

信息和网络安全专题

开放网络环境下电信领域可信软件模型 和安全评估

季一木¹, 扈罗全², 陈 志³

(1. 南京邮电大学 软件学院, 南京 210003;

2. 苏州出入境检验检疫局, 江苏 苏州 215104;

3. 南京邮电大学 计算机学院, 南京 210003)

摘要:面向应用领域的可信软件模型的建模与评估,是在现有的可信计算硬件平台和可信的操作系统之上,实现可信的 Web 应用、可信的应用软件和可信的开放网络环境的关键。详细介绍了可信软件建模技术、模型的验证及度量方法等,并讨论了所提的可信软件模型和安全评估方法在电信领域的应用及分析。

关键词:开放网络;可信计算;信息安全;电信领域

中图分类号: TN01 **文献标识码:** A **文章编号:** 1673-5692(2008)06-586-06

Trusted Software Model and Security Evaluation in Telecom Field with Open Network

Ji Yi - mu¹, Hu Luo - quan², Chen Zhi³

(1. College of Software, Nanjing University of Posts and Telecommunications, Nanjing 210003, China;

2. Suzhou Entry-Exit Inspection and Quarantine Bureau, Jiangsu Suzhou 215104, China;

3. College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: The modeling and evaluation on the trusted software models for application fields are the key technologies to implement trusted web applications, trusted application software and trusted open network environment on the foundation of trusted computing hardware and operating system. The modeling technology, verification of the models and measurement approaches of trusted software are introduced in detail. The application and analysis of the trusted software models and security evaluation approaches in the telecom field are discussed.

Key words: open network; trusted computing; information security; telecom field

0 引言

可信计算是指参与计算的组件、操作或过程在任意的条件下是可预测的,并能够抵御病毒和物理干扰^[1]。可信计算技术被认为是从根本上解决可

信问题的革命性技术。可信计算的核心是具有可信平台模块(TPM, trusted platform module)的安全芯片,系统启动前首先给安全芯片上电,然后相继对 BIOS boot block、OS kernel、OS 及上层应用的特征值进行完整校验,保证系统平台硬件环境的可靠性^[2]。

收稿日期: 2008-09-21 修订日期: 2008-11-25

基金项目:江苏省高校自然科学基金项目(08KJB520006);南京邮电大学教育科学“十一五”规划(GJS-XKT0801);南京邮电大学教学改革研究项目(JG01108JX36)

尽管可信计算平台研究取得了重要进展,但是随着互联网应用的快速发展,尤其是开放网络环境下,可信计算技术的外延在不断拓宽,计算机网络、无线通信网络和广播电视网络三网融合迫切的市场需求,国内外针对这方面做了很多研究工作,包括下一代网络、软交换技术、3G标准和各种终端等的研究和研制工作^[3]。尤其在电信业,随着无线通信技术与计算机技术的不断融合,移动终端正逐步取代PC机成为人机交互的主要设备^[4]。

文献[5]是国内最早对可信软件技术的研究,给出了基于形式化方法的高可信软件技术的发展趋势。这种基于形式化逻辑和语义描述方法在可信软件开发过程中一直起着至关重要的理论意义,如何将理论转化为应用是当前面临的重要挑战。针对移动终端的特性,以处理器 OMA P730为硬件平台,给出了可信平台模块的三种构建案例,并提出了通用用户识别模块(USM, universal subscriber identity module)和 TPM相结合的可信管理平台(TMP, trusted management platform)框架。文献[6]提出一种基于系统行为的计算平台可信证明模型(BTAM, behavior based trustworthiness attestation mode)。在可信计算环境下,根据可信行为期望策略,将平台状态证明转化为对平台历史行为序列的可信证明。该模型有效地避免了在准确描述计算平台状态方面的难题,并且不会暴露证明平台的配置信息。BTAM模型在防范诸如计算机病毒、木马类恶意软件攻击以及避免安全策略冲突行为等方面,具有一定的安全防范能力和良好的安全运行效率。文献[7]~[9]分别对信任模型、信任管理和网络开放环境下的任务调度等问题进行了研究。文献[10]在信任评估领域展开了深入的研究。

开放网络环境下的可信技术不是一蹴而就,它不仅需要可信硬件平台、可信的软件,还需要能够推动可信计算应用的更好的产业化契机。关于可信软件方面,已经有专家指出在 TPM基础上,如何开发可信软件栈(TSS, trusted software stack)是提高应用的安全保障的关键^[11]。可信软件栈以应用编程接口(API, application programming interface)的形式为应用提供可信接口,基于 TPM开发可信软件是一种必然。关于应用,电信产业是中国信息化的主力,然而目前电信网络时常受到威胁,一些网络攻击导致对骨干网的可靠畅通构成威胁、侵害应用服务提供者的利益、侵害用户的切身利益、影响人们使用互联网的信心,进而影响互联网发展。可信计算技术为

建立可信电信网络环境提供了新的支撑,反之,可信的电信网络环境为可信计算技术的发展提供推动力。本文介绍了开放网络环境下电信领域的可信软件模型和评估研究,包括模型的建立和生成技术,并对模型的度量和验证方法进行了探讨。

1 开放网络环境下电信领域可信软件体系结构模型

伴随着终端的计算和存储能力的不断增强,移动操作系统和各种无线应用的问世,移动终端也面临着越来越多的安全威胁,因此如何构建一个从硬件终端到应用业务层面的可信环境显得成为重要。以下将从终端、操作系统、支持软件和业务应用四个方面在可信软件构建方面,并结合现有的研究成果提出一种开放网络环境下电信领域可信软件模型如图1所示。图1中清晰地描述了可信软件概念模型不同层次对应的安全等级和技术模型,为全面实现开放网络环境下的可信软件模型提供了参考。其中硬件级和操作系统级均是在现在研究成果的基础上考虑对电信终端和嵌入式操作系统的集成问题;软件构建级主要从电信企业企业资源规划(ERP, enterprise resource planning)和电信企业的业务运营支撑系统、经营分析系统和客户关系管理系统的实现来构建,从实现技术角度主要考虑计费管理监控、主备系统同步和高额欺诈等^[12]。业务应用级主要是指与电信等运营商相关的话音、短信和彩信等业务相关的概念模型,从技术模型角度主要是指传统业务、增值业务、融合方式、访问门户和一站式服务等实现模型。

1.1 基于MDA的开放网络环境下电信领域可信PM模型构建技术

当前模型驱动框架(MDA, model driven architecture)开发过程中平台独立模型(PM, platform independent model)的建立都是通过使用UML的形式化模型(亦称元模型)实现的,元模型可通过非形式化的文本和形式化的约束对象约束语言(object constraint language)来描述所建立模型的语义。

如何将电信领域软件系统中涉及到的各种对象实体抽象出来,并通过加入XML509证书、PK密钥机制、数字签名方案和对象实体间的关联模型R(O, D, f)等可信属性约束,形成规范的OCL约束语言,通过用户定义的OCL描述对电信领域软件进行

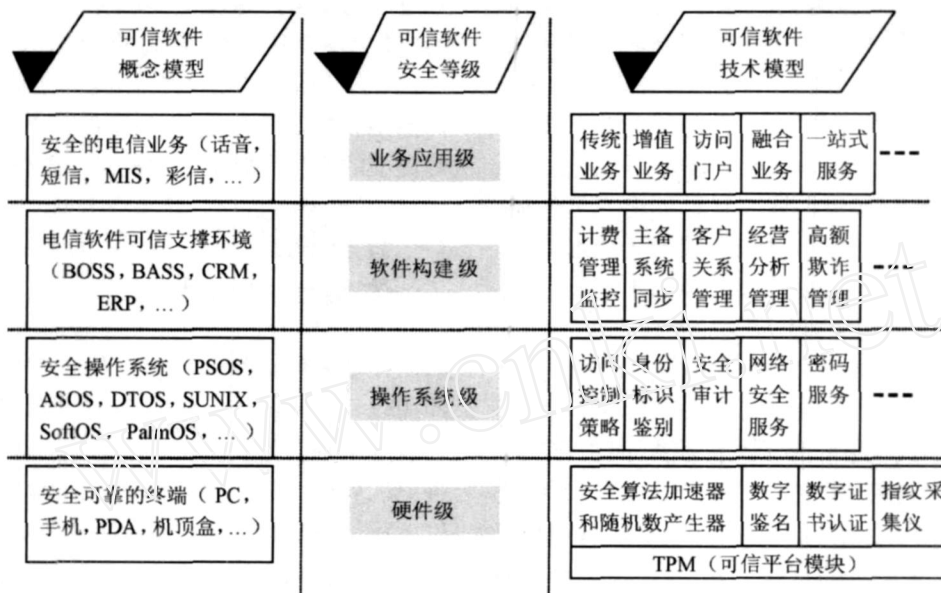


图 1 开放网络环境下电信领域可信软件的分级模型

统一建模语言 (UML, unified modeling language) 建模,从而达到可信建模的目的,具体流程如图 2 所示。形成的平台无关模型 PM 已经是明确了对象间的关联约束、对象的访问可信接口和相应的容错能力。

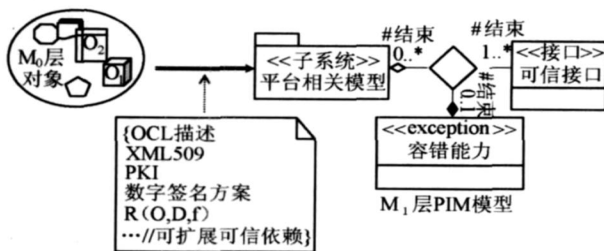


图 2 M₀对象实体到 M₁层可信 PM 模型的建立过程

为了实现图 2 的流程,主要考虑和解决两方面问题:一是如何引入安全手段,这样做可满足开放网络环境的需求;二是针对电信领域软件如何构建对象实现间的关系模型 R (这里 R 由对象 O、对象实体的空间域 D 和对象间的关联函数 f 三元组组成)。当然不同的企业和应用可以定制自己的需求,从而生成相应的 PM 模型。

1.2 开放网络环境下电信领域可信软件自动生成技术

第 1 步:基于 TPM 与电信规范的可信软件可信性自动分析与抽取

TPM 是可信计算的核心, TSS 是 TPM 向应用提

供的 API,可信软件的开发需要对 TSS 进行继承,并根据软件面向的领域需求进一步增加可信约束。因此,电信软件的可信性一方面需要基于 TPM,另一方面必须对电信领域的可信需求 [包括安全需求、可靠性需求、容错性需求、服务质量 (QoS, quality of service) 需求] 进行分析。由于电信领域的软件种类繁多,制造商和运营商较多,而且各省市的市场不同,采用人工手动的方法对软件的可信性需求进行分析与抽取不可行。基于 TPM 的自动分析与抽取软件可信性在 TPM 认证规范基础上,研究出电信软件的可信性自动分析方法,为电信可信软件高效自动的构造奠定基础。通过对电信领域软件的规范、框架、结构、目的、要求、应用等解析,采用反向挖掘技术,对挖掘的出的可信属性结果进行转化、最后建立可信软件可信性在线分析数据仓库。

第 2 步:基于 XML 语言的可信软件可信性的描述与定义

预期的表现形式应该考虑到异构系统的差异性和兼容性要求,采用一种标准的、跨平台支持的并且可以灵活扩展的安全策略描述语言是一种必然,XML 提供了一个很好的支持基础,目前一些开放网络环境 (如网格) 都是基于 XML 语言构成安全基础设施。其中 SAML (security assertions markup language) 和 XACML (extensible access control markup language) 是两个影响力较大的安全策略描述语言,但是作为软件行为的验证,二者又存在诸多不足,需要对 XML 描述语言进行相关的安全功能扩充,对电

信领域的可信性策略进行更好的描述与定义。

第3步:基于动静适配器增强可信软件的容错性

这里认为,一个可信的电信软件必须能够建立在任何一个 TSS之上,并且随着 TSS的改变,应用不需要改变仍然可信。对此,可以通过一种动静结合适配思想来解决这个问题。动静结合是指当 TSS没有改变时,软件调用的 API不需要改变,静态调用即可,当 TSS改变了,并采用动态匹配满足 TPM 规范的 API,此时不依赖于 TSS。一般来讲 TPM 规范是不变的, TSS则各厂家提供的 API不同,可以使用动静结合适配技术从最低层增强了可信软件的容错性。

第4步:基于模板实现可信软件的代码自动生成技术

可信软件无论是服务还是构件形式,都是以程序代码为基础的。如何保证软件代码的可信性,只能依据 TPM 认证及领域需求。为了保证软件的可信,开发人员必须理解 TPM 规范,必须理解电信领域需求,显然,这制约了开发人员专注于功能的开发。在 TPM与电信规范软件可信性自动分析与抽取研究、容错性增强,以及适配技术的基础上,基于模板技术自动生成可信的电信软件框架,以此实现可信软件的自动开发。基于模板的可信软件暂时拟定采用 X模板与 V模板两种技术^[13],该内容的研究将实现可信软件代码自动生成,提高软件开发效率。

2 开放网络环境下电信领域软件可信性度量与验证

2.1 电信服务可信性质的度量

电信服务可信性质的度量是评估模型计算可信度向量的基础,电信服务的可信性质表现为电信服务的行为特征,特征值反映了电信服务的可信性质的可信度,例如电信服务的可靠性,将请求匹配率

$$= \frac{R_h}{R_k}, \text{其中 } R_h \text{ 是总的请求服务次数中获得匹配}$$

次数, R_k 是总的请求次数,作为该可信性质的特征,那么根据 的值及可靠性的特征函数就可以计算可靠性的可信度向量^[10]。但是可信性质特征并不惟一,例如可靠性同样可以根据服务成功率 来描述,

$$= \frac{S_s}{S_a}, \text{其中 } S_s \text{ 为成功服务的次数, } S_a \text{ 为接入服务的}$$

次数。在开放网络下,对可信性质特征的度量需要

建立一个分布式测量特征的测评体系结构。每个电信服务端包含多个特征传感器,每个特征传感器获得的是基于经验的客观的可信性质的特征值,它负责收集服务的历史信息,定期的通过计算该特征的算法计算特征值,并将该特征值通过特定的协议反馈给测评系统。同理,电信客户端将主观可信性质的特征值反馈给测评系统。

2.2 基于模型验证的电信可信性质形式化验证

在目前利用形式化方法验证软件性质的技术中,比较成熟的有两种:一种是模型检验技术;另一种是定理证明技术^[6]。针对可信性质形式化验证系统拟采用模型验证技术。利用模型验证技术通过 TPM与电信规范软件可信性自动分析与抽取环节获取抽象软件的行为特征,接着研究软件可信性质的表示,如何基于时序逻辑的逻辑公式来表示软件的可信性质,以便能够在模型验证的过程中进行规约。根据模型验证技术在过去的成功应用来选择适当的时序逻辑(如命题线形时序逻辑,计算树逻辑和 μ 演算)来表示验证软件是否具有可信需要的可信性质。最后研究软件行为和可信性质的关系,如何通过表示可信性质的逻辑公式上的规约来验证软件符合可信性质。如软件行为不符合可信性的逻辑公式,则能认为软件为不可信的。

2.3 基于模糊集合理论的电信服务可信评估模型

电信服务可信这个概念定义为一个可信概念树来描述,可信概念树的叶子为不可分解的可信性质。在构建可信树的基础上,拟采用模糊集合理论对其度量^[14],用多个模糊子集 $C_j (j=1, 2, \dots, M)$ 定义具有不同可信度的电信服务的集合,即用离散的标度 $\{1, 2, \dots, M\}$ 来描述电信服务可信的高低。同时,采用自然语言对 C_j 命名,赋予其直观的含义。例如定义 2级的可信度可以定义 C_j 的含义如下: C_1 表示不可信, C_2 表示可信。通常无法明确的判断电信服务究竟是属于哪一个可信集合,因此,用电信服务对各 C_j 隶属度所构成的向量来描述电信服务的可信度更符合电信服务可信的实际情况。设 $x_i \quad \mathbf{X} = \{x_1, x_2, \dots, x_i, \dots, x_n\}$ 为某个电信服务,那么 x_i 的可信度可以描述为向量 $\mathbf{V} = (v_1, v_2, \dots, v_k, \dots, v_M)$ 来表示,其中 v_k 表示 x_i 对 C_j 的隶属度。对于叶子节点,即可信性质可信度向量的计算需要构造其特征函数

$F_j(x, j), F_j(x, y)$ 一般定义为关于可信性质特征值 y 的分段函数,在第 k 分段上再定义一个评价函数 $f_k(x)$ 用于计算该可信性质对每个可信集合的隶属度。在构造的可信概念树,以及所有可信性质可信度向量的基础上,通过递归计算每个父节点可信度向量,直到根节点的可信度向量 v 。最终的电信服务属于 $\max(v_1, v_2, \dots, v_k, \dots, v_M)$ 对应的可信集合。

3 应用分析:开放网络环境下可信电信客户关系管理系统

3.1 基于可信智能卡的用户身份鉴别

在现有的开放式网络环境下,电信客户关系管理(CRM, customer relationship management)系统进行数据传输时,用户在电信终端面临着很大的安全危险。传统的用户身份鉴别都是由应用程序本身来完成,那么对于一个恶意的或者存在安全缺陷的电信 CRM 应用程序来说,攻击者很容易获取到用户的密钥,从而获取到用户的所有权限和信息,传统的方法并不能很好地解决用户身份安全的问题^[15]。在本方案中利用可信智能卡来从硬件的层次解决用户身份鉴别,可信智能卡是一种有关用户密码的计算和处理设备,它可以有自己的存储和计算单元,并且用户在输入相关验证信息后产生登陆应用程序的密码,用户自己的密码不需要经过应用程序的检验,而且用户密码一次一密,提高了用户密码本身的安全性。

3.2 基于可信技术的数据安全分析

通过身份认证解决用户在登录电信 CRM 的分布式数据库或分布式数据库系统服务器与服务器之间进行数据传输时用户的身份确认;在身份认证的前提下,赋予不同的用户不同的访问控制权限;在身份验证成功后,拥有相应权限的用户就可以进行数据传输,此时需要对传输数据的信道进行加密,同时对传输的内容也要进行加密,这样就可以充分保证数据库内容的安全性。

此外,用户对数据的副本选择具有一定的规律,即服从一定的概率分布,一般认为服从 Zipf 分布。Zipf 分布最初是由 G K Zipf 发现于语言学中^[16],表现为如果将语言中的词汇,按照出现的频率由高到底排序,那么某个词出现的频率与该词所对应的序号之间有如下关系: $P(t) = \frac{1}{t}$, 其中 $P(t)$ 表示某

个词汇出现的频率, t 表示该词汇所对应的序号。在某种具体的分布中, $(0 < \alpha < 1)$ 为一个正常数,称之为 Zipf 常数。

假设用户对电信数据的选择服从 Zipf 分布,可以表示为: $P_k = \frac{k^{-\alpha}}{c}$, 其中 $c = \sum_{k=1}^n k^{-\alpha}$, $0 < \alpha < 1$, 表示在所有的 n 个数据中,第 i 个数据被访问的频率。式中的 α 为常数,称为深度因子,越大表示热门数据的选择率越高。显然,不同的数据,是不同的。在开放网络环境下,可以根据数据实际选择情况求出 α 。比如,假设一个数据业务中有存储 N 个数据文件,其中 N 个数据文件分别为 $F_i (i = 1, 2, \dots, n)$, 设用户对数据文件 F_i 的访问符合 Zipf 分布,一段时间,用户对数据文件 F_i 的访问次数为 q_i , 网络中数据文件 F_i 的受欢迎程度为 $\rho_i = \frac{q_i}{N}$, 其中 N 为数据文件总共被访问的次数, ρ_i 越大,说明该数据文件 F_i 越受用户欢迎,也表示存储数据文件 F_i 的存储资源越繁忙。知道了每一个数据文件访问的概率,那么就可以通过样本对 ρ_i 进行估计。得到 ρ_i 值,对于所有的数据知道了其可能被访问的概率情况。因而,可以根据数据访问的频率达到对数据优化和安全存储。

3.3 基于协议加密的安全通信

现有的电信 CRM 系统是一种分布式的 Web 应用程序,它需要定期处理机密信息。无论此信息是存储在数据库中,还是正通过网络在分布式 CRM 应用程序的不同组件之间传递,时刻保证此信息的安全都非常重要。在电信 CRM 系统的应用程序进行 Web 部署时,一个客户端请求要经过三个不同的通道。客户端到 Web 服务器的连接可能通过 Internet 或者 Intranet 实现,同时使用 HTTP 协议。其余两个连接则在电信运营商内部网络中实现。尽管如此,三种连接的安全则令人担忧,各种可能的客户资料和资费信息会被截取、修改等。一般来说通过对某些协议来完成数据的加密传输,但是这些协议本身在开放网络环境中也会遭到黑客的攻击,这样势必会造成传输数据的泄漏。因此必须要通过一定的安全通信手段保证信息在传递时是安全可靠的。主要通过结合使用加密的安全套接层(SSL, security socket layer)、IPSec,以及远程过程调用(RPC, remote process call)等技术来保证安全通信,使得这些协议本身在网络中更加安全。

3.4 基于安全保护的 SAN 网络远程数据容灾处理

电信客户关系管理系统是电信运营商制定运营策略的重要依据,故建立一个良好的电信 CRM 系统的远程数据容灾处理十分重要。目前大多数的容灾方法就是通过存储区域网络(SAN, storage area network)建立一个强健的集中存储平台,能够兼容各种数据库平台、存储设备和主机操作系统平台的容灾解决方案,从而有效的避免自然灾害、供电问题、人为因素、病毒等各方面的破坏,确保信息资源安全。但是该方法没有考虑到在数据备份过程中也会造成数据被恶意的攻击和篡改,故本方案在数据从源节点通过 SAN 网络经过网络传输到目标节点时,采取对数据进行加密传输的安全保护措施。

4 结 语

本文围绕可信软件的模型、开发、验证与评估和行业应用展开研究分析。在现有的研究成果对电信可信性抽取、定义与描述和 MDA 建模,解决电信行业可信软件的建模和生成技术,提高可信软件生产效率。通过电信服务可信性质的度量研究、可信性质形式化验证,建立基于模糊集合理论的电信服务可信评估模型,为可信软件度量提供了保障机制。在开放网络环境下,通过电信客户关系管理系统的可信应用研究分析,为构建一个面向电信领域或其他领域的应用起到了示范作用。针对具体的安全评估方法如何在开放网络环境下的可信软件模型中进行验证,有待今后进一步研究。

参考文献:

- [1] ROY THOMAS FIELD NG Architectural Styles and the Design of Network-based Software Architectures[D]. University of California, Irvine, School of Information and Computer Science, 2000.
- [2] 郝平,何恩.可信计算的安全防护机制及其在高可信网络中的应用[J].中国电子科学研究院学报,2008,3(1):14-19.
- [3] SMITH S Magic Boxes and Boots: Security in Hardware[J]. IEEE Computer 2004, 37(10): 106-109.
- [4] 郑宇,何大可,何明星.基于可信计算的移动终端用户认证方案[J].计算机学报,2006,29(8):1254-1264.
- [5] 陈火旺,王戟,董威.高可信软件工程技术[J].电子学报,2003,31(12):1933-1938.

- [6] 李晓勇,左晓栋,沈昌祥.基于系统行为的计算平台可信证明[J].电子学报,2007,35(7):1234-1239.
- [7] 王伟.一种基于 Bayes信任模型的可信动态级调度算法[J].中国科学(E辑:信息科学),2007,37(2):285-296.
- [8] 怀进鹏,胡春明,李建欣,等. CROWN:面向服务的网格中间件系统与信任管理[J].中国科学(E辑:信息科学),2006,36(10):1127-1155.
- [9] 袁禄来,曾国荪,姜黎立,等.网格环境下基于信任模型的动态级调度[J].计算机学报,2006,29(7):1217-1224.
- [10] 王远,吕建,徐锋,等.一个适用于网构软件的信任度量及演化模型[J].软件学报,2006,17(4):682-690.
- [11] Trusted Computing Group. TPM Software Stack (TSS) Specifications[EB/OL]. <http://www.trustedcomputinggroup.org/specs/TSS/>.
- [12] 赵贤敬,郭利江,郑明忠,等.移动通信国际漫游欺诈与反欺诈博弈[J].通信技术,2008,14(07):171-174.
- [13] 蒋凌云,王汝传.用于网格计算的复合代码生成技术研究[J].南京邮电大学学报(自然科学版),2005,25(6):73-78.
- [14] 张艳群,张辰.基于模糊理论的信任度评估模型[J].计算机工程与设计,2007,28(3):532-533.
- [15] 王会,安常青,李学农,等.基于用户的计费系统中的身份认证机制[J].计算机工程与设计,2002,23(4):13-15.
- [16] 焦建玲,范英,魏一鸣,等.基于 Zipf的汽油价格行为研究[J].系统工程理论与实践,2006,21(10):44-49.

作者简介



季一木(1978-),男,安徽无为,人,博士,南京邮电大学讲师,研究方向为软件工程、中间件技术和网格计算等;



扈罗全(1972-),男,江苏宜兴人,博士,苏州出入境检验检疫局信息产品检测中心电磁兼容实验室主任,研究方向为无线通信与电磁兼容、随机模型,已在包括 IEEE/ IET 学报在内的国内外各类学术刊物和学术会议上发表论文 70 余篇,SCI/EI/ISTP 收录 20 余篇;

陈志(1978-),男,江苏淮安人,博士,南京邮电大学讲师,主要研究方向是无线传感器网络、Agent 和多 Agent 系统、普适计算等。