Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 11, November 2015, pg.40 – 47

RESEARCH ARTICLE

FAST AND SECURE TRANSMISSION OF INFORMATION AMONG GROUPS USING A KEY MANAGEMENT SCHEME

R.Kumar, S.Lokesh

Abstract: ***Fast and Secure Transmission of Information among Groups Using a Key Management Scheme (FSTIG) is a technology which allows the information to be transmitted securely and also efficiently among groups by managing the keys used for encryption and decryption. This scheme efficiently overcomes the limitations like limited communication from the group and sender, the unavailability of a fully trusted key generation center, and dynamics of the sender. Also this scheme facilitates the addition and deletion of members from a particular group and accordingly the key will be recalculated. It is the key management scheme in which every user is provided with a public/secret key pair. Whenever a group or cluster is formed, secret key and the public key will be generated for all members of that group. Public keys of all groups will be stored in the certification authority to which every group will have a local connection.***

Whenever a sender of a particular group wants to communicate with other group, the sender will request the public key of the destination group from the certification authority. Then the data to be transmitted will be encrypted with public key of the source group and the encrypted data will be sent along with the public key of the destination group. If a new member joins a group or if a member leaves a group, public keys and secret keys of those particular groups will be recalculated. The proposed method is algorithmically simple but more secure and applicable for real time implementation and application.

Keywords: key management, certification authority.

1. Introduction

In many newly emerging networks, there is a need to broadcast to remote cooperative groups using encrypted transmission. This Group communication is used in networks like wireless mesh networks (WMNs), mobile ad hoc networks (MANETs), and vehicular ad hoc networks (VANETs). Various data such as military data and commercial information are transmitted among groups. Though it provides ease for transmission of data among groups, it brings some problems that we could not be sure that the information we get from senders are trustable or not. The data may be illegally accessed and tampered by unknown users. Therefore, information security has become an important issue in recent years. The keys used for encrypting the contents have to be securely transferred to the receiver. The number of keys increases as the number of users is increased and the key has to be calculated again when the users of group changes in order to ensure security which makes the key management difficult. To deal with the security of the data transmitted, various schemes have been developed. Fast and secure transmission of information among groups using a key management scheme (FSTIG) has been proposed to provide an efficient and secure data transmission among groups by providing a key management which ensures security against collusion and various hacking techniques.

2. Related work

Basic Group key management system is a cryptosystem is based on the management of group keys. In this approach group keys are generated immediately after the clustering of members into groups. These group public keys which are created will be stored in the certification authority and given to the sender of a particular group based on request.

Y.Kim , A.perrig, and G.T.Sudik [3] proposed a tree based scheme for multicast key distribution called Tree based Group Diffie-Hellman(**TGDH)**. In consists of the four basic protocols that form the TGDH protocol suite: join, leave, merge, and partition. The member addition and deletion features provided by this scheme is not efficient .To overcome this a chain based scheme is introduced. It provides an efficient member addition and deletion mechanism which is not provided by Tree based scheme used for group communication. It establishes a chain based mechanism instead of tree based mechanism, in which it provides an efficient member organization, member addition and deletion mechanism. Whenever a member is added to a group or deleted from a group, the chain will be reformulated again and keys are calculated again for those particular groups which will gets updated in the certification authority.

3. Proposed system

Figure.1 represents the system model functioning of the proposed system and the proposed system is mainly organized into 3major modules. In First module, the nodes are created and organized into clusters. In the second module, the keys are generated for the members of each cluster and the file that is to be transferred is encrypted using the key got from the certification authority and it is broadcasted to the destination. The third module consists of decryption and rekeying. Decryption involves decrypting the encrypted data in the destination using the secret key of the concerned group. Rekeying refers to the change of members. If a new member is added to or deleted from a particular group, the keys will be recalculated accordingly to that group.

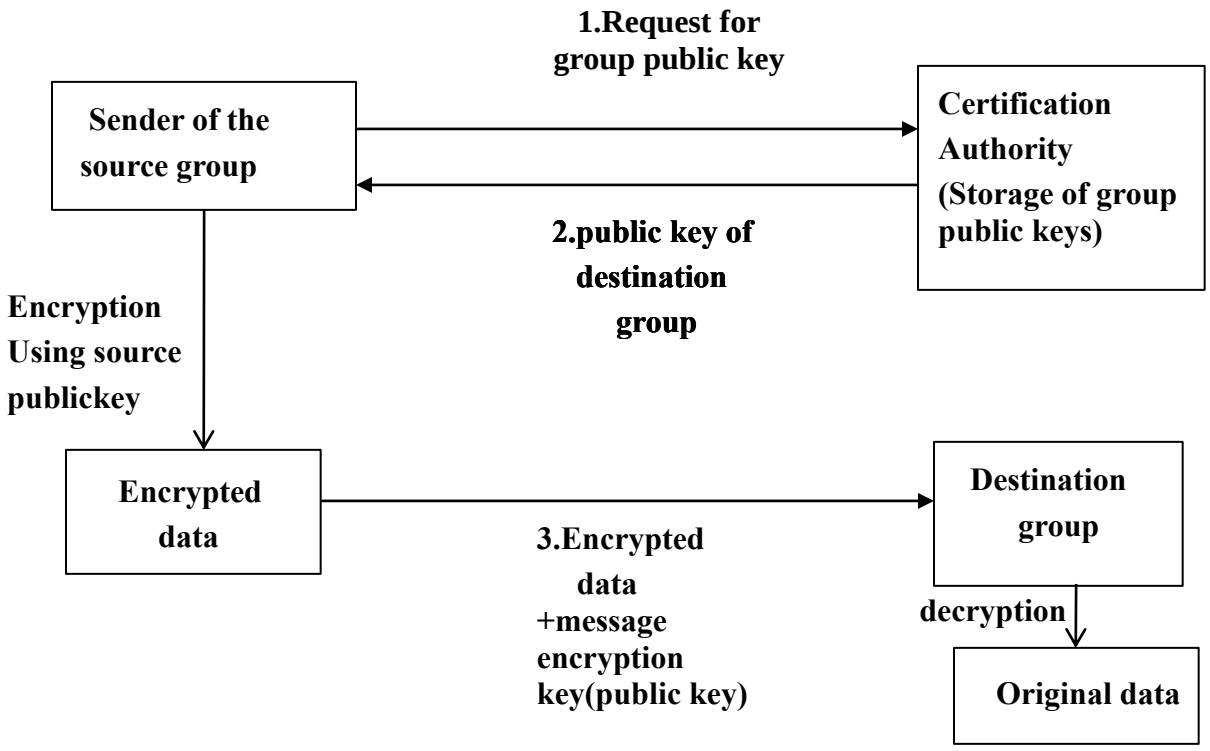

Figure 1: System model functioning

4. Implementation Details

The implementation methodology of Fast and Secure Transmission Of information Among Groups using a key management scheme is done using java, Net beans IDE and MySQL to store its database. Initially nodes are generated and clustered according to the region where they are located. **Figure 2** shows the clustering of the members in the network created. Keys are generated for the clusters generated and stored in

certification authority and given to the members to the members on request. **Table 1** shows the public keys generated for the clusters and **Table 2** shows the secret keys generated for all group members. Keys for group are generated using DIFFIE–HELLMAN ALGORITHM. Then the sender will request the public key of the destination to the certification authority and then encrypts the file to be transferred using the public key of the source group. Encryption and decryption is done using RSA ALGORITHM. **Table 3** shows the key got from certification authority. File transmitted from the source is broadcasted to the destination along with its destination public key. **Figure 3** shows the encryption of the file to be transmitted. **Figure 4** shows the decrypted content of the file encrypted. The file after received by the cluster head is then distributed to the members of the group and which in turn decrypted by them using their secret keys. If a new member is added to a cluster or removed from a cluster, the keys are recalculated again. **Table 4** represents comparison of tree based and chain based scheme.

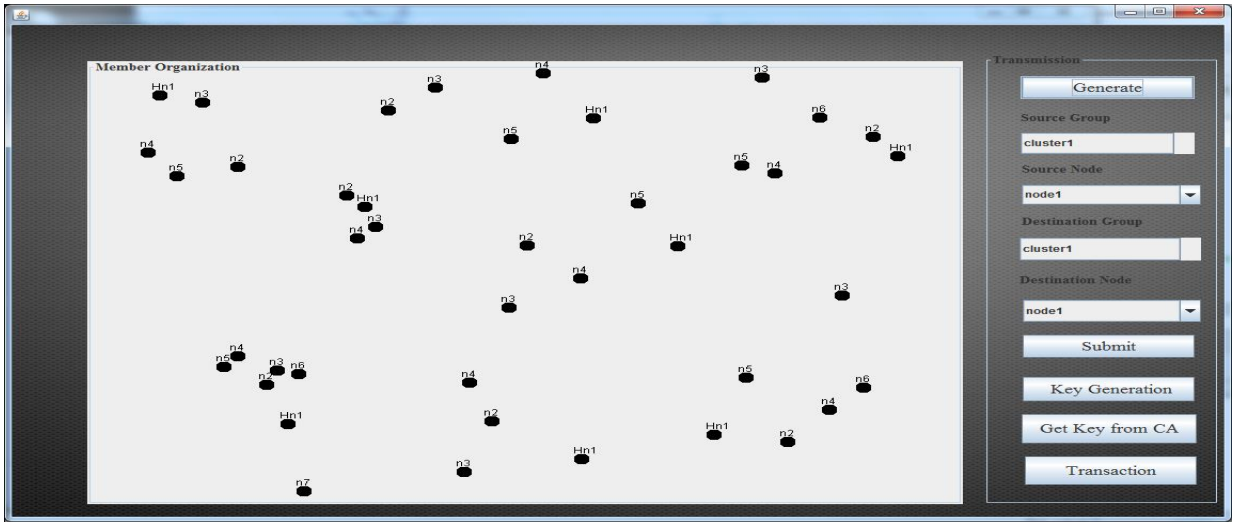

Figure 2. Creation and clustering of nodes in a network

CLUSTER ID	**KEY GENERATED**
CLUSTER 1	173e1bsj
CLUSTER 2	Fffe81c6
CLUSTER 3	17d90f2m
CLUSTER 4	169a2h2e
CLUSTER 5	178db0he

CLUSTER 6	17346jsr
CLUSTER 7	Fffe838e
CLUSTER 8	17fa63gs

Table 1. Public keys generated and stored in CA

MEMBER ID	**SECRET KEY**
1	Fffe9705
2	Fffe8eb4
3	Fffe879d
4	1728jgku
5	Uag886h
6	Fjo2jhh7
7	Jgi9470b

Table 2. Secret keys generated for cluster3

DESTINATION CLUSTER	**KEY FROM CA**
CLUSTER 6	8sj2mb8u

Table 3. Destination public key from CA

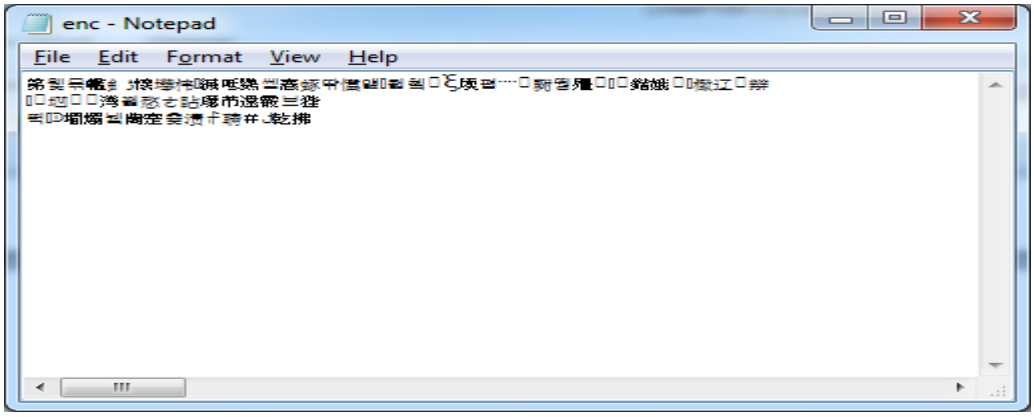

Figure 3. The encrypted file jsr.txt

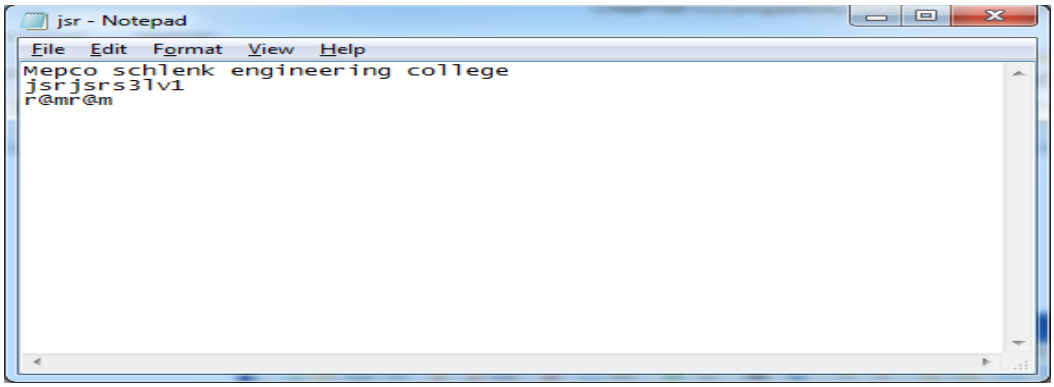

Figure 4. Decrypted content of the file.

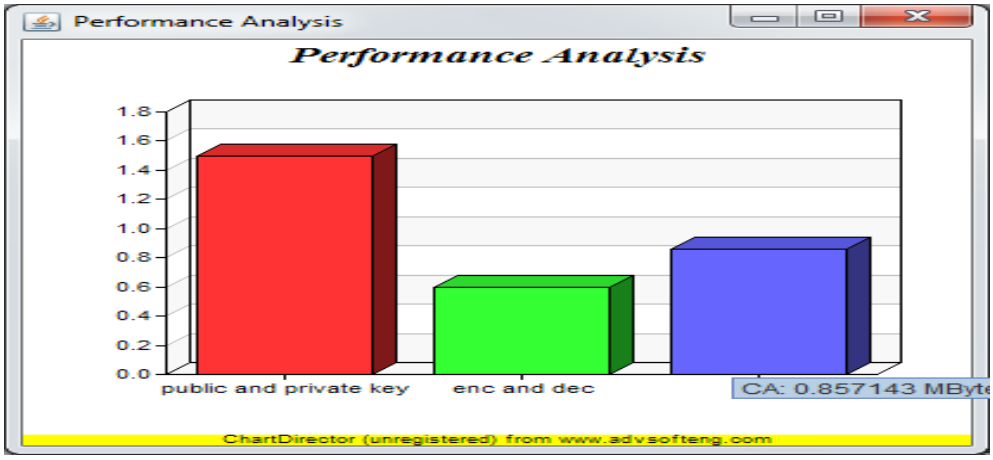

Figure 5 .Performance analysis for the overall processes.

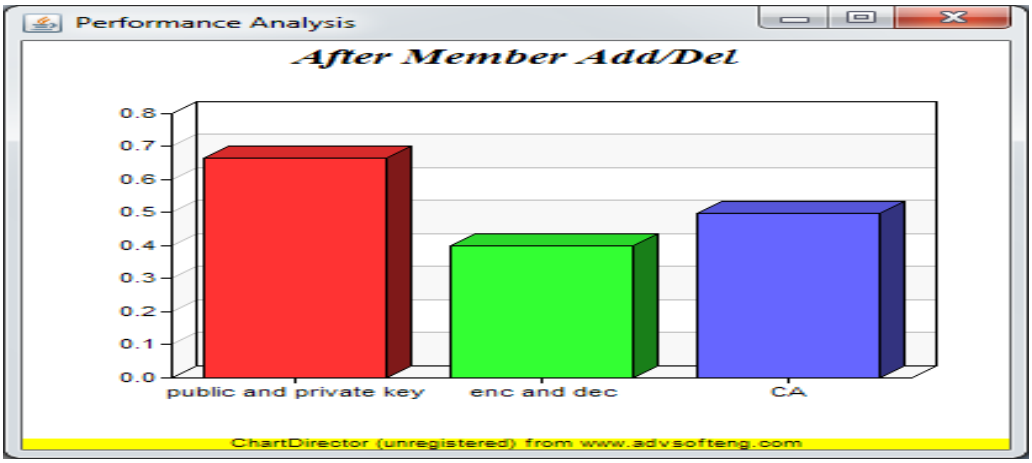

Figure 6. Performance analysis for the overall processes after rekeying

Method used	Time taken for generation of public and private keys(ms)	Time taken for encryption and decryption(ms)	Time taken to get the key from CA(ms)
Tree based scheme	1.5	0.5	0.9
Chain base scheme	0.8	0.4	0.5

Table 4. Comparison of tree based and chain based scheme

5. CONCLUSION

A new technique was proposed where group communication can be established in a fast and secure manner using a key management scheme. The Data can be securely transmitted and are decrypted in an efficient manner. The two schemes Chain based structure for group or cluster formation and rekeying are combined and an efficient key management scheme was proposed where the number of keys used for encryption and Decryption are reduced to a large extend which in turns increases the efficiency of the chain based scheme when compared to tree based scheme. The proposed scheme uses the various algorithms which are more effective and secure in implementation . This can be applicable to real time implementation where limited communication is only possible like battle fields. From the results obtained it is clear that this method is efficient when compared to the normal tree based scheme as it provides additional features for adding and deleting members in a group.

References

1. Qianhong Wu, Member, IEEE, Bo Qin, Lei Zhang, Josep Domingo-Ferrer, Fellow, IEEE, and Jesús A. Manjón, " Fast Transmission to Remote Cooperative Groups:A New Key Management Paradigm," IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 21, NO. 2, APRIL 2013.

2. 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.

3. Y. Kim, A. Perrig, and G. Tsudik, "Tree-based group key agreement,"*Trans. Inf. Syst. Security*, vol. 7, no. 1, pp. 60–96, Feb. 2004.

4. 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.

5. Y.Piao,et al.," Polynomial-base key management for secure intra-group and inter-group communication" ,Computers and Mathematics with application(2012).

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. 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.

8. A. Sherman and D. McGrew, "Key establishment in large dynamic groups using one-way function trees," *IEEE Trans. Softw. Eng.*, vol.29, no. 5, pp. 444–458, May 2003.

9. 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.

