Key Management for Simultaneous Join/Leave in Secure Multicast[1]

G. Noubir, F. Zhu, A. H. Chan
College of Computer Science, Northeastern University, Boston, MA, 02115, USA
{noubir, zhufeng, ahchan}@ccs.neu.edu

Abstract - **In this paper, we address the problem of key update for secure group communication. We focus on the case where multiple requests for join or leave are received within short intervals of time. We have shown that there exists an optimal tree structure that minimizes the communication complexity of the key update. We introduce and compare several algorithms for simultaneous key update, efficient tree construction, and tree adaptation to variable requests load.**

I. INTRODUCTION

Multicast communication offers the potential of delivery of data and multimedia to multiple receivers using fewer resources than unicast. Management of the multicast group keys faces a serious scalability problem. Indeed, whenever the group membership changes the multicast group key has to be changed. We have previously proposed an algorithm that reduces the communication complexity of key update for a single join/leave to O(log *N*) [2, 1]. This algorithm was independently discovered in [3]. The principle of this algorithm is to map the users with the leaves of a tree. Each user is provided with all the keys on the path from his leave to the root. The root key is the group key. When a user leaves/joins all the keys in his possession have to be renewed. This is done starting from the lowest level in the tree. For a binary, at each level the new key can be securely communicated by encrypting it using the two lower level keys. Thus communication complexity of the key update is O(log *N*).

II. PROBLEM AND THEORETICAL RESULTS

Given a dynamic multicast group such that simultaneous key update requests are possible. How can we reduce the communication complexity of key update given that, at each step of the algorithm of key update, each user has a probability *p* to request an update? In the rest of the paper, we assume that all users have the same probability of leaving or joining the group *p*. The proposed algorithms can be extended to the case where each user has a specific probability for joining/leaving the group. In [4], we have shown that the optimal tree structure that minimizes the communication complexity of key update has a special structure. These results are summarized in the following.

Theorem (optimal key structure): Let *G* be a multicast group where $|G| = N = 2^k$. Each user has a probability *p* to request a key update. If we restrict the key-tree to trees where each node can have an arity of 2^i, then the optimal tree that minimizes the communication complexity of the key update has the following structure: $2^a\ 2^2\ 2^2\ 2^2 \ldots 2^2\ [2^2|2^1]$. The root node has arity 2^a, the lowest level node has arity 2^2 or 2^1, and all intermediary nodes have arity 2^2. The value of *a* depends on *p*. The detailed proof of the theorem is described in [4]. To determine the optimal tree structure one can notice that whenever the probability of key update *p* is below some value p_{thrsh} then a single level tree (of arity $N = 2^k$) is not optimal and has to be broken. Combining the threshold probability and looking at the first two levels of the tree we can deduce the tree structure of the optimal tree. We assume that p_{thrsh} is pre-computed and stored in a table $p_{thrsh}[N]$.

k	3	4	5	k>6
$\boldsymbol{p_{thrsh}}$	0.262647	0.291468	0.292888	0.292893

Theorem: The optimal tree structure is either $2^a\ 2^2\ 2^2 \ldots 2^2 2^{2|1}$ or $2^{a-1}\ 2^2\ 2^2 \ldots 2^2 2^{2|1}$, where

$$1-(1-p)^{2^{k-(a+1)}} < p_{thresh} \le 1-(1-p)^{2^{k-a}}$$

. This result is based on the fact that in an optimal tree any sub-tree should also be optimal [4].

III. CONCLUSION

In this paper we have shown that when considering multiple requests, there exists an optimal tree structure that minimizes communication complexity. This tree structure can be determined as a function of the probability of a user requesting a key update. In [4] we also show that adapting the delay for processing requests can result in a lower communication complexity.

IV. REFERENCES

[1] G. Noubir, and L. von Allmen, "*Security Issues in Internet Protocols over Satellite Links*", In Proc. of the IEEE VTC'99.

[2] G. Noubir, "*Optimizing Multicast Security over Satellite Links*", European Space Agency Project, Work package 20 report, 1998.

[3] Ch.-K. Wong, M. Gouda, and S. S. Lam, "*Secure Group Communications Using Key Graphs*", Proceedings of ACM SIGCOMM'98.

[4] F. Zhu, G. Noubir, and A. H. Chan, "*Optimal Tree Structure for Key Management of Simultaneous Join/Leave in Secure Multicast*", TR-Wireless Security Laboratory, Northeastern University, October 11th, 2001.

[1] This work was supported by DARPA Air Force Grant F30602-00-2-0518