基于自适应认证的 P2P 安全通信模型

张敏霞,黄 剑
(浙江工业大学 信息工程学院,浙江 杭州 310023)

摘要:P2P 网络通信安全是制约其发展的重要因素,现有的模型虽然能保证通信节点间数据的真实性、保密性和完整性,但是却会带来很大的开销或系统的不稳定。针对上述问题,提出了一种基于自适应认证的 P2P 安全通信模型,采用 Certification Authority (CA)认证和 CA 监管机制,保障了系统的稳定性,并且只需要较小的开销,即可为 P2P 安全通信模型提供了一种新的思路。本模型可方便地加入到现有的 P2P 网络中。安全分析和仿真实验结果进一步表明,本模型具有有效性和可行性。

关键词:点对点;安全通信;认证;监管
中图分类号:TP393 **文献标识码**:A **文章编号**:1001 - 4551(2010)03 - 0067 - 04

A P2P security communication model based on adaptive-authenticity

ZHANG Min-xia, HUANG Jian
(College of Information Engineering, Zhejiang University of Technology, Hangzhou 310023, China)

Abstract: The secure of P2P networks communication is the main problem which restricts the development of P2P networks. Current models can guarantee the authenticity, confidentiality and integrity of datas in P2P networks communication; however, they bring great overhead or instability. Aiming at solving these problems, a novel P2P security communication model based on adaptive-authenticity was presented, CA (Certification Authority) and CA supervise mechanism were used, the stability of P2P and less overhead were guaranteed, and a new thought in P2P security communication model was provided. The model can be joined into existing P2P networks easily. The test results indicate that the proposed model is efficient and feasible.

Key words: point to point(P2P); security communication; authenticity; supervise

0 引 言

P2P 网络是一种不依赖中心服务器、没有固定网络拓扑结构、每个节点都可以充当服务器的网络模型。P2P 网络的这种开放的特性,使得它在分布式计算、分布式协作、信息共享等领域有着广泛的应用。但是,P2P 网络本身也存在安全缺陷,这是由于 P2P 网络无节点能够对网络节点提供有效的监管,使得网络中各个节点间的信息传递面临着身份被假冒、信息被窃取和信息被篡改等安全威胁[1],因此安全问题成为制约 P2P 网络发展的重要因素之一。

目前,认证服务是保证 P2P 网络安全的极为重要的手段之一。认证服务用于为合法的用户提供有效身份证明,为通信过程提供加密服务,区分合法用户和非法用户[2]。然而,P2P 网络的开放性和随意性使得 CA 认证不能直接应用于 P2P 网络。

本研究提出一种基于分布式自适应认证的 P2P 网络安全通信模型,采用 CA 来提供认证服务,并提出 CA 监管机制以管理 CA。模型具有通用的特性,可以加入到现有的 P2P 网络中以提供安全服务。

1 认证服务的安全问题分析

目前,在 P2P 网络中的认证模型主要有 3 类:文献[3]中的集中式的认证模型,文献[4-5]中的分布式认

收稿日期:2009 - 08 - 20

作者简介:张敏霞(1969 -),女,浙江宁海人,副教授,硕士生导师,主要从事网络计算、信息安全、嵌入式系统方面的研究. E-mail: zmx@ zjut.edu.cn

证模型,以及文献[6-7]中的基于门限密码的分布式密钥管理认证模型。在集中式的认证模型中,系统只有一个 CA 负责提供网络中所有节点的认证服务,然而单个 CA 中心必然会造成 P2P 网络的性能瓶颈[8],而且存在单点瘫痪的危险。在分布式认证模型中,系统有多个 CA,每个 CA 负责一定数量节点的证书签发和管理,当一个或多个 CA 受到攻击或因为其他的原因不能提供认证服务时,会造成系统不稳定,甚至瘫痪。在分布式的密钥管理认证模型中,将一个 CA 分配到网络中的 n 个节点上,由这 n 个节点中的任意 k 个节点合作签发证书。每个申请认证的节点都必须与任意 k 个节点建立通信并成功申请到 k 份证书,最后将 k 份证书合成一份有效的证书。如果 k 个节点中任意一个节点通信中断或返回证书错误,则无法合成有效证书,将导致申请失败,必须重新再找 k 个节点开始申请。该模型虽然防止了单点瘫痪,但是延长了服务的时间,增加了网络的负载,降低了认证的成功率。

本研究提出自适应的认证模型,加入对 CA 进行监管的机制,从而提高系统的效率、稳定性和抗攻击性。

2 自适应认证模型的设计

本模型将网络中的节点分为 3 类:认证节点 CA,监管节点 SP,普通节点 CP。其中,每个 CA 节点只为其管理的节点提供认证服务,一个 CA 节点只管理 P2P 网络中的部分节点。SP 节点对 P2P 网络中所有的 CA 节点进行监管。网络的拓扑结构如图 1 所示。

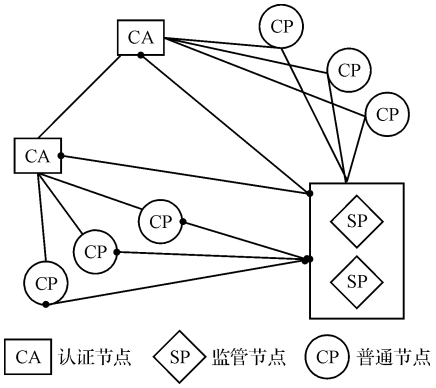

图 1 网络拓扑结构图

2.1 系统构建

从整个 P2P 网络的节点中挑选出一定个数的计算能力强、带宽高、存储容量大、可信度高的节点作为 SP 节点,记为 SP_i,每个 SP 节点都以 $<SP_i, ID>$ 的形式存储着其他 SP 节点的信息,其中,ID 为 SP_i 的网络惟一标识符,例如可以是 IP 地址。网络中所有的 CA 节点由 SP 节点组通过投票的方式选出,投票选取规则为:SP_i 节点选取一个带宽高、性能好的节点作为候选节点,并以广播的形式将选票 $vote<ID, SP_i, T>$ 发送给其他 SP 节点,其中,ID 为 SP_i 选出的候选节点的网络惟一标识符,SP_i 为发送选票的 SP 节点,T 为发送选票的时间。每个 SP 节点收到选票后,查看选票的发送时间 T 及不等式 $T_{now} - T < T_{dim}$,其中 T_{now} 为当前时间,T_{dim} 为系统设定的一个有效期。若满足该不等式,则记录下选票,否则,视为废票。SP 节点统计收到的选票,将票数最多的节点作为选取的节点,若有若干个票数相等的节点,则选取 i 值最小的节点作为选取节点。

2.2 证书发放

模型中的 CA 节点除了实现自身网络应用的同时,还为其所管理的节点提供认证服务。需要进行认证的节点 P 先产生一对非对称加密密钥,将证书认证请求 $Cert<username, ID, PK, T_{start}, T_{expir}>$ 发送给其所属的 CA 节点,其中 username 为节点 P 的用户名,ID 为节点 P 的惟一标识符,PK 为节点 P 自身产生的公钥,T_{start} 为认证请求发送的时间,T_{expir} 为证书有效时间。CA 节点收到请求后,产生证书 $<$P's username, P's ID, P's PK, T_{start}, T_{expir}, Signature$>$,其中,Signature 为 CA 的签名,最后,CA 将证书返回给请求认证的节点。

2.3 证书的撤销和更新

为了有效抵抗恶意节点的攻击,模型采取证书撤销和更新机制。网络中的证书必须满足 $T_{now} - T_{start} < T_{expir}$ 才有效,反之,则认为是过期证书。如果节点 P 提供的证书是过期的,那么其他节点将不能为其提供 P2P 应用服务。证书一旦过期,节点 P 必须更新证书。首先产生一对新的非对称加密密钥,然后发送证书更新请求 $Certupdate<username, ID, PK', T_{start}', T_{expir}'>$ 给 CA,CA 节点收到请求后,产生证书 $<$P's username, P's ID, P's PK', T_{start}', T_{expir}', Signature'$>$,并将证书返回给请求节点 P。

2.4 安全通信设计

在两个节点通信之前,必须先确认对方身份,为了防止重放攻击,双方需发送身份证书及一个随机数。当双方建立起通信通道后,发送的信息采用对方的公钥加密、自身的私钥签名。安全通信通道的建立过程如图 2 所示。

(1) 两个节点都向对方发出自己的证书,双方收到对方证书之后,用 CA 的公钥检查证书的合法性,如果证书不合法则返回一个警告信息,要求对方及时更新证书。

(2) 当双方证书都合法时,双方互相发送一个用

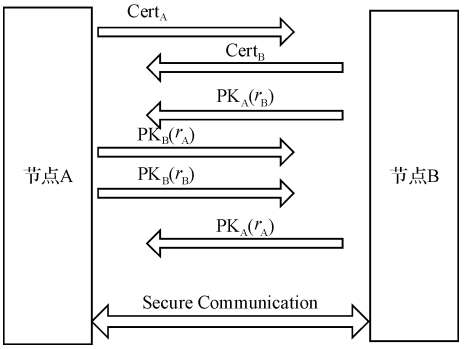

图 2　安全通信通道建立过程

对方公钥加密过的随机数 PK(r)。

(3) 当节点收到 PK(r)后,用自身的私钥解密得到随机数 r,并用对方的公钥加密 r,得到 PK′(r),然后发送回去。

(4) 双方收到 PK′(r)后,核对随机数 r,如果与自身节点发出的不同,则返回一个错误信息,若相同,发出一个握手信号,建立起通信信道。

2.5　监管机制

P2P 网络中的节点都具有随意性,CA 作为提供认证服务的节点,一旦因为“性能或网络带宽下降及受到攻击”等原因而不能为其他节点提供认证服务,就会造成系统不稳定,甚至瘫痪。本模型提出了监管机制,由 SP 节点组对所有 CA 的认证服务进行监管。如果发现某个 CA 不能正常提供认证服务,则及时选取其他节点替换该 CA。

模型中的节点可以在以下任意一种情况下投诉 CA:①当节点向 CA 发送证书认证请求或证书更新请求时,CA 未响应;②当节点收到证书后,检查证书,发现证书不合法。当节点要投诉时,请求投诉的节点将投诉请求 Complaint < ID, T_i, ID_{CA} > 发送给所有的 SP 节点。其中,ID 为发送投诉的节点的 ID,T_i 为发送投诉的时间,ID_{CA}为被投诉的 CA 节点的 ID。

每个 SP 节点记录下投诉请求并且统计投诉请求,若在一个时间周期 T_0 内,同一个 CA 被投诉的总数超过一个阈值 M,并且发送投诉的节点数超过 N 时(例如 N 可以是 CA 管理的 CP 总数的 1/10),则该 SP 向其他 SP 发出更换该 CA 的请求。当发出更换请求的 SP 节点数超过一个阈值 K 时(例如 K 可以是整个 P2P 网络中 SP 总数的 1/3),所有 SP 节点根据投票的方式选出新的节点替换原来的 CA 节点,最后,新的 CA 节点将信息广播给其他节点。

3　安全性分析

本模型是一种自适应认证模型,系统中的 SP 节点负责监管 CA 节点,根据运行环境的改变来管理 CA 节点。本模型的自适应性在于通过对 CA 的管理来保障系统的认证服务。当系统中的 CA 节点由于受到攻击或自身性能下降等原因而不能正常地为其管理的 CP 节点提供认证服务时,SP 节点将根据投票规则选取新的 CA 节点代替该节点;当系统中所有的 CA 节点所管理的节点数都达到上限时,SP 节点将挑选新的 CA 节点加入到网络中,以增加系统能容纳的节点数。

在模型中,通信节点在建立安全通信之前,必须先验证对方的身份证书及发送的随机数是否正确。在通信的过程中,发送的信息采用对方的公钥加密、自身的私钥签名,以防止攻击者假冒通信节点的身份进行通信以窃取和篡改信息。

系统中的数字证书都有一个有效期限,过了有效期限之后,节点必须产生新的加密密钥,更新身份证书,从而减小了攻击者破解节点密钥的潜在可能性。

在所有认证模型中,提供认证服务的节点都潜在的遭受 DoS 攻击的目标。在传统的认证模型中,一旦 CA 因为受到攻击等原因而不能为其他节点提供认证服务,那么该 CA 节点所管理的所有节点将以新节点的身份寻找新的认证节点,这样不但影响了整个系统的性能,而且造成系统的不稳定。在本模型中,当 CA 节点不能正常为其他节点提供认证服务时,节点可以对 CA 节点提出投诉,SP 节点受理这些投诉,一旦 SP 节点认定某个 CA 节点无法正常工作时,则投票选出新的 CA 节点以替代原来的 CA 节点,新的 CA 将广播一个消息通知原来的 CA 所管理的 CP 节点,所以这些 CP 节点只需更新本地的 CA 信息,而不需要以新节点的身份寻找新的 CA 进行认证,从而不影响系统在其他方面的应用,这样提高了系统的稳定性和认证效率。本研究系统由于只有部分节点投诉,系统的开销相对于所有节点寻找新的 CA 进行认证所产生的开销要小。

在本模型中,对 CA 节点的监管是由系统中所有的 SP 节点共同完成的,所以当个别 SP 节点不安全时,并不影响系统的正常运行,只有当 $S-K+1$ 个 SP 节点不能正常工作时才会造成对 CA 节点的监管失效,其中 S 是网络中 SP 节点的总个数。系统中 SP 节点总数越少,则 SP 节点不能正常工作的风险越大,但是如果 SP 节点的数目越大,则系统的网络开销也越大。攻击者必须联合 N 个节点发出投诉,这样才能使得 SP 节点更换 CA 节点,可以根据实际情况设定 N 值,以提高攻击的难度。攻击者必须对 $S-K+1$ 个 SP 节点和网络中的所有 CA 节点进行连续的攻击才能造成系统的瘫痪,这样增加了攻击的难度。

4 仿真实验

基于 Linux 平台,用 C ++ 语言实现了模型的重要功能,包括 CA 节点的选取,证书的发放、更新、撤销,以及对所有 CA 节点的监管。在实验中,仿真了 500 个节点的 P2P 网络,其中 CA 节点 5 个,SP 节点 10 个。还模拟分布式的 CA 认证模型作为对比,其中节点数为 500,CA 个数为 5。在两个实验中,为了更接近真实的环境,每个 CA 节点和 CP 节点都会在一段随机的时间后退出系统 30 min,然后再次加入到网络中。本研究分别对 RSA 密钥长度为 256 位、512 位、1 024 位和 2 048 位的情况进行了对比仿真测试,节点认证的平均时间$\bar{t}$和密钥长度 L 的关系如图 3 所示。

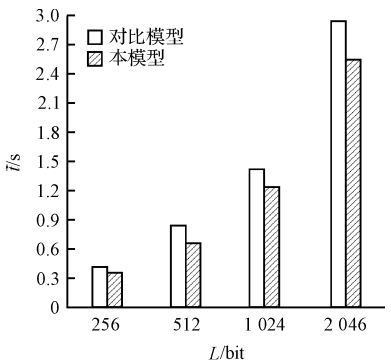

图 3 节点认证的平均时间与密钥长度的关系

从结果中可以看出,本模型中节点获取认证的平均时间要比集中式 CA 认证模型的时间短,从而提高了系统的性能。本模型中,每个 SP 节点只需要维护投诉信息表和网络中每个 CA 节点管理的 CP 节点列表,并且由于部分节点的投诉以及 SP 节点的投票而产生的网络开销要小于所有节点寻找新的 CA 进行认证所产生的开销。

5 结束语

本研究对 P2P 网络中现有的认证模型中存在的问题进行分析,提出了一种自适应的认证模型。该模型采用面向 CA 的监管机制,不仅保障了通信的安全,还保证了认证服务的稳定性,提高了系统效率。仿真实验进一步表明,该模型能够更高效地提供节点的认证,保证了通信的安全。对于模型中提出的两个阈值 M 和 K,没有计算出最优值,需要根据实际应用的情况设定最优值。

参考文献(References):

[1] BAILES J E, GRAY F. Managing P2P security[J]. **Communications of the ACM**,2004,47(9):95 - 98.
[2] 徐巧枝,刘林强,宋如顺. 一种用于 P2P 网络的访问控制模型[J]. 计算机工程与应用,2005,41(17):149 - 152.
[3] Groove Networks, Inc.. Groove Security Architecture[R]. Groove Networks, Inc.,2004.
[4] 王朝斌,王 杨,赵慧娟. 一种基于 PKI 的 P2P 计算平台设计与实现[J]. 计算机应用研究,2007,24(2):227 - 229.
[5] 王 涛,卢显良,段翰聪. 基于 SSL 的安全通信模型[J]. 计算机科学,2006,33(5):104 - 106.
[6] 刘汝正. 基于 P2P 环境的分布式数字签名研究及应用[J]. 计算机科学,2008,35(6):37 - 39.
[7] ZHOU L D, HASS Z J. Securing Ad Hoc networks[J]. **IEEE Networks Special Issue on Network Security**, 1999,13(6):24 - 30.
[8] ZHOU Li-dong, SCHNEIDER F B, RENESES-V R. A secure distributed online certification authority[J]. **ACM Transactions on Computer Systems (TOCS)**, 2002, 20(4):3 - 98.

[**编辑:**李 辉]

(上接第 62 页)

4 结束语

通过对单级旋转倒立摆系统结构和工作原理的分析,本研究建立了合理的数学模型,并对数学模型进行了线性化,为提高系统的控制效率奠定了重要的基础。对倒立摆系统分别通过极点配置和二次型最优控制进行了控制研究,并在 Matlab 中进行了仿真。通过对两种方式控制效果进行比较可知,后者具有更好的响应性能,二次型最优控制还具有算法简单等特点,在实际控制系统中有着重要应用价值。

参考文献(References):

[1] BRENIERE Y, RIBREAU C. A double-inverted pendulum model for studying the adaptability of postural control to frequency during human stepping in place[J]. **Biological Cybernetic**,1998,7(9):337 - 345.
[2] 黄菀红,梁慧冰. 从倒立摆装置的控制策略看控制理论的发展和应用[J]. 广东工业大学学报,2001,19(3):49 - 52.
[3] 蒋 珉. 控制系统计算机仿真[M]. 北京:电子工业出版社,2006.
[4] 楼建勇,林 江,钱雄伟. 注塑成型模具计算机辅助设计与工艺仿真[J]. 轻工机械,2008,26(4):24 - 28.
[5] 戴忠达,吕 林. 自动控制理论基础[M]. 北京:清华大学出版社,2001.
[6] 刘 豹. 现代控制理论[M]. 北京:机械工业出版社,2004.
[7] 陶文华. 旋转二级倒立摆的二次型最优控制研究[J]. 测控技术,2006,25(11):42 - 44.
[8] 刘 畅. 基于 CPLD 数控机床的加减速控制[J]. 现代制造技术与装备,2009(3):99 - 100.

[**编辑:**李 辉]