文章编号:2095-476X(2013)04-0074-04

基于信任域的网格认证模型

裴云霞[1], 程志蓉[2]

(1. 郑州轻工业学院 数学与信息科学系, 河南 郑州 450002;
2. 河南警察学院 实验中心, 河南 郑州 450002)

摘要:针对现有网格认证模型中PKI认证过程过于繁琐,建设和维护成本高以及IBC认证存在密钥托管的问题.研究了域内和域间资源提供者和资源请求者间的行为信任关系,利用该信任关系,在现有的组合PKI和IBC认证模型中引入临时信任域的概念,设计了基于信任域的网格认证模型.仿真实验表明,该模型具有较低的通信量和较短的认证时间.

关键词:网格;认证模型;信任域
中图分类号:TP302.7 **文献标志码**:A DOI:10.3969/j.issn.2095-476X.2013.04.018

Trust domain-based authentieation model in grid

PEI Yun-xia[1], CHENG Zhi-rong[2]

(1. *Department of Mathematics and Information Science, Zhengzhou University of Light Industry, Zhengzhou* 450002, *China*;
2. *Center of Experiment, He'nan Police College, Zhengzhou* 450002, *China*)

Abstract: Aimed at the problems that PKI authentication process is too onerous, construction and maintenance costs are high, and there is key escrow in IBC certification model in the existing grid authentication model, the behavior trust relationship between the resource providers and resource requester in the intra- and inter-domain was studied. We make use of the trust relationship to introduce the concept of temporary trust domain in the combination of the existing PKI and IBC certification model. The grid authentiation model based on the trust domain was designed. Simulation results showed that the model had low traffic and shorter authentieation time.

Key words: grid; authentieation model; trust domain

0 引言

网格是构建在互联网上的开放性、异构性的公共网络.网格安全是网格应用的基础保障,认证机制是网格安全的基础.在网格环境下,资源的分布性、异构性、动态性,决定了资源的组织形式——虚拟组织,每个虚拟组织形成独立的信任域.当用户访问资源时,需要进行域内和域间的资源访问请求和身份认证.由于网格用户请求的频发性与动态性,要求网格认证必须具备以下特点[1]:支持跨域的双向实体认证;认证过程高效;支持单点登录和委托代理.

在当前的网格安全标准中,实体间的跨域认证基于传统的公钥基础设施PKI交叉证书.认证过程过于繁琐,这对于资源申请非常频繁的网格而言,极易形成瓶颈.同时,PKI系统建设和维护的成本

收稿日期:2013-05-29
基金项目:河南省科技攻关项目(132102210056)
作者简介:裴云霞(1975—),女,河南省洛阳市人,郑州轻工业学院讲师,主要研究方向为网格安全.

高,限制了网格规模. 基于身份的认证技术虽然无证书、认证过程简便高效,但过份依赖私钥生成器,存在密钥托管的问题. 文献[2]提出的组合 IBC 和 PKI 安全认证模型中,跨域认证时采用 PKI 交叉证书,依然存在认证效率低的问题.

鉴于此,本文将以虚拟组织和信任度为基础,提出一种网格环境下基于信任域的网格认证模型,以期在不降低安全性的同时提高认证效率.

1　信任关系的描述

网格环境中,信任是对一个实体(节点)的行为和身份可信度的评估,与这个实体的可靠性、诚信和性能有关[3],可信度随实体的行为而动态变化. 一个实体的声誉是其他实体在过去与之交往的过程中所积累的对其可信度的综合评价. 网格实体间的信任取决于实体间的直接信任和间接信任,曾经交互过的实体间的信任为直接信任,而没有交互过的实体间的信任为间接信任.

1.1　域内信任关系描述

网格环境中,每个虚拟组织中设立一个域代理,如图 1 所示,域代理维护域内所有交易评价表,交易评价表记录评价节点、被评价节点、对该次交易的评价值. 在域内的每个节点维护与它有直接交易的节点的评价值表,该表记录项包括节点(node)、对该节点的总体评价值、对该节点评价的时间.

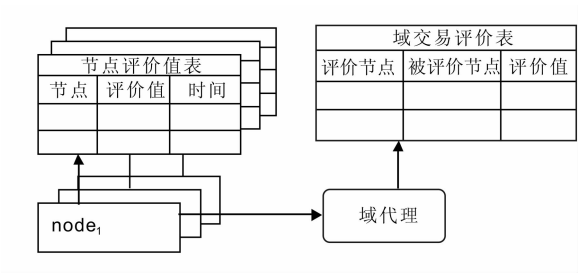

图 1　域内信任关系

定义 $R_a(b)$ 代表节点 b 在节点 a 上的声望值,其计算公式如下:

$$R_a(b) = \alpha R_a(b,dir) + \beta R_a(b,indir) \qquad ①$$

其中,α 是直接经验的比例,β 是间接经验的比例,$\alpha+\beta=1$;$R_a(b,dir)$ 表示节点 a 与 b 的直接交易经验的评价值,$R_a(b,indir)$ 是 a 对 b 的间接评价值.

$R_a(b,dir)$ 在该节点维护的评价值表中查询,该评价值为 a 与 b 所有交易评价的平均值,可以表示为

$$R_a(b,dir) = \left[\sum_{i=1}^{N} V_a(b,i)\right]^{-N} \qquad ②$$

其中,$V_a(b,i)$ 为节点 a 与 b 的第 i 次交易评价值,该值通过查询域交易评价表得到.

间接交易评价值可以表示为

$$R_a(b,indir) = \left\{\sum_{k=1}^{M}\left[C_r(a,k) \times R_k(b,dir)\right]\right\}^{-M} \qquad ③$$

其中,$C_r(a,k)$ 为节点 a 对 k 的信任值,通过查询 a 的评价值表得到;$R_k(b,dir)$ 为节点 k 对 b 的直接评价值;M 为域内其他提供反馈节点的数量. 综合式①②③即可得到节点 b 的信誉值.

1.2　域间信任关系描述

域间信任关系描述如图 2 所示. 每个自治域有一个域代理,该代理上维护 2 张表:一张是域间评价表,表中包含了所有与之有过直接交易的域的声望值,记录了交易的域名、评价值;另一张是本域节点评价表,记录了域内节点的评价值. 这里域间信任关系是指域作为一个整体与其他域之间的直接信任关系,域间节点之间的交易会影响域间信任关系. 例如域 A 和域 B 之间存在一定的信任关系,域内节点的行为可能增加或减少相应的信任值.

根据图 2 的域间信任关系,给出域间声望值的计算公式:

$$R\left(\frac{a}{M},\frac{b}{N}\right) = V_N(b)\left(\alpha T_M(N) + (1-\alpha)\frac{\sum_{U=1}^{X} T_M(U)T_U(N)}{X}\right) \qquad ④$$

其中,$T_M(N)$ 表示 M 域对 N 域的直接信任值,可以从 M 域评价表中查询;$\left[\sum_{U=1}^{X} T_M(U)T_U(N)\right]^{-X}$ 是其他域代理的声望值与其对域 N 的评价值的加权平均值;α 表示域间评价的比例,$1-\alpha$ 为域对节点评价的比例;$V_N(b)$ 表示域 N 对域内节点 b 的评价值.

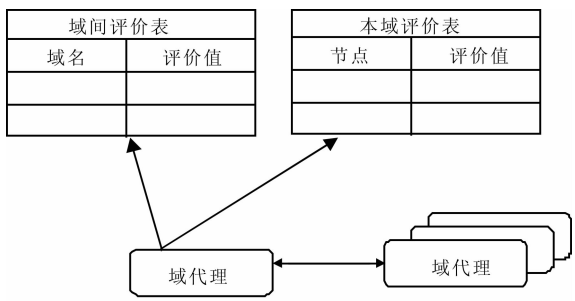

图 2　域间信任关系

2 安全认证模型

2.1 域内认证机制

网格环境下,资源的管理以虚拟组织为基本单位,同一个虚拟组织中的网格资源遵守一组共同的管理规范和共享策略. 每个虚拟组织形成独立的信任域,资源主体在加入信任域时必须通过域中认证中心的身份认证,同时也要遵守相同的本地安全管理策略.

该模型在域内采用文献[4]中提出的改进的基于身份的认证方案,域内认证机制如图 3 所示.

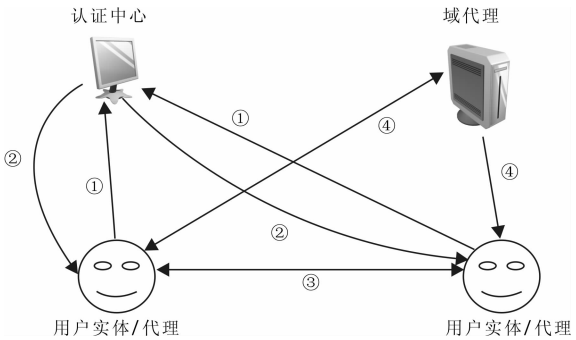

图 3 域内认证机制

图 3 中,域内认证过程如下:

①用户实体向认证中心注册.

②认证中心产生用户公钥及部分用户私钥,用户私钥最终由用户按照文献[4]的算法得出.

③域内用户实体根据文献[4]的算法进行双向认证.

④域内任何 2 个实体在认证前,可从对方实体和域代理处采用 1.1 节的算法获得对方信任值,如果对方信任值大于自己规定的门限值,则直接通信,不需要认证. 否则,按①②③步进行认证.

2.2 域间认证机制

通常情况下,网格中的许多任务需要多个自治域中的多个实体共同参与才能完成,而不同自治域中的实体之间通信时必须进行相互认证. 针对这种情况域间认证采用文献[5]提出的基于 PKI 的认证方案. 域间利用证书来交换各域的系统参数[5].

使用上述域内和域间认证机制,在网格中,任意 2 个实体在通信前能够进行安全的身份认证. 但通常网格中任务规模大且动态变化,需跨越多个自治域的资源间密切协作,并且执行同一任务的多个资源主体之间需要频繁通信,从而使得实体之间的认证过于频繁和复杂,认证效率不高.

鉴于此,本文基于信任度和虚拟组织,引入临时信任域 TTD(temp trust-domain)的概念. TTD 包括用户或用户代理、执行该任务的所有网格资源主体. 用户所在虚拟组织的网格资源调度管理中心负责对 TTD 和其中的资源进行管理. 临时信任域的构建如图 4 所示.

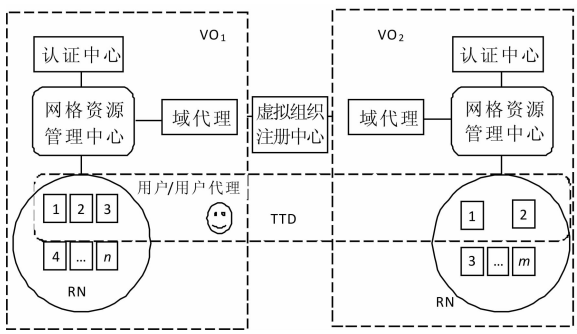

图 4 临时信任域的构建

TTD 的认证步骤如下:

1)假设 VO_1 作为本地虚拟组织,本地虚拟组织中的用户或用户代理利用本文描述的域内认证机制进行身份认证. 2)认证通过后,本地虚拟组织中的用户或用户代理向 VO_1 中的网格资源管理中心提出任务请求,该中心负责查找合适的资源给该任务,如果该中心发现有 n 个资源 $RN=\{R_1\cdots R_n\}$,但依然无法满足该任务需求,就向虚拟组织注册中心查询其他虚拟组织中的资源,假设获得虚拟组织 VO_2 中的 m 个 资源 $RN=\{R_1\cdots R_m\}$. 3)利用域间认证机制对用户或用户代理和 VO_2 进行双向实体认证. 4) VO_1 的网格资源调度管理中心在认证通过后,根据资源调度算法对任务进行分配,根据资源分配的结果,用户与本地资源使用域内认证机制进行身份鉴别,对远程资源则运用域间认证机制逐一进行身份认证. 5)认证通过后,用户用过 VO_1, VO_2 域代理获取该资源的声誉,声誉超过规定的门限值,则批准相应资源加入临时信任域. 网格资源调度管理中心将子任务分配给相应资源并在其上创建相应进程. 6)根据任务情况,各进程间进行通信时,运行进程的各资源主体,如果在临时信任域内,那么运行进程的各资源主体双方不再进行身份认证. 在任务执行过程中,临时信任域的资源可以随时增加或离开. 7)任务执行完成后,临时信任域撤销.

3 仿真实验

本文提出的认证模型使用 Gridsim 软件包进行仿真实验,实验硬件平台由 6 台当前主流配置的计

算机组成,软件平台为 Windows XP 操作系统,JSDK 1.6 和 Gridsim 5.2. 仿真实验模拟了域内、域间实体间的认证,并与文献[6]提出的 CSS、文献[7]提出的 NCSS 认证模型进行对比. 实验结果见图 5,图 6.

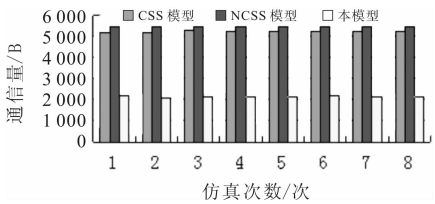

图 5　本模型与 CSS,NCSS 通信量对比

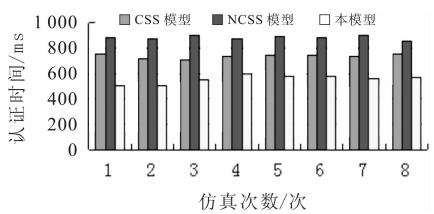

图 6　本模型与 CSS,NCSS 认证时间对比

由图 5 可以看出,本文给出的模型的通信量约为 2 100 B,而其他 2 个模型的通信量大约为 5 200 B,本文给出的模型的通信量约为其他模型的 40%. 由图 6 可以看出,本文提出的模型的认证时间约为 450 ms,而其他 2 个模型的认证时间约为 700 ~ 890 ms,本文提出的模型的认证时间约为其他模型的 50% ~64%. 图 5 和图 6 表明,与其他模型相比,本文提出的模型的认证过程相对于其他模型来说,具有较低的通信量和较短的认证时间.

本文认证模型,以虚拟组织和信任度为基础,在现有的组合 PKI 和 IBC 认证模型中引入临时信任域的概念,减少了认证次数,提高了认证效率.

4　结论

本文描述了网格环境下域内和域间信任关系,以虚拟组织和信任度为基础,并在该模型中引入临时信任域的概念,设计了网格环境下的组合 PKI 和 IBC 的跨域认证模型. 仿真实验表明,该模型具有网格环境下认证模型轻量、高效的特点.

参考文献:

[1] Butley R, Welch V, Engert D, et al. A national scale authentication infrastructure[J]. IEEE Computer, 2000, 33(12):60.

[2] 杨斌. IBC 和 PKI 组合应用研究[D]. 郑州:解放军信息工程大学,2009.

[3] 王珊,高迎,程涛远,等. 服务网格环境下基于行为的双层信任模型的研究[J]. 计算机应用,2005,25(9):1974.

[4] 于代荣,杨扬,李盛阳,等. 基于身份的网格安全体系结构研究[J]. 四川大学学报:工程科学版,2009(2):200.

[5] 张红旗,张文波,张斌,等. 网格环境下基于身份的跨域认证研究[J]. 计算机工程,2009(19):160.

[6] Liu Z, Hu Y, Zhang X, et al. Certificateless signcryption scheme in the standard model[J]. Information Sciences, 2010, 180(3):452.

[7] Wu C, Chen Z. A new efficient certificateless signcryptions cheme[C]//Information Science and Engineering, [s.l.]:International Symposium on, 2008:661 - 664.

(上接第 73 页)

4　结论

本文通过借鉴其他自动调平系统的经验,结合砂浆车的实际应用情况,设计了基于 PLC 的液压三点自动调平系统. 该系统以汽车轮胎为支撑基准面,箱体和汽车底盘分离,液压缸直接支撑在汽车底盘上,施工结束后,沥青水泥砂浆车可以同时移动和收腿,而分别设定不同倾角进行试验,试验结果表明,设计的系统能够实现精度为 ±0.3°,调平时间 <6 s 的沥青水泥砂浆车搅拌平台快速自动调平.

参考文献:

[1] 宋刚. 沥青水泥砂浆车在无砟轨道施工中的应用[J]. 现代城市轨道交通,2008(4):42.

[2] 褚新峰,杨曙东. 车载雷达电液自动调平系统[J]. 液压与气动,2007(5):56.

[3] 郭晓松,占金春,冯永保,等. 导弹发射台新型通用调平系统设计[J]. 机床与液压,2007,35(2):114.

[4] 单春贤. 车载雷达天线全自动调平控制模型的建立及系统仿真[D]. 扬州:江苏大学,2007.

[5] 邓飙,邱义,张宝生. 基于电液比例技术的快速自动调平系统[J]. 兵工自动化,2009,28(1):70.

[6] 卫国爱,许平勇,亓迎川,等. 基于 PLC 的液压调平升降控制系统[J]. 液压与气动,2004(5):11.

[7] 房怀英,杨建红,吴仕平. 基于模糊 PID 控制沥青砂浆车液压调平系统[J]. 长安大学学报:自然科学版,2011,31(1):98.