Multigroup Rekeying for a Wireless Network*

Kuang-Hui Chi[1], Ji-Han Jiang[2], and Yu-Ching Hsu[3]

[1] Department of Electrical Engineering, National Yunlin University of Science and Technology, Taiwan
chikh@yuntech.edu.tw
[2] Department of Computer Science and Information Engineering, National Formosa University, Taiwan
[3] Information and Communications Research Laboratories, Industrial Technology Research Institute, Taiwan

Abstract. In the context of secure group communication, a shared secret key is generated anew for data protection whenever group membership changes. This paper presents an approach to fast rekeying in a wireless network that is subject to time-varying channel conditions. We address a scenario where a station joins one group at a time, but may leave multiple groups at once for abrupt link failure or cascading application termination. In our architecture, each station is assigned a private number and a code, so as to exploit Fermat's Little Theorem and an orthogonal coding methodology, respectively. The former is used to protect the delivery of updated group keys, while the latter to encode keying material meant for different sites in an aggregate form as a payload for message distribution. Since rekeying messages are delivered via multicast, intended stations can decode information of interest at the same time. Therefore rekeying among multiple groups can still be carried out timely with $O(1)$ message complexity. Our design provides a complementary facility to current schemes for performance improvement. Pragmatic considerations of our approach are discussed as well.

1 Introduction

Secure group communication is generally accomplished by using a shared cryptographic key for data protection. For forward and backward secrecy, however, a rekeying process is performed whenever group membership changes. As far as a wireless network is concerned, group membership is likely to change over time due to link outage on account of radio signal characteristics or user's mobility. Such network dynamics may cause frequent group rekeyng, at the cost of repeated message exchanges taking nontrivial delay. This gives rise to an *out-of-sync* problem between keys and data [9] or disruptions of message delivery among communicating parties. In addition, group keys are generally meant for

* This work was supported by the National Science Council, ROC, under grants NSC 95-2221-E-224-016-MY2 and NSC 95-2622-E-150-035-CC3, and by the Ministry of Economics, ROC, under the grant 6301XS2430.

T. Enokido, L. Barolli, and M. Takizawa (Eds.): NBiS 2007, LNCS 4658, pp. 147–156, 2007.

temporal use, requiring updates from time to time. Therefore the development of a fast group rekeying procedure is essential.

There has been active research on group key management. For an expository survey, we refer the reader to [3,7]. A common treatment is to organize a group of nodes in a tree or in a logical key hierarchy (key graph [14].) Considering such a hierarchy, schemes like [11] reduced rekeying overhead by keeping the tree balanced. Another avenue to reduce the overhead results from batch rekeying, as opposed to individual rekeying after each join or leave (see [4,9] for example.) Group rekeying can also be approached by one-way hash functions, e.g. in [8,15], or the Group Diffie-Hellman contributory key agreement, e.g. in [2,13]. Though effective, these schemes incur communication or computational costs in some sense. Additional cost results from rekeying when a node belonging to multiple groups leaves the system or when periodic updates to different group temporal keys are required. In that event, the blackout period of disrupted traffic grows longer unless rekeying among multi-groups is properly designed.

As a remedy, we tackle above issues by exploiting Fermat's Little Theorem and an orthogonal coding technique. These two techniques enable stations of different groups to retrieve keying information of interest to respective sites parallelly from a single, scrambled message. In this fashion, multigroup rekeying can be completed sooner than would otherwise be possible. Our approach allows for the broadcast property of wireless media or network-level multicast where available. It is also feasible to incorporate our development in counterpart schemes for performance improvement. Our proposed approach is not a trivial extension of conventional group rekeying protocol in that we simplify an original procedure of repeated message exchanges and represent information for separate groups in a compact form in a single message. This saves overall rekeying delay and space overhead of separate rekeying messages per group like redundant message headers and trailers. Communication activities will thus become better streamlined to the user's benefit.

The rest of this paper is organized as follows. In Sect. 2, we shall first describe our system model and the rationale behind the proposed scheme. Then we discuss how the scheme operates upon a join or a leave. Next we avail ourselves of an orthogonal coding technique to achieve rekeying across multiple groups by means of a single message. Subsequently complexity results of some well-known group rekeying schemes are compared in Sect. 3. Sect. 4 summarizes this study. Lastly, how the proposed scheme is related to a pragmatic IEEE 802.11i network is given in the Appendix.

2 The Proposed Approach

Consider a network containing a group key controller (GKC) and n wireless stations (Fig. 1.) These stations communicate via some point of attachment to the system, referring to a base station or multicast-capable router at which the GKC may be colocated. The GKC maintains a secure communication channel with the point of attachment to transport security information specific to stations. We