学校编码：10384　　分类号_____密级_____
学　　号：23020081153203　　UDC_____

硕　士　学　位　论　文

P2P 中无证书的密钥生成方案及密钥协商协议的研究

Research on the Certificateless Key Generation Scheme and Key Agreement Protocol in P2P Networks

徐志斌

指导教师姓名：黎 忠 文　教授

专　业 名 称：计算机系统结构

论文提交日期：2011 年　5　月

论文答辩时间：2011 年　6　月

学位授予日期：2011 年　　月

答辩委员会主席：_____

评　　阅　　人：_____

2011 年 6 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下,独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘　要

P2P 网络的“分散、半可信和动态性”使传统公钥基础设施(PKI)的证书管理困难和基于身份公钥密码体制(ID-PKC)的密钥托管问题特别突出，因此 P2P 网络的安全问题成为公认的难题。在 2003 年的亚洲密码会议上，Al-Riyami 和 Perterson 提出了一种新的公钥密码体制——无证书公钥密码体制(CL-PKC)。CL-PKC 既无证书管理问题，又无密钥托管问题，效率比 PKI 高，而安全性比 ID-PKC 强，非常适用于 P2P 网络。基于此，本文开展了 CL-PKC 在 P2P 网络中的应用研究，通过对密钥的分布式生成和密钥的可跨域协商等问题的研究，突破了 CL-PKC 在 P2P 网络中的应用瓶颈。主要做了以下几个方面的工作：

(1) 针对 P2P 网络的特点，提出了一种无证书的可验证分布式密钥生成方案，并分析了方案的动态性和安全性。方案通过引入门限密钥共享思想，合理分配超级节点于不同的权限，可指认出恶意的密钥生成中心(KGC)服务节点，并当有新 KGC 节点加入、KGC 节点退出或变节时，系统能够提供安全高效的更新机制，保障了系统的安全性和可靠性。

(2) 研究分析现有的无证书两方密钥协商协议的不足，提出了一种无证书的可跨域的认证密钥协商协议，并分析了协议的安全性和计算性能。分析表明协议具有高效、可跨域和可认证的性能，并满足所有的安全属性，更加适用于混合 P2P 网络。

(3) 对提出的新方案及一些主流的密钥协商协议进行具体设计和实现，验证新方案的正确性，并比较分析了协议的计算效率。

本文通过引用无证书公钥密码体制，为解决 P2P 网络安全问题进行了一次积极地探索，同时也丰富和发展无证书公钥密码体制的理论及应用领域。

关键字：P2P；CL-PKC；密钥生成；密钥协商；可跨域

Abstract

The “scattered, semi-trusted and dynamic” characteristics of P2P networks make the certificate management difficulties of the traditional public key infrastructure (PKI) and the key escrow issue of identity-based public key cryptography (ID-PKC) more prominent, so the security issue about P2P networks has become a recognized hard problem. In the Asia-CryPt-2003 conference, Al-Riyami and Perterson proposed a new public key cryptography - certificateless public key cryptography (CL-PKC). CL-PKC does not have the certificate management problem or the key escrow issue. Morever, CL-PKC is not only more efficient than PKI, but also more secure than ID-PKC, which is so suited for P2P networks. Based on this, we carried out the research about applying the CL-PKC in the P2P networks. Throuh researching on the distributed key generation sechme and key agreement protocol with across-domain, breaking the bottlenecks of making use of CL-PKC in the P2P networks.

The main contributions of the thesis are summarized as below:

(1) According to the characteristics of P2P networks, a verifiable certificateless distributed key generation scheme was proposed. We aslo gave the analysis of the dynamic nature and security. By introducing the threshold secret sharing scheme, our scheme could assign the different super-nodes with the rational rights and identify a malicious service node that was key generation center (Key Generateor Center, KGC). If a new KGC join the system, some KGC defect or quit, the system based on our scheme can provide a safe and efficient update mechanism to ensure the system security and reliability.

(2) After taking research on the proposed two-party key agreement protocols and find the deficiencies of them in P2P networks, a new certificateless authenticated key agreement protocol was proposed, which could be used at the different domains. We also analyzed the security of the scheme and computing performance. Our protocol met the across-domain, authentication, and all the security attributes,

which was more suited for the hybrid P2P networks.

(3) The proposed key generation scheme and the key agreement protocol were both implemented. Some other mainstream protocols were also implemented in the system. We verified the correctness of our schemes, tested and analyzed the efficiency of all the schemes which had been implemented.

In this thesis, in order to solve the security issues in P2P networks, by introducing the certificateless public key cryptography, we not only carried out a positive exploration, but also enriched and developed the theory and applications of CL-PKC.

Key Words: P2P; CL-PKC; Key Generation; Key Agreement; Across-Domain

目 录

Table of Contents

第一章 引言

1.1 研究背景与意义

P2P 网络(Peer-to-Peer Networks)是一种架构在 IP 网络之上的覆盖网络(Overlay Network)，是对等计算或对等网络[2]。P2P 作为一种与传统的服务器/客户端对立的网络结构，其最根本的思想（同时也是与 C/S 最显著的区别）在于网络中的节点(Peer)既可以获取其它节点的资源或服务同时又是资源或服务的提供者，即兼具服务器和客户端的双重身份。目前，P2P 应用在互联网中发展十分迅速，新应用更是层出不穷。最初，以 Nasper，BitTorrent 等为代表的 P2P 文件分享软件，以其飞快的下载速度和丰富的内容资源，迅速占据了下载软件的市场。近几年，以 PPstream，PPlive 等为代表的 P2P 网络视频技术又吸引了众多的网络用户。据德国互联网调研机构 ipoque 称，P2P 已经彻底统治了当今的互联网，其中 50-90％的总流量都来自 P2P 程序。

P2P 被《财富》杂志列为影响 Internet 未来的四项科技之一，拥有广阔的发展前景，其应用领域越来越广泛，主要包括对等计算、文件共享、协同工作、信息检索、即时通讯和流媒体等几个方面。但是，“安全研究滞后于功能研究”，在 P2P 领域也是如此。当前大多数对 P2P 系统的研究仅仅关注于服务，尽管在网络结构、路由和文件存贮等方面硕果累累，但安全性研究却并不多见。然而，虽然 P2P 网络结构的“分散、半可信、动态”等特性赋予其强大的功能和性能，但同时也给 P2P 带来比传统网络结构更加复杂的安全性问题[59]，如 VBS.Gnutella 蠕虫病毒[3]，女巫攻击[4]，Free-Riding 现象[5]等。相对于传统客户/服务器模式的服务器可以做主动和被动的防御，P2P 系统需要在没有中心服务器的情况下提供身份认证、授权、数据信息的安全传输、数字签名和加密等安全机制，但目前的 P2P 技术还未能完全实现这一目标，这使得其面临严峻的安全问题，也直接影响了 P2P 的大规模商用。此外，P2P 网络中的节点本身往往是计算能力相差较大的异构节点，而在一般的 P2P 应用中每一个节点都被赋予了相同的职责，系统并没有考虑到节点的计算能力和网络带宽等，其中局部性能较差的点将会导致整体网络性能的恶化，从而难以在这种异构的网络环境中实现优化的资源管理和负载

平衡。因此，在研究和设计 P2P 网络中的安全方案时，我们也应该充分考虑 P2P 网络结构的特性，平衡网络负载，提高资源的利用率。

通常网络系统的信息安全技术涉及到加密技术、鉴别和认证技术、访问控制技术等几个方面的内容。同样，构建 P2P 网络系统的安全保障也从这几个方面给予考虑：

(1) 加密技术。加密技术是解决网络信息安全问题的核心技术，通过数据加密技术，可以在很大程度上提高数据的安全性，保护传输数据在一个开放的网络环境中的机密性和完整性。要保证 P2P 网络中数据对等点间的交互消息不会在通信过程中被窃听，可以通过在对等点间建立起共享的会话密钥后由密钥对信息进行加密。如果在信息中同时加入数字签名或 MAC（消息认证码），那么节点双方还能确定交互信息没有被篡改过。

(2) 鉴别与认证[60][63]技术。该技术是为保证信息传递的安全性、真实性、可靠性、完整性和不可抵赖性。在 P2P 网络中，在对节点身份或传输数据进行验证、核实的过程，可以验证对方节点的合法性，保证传输数据的真实性和完整性、不可抵赖性等。

(3) 访问控制技术。访问控制就是通过某种途径准许或限制访问权利及范围的一种方法，通过访问控制服务可以限制对关键资源的访问，防止非法用户的入侵或因合法用户的不慎操作所造成的破坏。访问控制也是信息安全理论基础的重要组成部分，通常又与授权策略相结合。在 P2P 网络中，根据角色、信誉等授权策略进行有效地访问控制，从而建立一个安全、可控、公平的 P2P 网络。

本文以节点的密钥生成方案和密钥协商协议这两个基础问题为切入点，研究和构建 P2P 网络中的部分安全方案。节点的密钥生成方案和密钥协商协议作为认证技术和加密技术的基础技术，若在 P2P 网络中不能得到有效解决，则其他的安全服务便无可谈及，因此如何设计适用 P2P 网络的密钥生成方案和密钥协商协议是迫切需要深入研究的。

目前网络安全研究中涉及的公钥密码体制有三种：基于传统的公共基础设施(Public Key Infrastructure, PKI)[6]、基于身份的公钥密码体制(Identity-based Public Key Cryptography, ID-PKC)[7]和无证书公钥体制(Certificateless Public Key Cryptography, CL-PKC)[8]。PKI 的方案使用部分分布或者完全分布的证书权威