International Journal of Engineering & Technology, 7 (4.6) (2018) 438-443

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Subscription Based Architecture For Secured Group Key Management By Using Linear Equation

Sorabh kumar Mangal[1]*, Mr. k. Navin[2] , Dr. M. Sayeekumar

[1]PG Student, [2,3]Associative Professor
Department of Information Technology SRM Institute of Science & Technology, Kattankulathur, TamilNadu, India
**Corresponding author E-mail: sorabhmangal1@gmail.com@gmail.com*

Abstract

Various applications which are running on to a network require communicating of data onto one or many members. Security is the main focused area in group communication, thereby security of data in the groups is one of the main task for controlling and maintaining access. Unfortunately, IP multicast is not providing any security over the group communication. Therefore it is mandatory to have the group communication with common group key. Group key Management is a fundamental mechanism for secured multicast communication. In group communication it is mandatory for security reasons when the user is joining or evicting the group, the group key has to be change so that the user will unable to receive or fetch information or data, that means user will be unable to receive any new information after leaving the group likewise the new user will not be able to fetch the old information or data. The efficiency of the group key communication depends on the computational cost and communicational cost. The cost should be minimum for both join and eviction of users from the group. The proposed model with subscription algorithm in which divide the group in to subgroups like hybrid model on the basis of years, months, days and hours further divide these subgroups in small subscription time intervals. Linear equation is to be used to calculate these intervals by which predicted request is to be calculated. When the new user will join the group according to their subscription time will get the group and rekeying process will occur. After the subscription period get over the whole time interval of sub-group will be discarded so no rekeying is needed that means eviction cost is reduced to almost Zero (0).

Keywords: *Cost, Group Key Management, Security, Subscription*

1. Introduction

In modernization and increase in technological usage of internet in every growing field (Television, Banking, Medical, Audio and Video etc…) security is major point of concern. Till now the existence of unicast communication has been wide spread but the need for multicast communication is important to provide services for accessing the internet and distributing them to the local market. For a group communication integrity and authentication are the two major security services which has to be taken into account. For the mention issue key Management provides the better solution. To ensure proper security in peer-to-peer communication and multipoint communication a secret key is to be generated and to be shared by the users at the both client and server side. For this encryption to be made successful in broadcast messages common group key concept is been used. This will not reduce the computational cost but also majorly reduce the communicational cost by using subscription based hybrid architecture with Time Interval. For successful establishing the group communication each and every user of the group has been provided with a common group key. In case the user joins or evict the group the key is to be automatically renewed. In the proposed model the main techniques used for successful establishing the group key management are Distributed Group Key Management, Centralized Group Key Management and Decentralized Group Key Management.

Service quality, group member resources and security of the users are the basic needs which has to be fulfilled for an effective group key management model. In hybrid group key management areas following are the terms which commonly comes in to picture. They are

- Key in Dependence
- Forward Secrecy
- Backward Secrecy

The key in dependence means the key should be ideal enough to fit in a particular constraint. The forward secrecy means that the user should not be able to fetch the new information of his old group while Backward Secrecy which means the user who is newly joined should not be able to access the previous data of the group.

2. Related Work

Security plays a very vital role in maintaining the confidentiality of data in group communication. Rekeying of the message brings down the communication cost to Zero [1]. The above mentioned authors proposed architecture using CRT and reverse function is scalable for hefty size dynamically changing group.

The rekeying operation is made possible in multicasting when it is been used in group communication, unfortunately IP multicasting does not provide any security over group communication therefor to have secure multicast group key management is a fundamental mechanism [2].

Key Generation center plays a very vital role for generation and transportation of group key to all the authorized user in very secre-

tive and secured manner. This will ensure forward and backward secrecy
[3]. The above mention researchers used cryptographic techniques to generate the keys which provide efficient computation. Decentralized and batch based group key management is also be wide spread protocol which ensures forward and backward secrecy [7].
Code for key calculation is an effective way to reduce the computational as well as communicational cost [6]. Using multipoint relaying technique in multicast key distribution also increases the efficiency by effective key delivery reducing the energy consumption and key delivery ratio [4].
Using wireless sensor networks shows an efficient group key management with low in storage requirement, computational and communicational cost [5]. Broadcast group key management scheme is another trust effective technique which shares a secret key with the users and follows the subsequent rekeying for entering and eviction of users [8]. Various subgroups are formed under one management protocol by using the subscription based hybrid cluster [9].
The proposed model of the authors provides less computational and communicational overhead during the renewal of keys.

3. Material and Methods

In this research study efforts has been taken to overcome the limitations of contributory and centralized key management by proposing a hybrid architecture subscription based group key management protocol model.

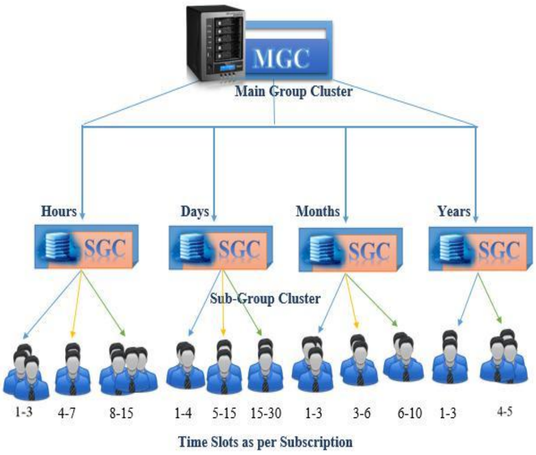


Fig 1: Hybrid Architecture of Group Key Communication

In this model the users are been grouped and sub grouped according to their convenient plans (Years, Months, Days, Hours) available for subscription by a particular firm. Once the user is sorted with his subscribe plan the model will redirect him to the particular group (Years, Months, Days, Hours). Once the user ends with its subscription period the whole group will be discarded by the firm. Dis-cardation of the users from the group will lead to “ZERO leaving cost”, adding this as an advantage to our proposed model. If the user is still interested to continue the service he can re-subscribe the plan easily. Once the user is been re-subscribed to the other plans the system will redirect to the existing group which matches the subscription plan of the user. For example initially the user subscribed for one month plan and at the end of the subscription the user is interested in re-subscription but now for one year plan. So this system will redirect the user to its existing group whose validity is one year, in case of un-availability of existing one year validity group the system will create one year validity group in which the user will be add-on.
Efforts has been taken by us to collect the data of the number of users subscribed in whole decade from the firm. The data collected has been linearized using linear equations. The linearized equations will help us to predict the most used durations of the users. Hence we will be knowing the most liked subscription plans by the users. According to the survey followed by the linearization we will divide groups and subgroups (Eg:- three years, one years, nine months, six months etc…) from this example we get that the most liked subscription plans of the user is three and one year. Henceforth we will create groups of three years and one year not giving much attention to two year. This will result in decreasing computational as well as communicational cost adding this an advantage to our proposed model.

3.1 Time Interval

In this model linear equation is used to calculate the predicted request for the particular year in a particular period of time.

Let PR be the Predicted Requests.

$$PR = mx+c \tag{1}$$

$$m = \{\sum (xy)/\sum(x^2)\} \tag{2}$$

$$c = \sum \{(y)/n\} \tag{3}$$

Where, x = Current year – Median Year

y = Request in the year of Consideration n = Number of Years
Median Year = (n+1 / 2)

3.2 Creation of Initial Group

A subscription based hybrid cluster is generated by forming a group which contains group of users having mutual interest. Subgroups have been formed by master group Controller once it gets the suitable sum of users. The Figure 2 explains the steps in creation of initial group. The user has to contact MGC once want to join the group. Using model of subscription user will be grouped and time interval is been used for slot allocation. Once this is been done subgroups are also been formed based on the subscription type.
The whole data of this subscription is been store it which is been used to calculate the predicted request in a particular year for a particular time of our consideration. Table 1 is maintained by MGC in which it is stored Group ID, Subscription Period and Sub-Group ID so that MGC can find out the groups according to subscription period and Table 2 is maintained by Sub-Groups of Hours here, it is maintained the Sub-group ID, Subscription time intervals, User ID, Initial Subscription time when user join the group and remaining time of the user by which it can calculate the requests and divide the groups in to time intervals.

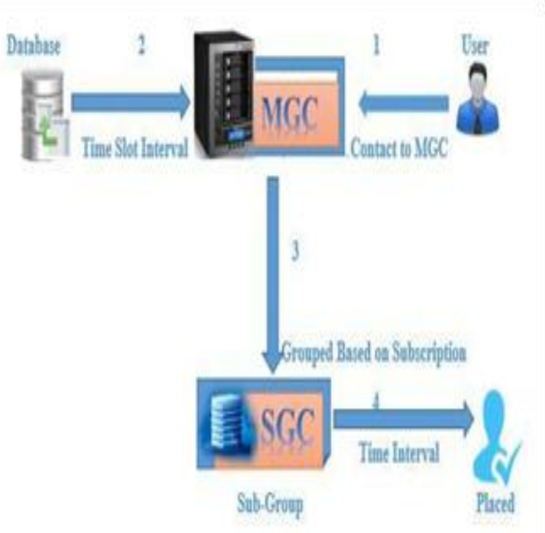
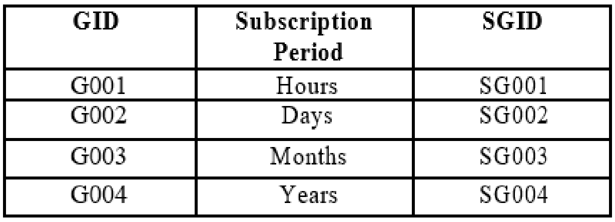


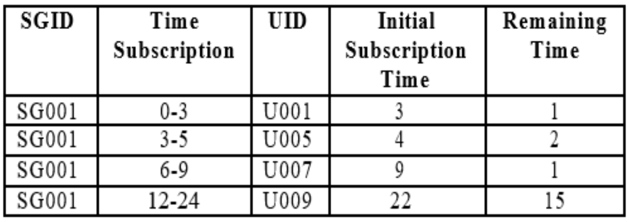
Fig 2: Creation of Initial Group

Table 1: Table Maintained By MGC



GID	Subscription Period	SGID
G001	Hours	SG001
G002	Days	SG002
G003	Months	SG003
G004	Years	SG004

Table 2: Table Maintained By SGC (Hours)



SGID	Time Subscription	UID	Initial Subscription Time	Remaining Time
SG001	0-3	U001	3	1
SG001	3-5	U005	4	2
SG001	6-9	U007	9	1
SG001	12-24	U009	22	15

3.3 User join

The following are the steps involved in user join.

The below figure 3 illustrate the user joining process. The interested user will initially contact MGC and based on subscription type they will be grouped. The data of this will be communicated to SGC. The function of SGC is to verify the subscription table and redirect the user to the particular slot with successful completion rekeying process. In case of unavailability of slots new slots will be created by SGC by calculating the time interval which is predicted using linear equation hence, the user will be redirect to new slots form

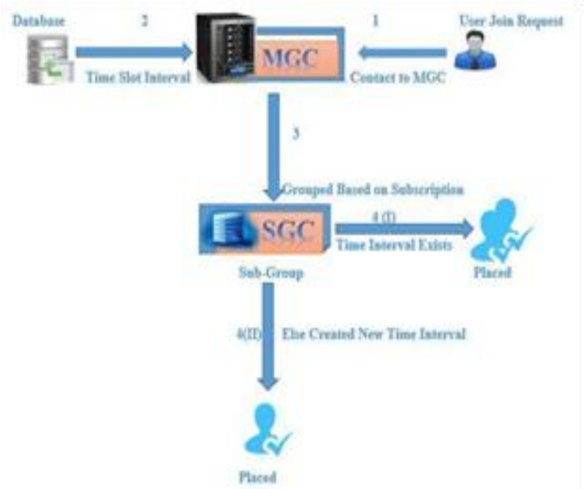


Fig 3: User join Request

3.4 Re-Subscription

Re-subscription is done if the user wants to enjoy the services provided by the firm this is been done by extending the subscription period of the user.

The group where the user has to be redirect will be analyzed by SGC and further process will be done. Figure 4 explains the re-subscription process. Users who wants to re-subscribe and continue with the services will contact SGC. SGC will check the subscription table if the re-subscription period group is available then the user will be redirect to it else new slot is been created and the user will be redirect to the new slot format. In both the case rekeying is done for the particular slot in case of failure in action by SGC, SGC will contact MGC and then after MGC will check and allot the SGC according to the subscription type.

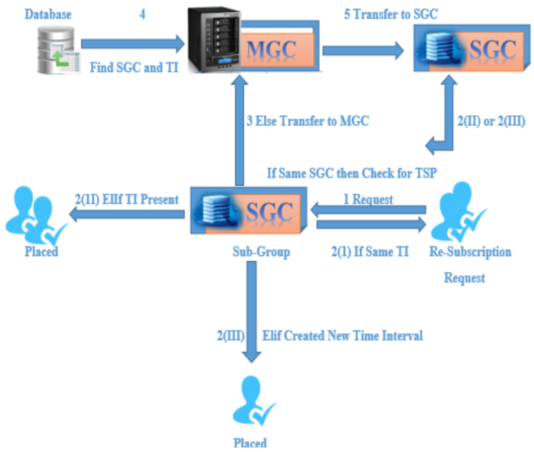


Fig 4: Re-subscription Request

3.5 Eviction of User

Once the user ends with its subscription period the whole group will be discarded by the firm. Dis-cardation of the users from the group will lead to “ZERO leaving cost”, Adding to it discardation does not required any rekeying.

4. Design and Implementation

In this research study Advance java is used for successful execution of Subscription based group key management. Each phase of the work contains of distinguish algorithms. The output of one algorithm is been used as an input to another. The various algorithms and the performance Subscription based group key management are discussed below.

4.1 Algorithm 1: Initial Sub-Group Establishment

TSP() ← MGC
Then calculate Prediction Request (PR)
PR = mx+c
$m = \{\sum(xy)/\sum(x^2)\}$
$c = \sum\{(y)/n\}$

Where, x = Current year – Median Year

y = Request in the year of Consideration n = Number of Years Median Year = (n+1 / 2)

If PR == Hours

Then, Create_SGC(Hours)

Create ST(ID)

Key Generation

Elif PR == Days

Then, Create_SGC(Days)

Create ST(ID)

Key Generation

```
Elif PR == Months
Then, Create_SGC(Months)
Create ST(ID)
Key Generation
Else
Create_SGC(Years)
Create ST(ID)
Key Generation
```

4.2 Algorithm: Creation of Initial Group

```
MGC ← User Join Request
Find Subscription ← Time
TI ← Calculate TI
Create_Slot (TI, Request)
Create_Table (ID)
KeyGeneration()
Update_Key
```

4.3 Algorithm: User Join

```
MGC(Request) ← User Join
Verify (SGC, Request)
SGC(Request) ← Commune(SGC, Request)
If ST_Data == True then
SID_Join ← Request
Update ST
Rekey()
Else
Generate_slot(SID, TI)
Update ST
SID_Join ← Request
Rekey()
End
```

4.4 Algorithm : Re-Subscription

```
SGC ← Re-Subscription(Request)
Verify (SGC, Request)
SGC(Request) ← Commune(SGC, Request)
If Request = RStype then
If check_ST then
If exists then
Create_NewSlot(TI)
Join(Request,NewSlot)
Rekey()Update STElse
Join(Request,slot)
Rekey()
Update ST
End if
Else
MGC ← SGC(RSType,Request)
Check SGC(RStype)
If SGC exists
SGC ← MGC(RSType,Request)
If check_ST then
If exists then
Join(Request, Slot)
Rekey()
Update ST
Else
Create_Newslot(TI)
Join(Request, NewSlot)
Rekey()
Update ST
End if
```

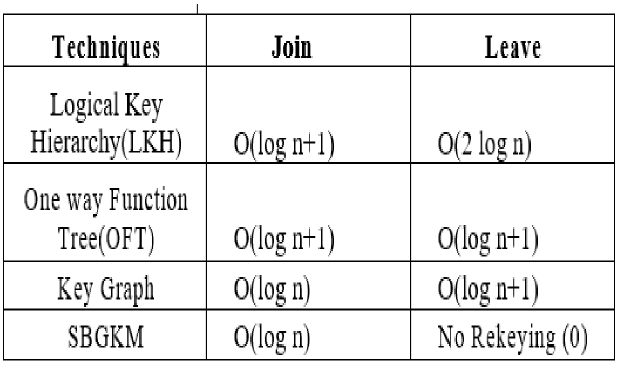
5. Result and Discussion

Subscription based group key management was carried out with Advance java as a front end and Oracle database as a back end. MGC act as a server and SGC as a terminals to its users which runs simultaneously with a common group key. The operations of joining/leaving of the users are successfully achieved and the key is versatile enough in all communications.

5.1 Communication Cost

Various different methods to calculate the communication overhead is analyzed and compared. After analysis found that the proposed model give Zero communication overhead as shown in Table 3. The graph plotted below on the basis of number of users subscribed in previous years and complexity of the algorithms shows the correctness of result.

Table 3: Communication Cost



Techniques	Join	Leave
Logical Key Hierarchy(LKH)	O(log n+1)	O(2 log n)
One way Function Tree(OFT)	O(log n+1)	O(log n+1)
Key Graph	O(log n)	O(log n+1)
SBGKM	O(log n)	No Rekeying (0)

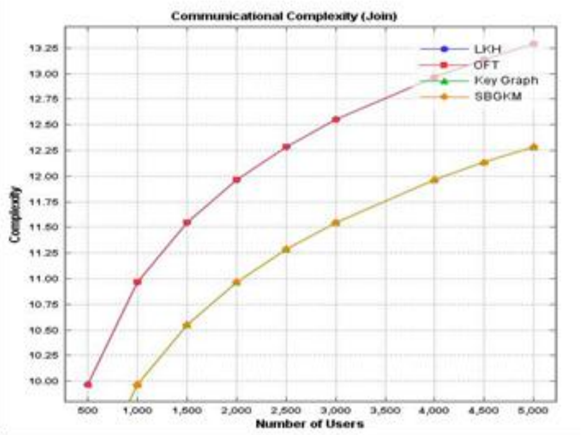


Fig 5: Communicational Complexity (Join)

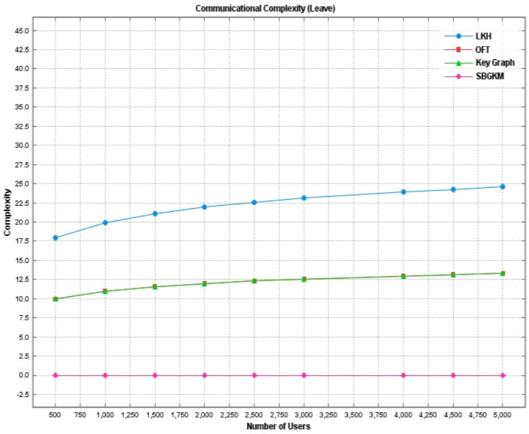
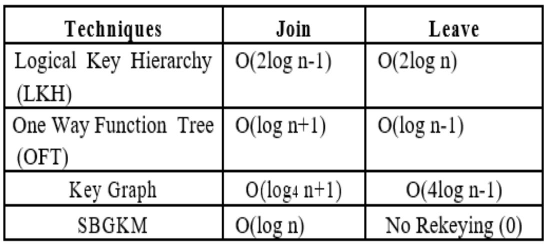


Fig 6: Communicational Complexity (Leave)

5.2 Computational Cost

To ensure high grade of security backward and forward secrecy restoring of group key is needed on every count of users join or leaves the group. After analysis found that proposed model give Zero computational cost as shown in Table 4. The graph plotted below on the basis of number of users subscribed in previous years and complexity of the algorithms shows the correctness of result.

Table 4: Computation Cost



Techniques	Join	Leave
Logical Key Hierarchy (LKH)	O(2log n-1)	O(2log n)
One Way Function Tree (OFT)	O(log n+1)	O(log n-1)
Key Graph	O($\log_4$ n+1)	O(4log n-1)
SBGKM	O(log n)	No Rekeying (0)

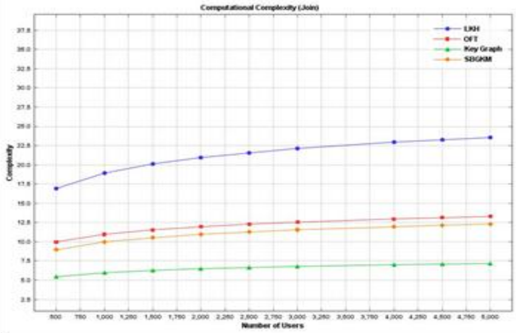


Fig 7: Computational Complexity (Join)

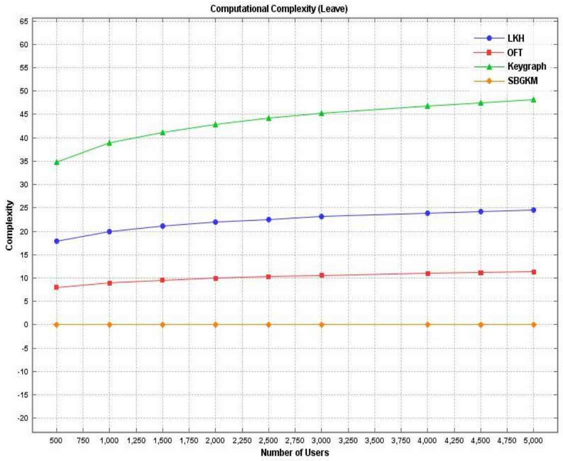


Fig 8: Computational Complexity (Leave)

6. Conclusion

The proposed model gives the better results than all the existing models in terms of less computational key cost and the communicational cost at the time of eviction. In Subscription based group key management model various techniques were used and the performance analysis was carried out. Here as per proposed model to maintain the security and communication over large group in less computational and communicational cost groups was divided in to sub-groups according to their subscribed time interval. To divide these time intervals linear equation is used which predicted the requests. To prove that the communicational overhead reduced to Zero. No need to generate more keys because of hybrid clusters and time intervals. Proposed model act as a perfect model in terms of cost effectiveness creating a secured environment. Adding to this model is adaptable to large group which is the need of now a days fast growing internet services.

References

[1] Sayee Kumar, M. and T. Purusothaman “Hybrid broadcast group management protocol for secure, scalable and efficient group communication” Journal of Computer Science, 11 (2): 344-350, 2015 ISSN: 1549-3636

[2] R. Siva Ranjani, Dr.D.Lalitha Bhaskari, Dr.P.S.Avadhani, “Current Trends in Group Key Management” (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 11, Nov 2011

[3] R. Velumadhava Rao, K Selvamani, R Elakkiya, “A secure key transfer protocol for group Communication” Advanced Computing: An International Journal (ACIJ), Vol.3, No.6, November 2012

[4] Mohamed Salah Bouassida and Isabelle Chrisment and Olivier Festor, “Efficient Group Key Management Protocol in MANETs using the Multipoint Relaying Technique”, Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL’06),2006

[5] Xiao yuan, Yang, Liqin Wang, Qian Zhang, “A new group key management protocol in WSNs based on secret sharing” , 978-1-4244-4813-5/10/ ©2010 IEEE

[6] Melisa Hajyvahabzadeh, Elina Eidkhani, Seyedeh Anahita Mortazavi, Alireza Nemaney Pour, “A New Group Key Management Protocol using Code for Key Calculation: CKC”, 978-1-4244-5943-8/10/ ©2010 IEEE

[7] Mohammed Riyadh Abdmeziem, Djamel Tandjaoui, Imed Romdhani, “A Decentralized Batch-based Group Key Management Protocol for Mobile Internet of Things (DBGK)”, 978-1-5090-0154-5/15 © 2015 IEEE DOI 10.1109/CIT/IUCC/DASC/PICOM.2015.166

[8] M. Sayee Kumar and Dr. T. Purusothaman, “An Effective Subscription Based Hybrid Cluster Architecture using Confidence Interval for Efficient and Scalable Communication”, International

Journal of Applied Engineering Research ISSN 0973-4562 Volume 9, Number 21 (2014) pp. 10689-10702 © Research India Publications,2014.

[9] Aparna S. Pande, Ravindra. C. Thool, “Survey on Logical Key Hierarchy for secure group communication”, IEEE 978-1-5090-2081-2, 16 March 2017.

[10] Wong, C.K., M. Gouda and S.S. Lam, 2000. Secure group communications using key graphs. IEEE/ACM Trans. Network., 8: 16-30. DOI: 10.1109/90.836475

[11] Saroit, I.A. S.F. El-Zoghdy and M. Matar, 2009. A scalable and distributed security protocol for multicast communications. Int. J. Network Secur., 12: 61-74

[12] Rafaeli, S. and D. Hutchison, 2003. A survey of key management for secure group communication. ACM Comput. Survey, 35: 309-329. DOI: 10.1145/937503.937506

[13] Pour, A.N., K. Kumekawa, T. Kato and S. Itoh, 2007. A hierarchical group key management scheme for secure multicast increasing efficiency of key distribution in leave operation. Comput. Networks, 51: 4727-4743. DOI: 10.1016/j.comnet.2007.07.007

[14] Poovendran, M.L.R. and D.A. McGrew, 2004. Minimizing center key storage in hybrid one-way function based group key management with communication constraints. Inform. Proc. Lett., 93: 191-198. DOI: 10.1016/j.ipl.2004.10.012

[15] Lee, F.Y. and S. Shieh, 2004. Scalable and lightweight key distribution for secure group communications. Int. J. Network Manage., 3: 167-176. DOI: 10.1002/nem.515