一种基于PKI的P2P身份认证技术

贺 锋,王汝传
(南京邮电大学 计算机科学与技术学院,江苏 南京 210003)

摘 要:目前P2P技术发展非常迅速并且得到大量应用,但由于P2P网络本身的结构特点使之面临很多安全问题,尤其是身份认证技术几乎在所有主流的P2P软件中研究的都不够细腻,而身份认证却是P2P网络安全的重要组成部分。文中提出一种基于PKI的P2P身份认证技术,在中心化结构P2P网络中设置认证机构,认证机构中存储P2P网络中节点的地址和公私钥对。由于认证机构中公私钥对的唯一性,节点通过私钥加密,公钥解密可以达到确认节点身份的目的,同时可以实现重要信息的加密传输。模拟实验表明该技术有效地提高了中心化结构P2P网络的安全性和健壮性。

关键词:对等网络;身份认证;安全;公钥基础设施
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2009)10-0181-04

A Peer-to-Peer Identity Authentication Technology Based on PKI

HE Feng, WANG Ru-chuan
(College of Computer Science and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: P2P technology currently is developing very rapidly and has been widely used, because of characteristics of its network structure, it is facing many security issues, especially the identity authentication technology in almost all mainstream P2P software is not deeply studied yet, and identity authentication is an important component of network security, a peer-to-peer identity authentication technology based on PKI is researched, the center structured peer-to-peer networks setup a certificate authority, the certificate authority keeps peer's internet protocol and couple of public and private keys in center structured peer-to-peer network. Because the couple of public and private keys are unique in the certificate authority, the peer can be identified by using its private key encryption and public key decryption, it also can be used in encrypting massage, simulation results show that this technology enhances the security and stability efficiency in center structured peer-to-peer networks.

Key words: P2P; identity authentication; security; public key infrastructure

0 引 言

近年来,随着P2P技术的日益成熟,越来越多的基于P2P技术的网络软件在互联网上悄然兴起。从早期的Nasper,到时下最为流行的用于文件共享和下载的BitTorrent, P2P网络已经成为了互联网不可或缺的一部分。P2P网络的结构也在不停地发展,从有中心节点的Nasper,到无中心非结构化的Gnutella和Freenet,再到现在的基于DHT(Distributed Hash Table)的结构化P2P网络如Chord和Pastry也在不断地进化[1]。然而,目前的P2P网络,无论是结构化的还是非结构化的,目前还没有很好地解决节点身份认证的问题。随着公钥基础设施(Public Key Infrastructure, PKI)建设的完善,运用PKI技术可以构建出完整的加密/签名体系,可以有效地解决网络安全性,在充分利用互联网资源共享的前提下,从真正意义上确保网上交易与信息传递的安全[2]。

该文的贡献在于:提出了一种基于PKI的P2P身份认证技术,而PKI认证是要有中心服务器参与的,但是中心服务器会带来流量瓶颈和系统崩溃等网络问题,所以提出一种基于超级节点的全分布结构化P2P网络,在一个P2P网域中超级节点起到小型服务器的

收稿日期:2009-02-03;**修回日期**:2009-05-12
基金项目:国家自然科学基金(60573141,60773041);江苏省自然科学基金(BK2008451);国家高科技863项目(2006AA01Z439,2007AA01Z404,2007AA01Z478);南京市高科技项目(2007软资127);现代通信国家重点实验室基金(9140C1105040805);江苏省博士后基金(0801019C);江苏高校科技创新计划项目(CX08B-085Z,CX08B-086Z)
作者简介:贺 锋(1983-),男,江苏连云港人,硕士研究生,研究方向为计算机网络、对等计算和信息安全等;王汝传,教授,博士生导师,研究方向是计算机软件、计算机网络和网格、对等计算、信息安全、无线传感器网络、移动代理和虚拟现实技术等。

作用,这既可以使网络拥有易管理性又可以拥有 P2P 网络分散性、协作性和对等性等优点,这样 PKI 的认证思想就可以应用在拥有超级节点参加的结构划 P2P 网络中,可以有效地防止信息的泄露、篡改、欺骗和抵赖等,而且还可以使目前的 P2P 网路中的节点身份得到认证,具体的认证方式将在下文中详细地讲解,使 P2P 网络环境的用途更加广阔而不仅仅是现在的普通数据资源的共享和下载。

1 PKI 分析

PKI 技术就是利用公钥理论和技术建立的提供信息安全服务的基础设施。公钥体制是目前应用最广泛的一种加密体制,在这一体制中,加密密钥与解密密钥各不相同,发送信息的人利用接收者的公钥发送加密信息,接收者再利用自己专有的私钥进行解密。这种方式既保证了信息的机密性,又能保证信息具有不可抵赖性。目前,公钥体制广泛地用于权威认证机构(Certificate Authority, CA)认证、数字签名和密钥交换等领域。作为一种技术体系,PKI 可以作为支持认证、完整性、机密性和不可否认性的技术基础,从技术上解决身份认证、信息完整性和抗抵赖等安全问题,为网络应用提供可靠的安全保障,完整的 PKI 系统是由权威认证机构(CA)、数字证书库、证书作废系统、应用接口(Application Program Interface, API)等组成[3]。

在双方进行通信以前,必须首先确认对方身份的真实性。如果不知道正在通信的对象是谁,那么整个过程是毫无益处的,甚至会造成损失。为了保证只有事先约定好的一方才能获取机密信息,对身份进行验证就显得极为重要。这是保证通信正常进行的前提条件。PKI 的认证服务在 ITU-T X.509 标准中定义为强鉴别服务,即采用公开密钥技术、数字签名技术和安全的认证协议进行强鉴别的服务[4]。在通信过程中,发送方 A 通过自己的私钥对信息进行签名,若接收方 B 用 A 的公钥验证了该签名,则达到了验证对方身份的目的,同时该签名还可以作为不可否认的证据。PKI 的特点可以有效地应用到结构化 P2P 网络中,但 P2P 网络具有随机性、鲁棒性和不可预测性,所有在网络选用信誉值 Rep(Reputation)高的节点作为结构化 P2P 网络中的超级节点(Super Peer, SP)起到局域网中心服务器的作用,下面详细介绍身份认证算法。

2 P2P 身份认证过程

为了将 PKI 技术应用到 P2P 网络中,所以要在 P2P 网络中加入认证机构(CA),CA 设置在每个结构化 P2P 局域网的 SP 上,首先需要将结构化 P2P 网络划分为一个个局域网络,每个局域网中都有一个 SP 和一个替补超级节点(Sub Super Peer, SSP),SSP 的作用是当 SP 退出时起到替补 SP 的作用,这样可以弥补 P2P 网络的随机性和不可预测性。SP 和 SSP 在 P2P 网络中的选择由节点的 Rep 决定,SP 和 SSP 中 CA 认证文件保持同步,整个 P2P 网络中的 SP 节点组成一个特殊的结构化局域网,以方便网络中节点跨越局域网进行认证,例如 SP1 域中的节点 P1 和 SP2 域中的节点 P2 进行认证时,由于 P1 和 P2 不在同一个局域网中,首先由 SP1 和 SP2 通信取得 P2 的公钥,SP1 并将 P2 的公钥返回给节点 P1,这样 P1 就有了 P2 的公钥,这样就可以进行身份认证过程,整个过程如图 1 所示。

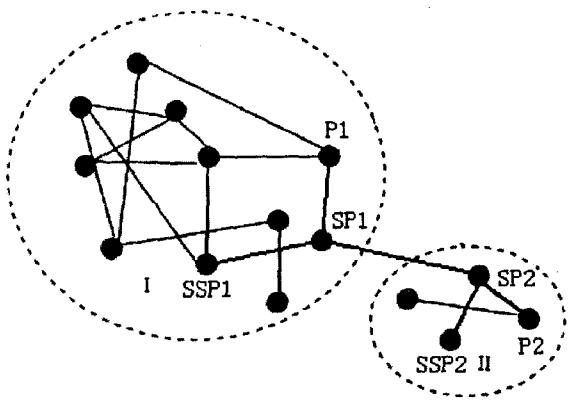

图 1 拥有 SP 的结构化 P2P 网络

上图的粗黑实线表示了节点之间通信和跨越局域网节点之间通信的方式,节点之间通信时可以选择需要身份认证方式和不认证的方式,当节点之间交易的是普通的文件时,节点可以选择不认证直接交易的方式来提高网络的效率,而当两个节点因为要进行交易秘密信息并且认证对方身份时,P2P 网络可以借助 CA 中心的作用进行节点与节点之间的身份认证和数据的加密传输,这样既保证了 P2P 网络的高效性又能保持 P2P 网络的安全性,使得 P2P 网络的用途更加广阔[1]。

节点的认证包括身份认证和公私钥的管理,新节点 P 在加入 P2P 网络之前首先去注册机构(Register Authority, RA)申请证书,注册机的功能在选定的 SP 上实现,RA 审核节点 P 是否具有获得证书的权利,当节点 P 通过 RA 的审核后,RA 将节点 P 的信息传输给认证中心(CA),CA 通过非对称加密算法 RSA 生成节点 P 公钥(Public Key, PUK)和私钥(Private Key, PRK),PUK 的长度为 320 位(bit),PRK 的长度为 1024 位[5,6],CA 将节点 P 的 PUK 和 PRK 保存在证书库中方便身份认证时对公钥的查询和对公私钥的管理,CA 同时将节点 P 的 PRK 发送给节点 P 保存,这样节点就完成了注册功能。

2.1　身份认证

在 P2P 网络环境中,节点之间交易秘密的或有价值的资源时,节点之间的交易就有身份认证的需求,例如节点 P1 向节点 P2 请求秘密资源时,节点 P2 首先要确认来访节点 P1 是不是它所声明的真正的 P1 身份,P2 就查询 CA 中心 P1 的 PUK1,然后将一个长度为 L 的随机字符串 M 加密为字符串 EM,然后 P2 将 EM 发送给节点 P1 解密,P1 将解密字符串 N 发送给 P2,P2 将 N 和 M 进行字符串匹配,如果匹配失败就退出认证;如果匹配成功,为了防止 P2 冒名顶替发送恶意文件,P1 也需要验证 P2 的身份,这样能够实现双向身份认证,身份认证具体过程如图 2 所示。

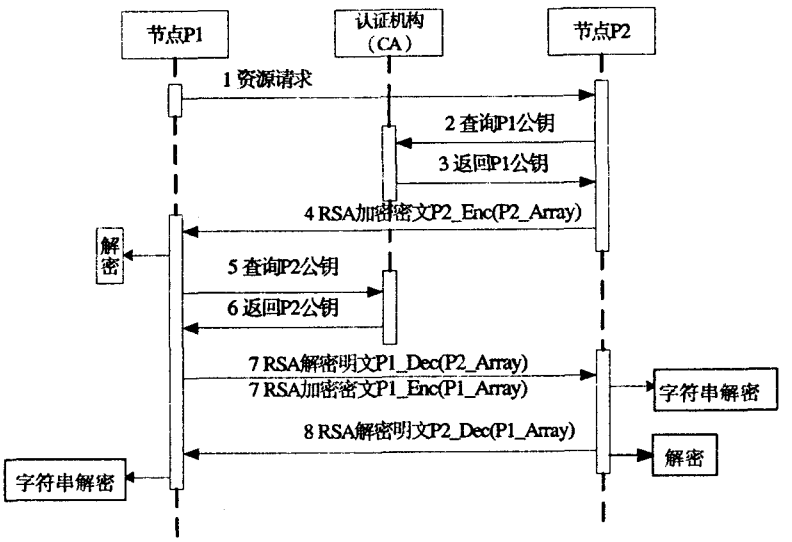

图 2　身份认证简单序列图

其中认证过程如下:

(1)节点 P1 请求节点 P2 的资源,节点 P1 向 P2 发送资源请求消息,消息中包含节点 P1 的身份标识符 PID1(Peer Identity,PID)和资源的名称。

(2)节点 P2 首先根据节点 P1 所声明的 PID1 去 CA 查找节点 P1 的公钥(P1_PUK)。

(3)CA 将节点 P1 的 P1_PUK 发送给节点 P2。

(4)节点 P2 在本地用随机序列发生器函数(RanMac())生成 40 位长度的随机序列 P2_Array 并且每次生成的序列都不一样,节点 P2 用 P1_PUK 通过 RSA 算法加密随机序列 P2_Array 得到密文 P2_Enc(P2_Array),节点 P2 将密文 P2_Enc(P2_Array)发送给节点 P1。节点 P1 用自己的私钥(P1_PRK)通过 RSA 算法解密密文 P2_Enc(P2_Array)得到明文 P1_Dec(P2_Array)。

(5)节点 P1 根据节点 P2 所声明的身份 PID2 去 CA 查找节点 P2 的公钥(P2_PUK)。

(6)CA 将节点 P2 的 P2_PUK 发送给节点 P1。

(7)节点 P1 在本地用随机序列发生器函数(RanMac())生成 40 位长度的随机序列 P1_Array 并且每次生成的序列都不一样,节点 P1 用节点 P2 的 P2_PUK 通过 RSA 算法加密随机序列 P1_Array 得到密文 P1_Enc(P1_Array),节点 P1 将密文 P1_Enc(P1_Array)和明文 P1_Dec(P2_Array)发送给节点 P2。节点 P2 首先将明文 P1_Dec(P2_Array)和 P2_array 进行字符串匹配,如果匹配失败则 P2 拒绝服务,整个过程结束;如果匹配成功,节点 P2 用自己的私钥(P2_PriKey)通过 RSA 算法解密密文 P1_Enc(P1_Array)得到明文 P2_Dec(P1_Array)。

(8)节点 P2 将明文 P2_Dec(P1_Array)传送给节点 P1,节点 P1 将明文 P2_Dec(P1_Array)和字符串 P1_Array 进行比较,如果匹配成功则进行资源交换,如果失败说明 P2 是冒名顶替身份,身份认证失败并且整个认证过程结束。

2.2　公私钥管理

PKI 系统中的证书库在用户节点注册的时候就将节点的 PID、PUK 和 PRK 都在证书库中作了备份,PUK 和 PRK 管理主要分为公私钥更新、公私钥查询和公私钥撤销。

a)公私钥更新主要是当节点觉得自己的私钥已经被窃取,或者密钥被节点自己无意中泄露,节点可以选择向 PKI 申请更新一个公私钥对保证自己的信息更加安全和自己的身份不被冒充。

b)私钥查询是节点在无意中将自己的密钥遗失(如重装操作系统,因为用户并不知道自己的密钥藏在何处,所以并不能自行备份),用户可以通过密钥查询的方式找回自己在证书库中备份的密钥,使自己的身份重新得到使用,公钥查询是节点在相互认证时常常用到。

c)公私钥的撤销功能就是节点离开 P2P 网络撤销自己身份的一种行为,使自己在证书库中的备份彻底消除,清空证书库中关于节点的所有备份数据。

由于公私钥的管理并不是要讨论的重点,所以公私钥的管理在文中只作简要的介绍,节点的信息包括节点的 PID 和节点的 PRK 等信息在本地用 XML 文件存储,如下图 3 所示,图中的密钥是截取了 1024 位长度中的一部分,因为全部显示太长。

虽然基于 PKI 的 P2P 身份认证使得 P2P 的用途更加的广阔,但是基于 PKI 技术也使得 P2P 网络环境中需要超级节点参加实现中心服务器的功能,使得

P2P 网络中超级节点的负荷过大,在进行身份认证的时候需要网络中的 CA 参与认证,而其他的时候节点与节点之间的交易依然是无超级节点参与的 P2P 方式,所以超级节点的引入并没有太大影响 P2P 网络的效率,却使 P2P 网络的用途变得广阔,增强了网络的安全性和稳定性。

3 试验结果

运用上述设计的身份认证方式运用 VC++6.0 编写了一个原型系统,系统中的公私钥产生和加解密应用程序接口(API)在 Crypto++[6,7]库中都已经给出,Crypto++库是开源的,大家可以很方便地在网上下载下来用,程序员只要将其编译成相应的库就可以很方便地调用了。文件下载的流程是当用户选择要下载的文件时,客户节点首先要通过服务节点的身份认证,当认证通过时就可以顺利地进行文件下载,如果认证失败,客户端节点就会弹出认证失败的消息框。图 4 中的认证失败是通过数据包回放对认证进行攻击,系统可以有效地防止数据包回放攻击。

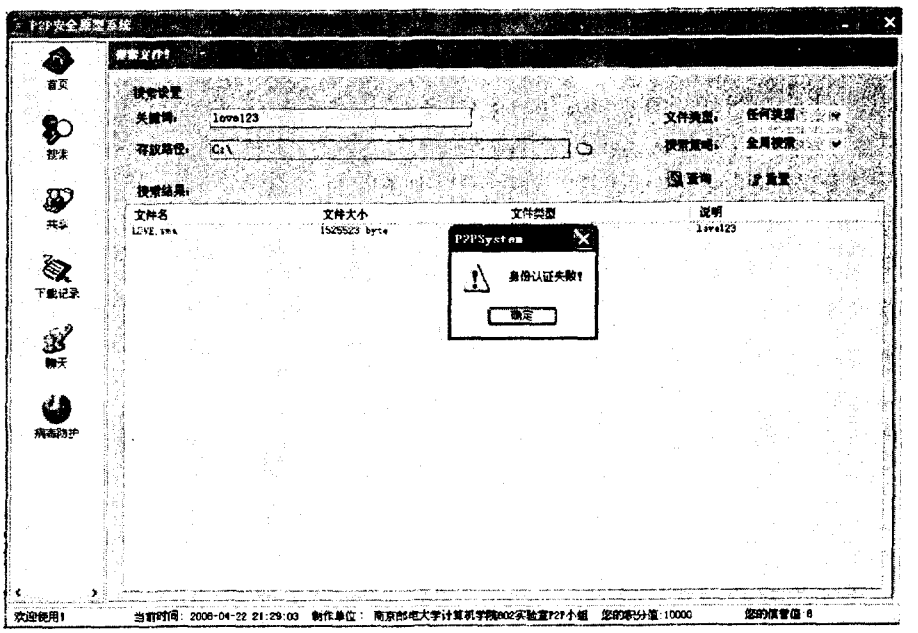

图 4 实验编写的原型系统

```
- <xmlRoot>
    - <P_InFo>
        <PeerID>7883DBFB5875A0B88F5F0FCA09072D2045A4844A</PeerID>
      </P_InFo>
    - <PriKey>
        <privatekey>B6BB23C1EDC81D9D3B8C0877505D55A6029D71D70E29B71024
                    035B0252F7DB6893A6C404BA3AA6FDF72F092D2AA516516EE2F
                    20E0808ED713EACA3D01A8395753B657801817C1BA59AAAE13E
                    C1B1EB2ECDA6FC776BEA1E55DB1024056038 5F3702C7EDE8912
                    7D3CC6870274936BAD7084D0A74F4954812D86684C53DD56AB
                    1C13BCCCA3A8265DBCDD41272F954C10C71DB4939780713504
                    93641B74</privatekey>
      </PriKey>
  </xmlRoot>
```

图 3 节点信息 XML 图

(1) 优点:

* 通过每次改变被加密的字符串可以有效地防止重放攻击,比通过数字签名更有效的实现身份认证。

* 认证是双向的,不仅可以防止客服端节点冒充欺骗也可以防止服务节点的冒名顶替。

* 身份认证可以用在许多的不同的系统认证中,用节点 PID 作为索引可以在一张密钥表中查找正确的密钥,这样可以在一个系统中支持多个 PID/PRK,在会话中随时改变密钥。

(2) 缺点:

* 身份认证要求密钥以明文的形式存在,无法使用通常的不可恢复加密口令数据库,这在大型设备中不适用。

* 节点在注册的时候,CA 将密钥在网络中传输。

4 结束语

在 P2P 网络被大量应用的今天,P2P 网络成为一种新型的网络结构被大家所熟悉,然而目前的 P2P 网络主要被用于普通资源的共享和下载,功能比较单调和简单,而造成这样结果的主要原因之一是 P2P 网络安全得不到保证,身份认证又是网络安全的重要组成部分。所以文中提出的基于 PKI 的 P2P 身份认证技术可以有效地防止节点身份被冒充、欺骗、篡改和抵赖等攻击行为,而且文中的加密技术又区别于数字签名可以有效地防止报文回放攻击,这样就可以使得 P2P 网络变得更加安全,相信当 P2P 网络模式像现在的客户机/服务器(C/S)网络模式一样安全的时候,P2P 网络的用途将会是无处不在。

参考文献:

[1] 张国治,党小超,魏伟一.基于信任域的 P2P 访问控制模型研究[J].计算机技术与发展,2006,16(8):228-230.

(下转第 188 页)

DNS服务器用于将域名转换为其对应的 IP 地址。有了 DNS 服务,使用者就能通过在浏览器中输入域名来直接访问该系统,而不必输入该系统所在服务器的 IP 地址和访问端口号[7]。

系统发布时打包成为标准的 Windows Installer 安装程序包,可直接在安装包上双击执行。安装程序自动搜索并列出目标计算机 IIS 中可用的站点,在"Site"中选择将程序部署在哪个站点下,Virtual Directory 为虚拟目录名,在此指定为高校进修人员管理系统,单击下一步自动完成安装。

安装结束后,在 IIS 中找到"高校进修人员管理系统",右键点击"浏览"将出现系统默认的页面,部署工作完成(如图 4 所示)。

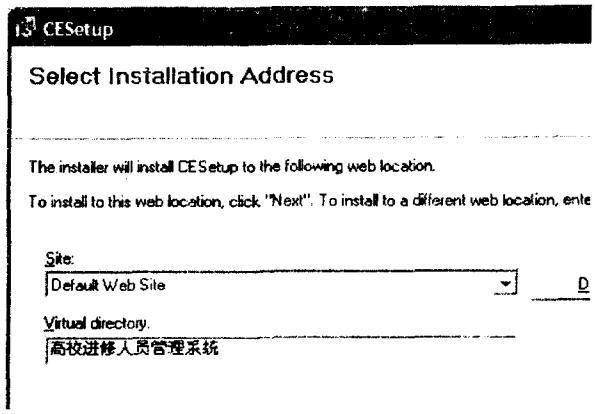

图 4 用 Windows Installer 安装本系统

除此之外,系统还可以通过 XCOPY 的方式将本站点所有内容直接拷贝到目标计算机 IIS 指定的虚拟目录下进行安装。

5 结束语

系统采用 B/S 架构模式设计,完全基于浏览器界面,安装方便,客户端只需安装普通的 IE 浏览器即可使用。CDM 不具体依附某一 DBMS,只是描述了数据库整体逻辑结构,通常包含了与具体物理数据库无关的数据对象,开发人员可以不受不同数据库管理系统实现上会有区别的影响,专心于数据库自身的设计中,通过 PDM 构建的数据库能充分发挥每种 DBMS 自身的特性。系统在安全上提供用户权限、密码验证并结合了操作系统、数据库的安全管理机制等各种安全策略,为系统正常运转提供安全保障。

参考文献:

[1] 魏宗秀.用 DIV 与 CSS 设计易于改版的 JKL 信息网页[J].淮北煤炭师范学院学报,2006,27(3):40-42.

[2] Jeffrey R. Applied Microsoft. NET Framework Programming [M]. US: Microsoft Press, 2002.

[3] 王 蕾,李培峰,杨季文.基于 ASP.NET 的 Web 应用系统架构探讨[J].计算机工程与设计,2006,16(7):55-58.

[4] Norman R J. Object - oriented Systems Analysis and Design [M].北京:清华大学出版社,2000.

[5] 陈 渝,秦开大,田 亮.基于 PowerDesigner 的信息系统数据建模建设[J].昆明理工大学学报:理工版,2004,29(1):45-47.

[6] 周晓锋.高校进修人员管理系统[D].芜湖:安徽工程科技学院,2007.

[7] 赵 玮,唐 亮,张结魁.基于.NET2.0 的旅行社管理信息系统的设计与实现[J].计算机技术与发展,2007,17(12):158-161.

(上接第 180 页)

158-165.

[5] 肖 龙,方 勇,戴忠坤.基于模糊神经网络的信息系统风分析[J].计算机应用研究,2006(5):137-139.

[6] 杨慧敏,付 萍.基于熵权的多级模糊综合评价的应用[J].华北电力大学学报,2005(5):105-106.

[7] Zhao D M, Zhang Y Q, Ma J F. Fuzzy risk assessment of Entropy-weight coefficient method applied in network security [J]. Computer Engineering, 2004, 30(18): 21-23.

[8] 陈 亮.信息系统安全风险评估模型研究[J].中国人民公安大学学报:自然科学版,2007(4):51-52.

[9] 梁保松,曹殿立.模糊数学及其应用[M].北京:科学出版社,2007:146-147.

(上接第 184 页)

[2] 屈晓辉.网络安全身份认证研究[M].北京:清华大学出版社,2006.

[3] 范林秀,陈舒娅,王喜进.基于 PKI 的身份认证在电子商务中的研究[J].电脑知识与技术,2007,16(9):979-980.

[4] 徐小平,尹颖禹.基于数字签名的身份认证模型的一种方案[J].计算机技术与发展,2006,16(2):121-123.

[5] 邢长明,刘方爱.基于 P2P 的网格资源发现机制研究[J].计算机技术与发展,2006,16(8):21-24.

[6] Isomura M, Decker C, Beigl M. Generic Communication Structure to Integrate Widely Distributed Wireless Sensor Nodes by P2P Technology [EB/OL]. 2006-04. http://www.teco.edu/michael/publication.

[7] Ripeanu M, Foster I, Iamnitchi A. Mapping the Gnutella network: Properties of large-scale peer-to-peer systems and implications for system design[J]. IEEE Internet Computing, 2002, 6(1): 50-57.