ISSN:0975-9646

Fast Transmission to the Remote Co Operative Group: A New Key Management VPN and Security Policy Enforcement

Anil s Naik [#1], Prakash C Pawar [#2], Santosh C Pawar [#3]

[#1] *Department of Information Technology, Solapur University, Solapur (MH), India*
[#2] *Department of Electrical and Electronics Department, VTU Karnataka, Bijapur (KAR), India*
[#3] *Department of Computer science and Engineering Department, JNTU, Hyderabad (AP), India*

***Abstract*: The problem of efficiently and securely broadcasting to the remote cooperative group occurs in many newly emerging networks. A major challenge in devising such systems is to overcome the obstacles of potentially limited communication among the group to the members, the unavailability of fully trusted key generated center and the dynamic of the sender. The existing key management paradigms cannot deal with these challenges effectively.In this paper we circumvent these obstacles and close this gap by proposing a novel key management paradigm.In addition to this it can also provide internet data safe.The customer can securely deposit there important property or sentimental assets such as pictures and correspondence in the personel online vault.The digital safe deposit box can then be offered as an extension to an existing online banking solution.It also uses an vpn security concern and policy enforcement in order to provide information securely to the intended user.This new paradigm is the hybrid of the traditional broadcast encryption and the group key aggrement.Even if all the non intended members collude they cannot extract any usefull information from the transmitted message.After the public group encryption is extracted ,both the computation overhead and the communication cost is independent of the group size.Further more ,our scheme facilitates simple yet efficient member addition/deletion and flexible rekeying strategy.**

***Keywords:* Adhoc networks,broadcast,cooperative computing access control,information security,key management,vpn security ,policy enforcement**

I. Introduction

As a result of the increased popularity of group-oriented applications and protocols, group communication occurs in many different settings: from network layer multicast to application layer tele- and video-conferencing. Regardless of the underlying environment, security services are necessary to provide communication privacy and integrity. In many newly 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 wireless mesh networks (WMNs), mobile ad hoc networks (MANETs), vehicular ad hoc networks (VANETs), etc.

The common problem is to enable a sender to securely transmit messages to a remote cooperative group. A solution to this problem must meet several constraints. First, the sender is remote and can be dynamic. Second, the transmission may cross various networks including open insecure networks before reaching the intended recipients. Third, the communication from the group members to the sender may be limited. Also, the sender may wish to choose only a subset of the group as the intended recipients. Furthermore, it is hard to resort to a fully trusted third party to secure the communication. In contrast to the above constraints, mitigating features are that the group members are cooperative and the communication among them is local and efficient, and also reduces the computation overhead and the communication costs are independent of the group size. The paper is simple that contains the efficient member deletion/addition and also contains the rekeying concept. This paper exploits these mitigating features to facilitate remote accesscontrol of group-oriented communications without relying on a fully trusted secret key generation center.

II. Related Work

The major security concern in group oriented communications with access control is key management. The existing key management systems used two approaches. One is Group key agreement (or group key exchange by some authors) which 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. And another one is key distribution systems (or the more powerful notion of broadcast encryption). In a key distribution system, a trusted and centralized key server presets and allocates the secret keys to potential users, such that only the privileged users can read the transmitted message. The early key distribution protocol [21] does not support member addition/deletion. Three aspects are important in our contribution. First, we formalize the problem of secure transmission to remote cooperative groups.

III. Contribution

We observe that the 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 online with the group members for multiple rounds of interactions to negotiate a common secret session key before transmitting any secret contents. On the other hand, broadcast encryption enables external senders to broadcast to noncooperative member s 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 member.

This implies that: 1) before a confidential broadcast channel is established, numerous 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 communications and has to be fully trusted by any potential sender and the group members. Second, we propose the new approach is a hybrid of group key agreement and public-key broadcast encryption. In our approach, each group member has a public/ secret key pair. By knowing the public keys of the members, a remote sender can securely broadcast a secret session key to any intended subgroup chosen in an *ad hoc* way and simultaneously, any message can be encrypted to the intended receivers with the session key. Only the selected group members can together decrypt the secret session key and hence the encrypted message.

In this way, the dependence on a fully trusted key server is eliminated. Also, the dynamics of the sender and the group members are coped with because the communication between the sender and the receivers before the transmission of messages is avoided and the communication from the group members to the remote sender is minimized. Third, The new key management paradigm and perform extensive experiments in the context of mobile ad hoc networks. In the proposed protocol, after extraction of the public group encryption key in the first run, the subsequent encryption by the sender and the decryption by each receiver are both of constant complexity, even in the case of member changes or system updates for rekeying. As to security, the proposal is shown secure against an attacker colluding with all the nonintended members. Even such an attacker cannot get any useful information about the messages transmitted by the remote sender. The proof is given under a variant of the standard Decision Diffie–Hellman (DDH) assumption.

IV. PROBLEM STATEMENT AND SYSTEM MODEL

A.ProblemStatement

A group composed of N users, indicated by $\{u_1 \ldots u_N\}$. A sender would like to transmit secret messages to a receiver subset S of the N users, where the size S of is $n \leq N$.

The problem is how to enable the sender to efficiently and securely finish the transmission with the following constraints.

1) It is hard to deploy a key generation authority fully trusted by all users and potential senders in open network settings.
2) The communication from the receivers to the sender is limited, e.g., in the battlefield communication setting.
3) N might be very large and up to millions, for instance, vehicular adhoc networks.
4) Both the sender and the receiver sets are dynamic due to *ad hoc* communication.

According to the application scenarios, there are also some mitigating features that may be exploited for solving the problem.

1) n is usually a small or medium value, e.g., less than 256.
2) The receivers are cooperative and communicated via efficient local (broadcast) channels.
3) A partially trusted authority, e.g., a public key infrastructure, is available to authenticate the receivers (and the senders).

B. System Model

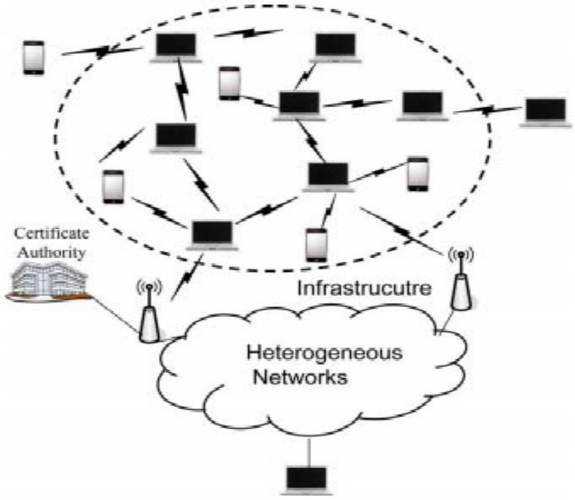

Fig:System model

The potential receivers are linked together with efficient local connections. Using communication infrastructures, they can also join 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 get back 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. We after that officially define the model of group key agreement based broadcast encryption. Since the heart of key management is to securely distribute a session key to the intended receivers, it is sufficient to define the system as a session key encapsulation mechanism. Then, the sender can at the same time encrypt any message under the session key, and only the intended receivers can decrypt.

Key Management

The major security concern in group-oriented communications with access control is key management. The key management paradigm al-lowing secure and efficient transmissions to remote cooperative groups by effectively exploiting the mitigating features and circumventing the constraints. This system is to securely distribute a session key to the intended receivers, it is sufficient to define the system as a session key encapsulation mechanism. Then, the sender can simultaneously encrypt any message under the session key, and only the intended receivers can decrypt.

Member Organization

Organize the nodes in the network. Each and every node should managed by Group Manager. Whenever the nodes want to move from one place to another place, they can easily move with the permission of group manager. Any node want to add in the network or group, the group manager should allow the new node in the group. Doing this process, we can easily manage the network members and avoid unwanted nodes.

Key Updating Process

In this process, whenever happened nodes addition and deletion, the key should rekey in the group and the network.

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.

Key Pre distribution Phase in dynamic key management

In proposed scheme an authentication key is a pair of public/private key and a certificate signed by the base station are pre distributed in each cluster head. The authentication key is used to verify member sensor node identities. Authentication key is known to all cluster heads and the base station. The public/private key pair is used to establish pair wise keys among cluster heads. An authentication key and the public key of the base station are pre distributed in each member sensor node. Public key is used to verify the certificates of the cluster heads. Authentication key can be calculated by the following hash function:

KAuthi = H (IDi||KCHAuth)

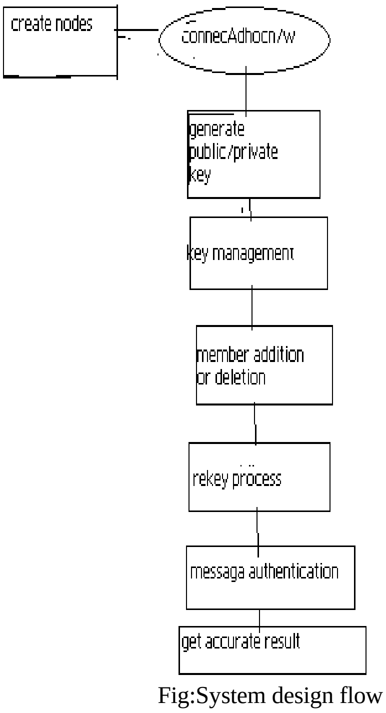

Fig:System design flow diagram

In this process first we create node and then Generate pair wise key .The pair wise key include private and public keys. The cluster head generate key management it will independent on membership addition and deletion of the node. If incase the pair wise key not satisfy the cluster head key generation means the cluster head will intimate to the particular node to perform the rekey strategy. Now the information is authenticated and transfer in secure manner.

V. Conclusion

We have proposed a new key management paradigm to enable send and leave broadcast to remote cooperative groups with out relying on a fully trusted third party. our scheme has been proven secure in the standard model. A thorough complexity analysis and extensive experiments show that our proposal is also efficient in terms of computation over head and communication. these features render our scheme a promising solution to the group oriented communication with access control in various types of adhoc netwotks

References

[1]. L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, “A scalable robust authentication protocol for secure vehicular communications,” IEEE Trans. Veh. Technol., vol. 59, no. 4, pp. 1606–1617, May 2010.

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

[3]. 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.

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

[5]. Q.Wu, J. Domingo-Ferrer, and U. González-Nicolás, “Balanced trustworthiness, safety and privacy in vehicle-to-vehicle communications,” IEEE Trans. Veh. Technol., vol. 59, no. 2, pp. 559–573, Feb. 2010.

[6]. Y. Amir, Y. Kim, C. Nita-Rotaru, J. L. Schultz, J. Stanton, and G. Tsudik, “Secure group communication using robust contributory key agreement,”IEEE Trans. Parallel Distrib. Syst., vol. 15, no. 5, pp. 468–480, May 2004.

[7]. 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.

[8]. Y. Zhang and Y. Fang, “ARSA: An attack-resilient security architecture for multi-hop wireless mesh networks,” IEEE J. Sel. Areas Commun, vol(1). 24, no. 10, pp. 1916–1928, Oct. 2006.