EFFICIENT KEY MANAGEMENT ARCHITECTURE WITH COPYRIGHT PROTECTION FOR DYNAMIC GROUPS

V.Vijayaraghavan
AP/CSE Department
Sona college of Tech.
Salem.5, TamilNadu.
India.

R.S.D.Wahida Banu
Professor/ECE Department
A.C. College of Engg and Tech.
Karaikudi.
India.

ragavijay2000@yahoo.com

ABSTRACT

The communication sector is flourishing in many ways, leading to a growing number of users and system attached to the Internet which drives the need for efficient multicast communication architecture over the Internet. Multicasting has been at the center of Internet in the area of Internet activities and has already contributed to some major successes. As multicast communication runs closer towards widespread deployment, security issues have become a central concern and are increasingly important. The features that make multicast particularly significant also make security in multicast difficult. This paper looks at the impressive changes that have been needed in multicast key management architecture and also attempts to avoid the unauthorized duplication of data. It uses tree based subgroups approach which helps to minimize re-keying overhead and also to protect unconstitutional distribution of multicast data without intended users concern.

Key words

Multicast communication, Group key management, Re-keying, Fingerprint.

1. INTRODUCTION

In recent years, multimedia applications have received a lot of attention of network researchers due to its lucrative features. The wide ranges of multimedia applications include teleconferencing, distance education, and shared workspace require secure communication to transmit the information and uses high bandwidth and power consumption. To lessen the high bandwidth utilization, multicast a scalable and efficient technique for group communication is used. Multicasting has been at the center of Internet in the area of internet activities and has already contributed to some major successes. As multicast communication runs closer towards widespread deployment, security issues have become a central concern and are increasingly important. The objectives of a secure multicast communication are ensuring confidentiality of the data so that legitimate members of the group only able to access the data and avoiding the unauthorized duplication of data. Enforcing confidentiality for group communication requires encryption. This requires a group key management [1] solution to distribute and maintain group keys with legitimate group members. The members of multicast group are highly dynamic. In this large and dynamic environment, the design of a secure multicast architecture faces many challenges. One of the challenging issues is the scalable group re-keying, the problem of delivering the updated keys to the members of the group in a reliable and timely manner [2]. Similarly, fingerprinting schemes are necessary to protect illegal redistribution of multicast data without intended users concern. Fingerprinting is a rearing technology to guard multimedia data from embezzled redistribution, where each distributed copy is labeled with unique identification information. In a multicast environment, inserting a fingerprint at the source does not provide any security, since many receivers will share a common fingerprint. Generating the identity based on the receiver's location in the tree and inserting it in the data incrementally as it traverses can overcome this.

This paper is structured as follows. Section 2 introduces the fundamentals of group key management, fingerprinting and the principal problems associated with the existing architectures. Section 3 deals with the proposed key management architecture which reduces re-keying overhead with ownership rights. Section 4 compares the proposed architecture with existing solutions and the last section concludes this paper.

2. EXISTING APPROACHES

2.1. Key management Issues

Secure Multicast communication requires scalable and efficient group key management. Key management incorporates generation and distribution of group keys to group members without permitting unauthorized parties to deduce the key. The main objective of this key management is that keys should be used only once and should be refreshed periodically to avoid compromise [3]. Group key management must update the keys to preserve group secrets, typically caused by either timeouts or membership changes in the group communication. Other important features of key management are forward and backward secrecy [4]. Forward secrecy guarantees that a member cannot learn about the new group keys after he leaves the group. Backward secrecy ensures the new member could not be able to deduce past secrets of the group. To ensure secrecy whenever there is change in membership, the key has to be updated which is costliest process in multicast because of its dynamicity. The key management architecture is classified into three types centralized, distributed and hierarchical [5]. In centralized key management scheme, a single key controller creates and distributes a common key to all the members in the group. This centralized scheme is inefficient, non-robust and not scalable for large dynamic groups. The main drawback of this approach is single point failure, which makes the entire architecture to collapse and also suffers by "1 affects all" problem. In distributed scheme, each member of the multicast group is responsible to create and distributes a key. The newly joined members in the group will receive the key from already existing controller. This scheme also suffers by "1 affects all" problem. In hierarchical scheme [6], entire tree is divided into multiple subgroups. Each subgroup has their independent subgroup key which overcomes "1 affects all" problem. The drawback in this approach is the increased computational overhead, whenever information needs to be transmitted from one subgroup to the other.

2.2. Fingerprinting Issues

The source providers may require copyright protection for the data, such that the ownership rights can be ensured [7,8]. Fingerprinting is a rearing technology to guard multimedia data from embezzled redistribution, where each distributed copy is labeled with unique identification information. The existing unicast solutions can not be applicable for multicast network because of the unique properties of the later. In a multicast environment, inserting a fingerprint at the source does not provide any security, since many receivers will share a common fingerprint. Judge and Ammar [9] proposed WHIM architecture which has two components; WHIM backbone (WHIM – BB) and WHIM last hop (WHIM – LH). WHIM backbone places a hierarchy of intermediaries as end systems in the network and forms an overlay network between them. The path from the source to each intermediary is to differentiate between intermediaries. The unique ID of the intermediary identifies each path. Each intermediary embeds its portion of path ID into the data as a fingerprint as it forwards the data through the network. WHIM last hop allows intermediaries to mark the content distinctly for any children receivers that they might have. WHIM-LH is a building block that when merged with WHIM-BB forms a complete solution for fingerprinting multicast content distinctly for each receiver in the group. Fingerprint is generated based on the receiver's location in the network and is inserted into the content incrementally as it traverses the overlay network. The fingerprint is based on the path from the source to the destination. The proposed architecture investigates tree based subgroups approach which helps to minimize re-keying overhead and the same architecture is utilized to guarantee ownership rights for the multicast content.

3. PROPOSED APPROACH

3.1. Tree Structure

Key management is complicated in dynamic groups, where members join and leave at any time. In order to reduce the key updating process, the proposed approach uses two keys for intermediaries. One key is used to commune

with its parent and another key is to commune with its children. Diffie-Hellman (DH) key agreement protocol is used to distribute the secret key among the members. Fig 1 illustrates a hierarchical tree structure. A key tree has two sub trees of intermediaries and key controller as the root. These intermediaries have two keys, one to communicate with the root node and the next is to communicate with its child nodes. Every user in the group are at the leaf node, have a single secret key used to commune with its intermediary. The communication between the end user is carried through the intermediaries, which decrypt and encrypts the message until it reaches respective destination. Using the key share of all the nodes in the subgroup, group key for the respective subgroup is generated with the help of DH algorithm. In this tree structure, K_1 is the share of key controller.

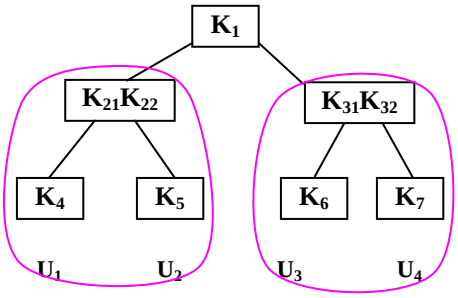
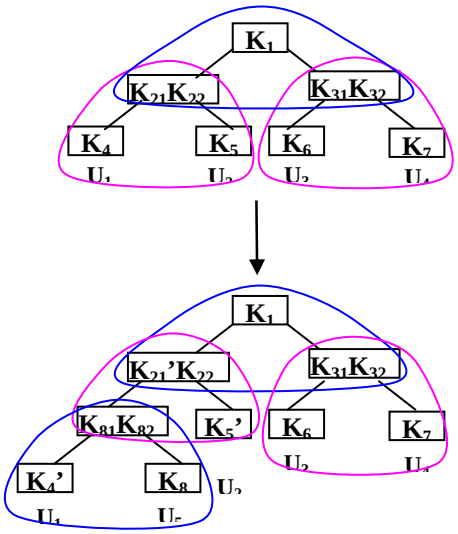


Figure 1 Tree Structure

$K_{21}K_{22}$, $K_{31}K_{32}$, K_4, K_5, K_6 and K_7 are share of the intermediary and end users respectively. Intermediaries have two shares one to generate secret key of its parent and another for its child subgroup. The advantage is that if there is any change in the membership, it is enough to change secret key of few subgroups only.

3.2 Member Join

If any user joins the group, the user contacts the key server. The server authenticates and finds a proper place for new user to insert. Then, only



the secret key of the concern subgroup is updated using the share of the new member. In Fig 2, user U_5 wishes to join the group, the new intermediary with shares $K_{81}K_{82}$ is attached in the tree which forms the subgroup for the user U_5. Then the secret key of the two reformed subgroup is generated for further communication.

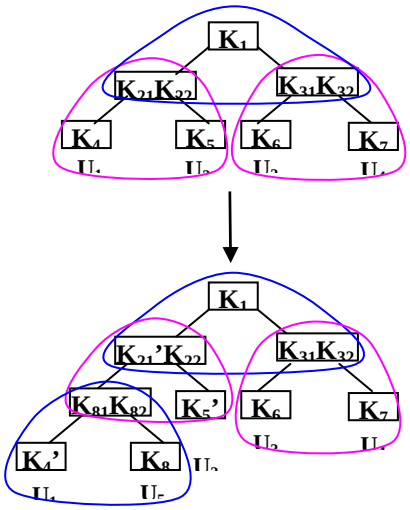


Figure 2 Member join event

3.3 Member leave

If the member wants to leave the group, the respective intermediary removes the member and updates the secret key of the concern subgroup. In Fig 3, U_4 wish to leave the group, the node U_4 and its intermediaries are removed from the group, its sibling U_3 is

attached to the root. The secret key of the newly formed subgroup is updated

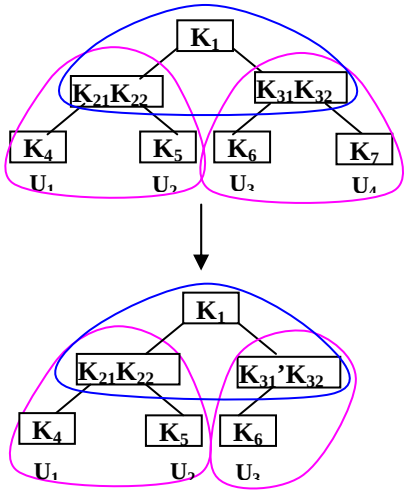


Figure 3 Member leave event

3.4 Fingerprinting

The source providers may require copyright protection for multicast data, such that the ownership rights of the data can be identified. The proposed secure multicast architecture uses the same tree structure to provide copyright protection. Fingerprint is generated based on the receiver's location in the tree and embedded in the data incrementally as it traverses. The fingerprint is based on the path from the source to the intermediary. Fig 4 shows the process of fingerprinting.

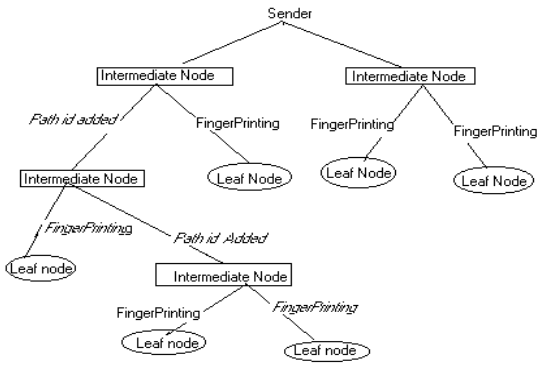


Figure 4Fingerprint generation

The path id of the users is traced by adding the id of all intermediaries in the path and the generated fingerprint is inserted in the leaf node.

4. PERFORMANCE EVALUATION

The proposed secure multicast architecture uses the same tree structure to ensure confidentiality and also to provide copyright protection, which makes the protocol for dual purpose. The analysis of the communication cost in terms of delay between the proposed architecture and other group key agreement architectures including Brumester-Desmedt [10] (BD) and Group Diffie-Hellmann [11] (GDH) is made. Delay is calculated as the time required by the node to join the group and to compute the secret key.

4.1 Membership Updation

Fig 5 shows the comparison for the membership updation for different architectures. In the proposed architecture, the secret key updation need not be reflected to the entire tree whenever there is change in membership, so it has minimal delay. As there are more modular exponentiations involved in Group Diffie-Hellman, the delay is very high. Brumester-Desmedt also has more delay, as it has significant hidden cost.

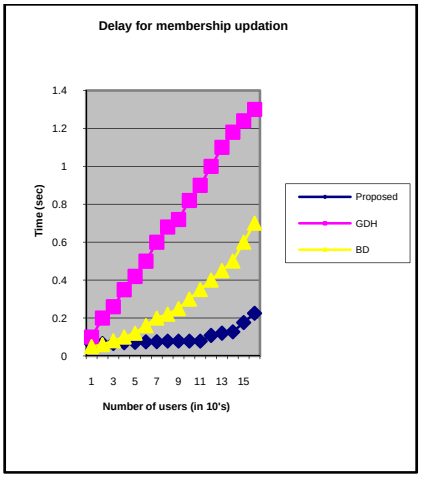


Figure 5 Delay Comparison for membership updation

5. CONCLUSION

Security in dynamicity is the major aspect for highly dynamic group communication as the members can join or leave the group at their will. Also the quest for copyright protection of their fruitful work is increasing. The existing architectures fail to address scalability of the groups and ownership rights of the contents. The proposed secure multicast architecture uses the same tree structure to ensure confidentiality also to provide ownership rights, which makes it efficient and scalable.

REFERENCES:

[1] Paul Judge, Mostafa Ammar, "Security Issues and Solutions in Multicast Content Distribution: A Survey", IEEE Network, Jan/Feb 2003, vol 17, pp 30-36.

[2] P. Kruus, J. Macker, "Techniques and Issues in Multicast Security", MILCOM 98, vol.3, Boston, MA, USA, pp. 1028-32, 1998.

[3] Bruce Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition", ISBN 0-471-11709-9 John Willey and Sons, Inc., 1996.

[4] Yacine Challal, Abdelmadjid Bouabdallah, Hamida Seba, "A Taxonomy of Group Key Management Protocols: Issues and Solutions", Transactions on Engineering, Computing and Technology V6 June 2005, ISSN 1305-5313.

[5] C. Wong, M. Ghonda, and S.Lam," Secure group communications using key graphs", Technical report TR97- 23, University of Texas at Austin, Department of computer sciences, August 1997.

[6] Adrian Perrig, Dawn Song, J.D. Tygar, "ELK, a New Protocol for Efficient Large-Group Key Distribution", In Proceedings of the IEEE Symposium on Security and Privacy, May 2001, pp. 247-262.

[7] H.Yin, C.Lin, F.Qiu, Bo Li and Z.Tan. A Media-Dependent Secure Multicast Protocol for Adaptive Video Applications, IEEE Communications Magazine, June 2005.

[8] H. hua Chu, L. Qiao, and K. Nahrstedt, A secure multicast protocol with copyright protection, ACM SIGCOMM Computer Communications Review, Vol.32, No.2, and April 2002.

[9] Judge, P.Q. and M.H. Ammar, WHIM: Watermarking Multicast Video with a Hierarchy of Intermediaries, Proc. NOSSDAV, Chapel Hill, NC, 2000,pp:699-712.

[10] Burmester, M. and Y.Desmedt, A secure and efficient conference key distribution system, In A.D. Santis, Editor, Advances in Cryptology, EUROCRYPT '94, number 950 in lecture notes in computer science, International Association for Cryptologic Research, Springer-Verlag, Berlin. 1998, PP: 275-286.

[11] Steiner, M., G.Tsudik, and M.Waidner, Key agreement in dynamic peer groups, IEEE Transactions on Parallel and Distributed Systems, 11: 2000, pp: 769-780.

Corresponding Author: V.Vijayaraghavan, AP/CSE, Sona College of Technology, Salem, India, Pin-636005. ragavijay2000@yahoo.com, Tel: +919894549259