Chapter 12
Distributed Key Management Scheme Based on CL–PKC in P2P Networks

Zhongwen Li
Chengdu University, China

Zhibin Xu
Xiamen University, China

Chen Liang
Xiamen University, China

ABSTRACT

P2P networks have characteristics of decentralization, autonomy, and dynamicity. The security problems caused by these characteristics have seriously affected further development of P2P networks. The authors did research on CL-PKC key management schemes. (1) They propose a certificateless-based key distribution scheme with multiple trusted centers that fits the characteristics of P2P networks, and analyzed its security. (2) They also propose an improved interactive key agreement protocol across multiple domains, and then compare it with some existing key agreement protocol from aspects of security and computational efficiency. (3) The authors have implemented the proposed key management schemes, then verified their correctness and tested their computational efficiency. Combined with master key share management and key management of nodes, this system constructed a complete certificateless-based key management model, which is an exploration to solve security problems in P2P networks.

BACKGROUND

P2P (Peer to Peer) that is peer computing or peer networks, is a new network technology. Pure P2P network does not have any client or server. Thousands of computers connected to each other are on the equal status, while serving as a client (resource requestor) and server (resource provider) role. With the development of P2P networks, complete anonymity of the safety problem has seriously affected the further development of P2P networks. For example, in file-sharing system, the selfish users only enjoy the service refused...
to provide services for other users (“freeriding” phenomenon) (Dinger & Hartenstein, 2006). This series of problem’s solution is to build a reputation system in P2P networks. To get the nodes’ reputation value, it needs authenticate the identity of the node at first. Therefore, the study on highly robust certification P2P system becomes one of the hot current P2P studies.

Traditional PKI needs a certificate to bind an identity and its public key, and certificate management in PKI is very complicated, including certificate distribution, certificate storage, certificate verification, certificate update, and certificate revocation. These processes need to consume a large amount of CPU resources and bandwidth resources. These problems prevent the implementation of PKI in the P2P network efficiently. The identity of public key cryptography (ID-PKC, Identity-based Public Key Cryptography) (Shamir, 1984), not only have the specific problem of key escrow, but also generally only is fit for small networks which do not ask for demanding security, but not fit for P2P networks which need for secure authentication (Aberer & Despotovich, 2002).

At Asiacrypt 2003, Al-Riyami and Paterson first proposed the notion of certificateless public key cryptography (CL-PKC, Certificateless Public Key Cryptography) (Al-Riyami & Paterson, 2003). As CL-PKC does not need certificates to authenticate public keys, therefore there is no certificate management problem, and it also avoids the key escrow problem in ID-PKC. Therefore, CL-PKC is considered as more suitable for P2P network authentication scheme.

The existence of single trusted center limits the network scalability, also causes risks of single-point failure. Therefore, many authentication schemes without trusted center in P2P networks have been proposed. However, those schemes are only applicable to applications which do not need high-level security, and the signature of node can not provide a true non-repudiation feature. In fact, all schemes without trusted center have the similar disadvantages. Using Multi-KGCs in P2P networks can avoid the shortcomings:

1. The number of trusted KGCs P2P network can dynamically adjust according to the number of nodes to improve the scalability of P2P networks.
2. Multi-trusted KGCs can avoid single-point failure, to improve the robustness of P2P networks.
3. It distributes the power of trusted KGCs to prevent the attacker to steal the master key, which can improve the security of P2P networks.

In summary, research on the certificateless-based multi-KGCs key distribution schemes that are fit for the characteristics of P2P networks is currently one of the problems needed to be solved. We apply the key generation schemes to the large-scale P2P networks, and study the corresponding session key generation and key management issues, thereby establishing a complete and reliable distributed key management system.

THE KEY DISTRIBUTION SCHEME WITH MULTIPLE TRUSTED CENTERS

In this section, we propose a certificateless-based key distribution scheme with Multi-KGCs that fits the characteristics of P2P networks, and analyzes its security.

A. Design Goals and Design Model

- **Design Goals**: The existence of single trusted center limits the network scalability, also causes risks of single-point failure. If the security of authentication can not be guaranteed, let along the security of signature and reputation systems. For the above reasons, our design will introduce a