

Agent 为中介的电子商务研究^{*}

Some Research on Agent-mediated Electronic Commerce

苏 敏 郭瑞景 陶先平 徐 锋 陈红强 吕 建

(南京大学计算机软件新技术国家重点实验室 南京210093)

(南京大学计算机软件研究所 南京210093)

Abstract Agent technology will play an increasing role as mediators in electronic commerce. This thesis introduces some technological areas that agent is applied for in electronic commerce. And though a classical business model, CBB model, analyses roles of agents as mediators in electronic commerce. Then introduces some agent-mediated electronic commerce systems, including our mobile agent-based electronic marketplace, MABEMS, which is designed and implemented by ourselves. At Last, give a summary for trends of next generation agent-mediated electronic commerce.

Keywords Electronic commerce, Agent, CBB model, MABEMS

一、引言

电子商务至今没有一个较为全面、权威的定义。一般地说,电子商务包括一切使用电子手段进行的商业活动。它是运用电子通信为手段的经济活动,通过这种方式人们可以对带有经济价值的产品和服务进行宣传、购买和结算。这种交易的方式不受地理位置、资金多少或零售渠道的所有权影响,个人、组织、团体都能自由地参加广泛的经济活动。电子商务能使产品甚至服务在世界范围内交易,并向消费者提供多种多样的选择。

智能 Agent 是一些软件实体,它们能代表用户或另一些程序,利用一些用户目标或欲望相关的知识或表示,以某种程度的独立性或自主性执行一系列操作。不同于传统的软件,它具有以下几个主要特性:(1)智能性:指 Agent 具有一定的自适应能力,能对所处环境发生的变化具有感知能力和应变能力;(2)自主性:指 Agent 可无需用户的干预按照自己的意愿完成特定的任务;(3)协作性:体现为若干个移动 Agent 可在网络中相互通信并合作完成某一任务;(4)移动性:Agent 能够跨不同的系统体系结构和平台从一台机器移动到另一台机器,并且可以在任意站点上暂时中断执行,然后移动到需要的站点上停留下来再恢复执行。

电子商务涉及领域广泛,包括安全、信任、电子支

付、广告、本源论(Ontology)、在线目录及虚拟现实购物体验等等;电子商务环境有如下一些特点:包含资源、信息量巨大,且广泛分布在网络上,缺少一个完全的目录来集中组织这些资源、信息;并且交易各方很多,各方的交互、判断、协商复杂。

Agent 的特质使得它们在处理大量的信息搜集和加工处理的电子商务环境中很有前途。在电子商务的技术领域里,需要具有个性化的、持续运行的、半自治行为特性的软件来运行。到目前为止,传统 Web 形式的电子购物手段大都是非自动化的,交易的各个过程都需要人的高度参与,这些手工过程增加了交易成本。然而 Agent 能在没有人类直接干预的情况下完成大部分任务,代替用户自主地执行;电子商务环境中的交易是个非常复杂的过程,而利用移动 Agent 移动到市场中与本地 Agent 进行交互协商,则可将远程交互变成本地交互,减轻网络负担,而且移动技术可以避免网络失效情况下不能正常完成交易的情况。为此,可以利用 Agent 节省更多的时间和金钱,因此 Agent 技术在电子商务中有着非常广阔的应用前景。

二、电子商务中的主要 Agent 技术

众多的 Agent 技术中,我们主要以下列一些 Agent 技术为主:Agent 产品推荐系统、以 Agent 为界面的人机交互、Agent 之间的协商机制与策略,以及为提

^{*} 1 本文受国家杰出青年基金项目(61525204)、九五科技攻关项目(96-729-1-06)和863高科技项目(863-306-ZT02-01-4)资助。苏敏 硕士生,研究方向:Agent、电子商务应用。吕建 博士,教授,博导,研究方向:形式化方法、分布对象技术、移动 Agent 技术、构件技术。

高各 Agent 系统之间互可操作性而需要的一些基础设施和技术。

Agent 产品推荐系统 是把对信息的基于内容、协作或限制的过滤作为它们的根本技术。在基于内容的过滤中, Agent 系统处理从不同的来源获取的信息,并试着抽取基于内容的有用特征和元素。不同的过滤技术可能在复杂度上差别很大,基于关键词的搜索是最简单的技术之一,过滤的另一种高级形式是基于文档内容提取语义信息。

Bargain Finder 和 Jango 这两个系统就是从许多不同的 Web 信息源收集信息(如:产品描述,价格等)。Firefly 使用一个基于协作的过滤技术来给消费者推荐产品、利用协作技术,加上反馈技术,为不同的消费者排序并过滤掉不相关的信息。基于限制的过滤是用项目的特征来取舍与他们相关的信息。给定产品,商家的限制集,过滤掉不满足限制的产品,而保留其它剩下的, Tete-a-Tete 就利用基于限制的过滤在产品代理、商家代理等阶段。

Agent 为用户界面的人机交互 传统的购物经历依据消费者的需求和产品的不同而不同。把系统的用户界面和消费者的购物行为无缝结合在一起,可以带来更大的客户满意度。

目前应用最广泛的系统界面是“电子目录”,包含一个搜索引擎。可是这些对消费者而言,仍比不上他们在真实世界里购物来得方便。克服这个问题的方法是:在线模拟消费者熟悉的物理世界,如提供三维的虚拟实境(3D VRML)购物中心等。另外 Agent 凭图形化、半自动的角色,以自然语言和用户保持长期“个性化”的交互,通过学习用户的交易习惯,并模仿真实世界中的买、卖代理的行为方式,为顾客达成最佳的交易。Agent 通过即时、积极的反馈和个性化的能力,和顾客建立可信任关系。当然,目前的人工智能技术还需继续增强,以贴近用户的期望。Agent 系统中增强信任的关键是提高 Agent 的能力,Agent 可以展示多少可信行为并为它的行为提供解释,根据对市场的分析不断调整自身行为。我们可以极大地从这种设计良好的交互界面中受益。

协商机制 以 Agent 为中介的协商可追溯到契约网(Contract Net)。最初契约网是个分布式问题解决系统,给 Agent 分配任务,由它们投出标书,并最终获得合同。协商是通向做出最终决定的一个过程,两方或多方以达成共识为目标,探寻一个可能的解决方案。经济和游戏理论描述了交互的协议和策略。对一个给定的商业协议,交易者用一策略(协商动作的计划安排),来最优化他们的交易。还可给定一些知识和处理优先级(如:动机、价值、风险等),来进一步优化协商策略。

Agent 协商的研究领域很广,多 Agent 系统在分布式人工智能(Distributed AI, DAI)中就早有研究。早期的 DAI 把协商模型提升到通过协作来解决分布式问题的高度,即在多 Agent 系统中,通过联合、协作来达到一个共同目标。最近更多的多 Agent 系统则把工作重点转向基于电子市场的系统中(如: AuctionBot)的协商研究。

基础设施、语言和协议 现在有很多以 Agent 为中介的电子商务系统,但每个系统关注的仅是整个 CBB 模式中的一到两个阶段。而且,这些系统并不是为满足互可操作性而设计的,要把这些分散的系统无缝地连接在一起,还有很多工作要做。

前面提到的几种系统,如 BargainFinder 和 Jango,都要用专门的“包装器”技术来包装产品和商家的描述内容。为了使通信各方能共享信息和语义,需要定义一个各方都能识别的“共同语言”,以便相互理解和信息交换。目前的 HTML 只能用于数据表示,不能用于信息组织,而 XML(eXtensible Markup Language)是个元标注语言,它提供一种描述数据结构的格式,允许定义带有语义的数据标签,有助于更精确地声明内容,用 XML 就有助于生成 Ontology(本源论)——“共同语言”。

当然,XML 并不是一个实现系统互操作性的万能药。需要建立一个工业化的标准的通用 Ontology。Commerce Net 和其它组织,以及 IBM、微软在内的一些大公司已经就这方面展开工作,并且取得了相当的进展。然而,交易系统如何被全球化的定义及由谁来管理该系统的演化,仍是个需要解决的问题。

相关的基于 Agent 的语言和协议包括 KIF(Knowledge Interchange Format), KQML(Knowledge Query Manipulation Language), 及 Ontolingua: 一个 ontology 共享协议。这些是为异构化 Agent 和系统而设计的能描述知识和通信的协议。在电子商务中,这个知识将包括消费者概貌(profile)、商家、商品、服务及协商协议的定义和语义。

B2B 电子商务的领域协议是 EDI(Electronic Data Interchange, 电子数据交换), EDI 是一套为商家交易而提供的符合 ANSI 和 U. N. 标准的协议集。EDI 便于特定工业中的商家间进行大规模的、反复的、预安排的交易。尽管 EDI 是企业间电子商务的协议,它仍有一些缺点:定义模糊、实现和维护代价昂贵,而且 EDI 关注的是大规模的 B2B 交易,中、小型企业之间却缺乏 B2B 交易协议标准。其它的电子商务协议包括基于 Internet 的 EDI(EDIINT), XML/EDI, 安全电子交易(SET, Secure Electronic Transactions)等等。

除了文档和协议标准,还有对象和基于 Agent 的

电子商务构件标准。现在有几种竞争技术,包括 OMG 的 CORBA/IIOP(Internet Inter ORB Protocol),微软的 COM+,Sun 的 Java 和 ObjectSpace 的 Voyager,Mitsubishi 的 Concordia,General Magic 的 Odyssey,以及 IBM 的 Agelets 等等,其中几个被提议加入到 OMG 的 Mobile Agent Facility(MAF)。此外还有相关的安全技术、数据库技术等等。

三、现有的一些 Agent 为中介的电子商务系统

在介绍一些典型的以 Agent 为中介的电子商务系统之前,先介绍一下 CBB 模式。

传统商务中有几种描述理论和模式试图捕获消费者购买行为(CBB—Consumer Buying Behavior,消费者购买行为)——如:Nicosia 模式,Howard-Sheth 模式,Engel-Blackwell 模式,Bettman 信息处理模式,Andreassen 模式。尽管各有差异,但这些模型都有一个类似的引导消费者购买行为的6个基本阶段,称之为 CBB 模式。CBB 模式是帮助我们理解 Agent 作为中介在电子商务中的作用的——一个强大工具。以这个典型的商务模式来探索 Agent 在电子商务中作为中介的作用是很有用的,CBB 的6个阶段如下:

(1)需求确认(Need Identification):阶段特征化消费者开始意识到的某些未满足的需求。在此阶段中,消费者能通过产品信息受刺激,这一阶段在 Engel-Blackwell 模式中被作为问题识别。(2)产品代理(Product Brokering):此阶段包含信息检索以助于决定买“什么”。该阶段包含一个可替换产品的评价(基于消费者提供的标准),该阶段产生的结果被称为产品的“考虑集”。(3)商家代理(Merchant Brokering):该阶段包含上一阶段获得的“考虑集”,带有商家专门的信息以帮助决定从谁那儿购买,包括基于消费者选择标准的可替换商家的评价(如价格,质保,可用性,递送时间,信誉等)。(4)协商(Negotiation):此阶段是“如何”决定交易条件的。协商依市场复杂性的不同而相异。在传统的零售市场中,交易中的价格和其它方面通常是固定的,几乎没有协商余地。在其它市场中,如股票、汽车、艺术等,交易中的价格和其他方面的协商已集成到产品和商家代理中去了。(5)购买及递送(Purchase and Delivery):购买和递送一件产品表明了协商阶段的结束,某些情况下,可用的支付选择(如仅能以纸币,现金支付等)或递送选择可能影响产品和商家代理。(6)服务和评价(Service and Evaluation):这个后购买阶段涉及产品服务、客户服务及整个购买经验和决定满意度的评价。该阶段主要依赖于产品是从谁那儿买的。

从 CBB 角度,可以标志 Agent 作为中介在电子商

务中的作用。Agent 的个性化、连续运行和半自治等的天性使得它们更适合代替消费者做某些行为的中介,做涉及信息过滤和检索、个性化评价、复杂协商和基于时间的交互协商等行为。特别是,这些作用对应于 CBB 模式中产品代理、商家代理和协商三个阶段尤为突出,下面着重介绍这三个阶段及这三个阶段对应的一些 Agent 电子商务系统。

目前已有的 Agent 为中介的电子商务系统主要应用在 CBB 模式中如下三个阶段:产品代理、商家代理和协商;这三个阶段中有代表性的系统有如下一些:PersonaLogic,Firefly,Bargain Finder,Jango,Kasbah,Auction Bot,Tete-a-Tete。

产品代理 CBB 模式的产品代理阶段是帮助消费者决定“买什么”,这发生在确定了用户的一个需求之后;当决定哪种产品最适合用户的个人标准,下列 Agent 系统降低了消费者的搜索代价:PersonLogic,Firefly 和 Tete-a-Tete。

PersonLogic 是个基于特征的过滤工具,通过对需要的产品特征加以指定,过滤掉特定领域中不符合购买者的产品,最后返回一个由所有满足限制的产品组成的有序列表供用户选择。Firefly 类似于 PersonLogic,该系统目前用于推荐音乐 CD 和书籍之类的商品。Firefly 向消费者推荐产品,不是通过基于特征来过滤,而是通过一个叫做 ACF 的推荐机制(自动协作过滤:Automated Collaborative Filtering),ACF 推荐他们高度评价的产品,使用的推荐选项类似理智的人的选择。

商家代理阶段 商家代理阶段比较相似商家来对商家做出选择。

Anderson Consulting 的 BargainFinder 是第一个在线价格比较购买 Agent。给定一个特定的产品,BargainFinder 通过 Web 浏览器,从几个互不相同的商家 Web 站点获取价格。但一个明显的缺点是:商家们仅仅在价格上受比较,他们所提供的其它增值服务则被忽略掉,因此没在消费者购买决定的考虑中。

Jango 可看作是一个高级的 BargainFinder。Jango 通过从每个用户的 Web 浏览器发出请求,获取产品信息。这种方式,对商家的请求,就象从“真实的”顾客发来的——一样。这种互操作性使得对购买产品的消费者来说更便利,却没给商家留下太多选择。

MIT 媒体实验室的 Kasbah 是个在线的、多 Agent 的分类广告系统。用户通过创建一个交易 Agent,给它一定的策略指导,并把它发送到一个集中的 Agent 集市上去。Kasbah 的 Agent 能够找出潜在的另一方交易者,并代表他们的主人和其它 Agent 协商。每个 Agent 的目标是根据一系列用户指定的限制,如期

待价格、最高(最低)可接受价格,及完成交易的期限等,完成一个可接受的交易,Kasbah 的最新版加入了一个分布式的信誉机制叫 BBB(Better Business Bureau),交易者可根据交易完成的情况,给对方评定等级,然后用户 Agent 就能根据这些级别来决定它们是否应和这些 Agent 协商,他们的信誉是否满足用户指定的信誉值。

协商(Negotiation) 从 CBB 的角度看,协商阶段是决定价格和其它交易条款的阶段,为一个产品动态制定价格而不是把它定死的好处在于它把商家从需要决定商品的价值中解放出来;更进一步,这个负担被推向市场本身,由此带来的结果是有限的资源得到了更公平的分配。

现实世界中,某些拍卖类型需要所有参与者地理上处在一起,如同在一个拍卖场中;还有,对用户而言,协商的过程可能太复杂或太困难。幸运的是,很多这些障碍在数字世界中都消失了。例如:OnSale 和 eBay 的拍卖站点就是两个很受欢迎的站点;不像拍卖场,这些站点不需要拍卖活动的参与者物理处在一起。然而,这些站点仍需要用户管理他们自己的基于时间的协商策略,而这正是 Agent 技术的切入点。

目前有几种具有代表性的 Agent 系统,可以辅助顾客在交易条款上进行协商,典型的几个是:AuctionBot、Kasbah 和 Tete-a-Tete。

AuctionBot 是密执根大学的一个通用的 Internet 拍卖服务器,AuctionBot 的用户通过选择一种拍卖类型,并指定它的参数(如:消除时间,解决投标关系的方法,可允许的卖的数量等)来创建一个拍卖。买、卖双方能根据多边分布式协商协议来竞标。AuctionBot 和其它大部分拍卖站点的不同之处在于:它提供一个应用程序可编程接口(API),让用户创建自己的软件 Agent 在 AuctionBot 集市中自动完成拍卖任务。

Kasbah 系统中,用户通过创建各自的买、卖 Agent 来完成交易。这些 Agent 为买、卖双方在商家代理和协商 CBB 阶段自动完成大部分工作。Kasbah 中的协商是直接的,在买、卖 Agent 匹配好后,协商协议中唯一合法的动作就是买 Agent 向卖 Agent 提供一份没有时间和价格限制的标书,卖 Agent 以“Yes”或“No”来作为响应。给定了这个协议,Kasbah 为交易者提供三种基于时间的价格协商策略供选择:“直率型”、“理智型”和“固执型”。分别对应于直线型、二次函数型及对数型(基于时间变化),这些协商策略的简单性使得用户很容易理解他们的 Agent 在市场中是如何做的。

Tete-a-Tete 为零售模式提供一个独一无二的协商目标,不同于其它大多数在线协商系统仅仅就价格

方面进行竞争性的谈判,Tete-a-Tete 的 Agent 可以对交易的多个条款进行合作式协商—如质保、递送时间、服务合同、信贷等选项。象 Kasbah 一样,这个内商用的是多 Agent 的模式,支持双边讨价还价,但是它不像 Kasbah 中用简单的价格升、降函数,取而代之的是,Tete-a-Tete 的购物 Agent 遵循一个“反复、积极的”协商类型。

四、基于移动 Agent 的电子市场空间 MABEMS

网上现有很多电子市场,典型的有零售市场(如 Amazon)、二手货交易市场(如 eBay)、拍卖市场(如 e-Trade)等以及企业间用于电子采购、销售、供应链管理的 B2B 平台(如 Commerce One、Arriba)。考察现有这些电子市场系统,不难发现它们存在几点不足:(1)普遍采用集中式的市场体系结构,系统扩展和维护困难;(2)每个市场各成一个自包含的系统,各个市场之间难以实现服务和信息的交换;另外,(3)市场中各个交易过程都需要人的高度参与,自动化程度较低。

Agent 技术的出现使得构筑新的、更适宜的电子市场体系结构和交易自动化程度更高的电子市场成为可能。为此,我们以本实验室开发的移动 Agent 系统—Magent 2.0 为支撑平台,设计了一个开放的、分布的和交易高度自动化的电子市场体系结构 MABEMS (Mobile Agent-Based Electronic Market-Space)。

4.1 基于移动 Agent 的电子市场空间(MABEMS)概述

MABEMS 是由南京大学计算机软件新技术国家重点实验室设计、实现的一个基于移动 Agent 的电子市场空间模型。MABEMS 由一组代表市场参与者(如买方、卖方、中介和公证等)进行交易活动的移动 Agent 和一组分布于 Internet 的为 Agent 之间的交易活动提供支撑环境的电子集市服务器(Electronic Marketplace Server, EMS)及其他相关设施,如产品 Ontology 发布服务器(Ontology Server)、个人商务助理(Personal Business Assistant, PBA)、中央银行(Central Bank)、企业业务集成器(Enterprise Integrator)等构成。为完成其所有者预先制订的目标,Agent 可以在 EMS 之间,或 EMS 与其他设施之间自主流动。Agent 还能按照预先设置的交易策略,与其他 Agent 进行一对一的协商、拍卖等交易活动。

MABEMS 原型系统,初步实现了市场空间中产品 Ontology 发布服务器、PBA、EMS 以及中央银行等部分,并实现了市场空间中买者与卖者,这两类典型的移动 Agent,其中,中央银行属于 Magent2 系统的一部分,用于移动 Agent 站点的资源管理,在 MABEMS

中,被用于交易各方之间的电子货币支付(或转账)。

MABEMS 支持多种交易模式,如零售、拍卖;用户所要做的仅仅是在本地通过图形化界面的 PBA 创建买、卖 Agent,给定它们的任务和一些协商策略,这

些 Agent 就可以在电子市场中移动,自主地和其它 Agent 协商、交易,一旦达成交易就通知用户确认。

4.2 MABEMS 总体框架

MABEMS 总体框架如图1所示。

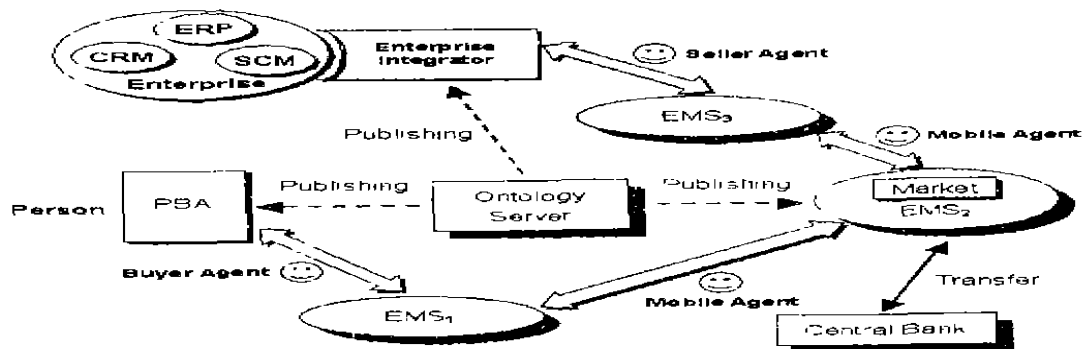


图1 基于移动 Agent 的电子市场空间示意

4.3 Ontology 发布服务器、EMS 和 PBA

产品 Ontology 由于商品与商品之间存在着类属和所有两种关系,前者描述了商品的分类的层次关系,后者描述了一个商品的各部分组成情况,这两种关系均可以用树形结构表示,XML 具有树形结构、支持项与项之间的类属和所有关系、结构简单、易于机器自动处理等特点,使 XML 较适宜用于实现市场空间中的产品 Ontology。通常情况,一个特定的产品(如,汽车、书)Ontology 可以用一个 XML-Schema 文件(+ xsd)表达。

在 MABEMS 中为了保持产品 Ontology 的一致性,我们设立了一个独立的产品 Ontology 发布服务器,通过其向市场空间的其他各部分如,EMS、PSA 等发布产品 Ontology 信息。市场空间中各部分,若要使用某个产品的 Ontology 信息,都可以通过 Ontology 发布服务器提供的编程接口获得。一般情况下,为了保证产品 Ontology 的一致性,采用即时获得的方式,但为了满足系统运行效率的要求,在 EMS、PSA 的实现中作了本地缓存。

电子集市服务器(Electronic Marketplace Server, EMS) EMS 是 MABEMS 的重要组成部分,为各种 Agent 提供接洽和协商的场所。一个集市(Marketplace)由多个独立的市场组成,通常这些市场按交易商品的类别(如书、汽车等)进行分类。同时,市场也按交易类型(如零售、拍卖等)进行分类。EMS 为这些独立的市场运行提供公共的服务和支撑。包括集市管理控制台(MMC)(含系统配置、管理、监控等功能),支持多种交易模式,对交易和交易者提供数据库支持,计费管理。

个人商务助理(Personal Business Assistant,

PBA) 市场空间中,个人用户使用 PBA 进行配置、发送和监控交易移动 Agent,使其能正确、可靠地代替用户完成交易任务。PBA 主要分为三部分:(1)创建交易 Agent 并发送,(2)交易 Agent 的监控,(3)交易历史决策数据库。用户通过指定交易任务的选项,创建一个交易移动 Agent,并且将它发送到电子市场空间中去,让它代替用户自主的和市场其它 Agent 协商、交易;用户原则上是仅仅在确认交易时和自己的 Agent 交互,但不排除用户对 Agent 进行监控、交互,甚至随时中止 Agent 的运行,对 Agent 的监控就负责完成这些工作;Agent 在出发之前,可以通过学习以往在市场中交易积累的经验教训,优化自己的交易策略,这部分工作就通过交易历史决策数据库来实现。

总结和未来方向 本文介绍了电子商务和 Agent 的概念,以及应用在电子商务中的 Agent 技术、现有的一些以 Agent 为中介的电子商务系统,并且介绍了我们基于本实验室的移动 Agent 系统平台—Mogent 2.0,设计并实现的基于移动 Agent 的电子市场空间—MABEMS。这个系统还将就理论和实践上做进一步的完善和增强。

今天的第一代以 Agent 为中介的电子商务系统已经创建了新的市场,进一步降低电子商务的交易成本,增加便利。然而,对于将 Agent 技术更好地应用到电子商务中,还有很长的路要走。这些在下一代以 Agent 为中介的电子商务中,面向 Agent 的电子商务涉及到社会和法律问题,体系结构、环境和语言设施,描述产品与服务语言,与遗产系统集成问题,Agent 的加密及信用授权,访问控制,人机界面,Agent 行为的可视化,Agent 的 Web 数据挖掘,面向 Agent 的中间件服务、Agent 性能衡量等,都是需要继续研究的课

一个新的电子商务的安全方案:HTML 表单签名^{*}

A New Resolution of Safe E-Commerce:HTML Form Signing

李 娟 左 春

(中国科学院软件研究所 北京100080)

Abstract Many kinds of e-commerce require the ability to prove that someone has authorized a transaction. One way to provide such proof is to associate a digital signature with data generated as the result of a transaction. However, until now, there has been no widely available, standards-based way to digitally sign forms or other transaction-related text on the Web. This paper presents an implementation of HTML form signing, which utilizes the Public-Key Cryptosystem and the Digital Signature technology. By providing components of client and server, the system signs the user's form at the client end and verifies it at the server end.

Keywords HTML Form, Form signing, ActiveX Control

随着计算机和电子通讯技术,包括因特网的迅猛发展,金融电子化的步伐大大加快,许多传统上基于纸面的、常常需要签名盖章的重要凭证,已陆续转化为数字电子媒体的形式出现。目前,许多网站都是通过HTML表单(或称为HTML页面)的形式在Internet上接受用户输入的请求信息,从非常简单的订阅电子杂志的请求到具有高度商业价值的信息,如BtoB、BtoC业务中用户和商家之间传递的商业信息。在交易过程中为双方提供不可伪造的、不可抵赖的签名信息将是非常必要的。虽然SSL技术在SSL连接期间提供暂时的客户身份认证,但它不能为连接期间发生的交易提供持续稳定的认证。一个提供这样认证的方法是把数字签名连同交易产生的数据作为交易的结果信息。

1 签名交易信息方法之分析比较

由于普通的HTTP协议不支持数据的加密与签名,信息以非加密的形式在网络上传播,这就可能被非法窃听、非法篡改,没有签名信息,又无法确认信息发送者的真实性,无法防止信息发送者抵赖交易。为了解决这个安全漏洞,目前,实现对传输信息进行加密和签名的方法主要有以下几种:

(1)采用HTTPS协议 SSL(安全套接层)是Netscape公司为通过互联网传送保密文档而开发的协议,SSL技术使用公开密钥的算法将要通过SSL连接传送的信息进行加密,保证传输的安全性,HTTPS加密协议就是通过SSL进行HTTP传输的协议,它是一种最通用的方式,目前Navigator和Internet Explorer都支持SSL。但是这种方法有以下的缺点:

^{*} 本文得到国家863计划项目(863-306-ZD06-02-8)的资助。李娟 研究生,研究方向:软件工程。左春 研究员,研究方向:软件工程。

题。

参 考 文 献

- 1 Moukas A, Robert Guttman and Pattie Macs, Agent-mediated Electronic Commerce: An MIT Media Laboratory Perspective. Software Agents Group, MIT Media Laboratory
- 2 Nwana H S, et al. Agent-Mediated Electronic Commerce: Issues, Challenges and some Viewpoints. In: Proceedings of Autonomous Agents'98
- 3 Tsvetovaty M, et al. MAGMA: An Agent-Based Virtual Market for Electronic Commerce
- 4 Chavez A, Maes P. Kasbah: An Agent marketplace for buying and selling goods. 1996
- 5 Dasgupta P, et al. A Supplier-Driven Electronic Marketplace Using Mobile agents. Department of Electrical and Computer Engineering, University of California, Santa Barbara, CA
- 6 Zacharia G, et al. An agent system for comparative shopping at the point of sale. Software agents Group, MIT Media Laboratory
- 7 Wurman P R, Wellman M P, Walsh W E. The Michigan Internet AuctionBot. A Configurable Auction Server for Human and Software agents. University of Michigan, Artificial Intelligence Laboratory