Secure and Efficient Distributed Relay-Based Rekeying Algorithm for Group Communication in Mobile Multihop Relay Network

A. S. Khan

Network Research Group, Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, 94300 UNIMAS, Kota Samarahan, Sarawak, Malaysia.
skadnan@fit.unimas.my

Abstract: In mobile multihop relay (MMR) networks, Relay multicast rekeying algorithm (RMRA) is meant to ensure secure multicast communication and selective updating of keys in MMR networks. However, in RMRA, the rekeying is carried out after a specific interval of time, which cannot ensure the security for multicast communication on joining the member. Secondly, the rekeying scheme generates a huge communication overhead on the serving multihop relay base station (MR-BS) on frequent joining of members. Lastly, there is nothing about when a member left the group communication. Thus, the rekeying scheme of RMRA fails to provide forward and backward secrecy and also is not scalable. To solve this problem, an improved rekeying scheme based on broadcasting a new seed value on joining and leaving of a member for updating the ongoing key management is proposed. The proposed scheme solves the issue of forward and backward secrecy and the scalability in a very simplified way. The forward and backward secrecy of the proposed scheme has been extensively validated by formal method using rank theorem. Furthermore, mathematical derivation showed that the proposed scheme out-performed the RMRA in terms of communication cost and complexity.

Keywords: Relay multicast rekeying algorithm (RMRA), security in WiMAX, Mobile Multihop Relay, 4G networks, SEDRRA, Distributed Algorithms.

1. Introduction

Multicast services in MMR network is an efficient and power saving mechanism which also facilitates the subscribers with strong protection from theft of service by encrypting the broadcast connections within the subscribers, and the serving multihop relay base station (MR-BS). This strong protection is in the shape of confidentiality, authenticity and the integrity of messages delivered within the group members[1-3]. Security of these multicast communications usually depends on secure group communications, which require privacy for participants and access control at the multicast server. In order to ensure secure communication within the group, several secret keys must be shared and updated periodically in that group. MR-BS needs to unicast or broadcast the keys with specific period of time to maintain the key's secrecy and to ensure the secure communication [4]. The group communication can be compromised by any adversary through the compromised group members. The compromised group members may not necessarily be the part of group communication at the time of attack; it may be the member who left the group, and still they have the key with an active lifetime. Thus, security is a critical issue, especially for stock option bidding, pay per view TV broadcasting, and video conferencing kinds of application. Those emerging applications usually depend on secure group communications, which require privacy for participants and access control at the group communicator server [5].

For secure group communication, rekeying mechanism must be efficient enough that the leaving or joining member cannot derive the future and past shared keys i.e. maintain forward secrecy and backward secrecy respectively. However, most of the algorithms by providing these secrecies, they do not care the issue of scalability. Therefore, for a dynamic group in which the membership changes frequently, the rekeying algorithm is a critical factor in overall service efficiency; it should guarantee forward secrecy and backward secrecy; on the other hand, the rekeying algorithm should be scalable to a large group. The challenge of a secure multicast service in MMR networks is to provide an efficient rekeying method for controlling access to a group and its communications that can ensure the issues of secrecies and scalability [6, 7].

Secure group communication is one of the emerging topics in the recent network technologies. During the last ten years, several protocols have been proposed to counter the above challenges. For instance, the initial works for secure multicast and broadcast communication are [8-9]. Later, logical key hierarchy (LKH) [10, 11] and one-way function tree (OFT) [12] were proposed. Several other protocol were proposed based on OFT and LKH [11, 13-15]. However, all these schemes were centralized and have the issues of forward secrecy, backward secrecy and the scalability [15]. Group communication for WiMAX networks recently gained popularity, especially for MMR networks (e.g. smart grid applications) [16-18]. Multicast and broadcast rekeying algorithm (MBRA) is the primary scheme proposed by the standard to ensure the secure group communication in single hop networks [4, 19]. However, several analyses [1, 5, 20-22] showed that the scheme fails to provide the main group communication properties, i.e. forward secrecy, backward secrecy and the scalability. To address the above issues, ELAPSE (Efficient sub-Linear rekeying Algorithm with Perfect Secrecy) has been proposed [1, 5, 23]. ELAPSE