A Robust and Efficient Broadcast Encryption Technique for Secure Communication Under Dynamic Setting in Remote Cooperative Group

Manasa M P[1] **Sharath A H[2]** **Dr Suresh L[3]**

[1] PG Scholar, Department of CSE, Cambridge Institute of Technology, India
[2] PG Scholar, Department of CSE, Cambridge Institute of Technology, India
[3] Principal, Cambridge Institute of Technology, India
[1] manasa.m.p@outlook.com [2] sharathah@outlook.com [3] principal@citech.edu.in

Abstract: The problem of efficiently and securely broadcasting to a remote cooperative group occurs in many newly emerging networks. A major challenge in devising such systems is to overcome the obstacles of the potentially limited communication from the group to the sender, the unavailability of a fully trusted key generation centre, and the dynamics of the sender.

The existing key management system cannot deal with these challenges effectively. By proposing a new key management paradigm these obstacles can be circumvented. The key management paradigm is a hybrid of traditional broadcast encryption and group key agreement. The proposed scheme facilitates simple yet efficient member deletion/addition and flexible rekeying strategies.

Its strong security against collusion, its constant overhead, and its implementation friendliness without relying on a fully trusted authority is a promising solution to many applications.

Keywords – Key Management, Broadcast, Secret Key, Cooperative Groups, Rekey, Cooperative communicating

I. INTRODUCTION

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.

WMNs have been recently suggested as a promising low-cost approach to provide last-mile high-speed Internet access. A typical WMN is a multihop hierarchical wireless network [2]. The top layer consists of high-speed wired Internet entry points. The second layer is made up of stationary mesh routers serving as a multihop backbone to connect to each other and Internet via long-range high-speed wireless techniques. The bottom layer includes a large number of mobile network users. The end-users access the network either by a directwireless link or through a chain of other peer users leading to a nearby mesh router; the router further connects to remote users through the wireless backbone and internet. It supports service-oriented applications [3].

A MANET is a system made up of wireless mobile nodes. These nodes have wireless communication and networking characteristics. MANETs have been proposed to serve as an effective networking system facilitating data exchange between mobile devices even without fixed infrastructures. In MANETs, it is important to support group-oriented applications [4].

A VANET consists of on-board units (OBUs) embedded 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 cooperative groups in their wireless communication range in the roads, and through roadside infrastructures, vehicles can access other networks such as Internet and satellite communication. VANETs are designed with the primary goal of improving traffic safety and the secondary goal of providing value-added services to vehicles [5].

II. 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 as group key agreement and key distribution systems [6]

Group key agreement [7] 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.

In a key distribution system [6], 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 does not support member addition/deletion after the system is deployed. This notion was subsequently evolved to allow the sender to freely choose the intended receiver subset of the initial group, which is usually referred to as broadcast encryption.

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 centre generates all the secret keys and broadcasts messages to users. Hence, only the key generation centre can be the broadcaster or the sender. In the public-key setting, in addition to the secret keys for each user, the trusted centre also generates a public key for all the users so that anyone can play the role of a broadcaster or sender.

III. PROPOSED SYSTEM

The proposed scheme [1] 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 adhoc way and simultaneously; any message can be encrypted to the intended receivers with the session key. Only the selected group members can jointly 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 interaction 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.

IV. SYSTEM MODEL

In this Module (fig 1) create nodes and made ad hoc network. Each and every node has to generate public and secret key and allocate a certificate authority (CA) to provide certificate for public key during data transmission but CA does not have secret key, receiver only have that secrete key. The remote sender can retrieve the receiver's public key for checking 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.

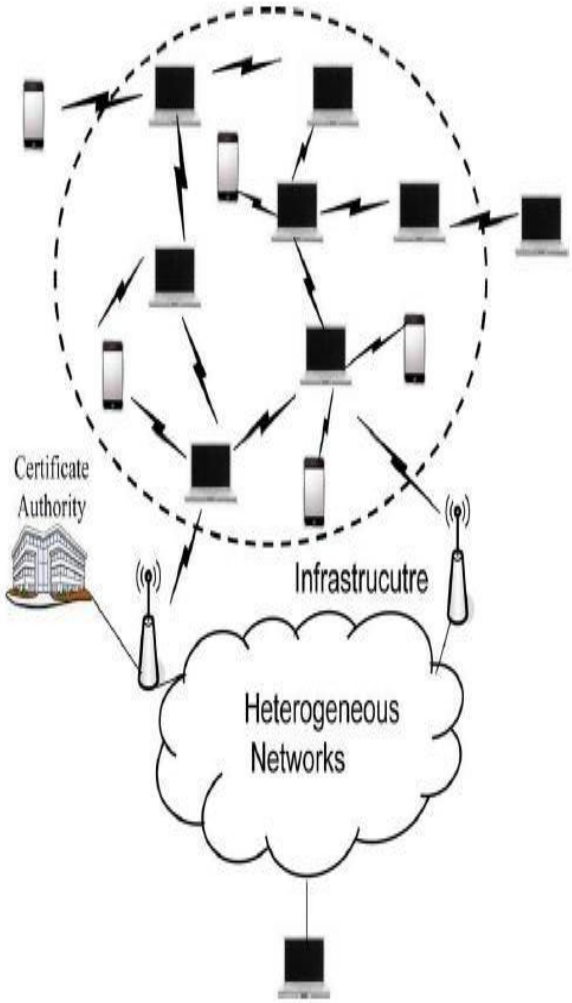

Fig. 1. System Model

Architecture Key Management

The major security concern in group-oriented communications with access control is key management. The key management paradigm allows secure and efficient transmissions to remote cooperative groups by effectively exploiting the mitigating features and circumventing the constraints. This

system securely distributes 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.

The key management system consists of the following Polynomial-time algorithms:

KeyGen (i, n,N): This key generation algorithm is run by each user $U_i \in \{U_1, \ldots, U_N\}$ to generate receiver public/private key pair. A user takes as input the system parameters n, N and receiver index $i \in \{1, \ldots, N\}$, and outputs $<pk_i, sk_i>$ as receiver public/secret key pair. Denote $\{<pk_i, sk_i>$

$|U_i \in S \subseteq \{U_1, \ldots, U_N\}\}$ by $<pk_i, sk_i>_S$ and similarly, $\{<pk_i> |U_i \in S \subseteq \{U_1, \ldots, U_N\}\}$ by $<pk_i>_S$. Here, we implicitly omit the input security parameter λ actually, n,N are polynomials in λ.

We assume that each user's public key is certified by a publicly accessible certificate authority so that any one can retrieve the public keys and verify their authenticity. This is plausible as public key infrastructures have been a standard component in many systems supporting security services. The key generation and the registration to the certificate authority can be done offline before the online message transmission by the sender.

It takes as input a recipient set $S \subseteq \{U_1$

$, \ldots, U_N\}$ and the public key pk_i for $U_i \in S$. If $|S| = n$, it outputs a pair <H dr, k> where Hdr is called the header and k is the message encryption key. (S,H dr) is sent to the receivers. This algorithm incorporates the functionality of the encryption procedure in traditional broadcast encryption systems.

• Decryption $(U_j(sk_j)_S$,H dr, $<pk_i>_S)$: This algorithm is jointly run by the intended receivers to extract the secret session key k hidden in the header. Each receiver U_j privately inputs her secret key sk_j . The common inputs are the header H dr and the public keys of receivers in the recipient set S. If $|S| = n$, each receiver in S outputs the same session key k. This procedure incorporates a traditional group key agreement protocol. It exploits the cooperation of the receivers with efficient local connections.

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. If any node wants 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 the addition and deletion of nodes happen, the key should rekey in the group and the network. Updating the long-term secret key of a member causes more overhead than updating session key or 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 this each member in a group generates the pair of public key and private key. User's public key is certified by a certificate authority so that anyone can retrieve the public keys and verify their authenticity. Any sender who may or may not be in the group encrypts the message and send encrypted message and secrete session key to the intended recipients. Intended recipient decrypts the message.

System Design Flow Diagram

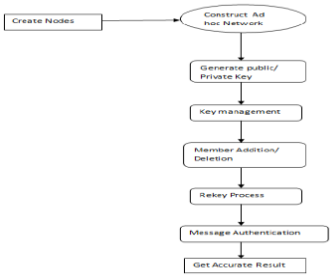

Fig. 2. System Design Flow Diagram

In this (fig 2) 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 in case the pair wise key does not satisfy the cluster head key generation, the cluster head will be intimated to the particular node to perform the rekey strategies. Now the information is authenticated and transfer in secure manner.

V. CONCLUSION

The new key management paradigm enable send-and-leave broadcasts to remote cooperative groups without relying on a fully trusted third party. This scheme has been proven secure in the standard model. These features render this scheme a promising solution for a group oriented communication with access control in various types of ad hoc networks.

REFERENCES

[1] Qianhong Wu, Bo Qin, Lei Zhang, Josep Domingo-Ferrer, Fellow, IEEE, and Jesús A. Manjón, "Fast Transmission to Remote Cooperative Groups: A New Key Paradigm". IEEE/ACM Transaction on Networking Vol.21 No.:2 April 201.

[2] Y. Zhang and Y. Fang, "ARSA: An attack-resilient security architecture for multi-hop wireless mesh networks," IEEE J. Sel. Areas Communication., vol. 24, no. 10, pp. 1916–1928, Oct. 2006.

[3] K. Ren, S. Yu, W. Lou, and Y. Zhang, PEACE: A novel privacy-enhanced yet accountable security framework for metropolitan wireless mesh networks," IEEE Trans. Parallel Distrib. Syst., vol. 21, no. 2, pp. 203–215, Feb. 2010.

[4] 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.

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

[7] 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.