Efficient Key Distribution for Closed Meetings in the Internet

Fuwen Liu and Hartmut Koenig

Brandenburg University of Technology Cottbus,
Department of Computer Science,
PF 10 33 44, 03013 Cottbus, Germany
{lfw, koenig}@informatik.tu-cottbus.de

Abstract. Many emerging group oriented and collaborative applications such as audio/video conferences use the peer-to-peer paradigm. Confidentiality is an often demanded feature for such applications, e.g. in business meetings, to provide group privacy. To assure confidentiality in a meeting the partners have to agree upon a common secret key for encrypting their communication. This requires efficient distributed group key exchange protocols. We present the principle of the key distribution protocol TKD which achieves a lower key refreshment delay compared to existing key exchange protocols.

1 Motivation

In order to assure confidentiality in a peer-to-peer (P2P) meeting the partners have to agree upon a common secret key for encrypting their communication. It is intuitive that a decentralized key management protocol in which the members themselves manage the group key renewal should be deployed in P2P systems. In particular, real-time settings strongly require efficient decentralized key exchange protocols.

In this contribution we sketch the principle of a novel distributed key distribution protocol, called TKD (*token based key distribution*), which has been designed for small dynamic peer groups to support a secure and efficient group key renewal. Unlike other protocols it also provides a mutual authentication of the partners when entering the group. We focus on closed dynamic peer groups of less than 100 participants here. The entrance is by invitation. Many every-day life meetings such as business talks have usually a considerably smaller number of participants.

Decentralized group key management protocols can be divided into two groups: group key agreement and group key distribution protocols [1]. Among the group key agreement protocols, TGDH has proven to be the most efficient one [1], whereas the protocol of Rodeh et al. provides the best performance of existing key distribution protocols [2]. Both protocols, however, are not efficient enough for small group settings. TGDH intensively utilizes asymmetrical cryptographic computations. The Rodeh protocol requires two communication rounds. TKD is a group distribution protocol which has been proven more efficient than the both mentioned ones. It has been integrated in our P2P conference system BRAVIS [3]. TKD requires like other decentralized key management protocols an underlying group communication protocol with virtual synchrony.

J. Dittmann, S. Katzenbeisser, and A. Uhl (Eds.): CMS 2005, LNCS 3677, pp. 271 – 272, 2005.

2 Principle of TKD

TKD is a token based protocol. The group members form a logical ring. The rotating token determines the group member responsible for generating a new group key and for distributing it to the members. The group key is renewed whenever the group composition changes (join, leave, and failure of peers). The token holder is further the group member who authenticates the joining partners using the IKEv2 protocol [4].

The group key renewal is based on the Diffie-Hellman (DH) key exchange principle [5]. When the token holder has generated a new group key it establishes a temporary secure channel to each member to deliver the new key. For this, each group member stores a shared DH secret with each other member. To set up the channels it uses the shared DH secrets and a newly generated nonce which is only valid for this group key renewal cycle. The Figure 1 shows the principle.

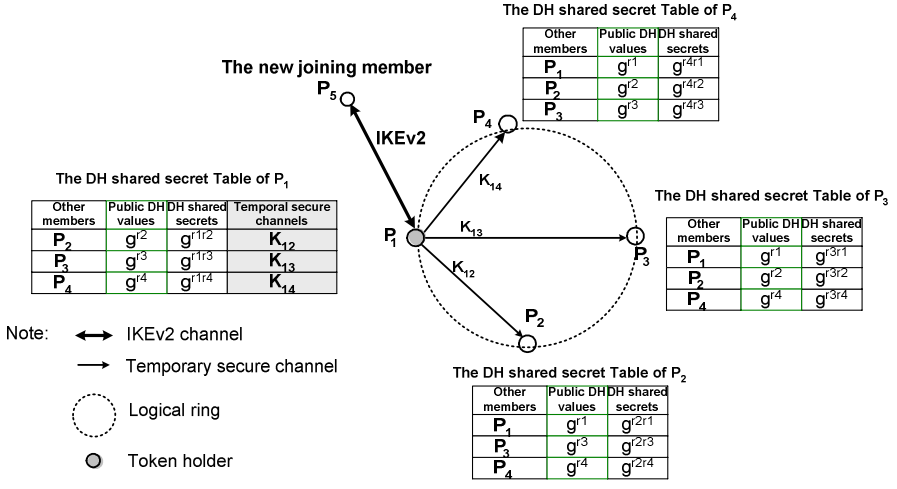

Fig. 1. Key exchange in TKD with temporal secure channels

The efficiency gain of TKD results from the main use of symmetric cryptographic operations and only one communication round for the group key renewal. Thus TKD considerably reduces the group key refreshment delay compared to TGDH and the Rodeh protocol.

References

1. Y. Kim, A. Perrig, and G. Tsudik: Tree-based Group Key Agreement. ACM Transactions on Information Systems Security (TISSEC) 7 (2004) 1, pp.60-96.
2. O. Rodeh, K. P. Birman, D. Dolev: Optimized Group Rekey for Group Communication Systems. Network and Distributed System Security Symposium 2000(NDSS'00), pp. 39-48.
3. The BRAVIS video conference system. http://www.bravis.tu-cottbus.de.
4. C. Kaufman: Internet Key Exchange (IKEv2) Protocol, draft-ietf-ipsec-ikev2-17.txt, September, 2004.
5. E. Rescorla: Diffie-Hellman Key Agreement Method. RFC 2631, June 1999.