Journal of Computer Science, 9 (4): 477-487, 2013
ISSN 1549-3636
© 2013 Science Publications
doi:10.3844/jcssp.2013.477.487 Published Online 9 (4) 2013 (http://www.thescipub.com/jcs.toc)

An Enhanced and Cost Effective Group Key Management Scheme for Multicast Network

[1]Saravana Kumar Muthusamy, [2]Purusothaman Thiyagarajan and [1]Lavanya Selvaraj

[1]Department of CSE, Bannari Amman Inst. of Tech, Erode, Tamil Nadu, India
[2]Department of CSE and IT, Government College of Technology, Coimbatore, Tamil Nadu, India

Received 2013-01-05; Revised 2013-04-15; Accepted 2013-05-10

ABSTRACT

Key management plays a vital role in the data communications. The proposed scheme is a key management scheme that provides more efficient and secure methods for key generation and utilization. Enhanced and cost effective key management scheme achieves a secure communication between the members within the group-based network. In this scheme, the group key is generated only once which is static. Hence, it reduces the computation cost at any change in the network like member leave and member join. This papers deals with the analysis of enhanced and cost effective key management scheme with respect to communication overhead, computation cost. The analysis shows that the proposed key management scheme comprises of the most reliable methods for key generations and hence, the data communication. Enhanced and cost effective key management scheme is compared to some of the other key management techniques and proved to be the better choice in this study.

Keywords: RSA, Rekey, Multicast, ECC, Random Number, Key Management

1. INTRODUCTION

Key management plays a vital role in any network. Main dilemma in multicast group communication is its security. To get better security, various keys have to be distributed to the group members. Using those keys the members can encrypt their messages and send secretly. Group key management protocol is required to be scalable, secure and efficient to meet an application need. Many techniques have been proposed and are in use in current networks. This study aims at providing convincing proofs for the scheme Enhanced and Cost Effective Group Key Management Scheme in Multicast Networks, to be the one among the efficient key management and also performs better than some of the existing key management schemes.

In enhanced and cost effective key management scheme, the group key once generated is not changed. Hence, it reduces the computation cost at any change in the network like member leave and member join. The multicast network is designed and updated in such a way that it supports multiple leaves and joins along with scalability of number of members. The scheme performs well even with a static group key with the help of a well-structured procedures to be followed to guarantee an efficient key management and hence the security of the communication.

This study is organized as follows: Section 2 lists some of the existing key management schemes; Section 3 explains the concept of proposed work; Section 4 analyses and gives some comparisons with existing approaches that lists some of the advantages compared to the other approaches and Section 5 draws conclusions.

1.1. Existing Key Management Schemes

Several key management schemes for the multicast networks such as Logical Key Hierarchy (LKH), Hybrid Tree Distributions are listed and explained in (Srinivasan *et al*., 2010). Also they propose a new key management for providing security in dynamic multicast networks that decreases the structure is cluster based and there is a sub-group controller that receives the public keys of the valid users from the group controller.

Corresponding Author: Saravana Kumar Muthusamy, Department of CSE, Bannari Amman Inst. of Tech, Erode, Tamil Nadu, India

A secure multicast key management scheme for cost optimization in case of single sender and multiple receivers is designed in (Li *et al*., 2002). A new algorithm is proposed to optimize with communication constraints. The scheme uses a hybrid tree scheme in which the storage and the update communication are functions of the cluster size.

An elliptic curve cryptosystem-based group (Sakarindr and Ansari, 2007) key management for secure group communications to provide security with a small key size is also presented. The scheme is made more efficient with a cluster structure of the communication network. This scheme well-support a single join and leave events. It explains rekeying processes undertaken in a periodic fashion.

Secure Group Key Management Scheme for Multicast Networks using Number Theory for providing security to a dynamic multicast networks efficiently (Munivel and Lokesh, 2008) makes use of the advantages of the LKH and Chinese Remainder Theorem to provide more effective key management. It also discusses about the security issues in multicast and also few key management techniques and then proposes a new key management scheme.

Scalable and Reliable Cost Effective Key Agreement Protocol for Secure Group Communication (Begum and Purusothaman, 2011) reduces the cost of computational overhead, number of messages needed during the time of key refreshing and the number of keys stored in servers and members.

Computation-and-storage-efficient key tree management protocol for secure multicast communications (Zou *et al*., 2002) manages the key tree structure to maximize the efficiency of the computation and storage costs and to minimize the increment of the communication cost. It uses Level-homogeneous key tree structure.

A survey on key management for multicast is given in (Li and Wu, 2010) which analyzes the problems in key management for multicast and reviews some typical schemes like Simple Key Distribution Center (SKDC), Group Key Management Protocol (GKMP), Scalable Multicast Key Distribution (SMKD), Iolus and Logical Key Hierarchy (LKH).

A survey on group key management is given in (Jiang and Hu, 2008) which introduces the security problems in multicast-oriented communication, centralized group key management protocols and analyzes the decentralization group key management. The protocols include member driven CGKMP like the GKMP protocol, LKH protocol, OFT protocol, Centralized Fat table Key Management (CFKM) protocol and time driven protocol. It explains the join and leave-procedures with respect to the IGKM protocol and time driven protocol.

A hybrid scalable group key management approach for large dynamic multicast networks is proposed in (Srinivasan *et al*., 2006), which tries to generate and distribute keys to the group members during leave or join of members by using key graph based Boolean minimization technique in order to improve scalability. It uses modified Huffman technique to generate UID for users in the group. It uses Petricks approach to deal with multiple leave of users.

Another approach for group key management is given in (Ilango, 2004), which utilizes Huffman and Petrick based approaches. Petricks method is utilized for the better performance in case of multi leaves. This work is proposed in order to overcome the large overhead in key distribution in multicast networks.

A brief detail about the Diffie-Hellman key exchange scheme can be obtained in (Wang and Wu, 2006) which solve the problem of sharing of a key by two communicating parties without an illegal user access to the key.

Efficient Key Agreement for Large and Dynamic Multicast Groups is proposed in (Lakshmanaperumal *et al*., 2010). It details a scalable, efficient, authenticated group key agreement scheme for large and dynamic multicast systems which is identity-based that uses the bilinear map over the elliptic curves. The computations are explained at members join and leave conditions along with some security aspects.

An efficient key management scheme for secure multicast in MANET is presented in (Bouassida *et al*., 2008). It uses hybrid key management scheme and is proved to be secure way of key management.

A survey on Group Key Management in MANETs is provided in (Rasslan *et al*., 2009). It details the specific challenges towards key management protocols for securing multicast communications. It proposes a new key management scheme that is based on a sequential multi-sources model and takes into account both localization and mobility of nodes, while optimizing energy and bandwidth consumptions.

A new secure multicast key distribution protocol using combinatorial Boolean approach is proposed in (Saroit *et al*., 2011). It is based on Key Management using Boolean Function Minimization (KM-BFM) technique. This technique is compared with the other approaches and is proven to be efficient with respect to the communication overhead.

A scalable and distributed security protocol for multicast communications is presented in (Pietro *et al.*, 2004). It is based on the Iolus and the logical key hierarchy protocols. This approach is proven to reduce complexities in member leave and member joins. A key management scheme for high bandwidth secure multicast is presented in (Kapil and Rana, 2009). It concentrates on re-keying algorithms based on the Logical Key Hierarchy (LKH) and also reduces the longest sequence of encryptions and decryptions that need to be done in a re-keying operation.

1.2. Enhanced and Cost Effective Key Management Scheme

The proposed multicast network has time-based cluster structure. Initially Key Generation Center/ Group Controller (KGC/GC) assigns the number of sub-groups (cluster) which is static and their respective subscription span values based on which the members are grouped.

This scheme is a key management scheme proposed to reduce the computation overhead and to support an efficient rekeying at multiple leaves and joins in the multicast network. The KGC/GC (i.e., Key Generation Center/Group Controller) handles the subgroups headed by Sub-Group Controllers (SGCs) each having several communicating members.

It uses Modified Huffman Coding technique for UID generation (**Fig. 1**) which reduces overhead in key management and the number of bits in encryption and decryption.

In this scheme, the group key, GK, is made independent of the Sub-group key, SGK. Consider there are 3 SGCs. The GK is generated using only the partial keys received from the Sub-group Controllers and the SGK (Sub-Group Key) is generated using the partial keys received from the members under respective Sub-group Controller as shown in Equations below. These partial keys are generated only once by all the members. Let there be 8 members under SGC1, then:

$$\mathrm{GK} = \mathrm{f}^{\mathrm{K}}1^{\mathrm{K}}2^{\mathrm{K}}3^{\mathrm{K}}\mathrm{GC}$$

$$\mathrm{SGKl} = \mathrm{f}^{\mathrm{L}}1,1^{\mathrm{L}}2,1^{\mathrm{L}}3,1^{\mathrm{L}}4,1^{\mathrm{L}}5,1^{\mathrm{L}}6,1^{\mathrm{L}}7,1^{\mathrm{L}}8,1^{\mathrm{K}}1$$

The above generated keys are distributed using proactive secret sharing scheme. Next step is to generate the private-public key pair and the signatures for each member. Thus scheme uses RSA concept to construct the public-private key pair where, public key is (M, E), where M is the product of any two large prime numbers, a and b and E is the number prime with respect to M and private key is (a, b, d, φ(M)), where d is the part of private key of KGC/GC and is equal to e^{-1} mod φ(M). RSA is having the application in encryption/decryption, digital signatures and also the key exchanges between communicating members. The signatures are computed using the UID of the member as given in equation below:

$$\mathrm{S}_{\mathrm{i,j}} = \mathrm{UID}_{\mathrm{i}}^{\mathrm{d}}\mathrm{modM}$$

Once all these basic data is available with the members, the communication can be done with the other members in the group. Before communicating, the two members verify each other and then construct a session keys for the communication, satisfying which, the information can be exchanged between them. The Session keys are compared using the following equation:

$$\mathrm{SK}_{\mathrm{i,j}} = \mathrm{SK}_{\mathrm{k,j}} = \alpha^{\mathrm{e*R1*R2}}$$

Enhanced and cost effective key management scheme also makes an efficient usage of the databases established to store the current members and the past members separately along with the timestamps of the subscription spans in order to ensure forward and backward secrecies. It also supports both single and multiple leaves/joins.

When a member's subscription span is completed, the data about this member in the database of KGC/GC is removed and inserted in the leaving member database. The signatures, public-private keys and the group key of the other members remain same. Only the sub-group key is changed.

The new member joined will be given a new UID. The data about new member is stored in the existing members' database at KGC/GC. Then the process of key generation, signature generation and communication is done.

Operations involved in the proposed scheme is summarized in **Fig. 2**.

1.3. Analysis of Enhanced and Cost Effective Key Management Scheme

1.3.1. UID Generation

In comparison to existing user identity generation, it suggests random number generation and fixed length identity but the proposed concept says that , before the UID generation under any Sub-group, the subscriptions spans of all the members willing to join the group initially are to be sorted in increasing order.

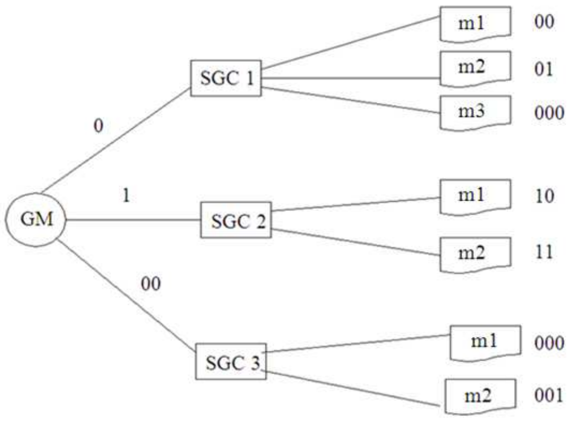

Fig. 1. UID generation

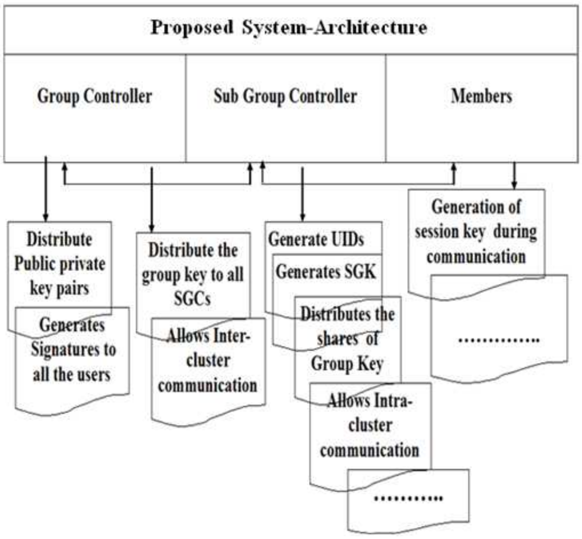
Proposed System-Architecture
Group Controller
Sub Group Controller
Members
Distribute Public private key pairs
Generates Signatures to all the users
Distribute the group key to all SGCs
Allows Inter-cluster communication
Generate UIDs
Generates SGK
Distributes the shares of Group Key
Allows Intra-cluster communication
....
Generation of session key during communication
....

Fig. 2. Overall process of the proposed system

A simple sorting operation requires minimum N number of comparisons and maximum N^2 where 'N' is the number of members. Further, UIDs are generated using Modified Huffman Coding technique. It operates in O(N log N) times. If the subscription spans are already sorted and then this coding technique applied, then it operates in O(N) time where the sorting takes O(N log N) times.

1.4. Sub-Group Key and Group Key Generation

Let the number of Sub-group Controllers (SGCs) under Group Controller (GC) be C and number of members under any SGC be N_i, where, i = 1,2…C. The GC uses the partial keys received from each SGC and also its own partial key to generate GK. Hence it takes O(log C+1) operations for GK generation. In the same way, SGC uses partial keys of its members and also its own to generate SGK. Hence it takes O(log N+1) operations for SGK generation.

1.5. Public-Private Key and Signature Generation

In random number generation, it provides way for adversary attack and not having enough security. In ECC, it provides more security with shorter key size but it is not efficient for larger group size. The proposed scheme uses RSA concept is used for public-private key generation. If K is the number of bits in modulus M then public key operations takes O (K^2) steps and private key operations take O(K^3) steps. It provide much security and also efficient for larger group size.

1.6. Rekeying

Whenever a change occurs in the number of members under a sub-group, it may be because of a member-leave or member-join. The proposed scheme supports multiple join and leaves at the same time ensuring both forward and backward secrecies. The group key once generated, will not be changed even when leaves and joins occur. Only the cluster key will be changed. Further, the *UID*s for the new members along with the public-private key pair and signature will be generated. Further the complexities and the overheads depend on the number of members present in the new sub-group.

1.7. Comparison

The first scheme in comparison to enhanced and cost effective scheme is one-way function trees for key establishment in large dynamic groups. David and Alan in (Rasslan *et al.*, 2009) have proposed a scheme for key establishment in OFTs. There are several points in One-way Function Trees (OFT) compared to which enhanced and cost effective key management scheme performs better.

Enhanced and cost effective key management scheme prefers top-down approach achieving advantages in both storage requirements and the key broadcasts. OFT can be used for both top-down and bottom-up references, where the former is used to reduce storage requirement of information and the latter is used to reduce rekeying broadcasts to about log n keys.

OFT uses binary tree structure and assigns randomly chosen keys for the users. Enhanced and cost effective key management scheme UID tree can accommodate new nodes based on the subscription spans of the new user.

In OFT there is a split in the leaf node of the tree making room for new member along with change in keys of the sharing sibling along with new member. In enhanced and cost effective key management scheme, when a new member joins, only the sub-group key of the other member falling under his group are changed to ensure forward and backward secrecies. All other keys of the existing users remain same.

In OFT, when a member leaves, sibling of the leaving member is reassigned with new parent causing in change of the keys. In enhanced and cost effective key management scheme, when a member leaves, the siblings still remain under same parent and the sub-group controller causing change in only cluster key to ensure forward and backward secrecies.

1.8. When Compared to LKH (Logical Key Hierarchy), the Following Points Can be Noticed

In LKH, the degree of the LKH tree is constant and the number of members under each sub-group is constant. In case of arrival of new members with time span falling under any sub-group and the respective sub-group is full, it causes in the formation of new root node that results in the addition of new sub-group and also the possibility of doubling the number of members. In enhanced and cost effective key management scheme, this is achieved with the constant number of sub-groups. The usage of Modified Huffman Coding technique helps the addition of new members in the same group with the flexibility in the group size.

In LKH, the group key and all the other keys for the members are regenerated at every member leave/join whereas in enhanced and cost effective key management scheme, the group key remains same for any change in number of members and also ensures backward and forward secrecies with the help of databases used. In LKH, each member stores the set of keys that store the path from the root node. Hence key storage is O(log N+1) where N is the sub-group size. In enhanced and cost effective key management scheme a member uses the cluster key and the session key for the communication.

2. RESULTS AND DISCUSSION

2.1. Communication Cost

Whenever a member leaves or joins, there is a change database which is notified to sub-group controller once for each change. Hence, only one message is sufficient for any change in the network. That is, O(1) is the communication cost for enhanced and cost effective key management scheme. **Table 1** presents the communication costs of other approaches compared to enhanced and cost effective key management scheme.

Figure 3 and 4 shows the statistical representation of the above analytical measures.

2.2. Computation Cost

Like all other approaches, there is a rekeying process in enhanced and cost effective key management scheme, except that the group key remains same for any change in the number of members along with ensuring securities necessary.

The rekeying is done only in the sub-group where the change takes place. **Table 2** gives a brief comparison of computation costs for group key generation of OFT, LKH and enhanced and cost effective key management scheme. **Figure 5 and 6** gives the statistical comparisons.

Here, m, is the sub-group size and n is the group size. When a member joins the group, the sub-group key is regenerated along with the UID, Public-privates keys pair and signature. For each newly joining member

Three new keys and one UID is generated. If there are n members joining at the same time, the 4n computations are done.

Whenever a member leaves the group, only the SGK is regenerated. Hence, if n members are leaving the group, n times the SGK is generated. If they leave at the same time, only one SGK is regenerated. If joining and leaving are occurred at the same time, the number of computations done is only 3n+1 where, 1 indicates the SGK generation.

2.3. Number of Rekeying Messages

Whenever a member joins or leaves, the number of computations done is given in Section 5.2. The comparison of number of rekey messages at single join and leave is given in **Table 3**. **Figure 7 and 8** show the statistical analysis.

2.4. Key Store at Leave and Join

In enhanced and cost effective key management scheme, there are databases to maintain the details of both joining and leaving members along with the existing members.

So, considering there are n members which includes both existing and non-existing members, the key storage is given in **Table 4**. **Figure 9 and 10** show the statistical analysis.

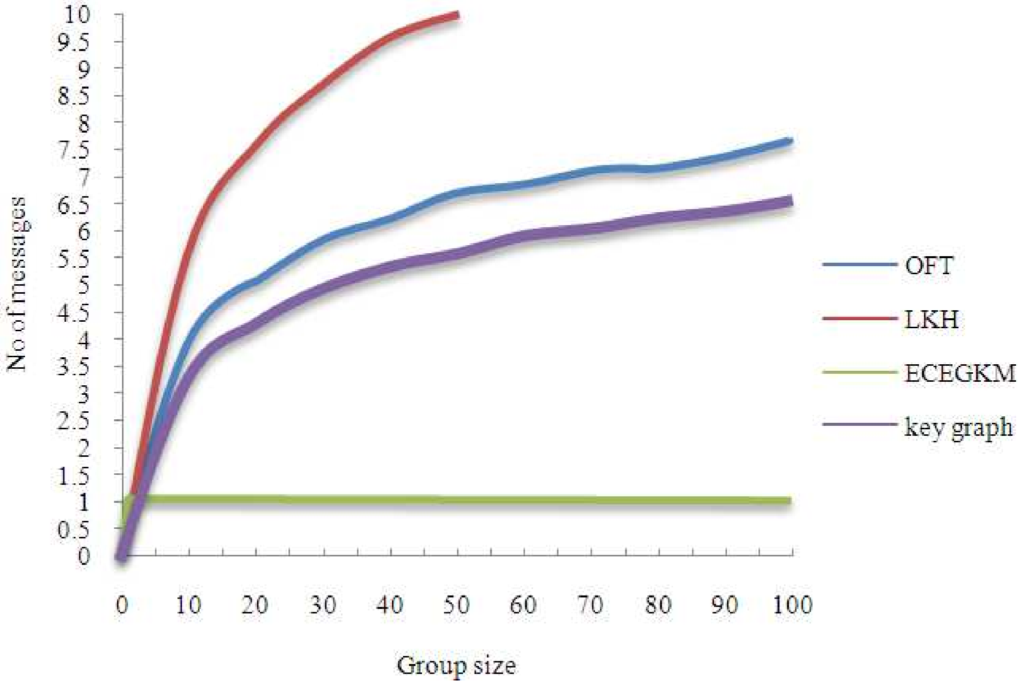

Fig. 3. Communication cost at joins

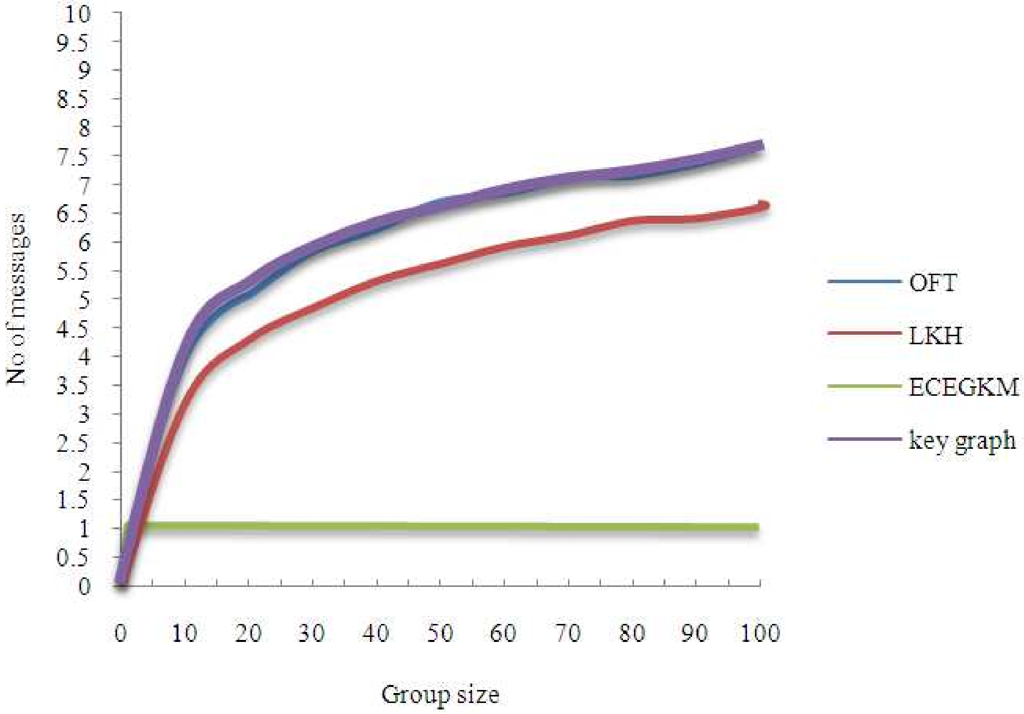

Fig. 4. Communication cost at leaves

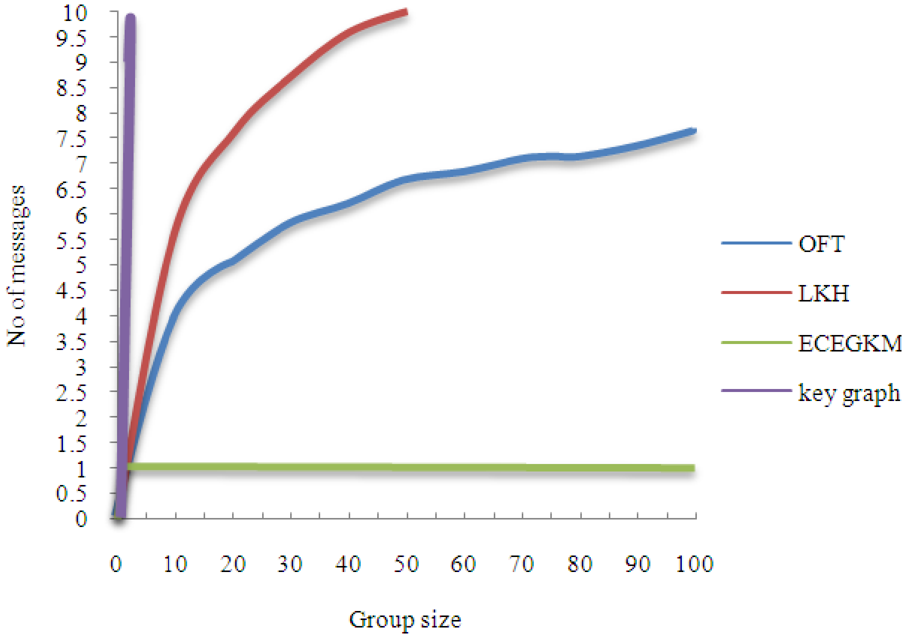

Fig. 5. Computation cost at joins

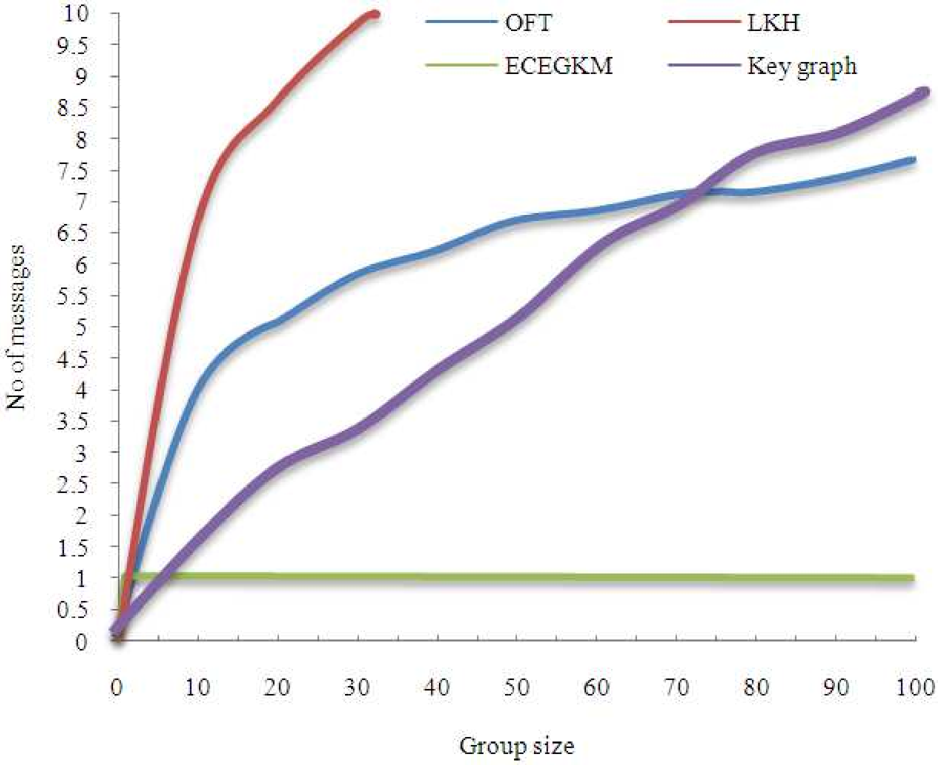

Fig. 6. Computation cost at leaves

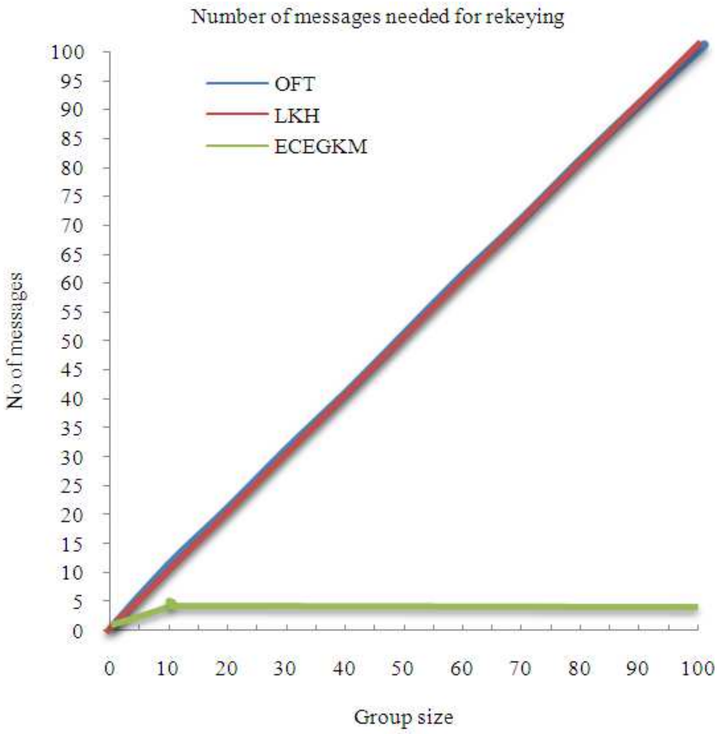

Fig. 7. Rekeying needed at joins

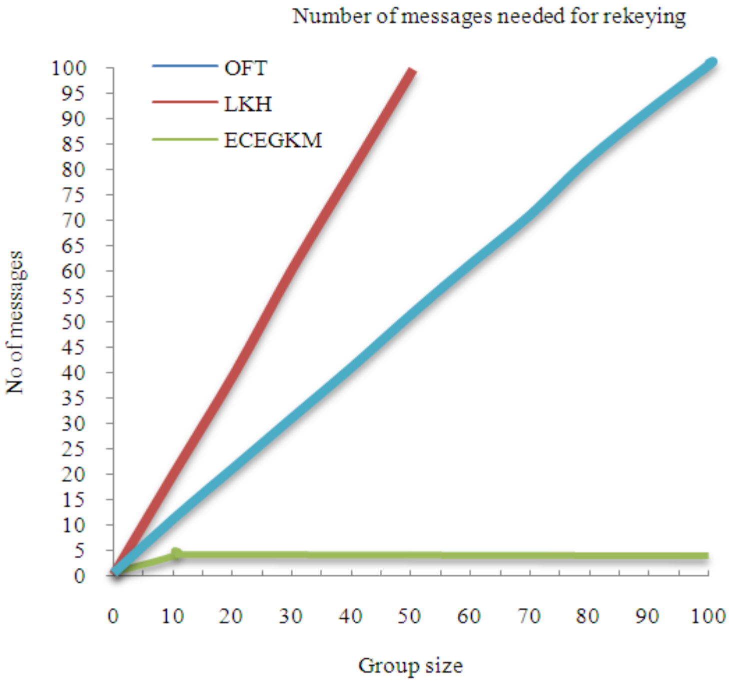

Fig. 8. Rekeying needed at leaves

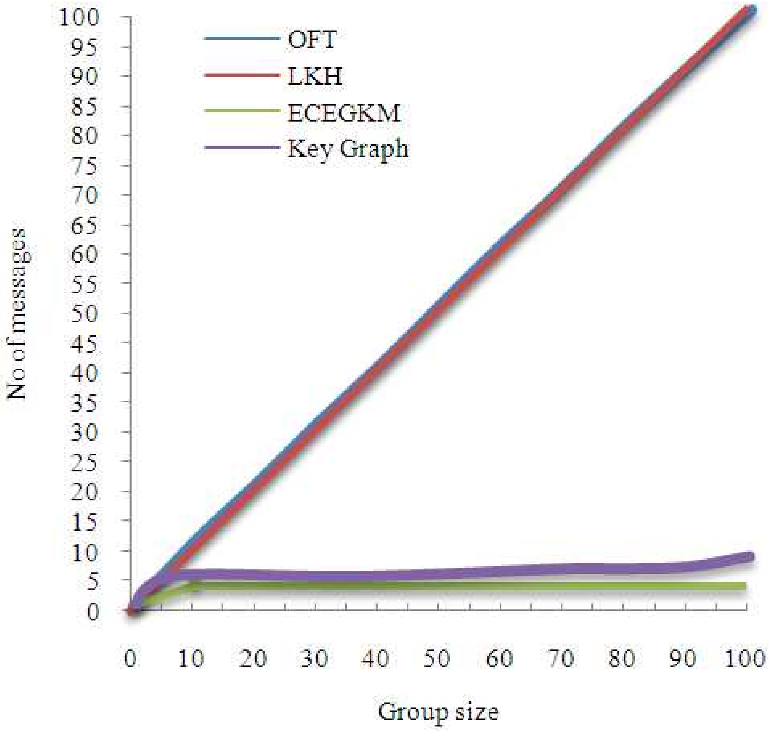

Fig. 9. Key storage at joins

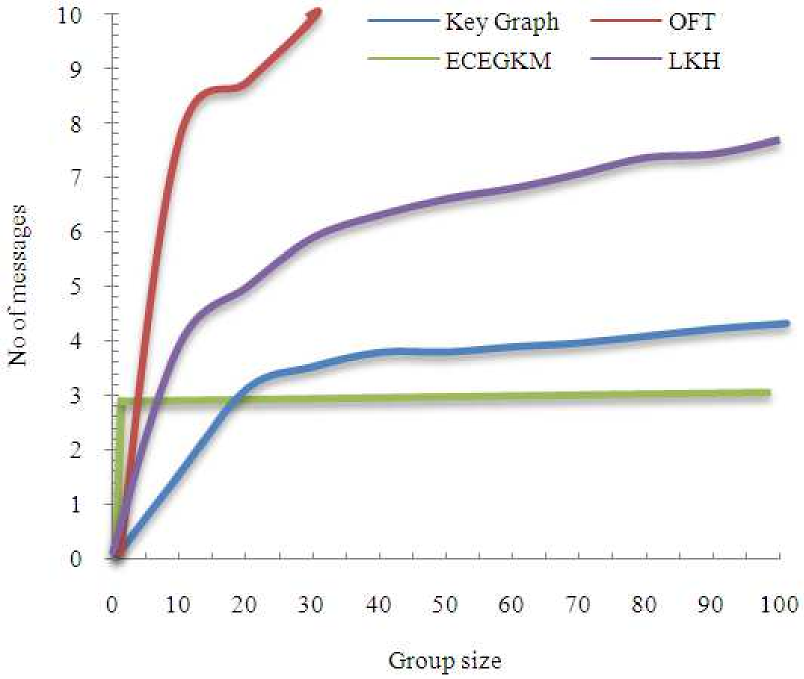

Fig. 10. Key storage at leaves

Table 1. Communication cost

Protocols	Join	Leave
Key graph	$\log_2 n$	$\log_2 n+1$
OFT	$\log_2 n+1$	$\log_2 n+1$
LKH	$2 \log_2 n-1$	$\log_2 n$
Proposed	1	1

Table 2. Computation cost

Protocols	Join	Leave
Key graph	$\log_4 n+1$	$4 \log_4 n-1$
OFT	$\log_2 n+1$	$\log_2 n+1$
LKH	$2 \log_2 n-1$	$2 \log_2 n$
RCEGKM	1	1

Table 3. Number of Rekey Messages Needed

Protocols	Join	Leave
OFT	n+1	n+1
LKH	n+1	2n
RCEGKM	4	1

Table 4. Key storage at join and leave operation

Protocols	Server	Member
Key Graph	[d/d-1] n	$\log_4 n+1$
OFT	2n	$2 \log_2 n+1$
LKH	2n	$\log_2 n+1$
ECEGKM	n+1	3

3. CONCLUSION

Enhanced and cost effective key management scheme is an efficient key management scheme which gains its advantage from a static group key. Also, the rekeying is independent of the number of members in the group and the members as well. From the analysis and comparisons done in this study, it is clear that the enhanced and cost effective key management scheme gives well organized key management for data communications in multicast networks.

4. REFERENCES

Begum, S.J. and T. Purusothaman, 2011. A new scalable and reliable cost effective key agreement protocol for secure group communication. J. Comput. Sci., 7: 328-340. DOI: 10.3844/jcssp.2011.328.340

Bouassida, M.S., I. Chrisment and O. Festor, 2008. Group key management in MANETs. Int. J. Netw. Sec., 6: 67-79.

Ilango, S., 2004. Group key management utilizing Huffman and Petrick based approaches. Proceedings of the International Conference on Information Technology: Coding and Computing, IEEE Xplore Press, pp: 362-366. DOI: 10.1109/ITCC.2004.1286664

Jiang, B. and X. Hu, 2008. A survey of group key management. Proceedings of the International Conference on Computer Science and Software Engineering, Dec. 12-14, IEEE Xplore Press, Wuhan, Hubei, pp: 994-1002. DOI: 10.1109/CSSE.2008.1282

Kapil, A. and S. Rana, 2009. Identity-based key management in MANETs using public key cryptography. Int. J. Sec., 3: 1-8.

Lakshmanaperumal, J., K. Thanushkodi, N.M.S. Kumar, K. Saravanan and D. Vigneshwaran *et al*., 2010. Efficient key management scheme for secure multicast in MANET. Int. J. Comput. Sci. Netw. Sec., 10: 157-164.

Li, M., R. Poovendran and C. Berenstein, 2002. Design of secure multicast key management schemes with communication budget constraint. IEEE Commun. Lett., 6: 108-110. DOI: 10.1109/4234.991148

Li, S.Q. and Y. Wu, 2010. A survey on key management for multicast. Proceedings of the 2nd International Conference on Information Technology and Computer Science, Jul. 24-25, IEEE Xplore Press, Kiev, pp: 309-312. DOI: 10.1109/ITCS.2010.82

Munivel, E. and J. Lokesh, 2008. Design of secure group key management scheme for multicast networks using number theory. Proceedings of the International Conference on Computational Intelligence for Modelling Control and Automation, Dec. 10-12, IEEE Xplore Press, Vienna, pp: 124-129. DOI: 10.1109/CIMCA.2008.29

Pietro, R.D., L.V. Mancini and A. Mei, 2004. Key management for high bandwidth secure multicast. J. Comput. Sec., 12: 693-709.

Rasslan, M.M.N., Y.H. Dakroury and H.K. Aslan, 2009. A new secure multicast key distribution protocol using combinatorial boolean approach. Int. J. Netw. Sec., 8: 75-89.

Sakarindr, P. and N. Ansari, 2007. Elliptic curve cryptosystem-based group key management for secure group communications. Proceedings of the IEEE Military Communications Conference, Oct. 29-31, IEEE Xplore Press, Orlando, FL, USA., pp: 1-6. DOI: 10.1109/MILCOM.2007.4455002

Saroit, I.A., S.F. El-Zoghdy and M. Matar, 2011. A scalable and distributed security protocol for multicast communications. Int. J. Netw. Sec., 12: 61-74.

Srinivasan, R., V. Vaidehi, R. Rajaraman, S. Kanagaraj and R.C. Kalimuthu, 2010. Secure group key management scheme for multicast networks. Int. J. Netw. Sec., 11: 33-38.

Srinivasan, T., S. Sathish, R.V. Kumar and M.V.B. Vijayender, 2006. A hybrid scalable group key management approach for large dynamic multicast networks. Proceeding of the 6th IEEE International Conference on Computer and Information Technology, Sep. 20-22, IEEE Xplore Press, Seoul, pp: 102-102. DOI: 10.1109/CIT.2006.9

Wang, L. and C.K. Wu, 2006. Efficient key agreement for large and dynamic multicast groups. Int. J. Netw. Sec., 3: 8-17.

Zou, X., B. Ramamurthy and S. Magliveras, 2002. Efficient key management for secure group communications with bursty behavior. University of Nebraska-Lincoln.