A Conference Key Multicasting Scheme Using Knapsack and Secret Sharing

Shiuh-Jeng Wang * and Jin-Fu Chang

*Department of Information Management
Central Police University
Taoyuan, Taiwan 333
E-mail: sjwang@sun4.cpu.edu.tw

Department of Electrical Engineering
National Taiwan University
Taipei, Taiwan 106

Abstract

In this paper, a conference key multicasting scheme is proposed and analyzed. Each network user $U_i$ is associated with a key pair $(x_i, y_i)$, where $x_i$ is a secret key and $y_i$ is a public key. A sealed lock is constructed from the public keys so that conference key can be enciphered by a chairperson and broadcasted to users in the network system, while only the authorized participants can recover the conference key. The packed sum property aspect of the well known knapsack problem together with the concept of secret sharing is utilized to accomplish the construction of a sealed lock.

I Introduction

With the progress in computer and communication (C&C), a large number of individuals now have personal computer. In order to share resource and to exchange information, these personal computers can be networked together. In network applications, the transmitted messages have the potential of being eavesdropped, altered and even destroyed. Therefore it is necessary to incorporate cryptographic protection into the network. Computer networks of various scales have widely existed. In general, communication within a network can be classified into two types: point-to-point and point-to-multipoint. To achieve secrecy, a message has to be encrypted before sending to the communication channel. Ciphers can be categorized into conventional and public key systems. The concept of public key was first due to Diffie and Hellman [2]. In public key system, each user has two keys: a secret and a public key. To send a secret message, the sender uses the intended receiver's public key to encrypt and the

* Correspondence addressee: Dr. Shiuh-Jeng Wang, Department of Information Management, Central Police University, Taoyuan, Taiwan 333
receiver uses his private key to decrypt. In this arrangement a total of $2n$ keys is needed if $n$ denotes the total number of users in the network. In conventional key system, however, a total of $n(n-1)/2$ keys is required. To further strengthen security, when two users wish to communicate with each other, a session key is first created and exchanged. Different session keys are used in different sessions to encrypt and decrypt messages. These session keys can be constructed from the public key system we mentioned in the above.

There are frequent applications where a user wishes to communicate with several other users. The style of point-to-point communication mentioned above would be obviously inefficient. Point-to-multipoint communication or multicasting has to be developed for fast and efficient delivery of a message to a group of recipients. Multicasting is somewhat different from broadcasting. The main feature of broadcasting is that a single transmission from an originating station can be heard simultaneously by, basically, all stations. The transmissions in radio links and local area network bus are both of this nature. In applications such as multicasting only a limited number of users are legitimate to receive a broadcast message. This aim can be achieved through encryption.

In this paper, we develop a new conference key multicasting protocol jointly out of knapsack and secret sharing. In our scheme, we embed the conference key into many sealed keys, pack these sealed keys into the sealed lock and broadcast it to all the intended recipients in the network, while only legal intended recipients can recover the secret conference key. In section II, we review the related works and tell our motivation. In section III, a secure multicasting protocol is presented. Cryptanalysis is done in Section IV. Finally, conclusions are given in Section V.

II Related Works

Secure broadcasting has received considerable attention from researchers [1],[4]-[5]. Ingemarsson et al. [4] proposed a conference key distribution system (CKDS for short) which generalizes the public key distribution system (PKDS for short) to a secure multi-destination communication. The network consists of a group of $n$ users connected into a ring. Each user has to process and send message received from upstream. This undoubtedly increases the threat of acquiring the common conference key by an eavesdropper who may try to intercept the message at each station along the ring. Chiou and Chen [1] proposed a broadcasting scheme in which session keys are packed into a sealed lock using the Chinese remainder theorem (CRT for short). The space requirement in [1] however is formidable. Later, Lin et al. [5] proposed a secret conference key algorithm to reconstruct the sealed lock. Although in comparison with [1] the space requirement in this scheme is reduced, the way that the sealed lock constructed is impractical for a multicasting application.

The well known $0 - 1$ knapsack problem [6],[7],[8] examines a sequence $v_1$, $v_2$, ..., $v_n$ of integers and a target sum $S$. It is to find whether a subset of $v_1$, $v_2$, ..., $v_n$ sums up to $S$. That is, given a sequence set $V = \{v_1, v_2, ..., v_n\}$, and