International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 11 (2018) pp. 9034-9041

A New Secure and Computational Efficient Multicast Key Distribution for Wireless Networks

***B. Srinivasa Rao[1] and P.Premchand [2]**

[1]Department of Computer Science and Engineering, Gokaraju Rangaraju Institute of Engineering and Technology (Affiliated to Jawaharlal Nehru Technological University Hyderabad), Bachupally, Hyderabad-500090, Telangana, India.

[2]Department of Computer Science Engineering, University College of Engineering, Osmania University, Hyderabad-500007, Telangana, India.

[1]Orcid: 0000-0001-8845-4303

Abstract:
In the present research work a simulation mechanism has been designed and implemented for a secure, computation efficient and dynamic multicast key distribution system that can be applicable to wireless networks. The present mechanism uses the concept of Maximum Distance Separable (MDS) codes to enhance the computation efficiency of the multicast key distribution system. Also an attempt has been made to improve the security of the multicast key distribution system against the previous multicast group members that had turned into adversaries. By encrypting the newly generated keys with the older one may provide improved security to the system against these adversaries. The DES algorithm has been used for encryption of the new session keys. The implemented results have presented and discussed.

Keywords: multicast key distribution, security, session keys, computational efficiency, wireless network, key security, dynamical distribution

INTRODUCTION

It is well understood that the multicast key distribution system plays a significant role in providing security and computation efficiency in various wireless network applications. In multicast key distribution system the security issue is attended by some key distribution systems using dynamic or time variant session keys. At the same time the efficiency of the communication system is decided by network features like low computation complexity, communication cost, storage cost etc. The balance between these two mechanisms yields a secure and efficient multicast key distribution system. One of the multicast key distribution methods is the distributed key management system in which the security design is based on either a cryptographic or non-cryptographic approaches. Over a time period several secure and efficient multicast models have been developed and implemented using any one of these two approaches. In this section, a brief review over the progress and development of multicast key distribution models has been presented. It can be seen that the recent research in this direction has paid much attention to cryptographic approaches [1-10] in comparison with non-cryptographic methods. This is may be due to the possibility of achieving ambient computation efficient features in their respective models by using different cryptographic tools conveniently. Dutta et al [1] proposed a key distribution model that recovers a session key that might have been lost during broadcast communication in WSN. For achieving less power consumption in networks a cluster based key distribution mechanism was proposed by Suganyadevi etal [2]. A time-invariant key structure model was introduced by Zhow [3] that manifests low computational complexity at server level. The SGCMKDS model reported by Palanisami and Annadurai [4] was designed for confidentiality and integrity using group key security. A highly secured model was designed for key distribution mechanism to provide key authentication and filter the malicious adversaries by Vijaykumar et al [5]. Elliptic curve cryptography based multicast key distribution mechanisms have been reported to provide reduced computational and communication complexity and improved security [6, 7]. A standard protocol was designed incorporating cryptographic methods for an efficient key management and distribution mechanism by Hanatani et al [8]. Recently dynamically variant cluster concept has been incorporated in to multicast key distribution model to solve the 'one affects many' problem in wireless network systems [9]. In order to overcome the intruder problem in the wireless networks Zhu [10] has presented a new protocol that adopts private key system and cryptographic random number generation. Many other models in this direction can be referred to the vast literature. On the other hand scant attention has been paid on non-cryptographic approaches. The necessity of development of diversified approaches and difficulty of achieving justified efficiency may be reasons for scant attention on non-cryptographic approaches. However, a computational efficient multicast key distribution scheme with reduced computational complexity was proposed implementing MDS codes by Xu et al [11]. Some other models have been reported considering MDS codes for secure and multicast key distribution [12, 13]. Recently, mobility based key distribution mechanism has been developed for providing security in mobile and adhoc networks [14]. A comparative study of the above discussed models indicates that in either of the above discussed approaches, it may be difficult to have a standard and sophisticated model for secure and computational efficient multicast key distribution with out any compromise [15-17]. This may be due to various inherent weaknesses and vulnerabilities of the wireless network systems. Further continuous improvement of these models to achieve high level

security and efficiency may be a possible solution. Hence, in the present research work, an improved secure and computation efficient multicast key distribution system using MDS codes has been proposed and implemented. But some of these models may have a security threat from former group members who could become adversaries. In the present model the security is improved by encrypting new session keys using the older one. As it would be difficult for a group member to have access to the group after leaving the group, the adverse group members cannot obtain the old keys [5]. Thus encryption of new keys with previous keys enhances security of the system further. In this paper, the existing multicast key distribution mechanism has been discussed in section-2. In section-3 the improved secure multicast key distribution system has been described. The detailed simulation mechanism of the present model has been described in section-4. The implementation part is presented in section-5. Finally the results have been discussed and concluded in section-6.

COMPUTATION EFFICIENT MULTICAST KEY DISTRIBUTION SYSTEM (CEMKDS)

Xu and Huang [11] proposed a Computing-Efficient Multicast Key Distribution scheme for wireless sensor networks to provide reduced computational complexity. The model used Maximum Distance Separable (MDS) codes to achieve the security and reduced computational complexity [11]. The complete details of the model and its implementation are available in ref. [11]. Here the mechanism of the model is briefly discussed. The interesting and complex feature of the multicast key distribution is the change of the session keys of the key distribution system dynamically due to frequent time variant inclusion and exclusion of group members of the system [11]. In the multicast groups it is essential to provide the keys only to authorised users through central system designated as Group Controller (GC) [11]. The GC requires communication storage and computation resources to provide session keys to the group members [11, 16, and 18]. While joining or leaving the group by a multicast group member, the GC selects a fresh value to compute the new session keys and old one are discarded [11]. But it is also essential to consider a security threat from members who leave the group and becomes adversaries later [5].

PRESENT SECURE AND COMPUTING EFFICIENT MULTICAST KEY DISTRIBUTION (SCEMKD) SYSTEM

The present secure and computation-efficient multicast key distribution system has been designed based upon the CEMKDS proposed by Xu and Huang [11] by enhancing the security of the system by considering the case of a former group member becomes a potential adversary [5]. The present model is designed in four modules as: 1. Group Controller. 2. Client. 3. Key_ generation. 4. Re-keying; [7, 13]. 1. Group Controller: It is a server that provides keys for chat members for secured chatting and communication. 2. Client: A new member authorized by the GC intended to join the chatting group. 3. Group Key Generation: It generates keys and supplies to the group/chat members to communicate information in secured manner .4.Re-keying: Generation of new keys to replace the old keys when member joins or leaves a chat group [7, 11, and 13]. During the rekeying process the security of the system can be further improved by considering the case of a former group member may become a potential adversary [5]. The newly generated keys may be encrypted by using old session key and any symmetric algorithm and communicated to the group members securely. It is very difficult to the adversary to recover the old key after leaving the group [5]. Thus the present model has an improved security. The simulation mechanism of presently proposed model is detailed in the next section.

SIMULATION DESIGN

The present section describes the design and development of the simulation mechanism intended for implementation of the secure and computation efficient multicast key distribution system. The simulation mechanism is designed in the framework of database design model to describe all the required logical and behavioural features of the multicast key distribution system effectively. As mentioned earlier, the important components of the computation efficient multicast key distribution are: group controller, client, group key generation and re-keying [7, 11, and 13]. The functionality of these components is discussed elsewhere [7, 11, and 13]. The overall architecture of the SCEMKD system can be visualized as shown in fig.1. Initially, the functional mechanisms of the individual component are designed. Later these mechanisms are combined into an overall single unit. In this process the database model concepts are used to design the mechanisms at different contexts.

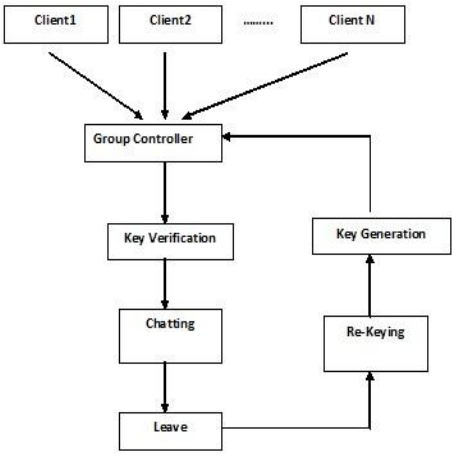


Figure.1. Architecture of the Computing- Efficient Multicast Key Distribution Design

The behavioural diagrams of the client and group controller are shown in fig.2. The client is authorized to login to have secure communication with fellow group mates by getting the

session key and secret key from the group controller during registration.

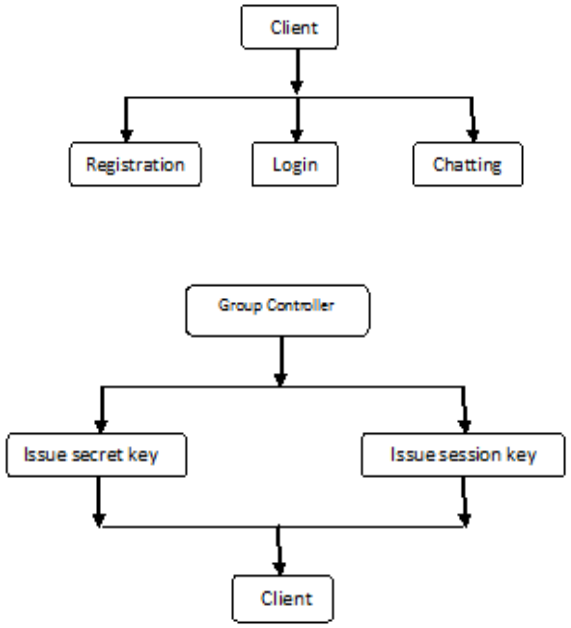


Figure.2. Behavioural diagrams of the client and group controller.

The roles, functionality, behaviour of individual objects and the overall operation of the system in real time are shown the collaboration diagram as shown fig 3.

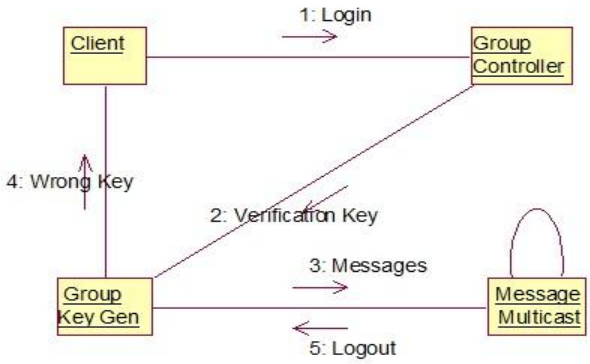


Figure.3. Design of Simulation Technique for Computing-Efficient Multicast Key Distribution

As mentioned earlier, the client logins with secret and session key to the group controller to communicate with a group in the system. The group controller verifies the existence of the particular multicast group in the database and forwards the request to group key generation module for activation of chat module. The client logins with a secret key and session key which is sent as a request to the group controller. The group controller (GC) checks the database thoroughly which consists of multi-cast group table, session key table and user details table. The multi groups table consists of different kinds of groups involved in an organization like the administrator, programmer, tester and others along with their session keys which are generated by the group controller. The session table consists of the registered user's names or member name, their group name and the session keys that they possess. The user detail's table consists of users name, their secret key and the password they use for login. The group controller checks all these tables thoroughly and then the client is allocated to the chat room. The relations and source code dependencies can be depicted by class diagrams for both client and server model as shown in fig.4 and fig.5. The client class diagram consists of four classes namely a login class, verification class, key verify class and SGSclient class. Each class consists of three fields namely name of the class; the fields present in that class; and the methods associated with them. The above classes posses a direct association relationship between each other since each class is dependent on other class for functioning. The client has to login using username and password which is then verified in the verification class. Hence, the secret key and session key which are entered are verified in the key verification class. If all the verifications are true then the client enters the chat room and can communicate with the server belonging to the same group.

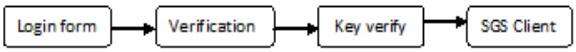


Figure.4. Client model class diagram

The server class diagram as shown in fig. 5 consists of three classes namely Select Group class, session key class, and SGSserver class. The server is initialized by selecting a group. In the next step the session key of that particular group acquired from the database. In this model the session key is generated by group key generation module. Then a form opens which is called as the Server form. All the information from the client who have joined the chat room or left the chat room will be stored in the server along with the communication that takes place.

Figure.5. Server model class diagram

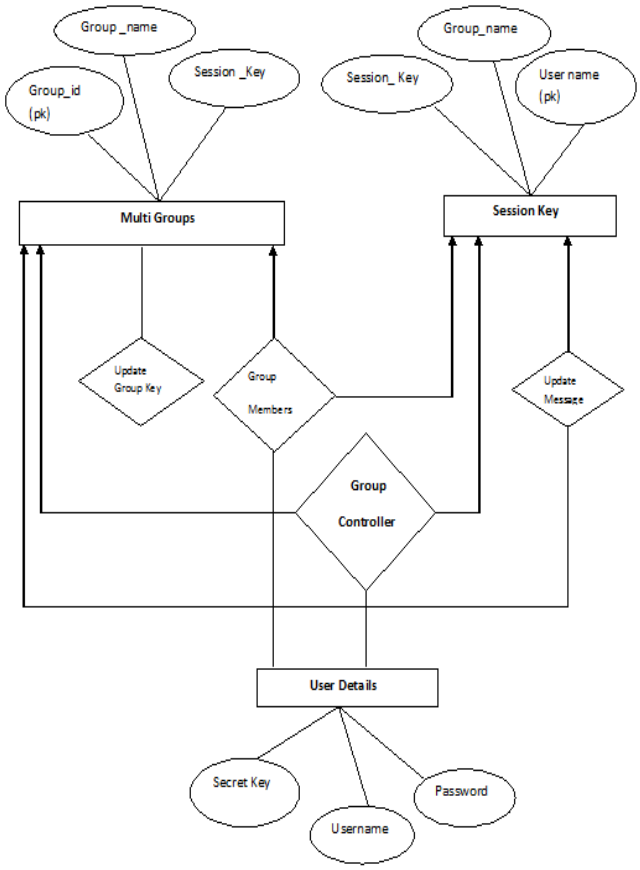


Figure.6. Entity Relationship diagram for overall simulation mechanism

The entity–relationship diagram (in fig.6) describes three entities which represent the tables that exist in the present database. They are Multi Groups, Session Key and User Details. The multi groups table consists of different kinds of groups involved in an organization like the administrator, programmer, tester and others along with their session keys which are generated by the group controller. It also consists of a group ID. The session table consists of the registered user's names or member name, their group name and the session keys that they possess. The user detail's table consists of users name, their secret key and the password they use for login. The group controller is in one-to-many relationships between with each and every table in the database. The multi groups table relates with the session key during the rekeying process. The user details table makes track of the members that have registered i.e. new and old members. Session table is also related to the user members and it also updates messages.

IMPLEMENTATION OF THE PRESENT MODEL

The implementation phase comprises of several activities. 1. The required hardware/ software acquisition is carried out. 2. The required software (code) is developed, verified and tested. For encryption of the new keys with old keys DES algorithm is used. 3. The tested system is used for simulation of the present SCEMKD system. The required code is developed for the scheme in C#.NET using Mrosoft.NET Technologies, Microsoft-SQL-Server-2005, Microsoft-Visual-Studio-2008, and MS_ Windows_XP. The Hardware Requirements are Intel Pentium, RAM: 512 MB (*Minimum*), Hard disk: 40 GB. The deployment of the resources for implementation of the presently designed simulation mechanism is in the following steps. Step1: Installing Microsoft visual Studio 2008. Step 2: Installing Microsoft SQL Server 2005. Step3: Attaching the database file to Microsoft SQL Server 2005. Step4: Execution of Software Step5: Collection of results into screen shots.

RESULTS AND CONCLUSION

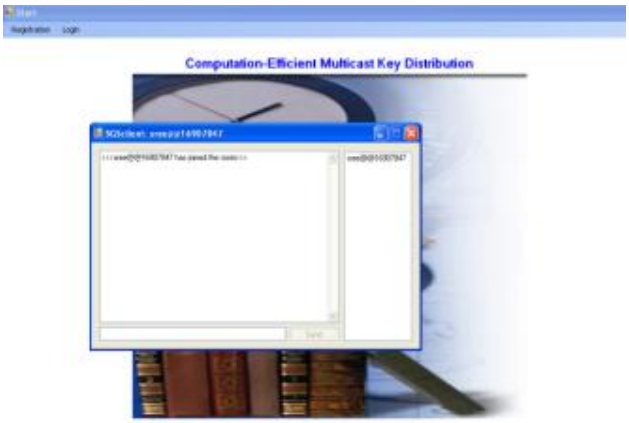
The implementation results of the simulation process are presented in the form of screen shots as shown in fig.7. Each screen shot describes a location and action taken at that location. The sequence of these descriptions constitutes the entire implementation of the present designed scheme. For better understanding and clarity of the outcome of the present simulation technique the descriptions of the screen shots have been tabulated and presented in Table-1. From Fig.7 and Table-1 it is very clear that the present simulation technique is working properly in simulating the present secure and computation efficient multicast key distribution scheme. The Group controller, Client, Key generation and Re-keying modules have been implemented successfully. Both the entry

and exit secrecy of the multicast group system has been ensured along with improved security by changing the session keys dynamically during the simulation. However, the improved security with use of old keys for encrypting the new keys is not directly visible. The internal security measures like validation of user-id, password, and password length have been taken properly. Thus a secure and computation efficient multicast distribution system has been designed and implemented successfully. Scope of the present work: Using of cryptographic algorithm for further improvement of the security may project the present system as a hybrid model. Also it is necessary to check the influence of this additional computation on computation complexity and other features of the entire model. In addition, a systematic comparison with presently existing models would give a better picture about the proposed model.


Registration Form


Log In
Log in
Login With Us


Registration Form


Computation-Efficient Multicast Key Distribution


Log In
Login With Us

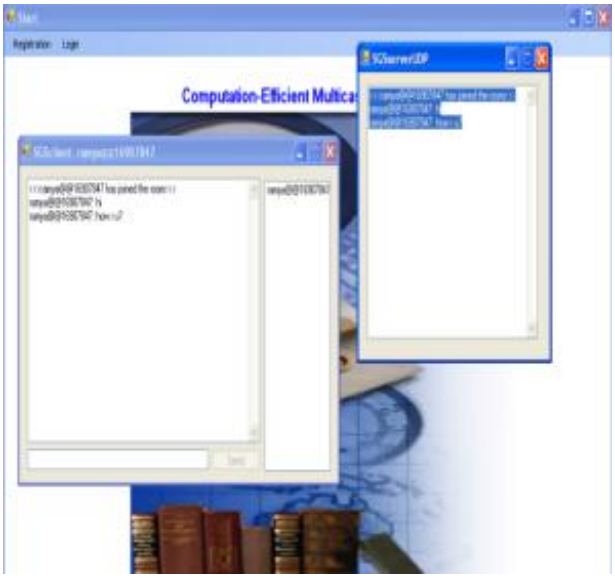

Computation-Efficient Multica

Figure.7 Screen shots during the implementation of the simulation process

Table-1. The simulation results of the present scheme

Screen Shot during simulation	Result during simulation
SS 1: Client start	Starting page for the client for login /registration
SS 2: Registration for Client	Secret key generation
SS3: Validations for User Name	Validation for the client side security
SS4: Validations for Password	Validation of the password-client security
SS5: Validation for Password Length	Password length should be >6 & <10: validation.
SS6: Generation of secret key	A secret key is generated for the client.
SS7: Sucessfull Registration	Registration is successful
SS8: Login page	Login page is opened for registered users.
SS9: Login page continuation	Server IP and security key are entered.
SS10: Chat room	The client joined the chat room
SS11: Client-server Communication	Communication between the client and server.
SS12: Chat room	Multiple numbers of clients joined the chat room.

CONCLUSION:

Thus the present scheme may be a prototype for further extension of the scheme for various multicast key distribution systems and other efficient key distribution systems.

ACKNOWLEDGEMENTS

B. Srinivasa Rao is very much thankful to Dr. L. Pratap Reddy, Professor, Department of ECE, JNTUH, Hyderabad, for his valuable suggestions. Also thankful to the Management of GRIET for their encouragement and cooperation for pursuing his Ph.D. work.

REFERENCES

[1] Datta, R., Mukhopadhyay, S., and Collier, M., Computationally secure self healing key distribution with revocation in wireless ad hoc networks, Adhoc Networks, vol.8, 6, pp 597-613 **2010** (*http://doi.org/10.1016/j.adhc.2009.11.005*)

[2] Suganyadevi, D., and Padmavathi, G., Energy efficient CBMT for secure multicast key distribution in mobile and adhoc networks, Procedia Computer Science, vol.2, pp 248-255 **2010**

[3] Zhou, J. and Ou, Y., Key tree and Chinese reminder theorem based group key distribution scheme, (Eds.) Hun, A. and Chang, S.L., Algorithms and Architectures for Parallel Processing, ICA3PP2009(LNCS), pp 254-265 **2009**

[4] Planisamy, V. and Annadurai, P., Secure group communication using multicast key distribution scheme in adhoc networks, IJCA, vol.1, 25, pp 86-91 **2010** (*www.ijcaonline.com*)

[5] Vijaykumar, P., Bose, S., Kannan, and Deborah, L.J., Computation and communication efficient key distribution protocol for secure multicast communication, KSII Transactions on Internet and Information systems, vol. 7, pp 878-894 **2013** (http;//dx.doi.org/10.3837/tiis.2013.04.016)

[6] Manjul, M. and Mishra, R., Secure group communication based on elliptic curve cryptography, Transactions on Networks and Communications, vol.2, 1 **2014** (DOI:http;//dx.doi.org/10.14738/tnc.21.7)

[7] Vijay, A., and Kumar D.S., Elliptic curve for secure group key management in distributed networks, IJCER, vol.6,6, pp21-28 **2016** (*www.ijceronline.com*)

[8] Hanatani, Y., Ogura, N., Ohba, Y., Chen, L. and Das, S., Secure multicast group management and key distribution in IEEE 802.21, Security Standardisation Research(Eds.) Chen, L. et al, SSR2016, LNCS10074, pp227-243 **2016** (DOI: 10.1007/978-3-319-49100-4_10)

[9] Yadav, A.K. and Soni, S., Secure multicast key distribution in mobile and adhoc networks, Advances in Wireless communications, vol.10, 4, pp781-782 **2017** (*www.ripublication.com*)

[10] Zhu, H., An efficient protocol for secure multicast key distribution in the presence of adaptive adversaries, Sci. China Inf. Sci., 60:52109 **2017** (http:/doi.org/10.1007/S11432-014-0911-8)

[11] Xu, L. and Huang, C., Computing efficient multicast key distribution, IEEE Transactions on Parallel and Distributed Systems, vol.19, 5, pp577-586 **2008**

[12] Sivani, Y.V. and Sudha, T., A novel approach for secured symmetric key distribution in dynamic multicast network, IJERA, vol.1, 4, pp1441-1447 **2011** (*www.ijera.com*)

[13] Rani, D. and Babu, K.G.P., Computationally efficient group keying for time sensitive applications, IJCER, vol.2, pp589-595 **2012** (*www.ijceronline.com*)

[14] Madhusudhan, B., Chitra, S. and Rajan, C., Mobility based key management technique for multicast security in mobile and adhoc networks, The Scientific World Journal, vol.2015, Article Id:801632 **2015** (DOI: http://dx.doi.org/10.1155/2015/801632)

[15] Amara, S.O., Beghdad, R. and Oussalah, M., Securing wireless sensor networks: A Survey. Journal of EDPACS, vol.47, 2, pp6-29 **2013**

[16] Seetha, R. and Saravanan, R., A survey on group key management schemes, Cybernetics and Information Technologies, vol.15, 3, pp3-25 **2015** (DOI: 10.1515/cait-2015-0038)

[17] El-Bashary, M., Abdelhafez, A. and Anis, W., A comparative study of group key management in MANET, IJERA, vol.5, 8, pp85-94 **2015** (*www.ijera.com*)

[18] Fu, K., Kamara, S. and Kohno, T., Key regression: Enabling efficient key distribution for secure distributed storage, proc.NDSS'06 **2006** (*www.microsoft.com*)