International Journal of Innovative Computing, Information and Control
Volume **6**, Number **2**, February **2010**

ICIC International ©2010 ISSN 1349-4198
pp. **487–500**

A LIGHTWEIGHT PREPOSITIONED SECRET SHARING TREE FOR MULTICAST KEY MANAGEMENT

Meng-Hsiun Tsai[1], Shih-Shan Tang[2] and Chung-Ming Wang[2]

[1]Department of Management Information Systems
[2]Department of Computer Science
Institute of Bioinformatics
National Chung Hsing University
250 Kuo-Kuang Rd., Taichung, 402 Taiwan
mht@nchu.edu.tw

Received August 2008; revised December 2008

Abstract. *Secure group communications are increasingly used in the continuous growth of the Internet applications. In a secure multicast environment, an identical data can be efficiently delivered from a source to multiple receivers within a dynamic group. A simple solution is to encrypt the transmitted data using a symmetric key. However, scalable group rekeying is the main challenge for large and dynamic groups. The key tree-based scheme is widely used to achieve logarithmic computational and transmitted costs in the rekeying process. Nevertheless, the key tree-based schemes use the fixed secret key to encrypt confidential messages until every membership changes, which is lack of security in protecting the high-value content. On the other hand, the key tree-based scheme may result in difficult problems in maintaining synchronization due to the interdependencies among rekeying messages. In this paper, we shall propose a key management scheme based on the secret sharing, in which we apply a new lightweight prepositioned secret sharing tree-based scheme to solve the problem in the key tree-based scheme. Furthermore, we eliminate the encryption/decryption processes during every membership and periodic key changes which can dynamically change the secret key frequently.*
Keywords: Group communication, Secure multicast, Group rekeying, Key management

1. **Introduction.** Recently, multicast has been widely used in network technologies. There are many types of group applications, such as pay-per-view, videoconferencing, distance education, on-line video games, which can benefit from the IP multicast [6, 11, 22, 26] for group communication. IP multicast is a bandwidth-conserving technology which can reduce the server bandwidth and overhead by simultaneously transmitting a single message to the participant of all group members. Nevertheless, IP multicast lacks a security service, in which unprivileged members can join the group and can easily to intercept the transmitted data. Therefore, the straightforward approach for secure multicasting is to apply access control to prevent unprivileged members from having access to the group communication. The simple solution for secure multicast communications is to use a symmetric key called the *Traffic Encryption Key* (TEK) to encrypt the transmitted data. The TEK is distributed by the key server and shared by all privileged group members. Because multicast groups are usually dynamic, the TEK used for group communication must be refreshed (rekeying process) for every membership changes to preserve the secrecy. The group rekeying for a member joining is trivial, but it has a complex problem for a member leaving due to the old TEK which cannot be used to encrypt the new ones. How to perform rekeying process for large dynamic groups in a scalable, secure and efficient manner becomes one of the most significant challenges.