一种面向分布式异构网络的基于可信计算的信任模型

彭 浩[1] 赵丹丹[1] 于运杰[1] 吴震东[2] 吴松洋[3]
(浙江师范大学数理与信息工程学院 金华 321004)[1]
(杭州电子科技大学通信工程学院 杭州 310018)[2] (公安部第三研究所 上海 201204)[3]

摘 要 针对分布式网络中可信计算平台与传统的非可信计算平台所组成的分布式异构网络,基于可信计算技术提出了一种信任模型,并对该模型的理论架构和实现过程进行了详细的分析和研究。仿真结果表明,该模型在没有明显影响分布式异构网络响应时间的情况下,使得分布式异构网站中的节点具有较好的匿名性,同时具有一定的抗恶意节点行为的能力。

关键词 分布式,信任模型,可信计算技术,异构网络
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.10.012

Trust Model Based on Trusted Computing for Distributed Heterogeneous Networks

PENG Hao[1] ZHAO Dan-dan[1] YU Yun-jie[1] WU Zhen-dong[2] WU Song-yang[3]
(College of Mathematics, Physics and Information Engineering, Zhejiang Normal University, Jinhua 321004, China)[1]
(College of Communication Engineering, Hangzhou Dianzi University, Hangzhou 310018, China)[2]
(The Third Research Institute of Ministry of Public Security, Shanghai 201204, China)[3]

Abstract In this paper, a trust model based on trusted computing technology was proposed for distributed heterogeneous networks, which is composed of trusted computing platform and non-trusted computing platform. The theoretical framework and implemention process of the model were analyzed and studied in detail. The simulation results show that in the model the nodes in the distributed heterogeneous network have better anonymity but no obvious effect on the response time of the distributed heterogeneous network. In this way, the proposed trust model has certain ability to counter malicious nodes.

Keywords Distributed, Trust model, Trusted computing technology, Heterogeneous network

1 引言

在与传统的C/S架构相比,分布式网络在文件共享和存储(Napster、Gnutella)、分布式计算(SETI@Home)、协同工作(Groove)以及即时通信(Jabber)等方面具有优越的特性和高效性。由于分布式网络中节点的随机性和分布性等特点,在设计实现分布式网络时,需要考虑的一个首要因素就是节点间的安全通信问题,该问题的核心便是信任问题。到目前为止,分布式网络中信任问题的研究主要集中在基于传统的非可信计算平台之上的信任机制,例如基于Web的信任机制(PGP)、基于信誉的信任机制[1-6]以及基于信任协商的信任机制[7-9]。

随着可信计算(Trusted Computing, TC)[10-13]技术的出现,TC平台可以把信任从底层硬件引入到应用程序,这就为分布式网络中的信任赋予了新的内容。同时,TC平台作为新的安全平台,将会同传统的平台一起应用于分布式网络中,形成异构平台的分布式网络。到目前为止,只有少量的研究考虑把TC技术引入到分布式网络中,主要包括:文献[14]在分布式网络中引入TC技术,提出了一种通用的架构来增强数据的真实性和完整性;文献[15]利用TC技术提出了一种适用于分布式网络的访问控制架构;文献[16]通过TC技术提供的功能,使得节点间通过一个匿名(Pseudonymous)来对身份进行认证;文献[17]针对分布式网络中的数字盗版,结合TC技术进行了初探。然而,所有的这些研究都是基于纯TC平台组成的分布式网络,并没有研究考虑传统平台与TC平台共存的异构平台的分布式网络。因此,我们针对这种异构的分布式网络建立信任模型。

2 TC技术概述

为了解决传统计算机系统存在的可靠性和鲁棒性等问

到稿日期:2015-08-20 返修日期:2016-01-02 本文受浙江省自然科学基金项目(LQ13F020007, LQ16F020002),教育部人文社会科学研究青年基金项目(15YJCZH125),信息网络安全公安部重点实验室开放课题项目(C15610),国家自然科学基金项目(61170108, 61402418),浙江省重点科技创新团队"固态存储和数据安全关键技术创新团队"(2013TD03),浙江省科技厅公益类项目(2013C33056)资助。
彭 浩(1982-),男,博士,讲师,主要研究方向为分布式安全、网络与信息安全、复杂系统安全;赵丹丹(1981-),女,博士,讲师,主要研究方向为网络与信息安全、社会网络,E-mail:ddzhao@zjnu.cn;于运杰(1991-),男,硕士生,讲师,主要研究方向为复杂网络、分布式计算;吴震东(1980-),男,博士,讲师,主要研究方向为网络安全、复杂网络;吴松洋(1982-),男,博士,副研究员,主要研究方向为信息安全、云计算和电子数据取证,E-mail:wusongyang@stars.org.cn(通信作者)。

题，可信计算组（Trusted Computing Group，TCG）[13]提出了TC技术的相关实现方法和机理。简单来说，TC技术就是在计算机主板上添加一个小的可信组件，即可信平台模块（Trusted Platform Module，TPM），该芯片可以为计算机提供基本的加解密功能，如可以基于硬件随机数生成器来实现密钥对生成、私钥签名以及公钥加密和私钥解密等。

另外，TC可以在计算机的底层建立信任的基础，将平台的信任关系从芯片级传递到主板和BIOS的层次，最后到操作网络的层面，从而从多个层面保证计算机系统的安全性。每个TPM拥有唯一的一个背书（Endorsement Key，EK），配有TPM的平台可以由EK唯一标识。验证功能是TCG的一个主要规范，是一种用来判断远程计算机平台是否完整的方法。如果某个平台（验证者V）想要判断某个远程TPM（被验证方A）平台的完整性，V首先会生成一个公/私钥对，称为验证身份证书（Attestation Identity Key，AIK），然后A使用AIK_i来对需要让V进行测量的数据$DATA$（表示为$AIK_i(DATA)$）进行签名。A应该向验证者证明$DATA$的完整性，同时要证明$AIK_i(DATA)$是它自己生成的。

简单情况下，A的EK可以用来标识平台本身的身份，但是这样会暴露A的身份，A所有的活动都可以通过这个身份被恶意节点跟踪。TCG采用了文献[18]中提出的DAA协议，该协议实现了在不需要可信任第三方的情况下对平台的直接匿名验证。

每个TPM平台拥有一个DAA证书，DAA证书是在TPM和颁发者之间进行交互时，使用保留在TPM中的唯一的不可迁移的密钥f（不是EK）生成的。在向TPM颁发DAA证书之前，TPM需要证明满足ζ_I^f形式的一个N_I，ζ_I来自于颁发者的名字基（basename）。对于一个给定的ζ_I，某个TPM就可以确定一个唯一的N_I。只用颁发者之前没有颁发过的“伪匿名”为N_I的DAA证书，同时N_I不在颁发者的黑名单中，那么才会向该TPM颁发DAA证书。

TPM可以使用DAA协议中的签名算法来向一个验证者V证明它拥有一个有效的由某个特定的颁发者颁发的DAA证书，但是验证者V却不能通过这张证书得到任何与平台身份相关的信息。

3 面向分布式异构网络的信任模型

3.1 模型架构

如图1所示，该模型面向异构的分布式网络，在分布式网络中有两种类型的节点：可信计算节点T（为可信计算平台）和非可信计算节点P（为传统的非可信计算平台）。这些节点以组为单位组织在一起，每个组G由一定数量的T和P组成。G的组成原则为：位于同一G中的所有T拥有同一个DAA颁发者所颁发的DAA证书。

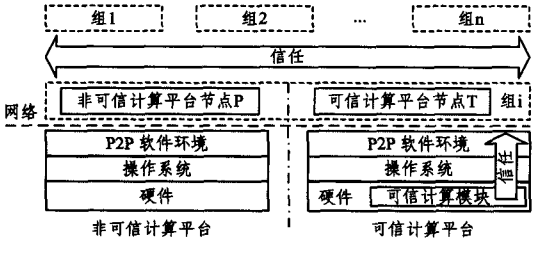

图1 基于可信计算的分布式异构网络信任模型

每个G通过一个唯一的ζ_G标识，其中G中的每个T拥有两个列表，一个为T成员信息列表，一个为P成员信息列表，分别如表1、表2所列。

表1 T成员信息列表

节点属性	描述
T_{ID}	T在该分布式网络中的ID
N_T	节点T在组G中的临时唯一ID，其形式为ζ_G^f，其中ζ_G是该组选择的，f为T的DAA密钥；该域也用来标识节点类型（T或P）
Rep	T的全局信誉值

表2 P成员信息列表

节点属性	描述
P_{ID}	P在该分布式网络中的ID
Rep	非可信平台组的信誉值

表1中的T成员信息包括T_{ID}，N_G和Rep 3个域，与表2相比多一个N_G域，该域用来标识节点为可信计算节点。

当有新的节点T_{new}加入G时，G中的T成员通过DAA机制让T_{new}计算其在该组中的唯一标识N_{new}，并验证其完整性。通过完整性验证后，根据T_{ID}来收集T_{new}的分布式信誉值并计算出一个全局信誉值，将其存储在T成员信息列表中。当某个T退出时，在列表中删除该成员信息。

当有新的节点P_{new}加入G时，根据P_{ID}来收集P_{new}的分布式信誉值并计算出一个全局信誉值，将其存储在P成员信息列表中。当某个P退出时，在列表中删除该成员信息。同时，定期对表1、表2进行更新，删除一些超时没有响应的组成员信息。

当某个节点访问自己所在组的成员提供的服务时，直接根据其全局信誉值与本地信誉值判断其信任程度，进而判断其访问权限。因此，在该模型中，G中所有的节点对于其所在组中的T不具有匿名性。当G中的某个节点p欲访问其他组中的成员V所提供的服务时，p首先需要获得该组T成员为它签发的DAA联合签名，该签名可以唯一标识该节点并证明该节点的全局信誉值，而不会暴露该节点的具体身份信息，即p对于V来说是匿名的。同时，G中的成员不知道P所访问的服务以及服务提供者的信息，故P的活动不会被任何节点跟踪。因此，该模型中的节点相对于其所在组中的T节点之外的节点来说是匿名的。下面对认证流程进行详细分析。

3.2 认证流程分析

3.1节描述了组内身份认证的方法，本节描述不同组成员节点之间的认证流程。假设节点p属于组G，G的公钥为$PK=\{n,g,g',h,R_0,R_1,R_2,S,Z,\gamma,\Gamma,\rho\}$。$p$欲访问节点$V$所提供的服务，且$V$不属于$G$。

在V许可p的访问之前按图2所示流程对P的身份进行认证。G的公钥PK的定义以及认证过程用到的参数w，$r,r_0,r_1,r_v,s,r_{ew},r_{ee},r_{er},\ell_f,_v,s_0,s_1,s_{ee},s_{ew},s_{er}$与文献[18]中的定义相同。

（1）p向V发送消息$R_1=\{PK \parallel ID_{ser} \parallel ran_P \parallel Rep \parallel [DAA_{req}]\}$来请求服务，其中$PK$为$P$所在组的$DAA$公钥；$ID_{ser}$为$p$欲访问的服务标识；$ran_P$为$P$生成的随机数，用于后续的DAA联合签名；$Rep$为$p$的信誉值，在后续步骤中会对该值进行验证；$[DAAreq]$为DAA验证请求信息，中括号“[]”表示可选项，仅当V为可信计算平台且p需要验证V的

平台完整性时才选择此项。

(2)如果 rep 的值足以访问服务 ID_{ser}，那么 V 响应消息 $M_1=\{ran_V \| H(ran_P \| ran_V) \| bsn_V \| MIN(cert) \| [\sigma]\}$，其中 ran_V 是 V 选取的临时随机数；$H()$为 hash 函数；bsn_V 为 V 指定的 $basename$，用于 DAA 联合签名；$MIN(cert)$为访问该服务所需要提供的 DAA 联合签名证书的最少数量；$[\sigma]$是 V 平台本身的 DAA 签名，供 p 进行验证，为可选项，依赖于消息 R_1 中的 DAA_{req}项。

(3)p 对 V 提供的 DAA 签名进行验证，为可选项。

(4)p 向自己所在的组 G 发送 DAA 联合 DAA 签名请求消息 $R_2=\{P_{ID} \| M_1\}$，其中 P_{ID} 为 p 在该分布式网络中的 ID。

(5)组 G 中 T 验证 P_{ID} 的合法性，需要签名的 T_i 分别提取 p 的临时特征，诸如共享的文件内容以及大小、IP 地址等，最后生成 DAA 联合签名，其过程如下：

1)组中的可信计算节点根据 V 提供的 bsn_V，ran_P 和 ran_V 计算：

$$\zeta:=(H_\Gamma(1 \| bsn_V \| H(ran_P \| ran_V)))^{(\Gamma-1)/\rho} (\mathrm{mod}\ \Gamma) \tag{1}$$

并检查 $\zeta^\rho \equiv 1 (\mathrm{mod}\ \Gamma)$是否成立，其中 $H(ran_P \| ran_V)$可以提供完全匿名性。根据签名请求 R_2 中的 $MIN(cert)$数值大小指定为 p 生成相应个数(计为 k)的 DAA 联合签名。

2)指定的每个 T 计算 P 的临时特征 $F_i=\{N_G \| P_{ID} \| Rep \| figure_{ID} \| figure\}$，其中 N_G 为组标识；$figure_{ID}$ 为指纹标识；$figure$ 为标识的内容；并随机选取 w_i，r_i，计算：

$$T_{1_i}:=(A_i h^{w_i})^{e_i} (\mathrm{mod}\ n) \tag{2}$$

$$T_{2_i}:=g^{e_i w_i} h^{e_i e_i} (g')^{e_i r_i} (\mathrm{mod}\ n) \tag{3}$$

$$N_{V_i}:=\zeta^{r_{0_i}+r_{1_i} 2^\ell f} (\mathrm{mod}\ \Gamma) \tag{4}$$

3)生成 DAA 联合签名，并对该签名进行证明，计算：

$$Z^k \equiv \pm R_0^{\sum_{i=1}^{k} f_{0_i}} R_1^{\sum_{i=1}^{k} f_{1_i}} S^{\sum_{i=1}^{k} v_i} h^{\sum_{i=1}^{k} -e_i w_i} T_1 (\mathrm{mod}\ n) \tag{5}$$

$$T_1 \equiv \prod_{i=1}^{k} (A_i h^{w_i})^{e_i} (\mathrm{mod}\ n) \tag{6}$$

$$T_2 \equiv \pm g^{\sum_{i=1}^{k} e_i w_i} h^{\sum_{i=1}^{k} e_i e_i} g'^{\sum_{i=1}^{k} e_i r_i} (\mathrm{mod}\ n) \tag{7}$$

$$N \equiv \zeta^{\sum_{i=1}^{k} f_{0_i}+f_{1_i} 2^\ell f} (\mathrm{mod}\ \Gamma) \tag{8}$$

采用零知识证明，计算：

$$T_1':=T_1 R_0^{r_0} R_1^{r_1} S^{r_v} h^{-r_{ew}} (\mathrm{mod}\ n) \tag{9}$$

$$T_2':=g^{r_{ew}} h^{r_{ee}} g'^{r_{er}} (\mathrm{mod}\ n) \tag{10}$$

$$N':=\xi^{r_0+r_1 2^\ell f} (\mathrm{mod}\ \Gamma) \tag{11}$$

$$c:=H(PK \| bsn_v \| ran_P \| ran_V \| \xi \| \{T_1 \| T_2\}_i^k \| \{N_G\}_i^k \| (T_1' \| T_2') \| N') \tag{12}$$

计算参数 $s_v:=r_v+c \cdot v$，$s_0:=r_0+cf_0$，$s_1:=r_1+cf_1$，$s_{ee}:=r_{ee}+c \cdot e^2$，$s_{ew}:=r_{ew}+c \cdot w \cdot e$，$s_{er}:=r_{er}+c \cdot e \cdot r$，然后输出签名 $\sigma:=(bsn_v, \zeta, ran_P, ran_V, T_1, T_2, N, c, s_v, s_0, s_1, s_{ee}, s_{ew}, s_{er})$。

(6)向 p 发送消息 M_2。

(7)由 p 发送该消息 $M_3=\{ran_P \| ran_V \| \sigma\}$到 V。

(8)V 验证签名，过程如下：

$$T_1'':=(Z^c)^{-c} T_1 R_0^{s_0} R_1^{s_1} S^{s_v} h^{-s_{ew}} (\mathrm{mod}\ n) \tag{13}$$

$$T_2'':=T_2^{-c} g^{s_{ew}} h^{s_{ee}} g'^{s_{er}} (\mathrm{mod}\ n) \tag{14}$$

$$N'':=N^{-c} \zeta^{s_{f_0}+s_{f_1} 2^\ell f} (\mathrm{mod}\ \Gamma) \tag{15}$$

其安全性依赖于强 RSA 问题：给定 n 和 Z，想要找到一对(a,e)满足 $Z \equiv a^e (\mathrm{mod}\ n)$是困难的。

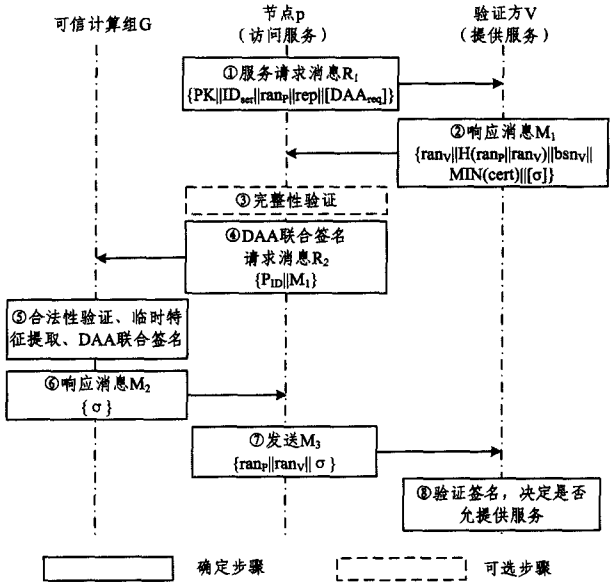

图 2 异构平台节点认证流程图

4 仿真与结果分析

4.1 认证消耗时间

本仿真实验中硬件平台是 Intel T430 2.5GHz 的双核处理器、4GB RAM 和 Windows Server 2008 R2 操作系统的 PC，软件平台是在 VC6.0 开发环境下使用第三方MIRACLv5.0[19]库对 DAA 协议进行仿真。仿真结果：DAA 签名时间为 109ms，DAA 签名验证时间为 187ms。

图 3 给出了在处理不同数目节点认证时的认证总时间和无认证总时间。在无认证中，时间消耗主要为计算节点信誉值的时间。在认证时，每个 G 预先收集到了节点的信誉值，认证过程中的主要时间消耗为 DAA 签名和 DAA 签名验证过程，但提高了信任。

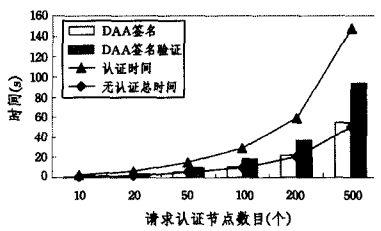

图 3 处理不同数量的进程认证所需要的时间

4.2 匿名度分析

分布式网络中，身份匿名性作为一个安全指标，可防止因身份暴露而引起的活动被跟踪等。在本模型中，节点的身份只为所处的组中的 T 可知，用组成员 T/N 来表示匿名度较为简单且科学，图 4 给出了随着网络节点的增加组成员对其节点匿名度的影响。可以看出在分布式网络节点数大于 1000 且可信计算组节点数大于 10 的情况下，其匿名度小于 0.1%。

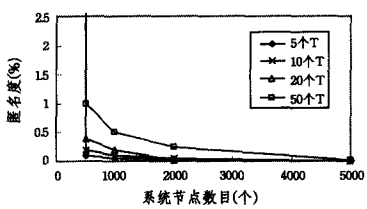

图 4 随着网络节点数目的增加匿名度的变化趋势

4.3 恶意节点行为对认证可信性的影响

这里的恶意节点是指分布式异构网络中同组中的节点生成认证信息时，出现了具有错误的节点信誉信息、指纹信息以及拒绝正常认证行为的节点。图5根据每个节点恶意行为的概率描述了在不同数量证书的情况下认证的可信性，假设以节点有30%的概率获得恶意证书或得不到任何证书为门限，在证书个数大于2时，当网络节点恶意行为概率接近70%时才能获得恶意证书。仿真结果显示，本文实现的信任模型具有比较高的可信性。

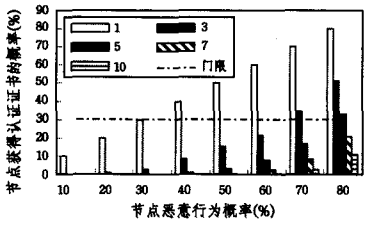

图5 节点恶意行为概率对恶意证书的影响

结束语 本文针对分布式异构网络，提出了一种基于可信计算技术的信任模型，从而为异构平台之间信任关系的建立提供了一种可行方案。该信任模型弥补了传统方法对非可信计算平台认证的不足，并在一定程度上保证了非可信计算平台的高匿名性和鲁棒性。仿真结果显示，本文提出的信任模型具有较高的可信性，从而确保了在异构的分布式网络中构建的信任关系更加科学和完善。但是，该模型并没有考虑"克隆"TPM[20]节点的检测等因素，相关解决方案可以参考文献[21]。在下一步的研究工作中，我们将考虑上述要素，结合分布式异构网络的特点，致力于设计更为具体的认证方案和优化的信任模型。

参 考 文 献

[1] Xiong L, Liu L. Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities[J]. IEEE Transactions on Knowledge and Data Engineering, 2004, 16(7): 843-857

[2] Tajeddine A, Kayssi A, Chehab A, et al. A comprehensive reputation-based trust model for distributed systems[C]// Workshop of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks. IEEE, 2005: 116-125

[3] Jiang W J, Xu Y S, Guo H, et al. Dynamic trust calculation model and credit management mechanism of online trading[J]. Scientia Sinica Informationis, 2014, 44(9): 1084-1101(in Chinese)
蒋伟进，许宇胜，郭宏，等. 网络在线交易动态信任计算模型与信誉管理机制[J]. 中国科学(信息科学)，2014，44(9)：1084-1101

[4] Hu J L, Zhou B, Wu Q Y, et al. A reputation based attack-resistant distributed trust management model for P2P networks[J]. Journal of Computer Research and Development, 2015, 48(12): 2235-2241(in Chinese)
胡建理，周斌，吴泉源，等. P2P网络环境下基于信誉的分布式抗攻击信任管理模型[J]. 计算机研究与发展，2015，48(12)：2235-2241

[5] Rebahi Y, Mujica-V V E, Sisalem D. A reputation-based trust mechanism for ad hoc networks[C]// Proceedings of the 10th IEEE Symposium on Computers and Communications (ISCC 2005), IEEE, 2005: 37-42

[6] Shu Z Y. Research on trust mechanism in service-oriented network environment[D]. Dalian: Dalian University of Technology, 2014(in Chinese)
苏志远. 面向服务网络环境中信任机制的研究[D]. 大连：大连理工大学，2014

[7] Bertino E, Ferrari E, Squicciarini A. X-TNL: An XML-based language for trust negotiations[C]// Proceedings of the 4th IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY 2003). IEEE, 2003: 81-84

[8] Shi Z G, He Y P, Zhang H. A scenario of trust negotiation based on TPM anonymous credentials[J]. Journal of Computer Research and Development, 2015, 45(8): 1279-1289(in Chinese)
石志国，贺也平，张宏. 一种基于TPM匿名证书的信任协商方案[J]. 计算机研究与发展，2015，45(8)：1279-1289

[9] Chen Z M, Wang H. Constructing optimal credential disclosure sequence in automated trust negotiation[J]. Computer Applications and Software, 2014, 31(11): 289-291(in Chinese)
陈泽茂，王浩. 自动信任协商中最优信任证披露序列的构建方法[J]. 计算机应用与软件，2014，31(11)：289-291

[10] Felten E W. Understanding trusted computing: will its benefits outweigh its drawbacks? [J]. IEEE Security & Privacy, 2003, 1(3): 60-62

[11] Vaughan-Nichols S J. How trustworthy is trusted computing? [J]. Computer, 2003, 36(3): 18-20

[12] Zhuang L, Cai M, Shen C X. Trusted dynamic measurement based on interactive Markov chains[J]. Journal of Computer Research and Development, 2015, 48(8): 1464-1472(in Chinese)
庄琭，蔡勉，沈昌祥. 基于交互式马尔可夫链的可信动态度量研究[J]. 计算机研究与发展，2015，48(8)：1464-1472

[13] Feng D G, Qin Y, Wang D, et al. Research on trusted computing technology[J]. Journal of Computer Research and Development, 2015, 48(8): 1332-1349(in Chinese)
冯登国，秦宇，汪丹，等. 可信计算技术研究[J]. 计算机研究与发展，2015，48(8)：1332-1349

[14] Bhasker L. Genetically derived secure cluster-based data aggregation in wireless sensor networks[J]. IET Information Security, 2014, 8(1): 1-7

[15] Wang J, Lin W, Li H, et al. A trusted mobile payment environment based on trusted computing and virtualization technology [J]. Wuhan University Journal of Natural Sciences, 2014, 19(5): 379-384

[16] Nageshwar P, Nagaraju I, Kumar M A. The trusted computing model for providing security in cloud computing[J]. International Journal of Mathematics and Computer Research, 2015, 3(6): 1018-1024

[17] Mendonça R D, Silva T R M B, Silva F A, et al. Dynamic bandwidth distribution for entertainment vehicular networks applications[C]// The 28th IEEE International Conference on Advanced Information Networking and Applications Workshops (WAINA). IEEE, 2014: 827-832

[18] Brickell E, Camenisch J, Chen L. Direct anonymous attestation [C]// Proceedings of the 11th ACM Conference on Computer and Communications Security. ACM, 2004: 132-145

[19] Shamus Software Ltd. Multiprecision integer and rational arithmetic C/C++ Library[EB/OL]. http://indigo.ie/~mscott

[20] Sumrall N, Novoa M. Trusted computing group (TCG) and the TPM 1.2 specification[C]// Intel Developer Forum. 2003

[21] Proudler G, Chen L, Dalton C. Trusted platform architecture [M]. Springer International Publishing, 2014: 109-112