基于 SSL 的 P2P 安全通信模型*)

王 涛 卢显良 段翰聪
(电子科技大学计算机学院 成都 610054)

摘 要 安全问题是限制 P2P 网络发展的重要因素,现有的模型不能很好地保证 P2P 节点间通信数据的真实性,保密性和完整性。针对上述问题,提出一种基于 SSL 的 P2P 安全通信模型,采用分布式 CA 和 SSL 协议对 P2P 节点间的通信安全加以保障。模型采用层无关技术,可以方便地插入到现有的 P2P 模型中。仿真试验结果表明,该模型可行且高效。

关键词 P2P,身份认证,SSL,安全

A Novel P2P Secure Communication Model Based on SSL

WANG Tao LU Xian-Liang DUAN Han-Cong
(College of Computer Science and Engineering, UESTC, Chengdu 610054)

Abstract Security is always the main problem which restricts the development of P2P networks. Current models can't guarantee the authenticity, confidentiality and integrity of the data in P2P communication. To address these problems, this paper presents a novel SSL-based P2P secure communication model. The distributed CA and SSL mechanism are provided in the model. By using layer-independence technique, the model can be inserted into existing P2P networks easily. Results of simulations show that the proposed model is feasible and efficient.

Keywords P2P, CA, SSL, Security

1 引言

P2P 网络摒弃了传统的 C/S 模式,每个节点既充当客户机,享用其它节点提供的服务,同时也充当服务器,为其它节点提供服务。这种开放性的体系结构,对分布式存储、分布式计算、分布式协作等应用带来诸多方便。因此,P2P 被广泛应用于各种娱乐和商业环境中。然而,随着网络攻击和冒名交易的增加,安全问题成为制约 P2P 网络发展的重要因素。

为了保证 P2P 系统中节点通信的安全性,研究人员提出了多种方案。文[1]在 P2P 系统中引入一个可信赖的第三方,负责节点的注册管理和监视,该机制起到了一定的安全管理作用,但其需要中心服务器的支持,有悖于 P2P 无中心节点的初衷,同时无法避免单点故障。SUN 的 JXTA[2]采用 Javacard. Security 安全服务程序包来给基于 JXTA 平台的 P2P 应用提高安全性。而 Intel 的 P2PTL (Peer-to-Peer Trusted Library)[3]专门提供了一些安全程序包来保证 P2P 应用的安全,包括了认证服务 Identity,加密服务 Store 和密钥管理服务 Key 的程序包。上述的几种开发工具都只适合开发全新的 P2P 安全应用,并不适合用来把已有的 P2P 模型改造成安全的 P2P 模型。

本文旨在构造一个通用的 P2P 网络安全通信模型,采用分布式 CA (Certification Authority)和 SSL 安全套接字协议来提供 P2P 网络中节点身份认证,数据传输保密和数据的完整性。模型采用层无关技术 Layer-independence(即第 n 层的实现和修改不影响第 $n-1$ 和第 $n+1$ 层的实现),使得安全机制对所有 P2P 网络应用提供透明性服务,并可以方便地插入到现有的 P2P 系统中。

文章第 2 节对 P2P 网络中的安全问题进行详尽的分析,第 3 节提出了 P2P 分布式 CA 和 SSL 的安全通信机制,第 4 节给出了仿真试验和结果分析,最后对全文进行总结。

2 P2P 网络的安全问题分析

P2P 网络中各节点间的信息传递面临的安全威胁[4]主要有:身份被假冒,信息被窃取和信息被篡改等。

·身份认证和授权(Certification Authority)。P2P 节点互不相识,要使交易成功,首先要能确认对方身份的合法性。防止假冒节点和未授权节点的访问。

·数据保密性(Confidentiality)。P2P 是建立在一个开放的网络环境中,节点间的信息若以明文的方式传输,有可能被非授权的第三方窃取,而导致信息泄漏。

·数据完整性(Integrity)。数据传输中信息的丢失,重复和乱序等都会导致信息数据不可用。因此,P2P 中的信息传输要能做到确保完整性。

针对上述的三个问题,本文基于 SSL 给出了如下解决方案:

身份认证。利用证书技术和可信的第三方 CA(Certification Authority),交易的节点间进行双向认证。为了验证证书持有者是其合法用户(而不是冒名用户),SSL 要求证书持有者在握手时相互交换数字证书,通过验证来保证对方身份的合法性。

保密性。节点间通过密码算法和密钥的协商,建立起一个安全通道。以后在安全通道中传输的所有信息都经过了加

*)电子信息产业发展基金资助项目,编号:信运部[2002]-546。王 涛 博士研究生,主要研究方向:分布式文件系统,P2P 计算。卢显良 教授,博士生导师,主要研究方向:计算机网络,操作系统,信息安全。段翰聪 博士研究生,主要研究方向:分布式系统,P2P 计算。

密处理，网络中的非法窃听者所获取的信息都将是无意义的密文信息。

完整性。SSL 利用密码算法和 hash 函数，通过对传输信息特征值的提取来保证信息的完整性。

SSL 协议的实现属于 SOCKET 层，处于应用层和传输层之间。SSL 由两个共同工作的协议组成：SSL 记录协议（SSL Record Protocol）和 SSL 握手协议（SSL Handshake Protocol）[5]。SSL 记录协议建立在可靠的传输协议（如 TCP）之上，为高层协议提供数据封装、压缩、加密等基本功能的支持；SSL 握手协议建立在 SSL 记录协议之上，用于在实际的数据传输开始前，通信双方进行身份认证、协商加密算法、交换加密密钥等。

3 P2P 中安全通信的设计

SSL 中基于 X.509 数字证书[6]的双向认证机制能够为 P2P 网络中各节点之间的安全通信提供透明认证。

3.1 P2P 中 CA 的构建

P2P 网络要求尽量避免中心节点的存在，而单个 CA 中心，势必成为 P2P 网络性能的瓶颈[7]。更为重要的是，单个 CA 中心的崩溃将会造成整个 P2P 网络无法获得认证，致使 P2P 网络完全失去安全性。

多个 CA 分布式协作的方式可以避免上述问题，具体到 P2P 网络中，为了不增加额外的认证服务器，我们采用超节点的思想，让 P2P 网络中计算能力强，存储容量大，高带宽，低延迟的节点成为超节点，充当 CA 中心。超节点在实现自身 P2P 应用的同时，提供认证服务。节点获取证书时，根据网络连接情况，就近选取合适的 CA，如图 1 所示。

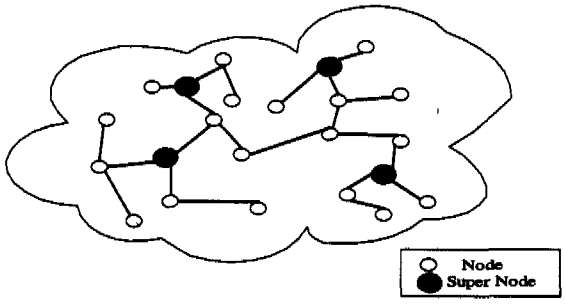

图 1 P2P 网络中 CA 分布图

P2P 节点间的双向认证根据其所属 CA 是否相同分为区域内和区域间认证，如图 2 所示。

区域内部认证：如果 $N1$，$N2$ 之间进行双向认证，可以通过本域的认证服务器 CA1 进行。

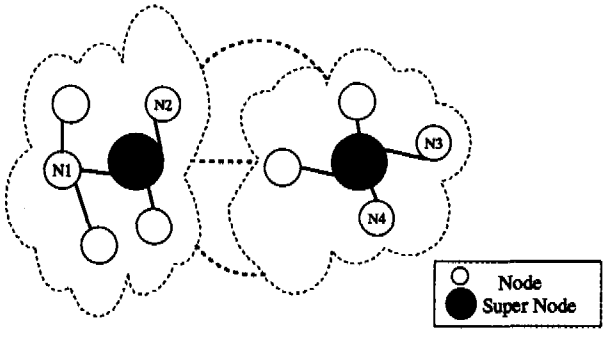

图 2 P2P 网络中节点认证过程

区域间的认证：如果 $N1$ 要和另外一个区域的节点 $N3$ 进行安全通信，它们之间的认证过程是 $N1$ 向自己区域的 CA1 进行通信，CA1 判断目的节点 $N3$ 在另外一个区域，CA1 向 CA2 请求为 $N1$ 和 $N3$ 之间分配一个会话密钥。CA2 产生好会话密钥后，直接传给 $N3$，并且通过 CA1 转发给 $N1$，这样 $N1$ 和 $N3$ 就可以进行双向认证。

3.2 P2P 安全通信建立

通信的节点双方在握手连接前必须获取对方的公钥证书及 CA 的公钥证书，而握手协议实现了 P2P 节点间的双向身份鉴别、密钥交换和保密会话。在达到安全通信之前，握手协议需进行 4 次交互，节点 A 和节点 B 的握手过程如图 3 所示。

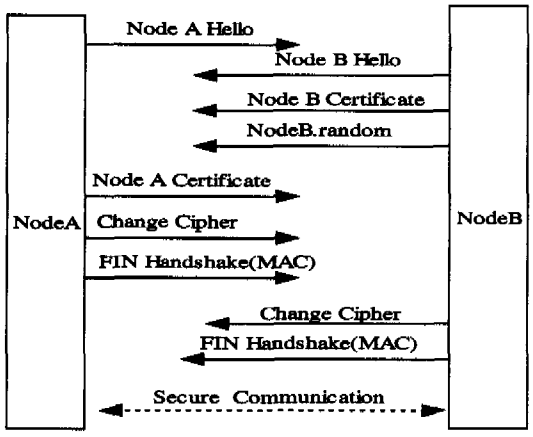

图 3 节点 A 和节点 B 的 SSL 握手过程

1）节点 A 与节点 B 建立握手连接，成功后向其发送会话序列号、加密说明及节点 A 随机数 NodeA. random。

2）节点 B 收到节点 A 发来的信息，并将会话序列号、加密说明、节点 B 公钥证书、节点 B 随机数 NodeB. random 及节点 B 密钥交换信息（用节点 B 私钥（N，ssk）加密后的节点 A 随机数）$X \equiv NodeA.\ random^{ssk} \pmod N$ 发送给节点 A。

3）节点 A 用 CA 的公钥验证节点 B 公钥证书的合法性，再用节点 B 的公钥（N，spk）验证节点 B 的身份。即

$$NodeA.\ random \equiv X^{spk} \pmod N \equiv NodeA.\ random^{ssk \times spk} \pmod N \quad (1)$$

若式（1）成立，则确认节点 B 身份。然后，将改变加密规格说明、节点 A 公钥证书和节点 A 密钥交换信息，包括用节点 A 私钥（N，csk）加密后的节点 B 随机数 $Y \equiv NodeB.\ random^{csk} \pmod N$ 和用节点 B 公钥加密后的节点 A 随机产生的前主密钥 $B \equiv PreMasterKey^{spk} \pmod N$。

4）节点 B 用同样的方法验证节点 A 的公钥证书的合法性及其身份，并用其私钥（N，ssk）对 B 解密

$$B^{ssk} \equiv PreMasterKey^{ssk \times spk} \pmod N \equiv PreMasterKey \pmod N \quad (2)$$

通过式（2），获得前主密钥 $PreMasterKey$；同时，将改变加密规格说明发送给节点 A，表示同意用协商好的加密规格进行通信。

通过上述握手过程，通信双方获得了 3 个共享的随机数，即 $NodeA.\ random$，$NodeB.\ random$ 和 $PreMasterKey$。以它们作为参数可以动态生成主密钥，报文加密密钥和报文认证密钥。

至此，节点 A 和 B 完成双向认证，并协商一份共享的会话密钥和相关的安全通信参数，建立了安全连接，P2P 应用程

序可以进行安全通信。

3.3 P2P 中的密钥交换协议

本系统采用 RSA 密钥交换协议，其安全性建立在大整数分解大素数因子的数学难题上。其安全素数生成算法基于文[8]的下述定理。

定理 1 设整数 F 的素因子分解为 $F=\prod_{i=1}^{s}q_i^{l_i}$，$q_i$ 为素数，l_i 为正整数，$P=2RF+1$，R 为整数；如果存在整数 a，使得

$$\begin{cases} a^{P-1}\equiv 1(\bmod P) \\ \gcd(a^{(P-1)/q_i}-1,P)=1(i=1,2,\cdots,s) \end{cases} \tag{3}$$

则 P 的每个素因子是形如 $mF+1$ 的素数，$m>1$；再者，如果 F 为大于 R 的奇数，或 $F>\sqrt{P}$，则 P 为素数。

4 仿真试验

为了评估本文提出的 P2P 安全通信模型，我们进行了一系列的仿真试验。仿真的应用场景是 P2P 网络中文件共享。试验环境为 5 台 PC(CPU：PIII 1G，RAM：256M，OS：Linux)通过 100M 以太网互联。试验仿真了 2000 个节点的 P2P 网络，其中 CA 中心 5 个，共享文件 5000 个，随机分配到所有节点上。节点对共享文件的请求是随机的，每个用户在仿真过程中平均完成至少 20 次交易。

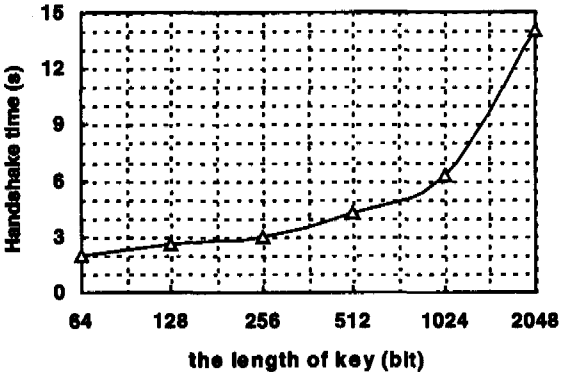

图 4 握手时间随密钥长度的变化

我们仿真了密钥长度在 64～2048 位的证书密钥和密钥交换过程，比较了相应情况下 P2P 的安全握手协议消耗的时间，结果如图 4 所示。

从图 4 中可以看出，密钥长度越长，将会导致握手时间延长，这是因为密钥的加密解密速度，以及 CA 证书在网络中的传送速度，将受密钥长度的影响。密钥越长，其被破解的可能性就越小，安全性也越高，但为之花费的处理时间也越长。仿真试验中，当采用常见的 1024 位密钥时，节点双向认证的握手时间在 6.2 秒。这时对 P2P 服务延迟的影响较小，而 P2P 网络通信安全也获得足够的保证。

结论 本文对 P2P 网络中存在的安全问题进行了分析，提出了一个 P2P 安全通信模型。模型采用分布式的 CA 认证中心，并在节点通信中使用 SSL 协议。通过分析和仿真试验说明，该模型能够保证节点间通信的安全性，达到了设计的目标并具有较好的性能。

参 考 文 献

1 Golle P, Leyton-Brown K, et al. Incentives for Sharing in Peer-to-Peer Networks. In: Proceedings of the ACM Conference on Electronic Commerce, Oct. 2001

2 Detsch A, Gaspary L P, et al. Towards a flexible security framework for peer-to-peer based grid computing. In: Proc. of the 2nd workshop on Middleware for grid computing, Oct. 2004

3 McKean C. Peer-to-Peer Security and Intel's Peer-to-Peer Trusted Library. SANS Institute Information Security, Aug. 2001

4 Bailes J E, Gary F. Managing P2P security. Communications of the ACM, Sep. 2004

5 Gupta V, Gupta S, Chang S. Performance analysis of elliptic curve cryptography for SSL. In: Proceedings of the ACM workshop on Wireless security, Sep. 2002

6 Chadwick D W, Otenko A. The PERMIS X. 509 role based privilege management infrastructure. In: Proceedings of the seventh ACM symposium on Access control models and technologies, California, Jun. 2002

7 Zhou Lidong, Schneider F B, Van Renesse R. A secure distributed online certification authority. ACM Transactions on Computer Systems (TOCS), Nov. 2002

8 Hastad J, Naslund M. The security of all RSA and discrete log bits. Journal of the ACM (JACM), Mar. 2004

(上接第 83 页)

4 系统性能评估

综上所述，本模型不仅解决了在应用层实现 Anycast 技术的网络负载问题，同时也解决了在 IP 层难以实现的采用多种距离度量方式查找最佳 Anycast 成员的问题，以及在客户与服务器之间可能存在的通信问题。最重要的是，本模型解决了在 IP 层存在的扩展性问题，而且 Anycast 成员在地理位置上分布越广泛，其提供服务的性能会越强大。所以，本模型是一个可扩展的、低消耗的 Anycast 通信模型，它根据每个 Anycast 组成员的当前状态，将客户的服务请求均匀地分布到各个成员中去，以便为用户提供最好的服务，同时，本模型还提供了 Anycast 组成员不可达的保护机制，极大限度地保证为客户提供优质服务。

本模型与当前的网络应用程序以及协议都能很好地兼容，因为本模型对路由器没做任何修改，只对 DNS 服务器、客户端的应用程序以及服务器稍加改动。

在本模型中，由于 Anycast 控制器与客户端之间的信息交换可以认为是在本地网络中实现的，因此对整个网络的性能基本上没有任何影响。虽然 Anycast 控制器的查询消息会占用一些网络资源，但是它的使用并不频繁，所以，对网络的主干网也不会有任何的影响。

目前，该模型在 IPv6 的模拟环境下运行良好。

结束语 Anycast 是 Ipv6 的一个新特性，它可以支持许多服务。本文在 IPV6 的模拟环境下，提出了实现 Anycast 服务的一种新的加权模型，用以解决当前在应用层以及 IP 层实现 Anycast 服务所存在的一些问题。Anycast 作为一种新型的通信模式，具有广泛的前景，但是它还存在许多问题，有待进一步探讨和研究。

参 考 文 献

1 Partridge C, Mendez T, Milliken W. Host anycasting service. RFC 1546, 1993

2 Deering S, Hinden R. Internet Protocol Version 6 (Ipv6) specification. RFC 2460, 1998

3 Hinden R, Deerings. IP version 6 addressing architecture. RFC 2373, 1998

4 Hagino J itojun, Ettikan K. An analysis of Ipv6 anycast Internet Draft. Internet Engineering Task Force, 2001

5 JohnSon D, Deering S. Reserved Ipv6 Subnet anycast addresses. RFC2526, 1999

6 Katabi D, Wroclawski J. A framework for scalable global IP-Anycast (GIA). In: Proc. of SIGCOMM, New York: ACM Press, 2000. 3～15

7 Narten T, Nordmark E, Simpson W. Neighbor discovery for IP version 6 (Ipv6), RFC 1970, 1996

8 Huitema C. Routing in the internet. Prentice Hall, 1996