include the individual node number and the total number of members exists in the group. Thus public/secret key pair and the session keys are generated. After the keys are generated, distributions of keys are carried out for the transmission of messages.

Encryption: After the keys are distributed to the group member, members can start to transmit the messages. The sender will encrypt the message and forward it to the receiver. To encrypt the data sender will retrieve the receiver's public key from the certificate authority; it checks and validates the certificate.

Decryption: The receiver will decrypt the data by using the session key which is distributed by the sender.

B. Member Organization

The key management (i.e., group key agreement or broadcast encryption) schemes organize the users in a tree-based structure. However, 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 by the least important bits of their unique public keys, and then a ring is formed by closing the chain with the sender.

C. Member Deletion/Addition

In the existing group key agreement system to exclude a group member or enroll a new member it includes several rounds of communication among the members are required before the sender securely broadcast to the receiver set. In the proposed system it is simple for a sender to exclude a group member by deleting the public key of the member from the public key chain. To insert 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 is carried out, a new ring structure is formed. After a member gets deleted its public key will be deleted from the certificate authority. Thus deleted member cannot read the previous transmission.

IV. MODULES

The proposed approach includes the following modules: User authentication, Group creation and provide keys, Join group and leave the group, rekeying and storage.

A. User Authentication

New node can join to the group and able to transfer messages. Once a member is added to the group its public/secret key will be created and the public key is send to the certificate authority for the checking purpose.

B. Group Creation and Provide keys

A group will be created to join the nodes for broadcast transmission. Once a group is created nodes will join to the group. Each node should have a public/secret key pair and the keys are verified and validated by the certificate authority. Only the public keys are known by the certificate authority but the secret key is kept only by the receiver. The certificate authority validates the key by checking its certificate. The sender will retrieve receiver's public key from the certificate authority and start transmission. Session key is created and sent by the sender. Sender will encrypt the message and also it sends the secret session key to the recipient for secure transmission. The receiver will decrypt the session key which is placed in the header and also the encrypted message.

C. Join and Leave the group

A new member can join to the group and sends its public key to the certificate authority, it validates by checking its certificate. Also member can get deleted from the group; once a member is deleted its public key also gets deleted. Deleted member cannot read the group transmission messages. Joining and leaving a member from the group is easier in the proposed approach.

D. Rekeying and storage

Each member has its own public/secret key for secure transmission. The keys are updated automatically by fetching its group name from the remote group. The transmission to the remote group is fast in the proposed approach using the novel key management approach.

V. EXPERIMENTAL RESULTS

In the proposed approach a new key management system is used for secure communication. A new member can join and also existing member can get deleted from the group. The keys are updated automatically by using the group member. The keys are distributed before starting the transmissions. Group is created to join the node, sender will encrypt the message and the session key is placed in the header. The receiver will decrypt the key and also the encrypted message. In the receiver side the sender node, transmission times are displayed.

VI. CONCLUSION

In this paper a new key management approach is proposed to enable send-and-leave broadcasts to remote cooperative groups without relying on a fully trusted third party. The proposed approach provides efficient member deletion/addition, flexible rekeying strategies and is also efficient in terms of computation and communication.

REFERENCES

[1] B. Rong, H.-H. Chen, Y. Qian, K. Lu, R. Q. Hu, and S. Guizani, “A pyramidal security model for large-scale group-oriented computing in mobile ad hoc networks: The key management study,” IEEE Trans. *Veh. Technol*., vol. 58, no. 1, pp. 398–408, Jan. 2009.

[2] C. Gentry and B. Waters, “Adaptive security in broadcast encryption systems (with short ciphertexts),” *Adv. Cryptol.*, vol. 5479, EUROCRYPT’ 09, LNCS, pp. 171–188, 2009.

[3] C. K. Wong, M. Gouda, and S. Lam, “Secure group communications using key graphs,” *IEEE/ACM Trans. Netw.*, vol. 8, no. 1, pp. 16–30, Feb. 2000.

[4] D. Boneh, C. Gentry, and B. Waters, “Collusion resistant broadcast encryption with short ciphertexts and private keys,” *Adv. Cryptol.*, vol. 3621, CRYPTO’05, LNCS, pp. 258–275, 2005.

[5] D. Halevi and A. Shamir, “The LSD broadcast encryption scheme,” *Adv. Cryptol.*, vol. 2442, CRYPTO’02, LNCS, pp. 47–60, 2002.

[6] J. H. Cheon, N.-S. Jho, M.-H. Kim, and E. S. Yoo, “Skipping, cascade, and combined chain schemes for broadcast encryption,” *IEEE Trans. Inf. Theory*, vol. 54, no. 11, pp. 5155–5171, Nov. 2008.

[7] M. Burmester and Y. Desmedt, “A secure and efficient conference key distribution system,” *Adv. Cryptol.*, vol. 950, EUROCRYPT’94, LNCS, pp. 275–286, 1995.

[8] M. Naor and B. Pinkas, “Efficient trace and revoke schemes,” in *Proc. 4th FC,* 2001, vol. 1962, pp. 1–20.

[9] M. Steiner, G. Tsudik, and M. Waidner, “Key agreement in dynamic peer groups,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 11, no. 8, pp. 769–780, Aug. 2000.

[10] N. Koblitz and A.Menezes, “Pairing-based cryptography at high security levels,” *Cryptogr. Coding*, vol. 3796, IMA2005, LNCS, pp. 13–36, 2005.