考虑安全与公平的电子市场

叶东海,吕 捷

(南京财经大学 信息工程学院, 江苏 南京 210046)

[摘要] 随着 Agent技术的不断发展,传统电子商务开始进入移动电子商务时代.但在实际应用中,移动 Agent面临恶意攻击、数据毁灭、商业欺诈等诸多安全威胁.本文提出一种由独立第三方设立的安全、公平的电子市场.它能保证客户和商家双方身份的不可伪造性和交易信息的不可拆分性,实现了各商家之间身份和交易信息的保密;市场通过信息公开、异常交易警示等措施来保证交易的安全、公平.

[关键词] Agent;公开密钥机制;电子市场
[中图分类号] TP39 [文献标识码] A [文章编号] 1672-1292(2010)04-0084-04

An E-Market with Security and Fair

Ye Donghai Lü Jie

(School of Information Engineering, Nanjing University of Finance and Economics, Nanjing 210046, China)

Abstract: With the development of mobile agent technology, the traditional e-commerce is entering into the era of mobile e-commerce. But in practical applications, mobile agents are facing malicious attacks, data destruction, commercial fraud, and many other security threats. This paper presents an e-market with security and fair which is set up by an independent third party. It can ensure that the identity of both customers and merchants can not be forged and transaction information can not be split, and moreover, it will secret one transaction information against others. Through information disclosure, warnings unusual transactions, the market guarantee the transaction security and fair.

Key words: Agent; security; PKI; e-market

随着 Web技术的迅速发展,电子商务逐渐繁荣起来.电子商务市场可能面向供应商或面向客户,无论哪一种都面临信息共享的问题.对于企业或个人来说,将自己的数据存储在其他公司的数据库中是不能接受的.移动 Agent的出现为传统电子商务模型提供了新的解决方法.国内在此方面的研究较典型的有南京大学开发的基于移动 Agent的电子市场模型——MABEMS[1],成都电子科技大学开发的基于移动 Agent的协作信息中间件 CISOM 电子商务模型 B-CISOM[2].

现有的移动 Agent电子商务模型,大多由委托人发布移动 Agent在网络上进行自由移动,由于移动 Agent具有自主行为,且本身往往带有大量数据、程序代码等,这给网络流量和网络的安全性带来了极大挑战.安全性是电子商务最关键的问题,也是必须解决的问题,其中黑客、病毒、恶意欺骗、哄抬、扰乱、操纵市场等已成为移动 Agent在电子商务应用中的最大障碍.

本文提出一种由可信的独立第三方设立的公开电子市场[3-8],它利用公开密钥机制实现市场参与各方数据的保密性和完整性;利用信息过滤机制、信息公开机制和信用评价机制实现市场的公开、公平.对比已有的研究成果,系统在安全性和防止恶意 Agent扰乱、操纵市场上有明显优势.

1 电子市场的基本结构

本文提出的电子市场由第三方单独设立,它本身并不参与市场交易而只提供交易服务,这样可以保证其立场中立,因为欺骗任何市场参与者只能导致自己利益受损.

收稿日期: 2010-08-17.
通讯联系人: 叶东海,硕士,讲师,研究方向:人工智能,多 agent系统. E-mail: donghai@njue.edu.cn

1.1 设立前提

(1) 电子市场由独立第三方设立, 假设其是中立的, 不会操纵市场, 也不会欺骗任何市场参与方.

(2) 所用的公钥密码机制是安全的; 所用的哈希算法是安全的; 市场参与方的私钥是安全的.

1.2 基本结构

公开电子市场的基本结构如图 1所示. 它由认证中心、交易系统、身份认证、信息过滤器等部分组成.

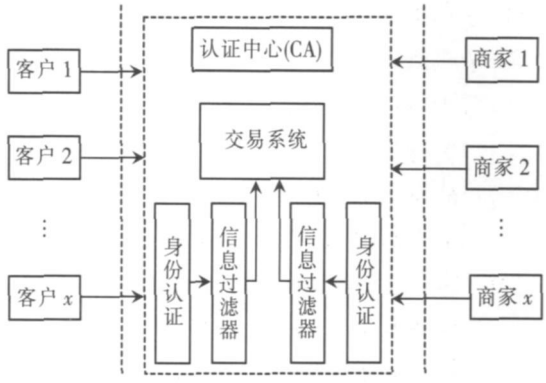

图 1 系统总体结构

Fig.1 System architecture

所有的市场参与方必须先在认证中心进行认证并获得数字证书. 客户或商家派遣移动 Agent参与市场时, 认证中心首先对其身份进行确认, 所有非法的 Agent将被拒绝访问. 商家或客户可以随时派遣 Agent加入市场执行新的交易、更新供需信息, 也可以用来取代过时的 Agent

信息过滤器用来对客户或商家的交易信息进行过滤, 所有不合法的或异常的交易信息将被屏蔽, 而有效的交易信息将传送到交易系统的信息管理器.

交易系统是整个电子市场的核心, 它包括信息服务器、Agent管理器、中介服务、信用管理器等组成部分. 其中信息服务器接收来自过滤器的信息, 并分别对客户需求、商家供应信息进行分类、整理并发布, 供所有市场参与者查询.

Agent管理器其实是对市场参与者进行管理, 包括名字管理、地址管理等. 因为 Agent的移动性, 其信息应及时更新, 以便其他 Agent可以随时找到并与其进行协商.

中介服务是一项可选服务. 商家或客户 Agent可通过查询信息管理器发布的信息自主选择谈判对象去完成交易, 也可要求市场提供更详细、具体的中介信息服务. 中介服务具有选择、评估和分配等功能. 选择功能是将客户的需求信息与商家的供应报价进行比较. 若客户很多, 系统会动态生成客户团购体 (客户联盟), 但不允许卖家结盟. 同时, 由于不同的商家可能在匹配客户的需求时有不同的规则, 因此被选择的商家可根据自己的交易规则挑选客户. 评估就是将动态形成的客户联盟的信息告诉多个商家, 等待商家的评估结果. 若商家愿意与客户进行下一步的协商, 即可利用分配功能来完成客户和商家的匹配. 完成匹配后代表商家和客户的 Agent可进一步谈判以真正达成交易.

信用管理[9]负责 Agent评价. 在交易完成以后, 交易双方应对对方进行评价, 市场采集双方的评价后, 将其作为信用指标向所有参与者公布, 以促进市场参与方诚信交易.

1.3 交易流程 (以客户为例)

(1) 通过 CA 认证的客户有交易需求时创建移动 Agent并将其派遣到电子市场;

(2) 通过电子市场身份认证的 Agent到 Agent管理器进行身份登记 (包括 ID、客户 ID、通讯地址等), 由于 Agent的移动性, 其地址应实时更新;

(3) Agent把部分交易信息告诉信息过滤器;

(4) Agent查询信息服务器的信息 (可直接向客户返回查询结果), 寻找潜在交易对象或等待中介服务的匹配结果;

(5) Agent分别与不同潜在交易对象进行谈判, 将最后的协商结果返回给客户;

(6) 客户 (商家) 对协商结果进行选择确认, 本次交易完成 (终止);

(7) 交易双方在一个时限内对对方进行评价, 并将评价信息告诉信用管理器;

(8) 信用管理器修改相关客户和商家的信用.

2 系统实现策略

2.1 市场安全性的实现

要实现电子市场的安全性, 需解决主机 (运行环境) 安全、代表客户或商家的移动 Agent的数据安全以及移动 Agent执行的完整性及机密性.

对于主机安全,主要通过对移动代码进行认证,虽然认证本身不能判断移动代码是否为恶意代码,但可以判断代码来源的可靠性,认证其是否来自于一个合法的来源. 因此要求市场参与方必须先向市场注册并获得自己的数字证书. 其他的安全机制由具体平台实现. 如 Java 2平台提供可配置的安全策略可防止 Java程序非法读取文件,或非法建立与其他主机的网络连接,或在未经允许的情况下访问打印机等. 此策略建立在 Java的存取控制机制上,相应的存取控制器则依赖于 Java的类装载器、安全管理器和语言保护等安全机制.

对于客户或商家的数据安全,主要用数字签名及加密来实现. 具体的实现方法为:

(1) 符号约定:H 为哈希函数; TS 为时间戳; E 运算为公开密钥机制的加密; D 运算为公开密钥机制的解密; SK 为私钥; PK 为公钥.

(2) 方案说明:假设移动 Agent由 3部分构成: Agent代码和基本数据(CBD)、客户(商家)的商业数据(BD)、客户(商家)的认证数据(CK). 方案的重点在于保护客户商业数据 BD 不被窃取、篡改和伪造.

为防止其他 Agent窃取商业数据, Agent需要用其公钥 PK 对 BD 做 E 运算得到 $BD^* = E_{PK}(BD)$,显然 BD^* 只有其私钥才能解密,即只有它自己才能访问. 同时 BD 的完整性由商家的认证数据得到认证.

算法如下:

1) Agent初始化时,首先生成时间戳 TS_0,然后对标识 ID, TS_0 进行哈希函数运算,得到 $H_0 = H(ID, TS_0)$. 最后用私钥对其进行数字签名得到 $CK_0 = E_{SK}(H_0)$. CK_0 作为其认证数据存储在 Agent中.

2) 当 Agent到达电子市场,认证中心用公钥对 CK_0 进行 D 运算得到 $H_0 = D_{PK}(CK_0)$,完成对 Agent的身份认证.

3) 当 Agent在电子市场中与其他 Agent进行协商产生了新的 BD 时,首先生成时间戳 TS_X,然后对对方标识 ID_X, BD_X, TS_X 用自己的公钥进行 E 运算得到 $BD_X^* = E_{PK}(ID_X, BD_X, TS_X)$,再对 BD_X^* 进行哈希函数运算得到 $H_X = H(BD_X^*)$,最后让对方用私钥进行签名得到 $CK_X = E_{SK}(H_X)$.

4) 重复步骤 3).

在协商结束时, Agent会得到一系列的协商数据 ID_X, BD_X, TS_X 及对应的认证数据 CK_X. Agent分别用对方的公钥和自己的私钥对它们进行 D 运算即可验证数据的真实性和完整性. 因为所有的认证信息都含有时间戳,故可保证 Agent执行的完整性,防止重放攻击.

2.2 市场公平的实现机制

要实现市场的公平,就要防止恶意 Agent发布虚假信息、制造虚假交易、垄断甚至操纵市场. 市场采用以下手段来实现交易公平:

(1) 信息过滤:通过认证的客户或商家首先要把自己的基本交易信息提交给信息过滤器,但无需将自己的谈判策略、价格底线等内容告知过滤器. 过滤器参考相同商品的历史成交记录,去除价格明显偏离的信息,并通知 Agent其交易要求不被市场接纳.

(2) 信息公开:经过过滤的交易信息被送到交易系统的信息服务器中. 信息服务器对信息进行分类、整理并写入数据库中,供所有市场参与者查询. 所有的历史成交信息也存储在信息服务器中并对所有市场参与者公开. 这样有利于所有市场参与者更准确把握市场行情. 客户或商家无法自行发布其交易信息(所有的交易信息都在信息服务器上公开),这样可以有效防止恶意 Agent发布虚假信息扰乱市场.

虽然客户或商家的基本交易信息及最终的市场成交价格完全公开,但由于客户(商家)的具体谈判策略、真实的价格底线、货物的运输仓储等信息是保密的,所以并不会泄露客户(商家)的商业秘密.

(3) 信用评价:在交易完成后,交易双方需对对方的产品质量、服务等做出评价. 系统会根据交易金额、频次等信息实时修改交易双方的信用. 所有客户(商家)的信用在 Agent管理器中可查.

(4) 防止虚假交易:为防止恶意的商家(客户)制造虚假市场信息或骗取信用而故意制造大量的虚假交易,信息管理器会对异常交易进行信息屏蔽,如价格明显偏离市场历史成交价格的、短时间内异常频繁的交易等,也可线上、线下结合,如要求交易双方提供真实有效的交易凭证(如完税凭证)以提高其制造虚假交易的成本.

3 交易系统的实现

如前所述,设计的交易系统如图 2所示. 该系统主要负责市场管理和信息服务,具体交易的协商策略

和交易细节由客户(商家)Agent负责并对市场保密. 客户(商家)Agent可在本地或局域网上对信息服务器、Agent管理器、信用管理器等进行数据查询,而数据的提交或修改则必须经过信息过滤器. 本系统采用 IBM 的 Aglets作为系统的平台,使用 Java进行程序开发,采用 Oracle 9i作为后端数据库. 例如,某客户 Agent查询某商品的供应信息,信息服务器均采用固定格式返回查询结果:@QID=Result#@GoodsName=* * * * #@Model=* * * * * * #…@Price-Between(Val1,Val2)#…@SID=(S1,S2,S3,S4)#. 其中,QID为查询 ID;GoodsName、Model描述商品名称、规格等属性;Price-Between表示查询到的该商品的价格区间;SID为该商品的多个供应商 ID;为提高效率,信息服务器一次只向客户返回 4个数量满足且 δ值($\delta=|Price_i-\overline{Price}|$)最小的供应商 ID. 客户 Agent在获得以上返回信息后,可选择供应商进行下一步的协商.

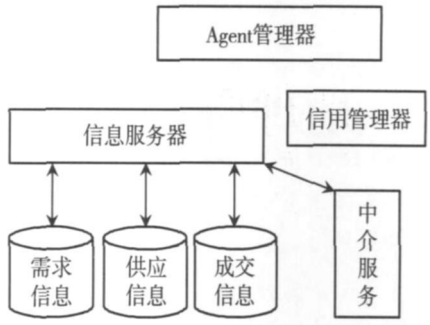

图2 交易系统基本结构

Fig.2 The architecture of trading system

4 结语

将移动 Agent技术用于电子商务领域是当前的研究热点,如何保证市场参与各方的信息安全、维护交易的公平、公正是电子商务成败的关键. 市场时刻面临恶意攻击、数据毁灭. 商业欺诈与操纵等诸多安全威胁. 本文提出一种由独立第三方设立的安全、公平的电子市场,它能保证客户和商家双方身份的不可伪造性和交易信息的不可拆分性,市场通过信息公开、信用评价等措施来保证交易的公平、公开. 对比已有的研究成果,系统在安全性和防止恶意 Agent扰乱、操纵市场上有明显优势,进一步的研究是如何在确保安全、公平的前提下提高市场的交易效率.

[参考文献](References)

[1] 徐锋,吕建,陶先平. MABEMS:一个基于移动 Agent的电子市场空间[J]. 南京大学学报:自然科学版, 2002, 38(2): 131-138.
Xu Feng, Lü Jian, Tao Xianping. MABEMS—a mobile agent based electronic market space[J]. Journal of Nanjing University: Natural Science Editon, 2002, 38(2): 131-138. (in Chinese)

[2] 胡健,刘锦德. 一个基于协作信息中间件的电子商务信息系统[J]. 计算机应用, 2001, 21(4): 4-6.
Hu Jian, Liu Jinde. A cooperative information middleware based on information system for E-commerce[J]. Journal of Computer Applications, 2001, 21(4): 4-6. (in Chinese)

[3] 叶东海. 合同网协议中的信用模型[J]. 计算机应用与软件, 2010, 27(3): 231-233.
Ye Donghai. Credit model of contract net protocal[J]. Computer Applications and Software, 2010, 27(3): 231-233. (in Chinese)

[4] Barbosa G P, Silva F Q B. An electronic market place architecture based on technology of intelligent agents and knowledge[J]. Lecture Notes in Computer Science, 2001, 2033: 39-60.

[5] He Minghua, Jennings N R, Leung Ho Fung. On agent-mediated electronic commerce[J]. IEEE Transactions on Knowledge and Date Engineering, 2003, 15(4): 985-1003.

[6] Li Jian, Wang Cong, Yang Yixian. An adaptive genetic algorithm and its application in bilateral multi-issue negotiation[J]. Journal of China University of Posts and Telecommunications, 2008, 15(1): 94-97.

[7] Choi J K, Park J S, Lee J H, et al. Key factors for e-commerce business success[C]//Proceedings of the 8th International Conference on Advanced Communication Technology. South Korea: Telecomm Res Institute, 2006(3): 1664-1672.

[8] Du T C, Li E Y, Chang A P. Mobile Agents in distributed network management[J]. Communications of the ACM, 2003, 46(7): 127-132.

[9] 郭文生,杜军平,尹怡欣,等. 多 Agent协作技术在电子商务中介平台中的研究与应用[J]. 计算机应用与软件, 2006, 23(6): 127-129.
Guo Wensheng, Du Junping, Yin Yixin, et al. The study of multi-agents incorporation in an E-Business intermediation platform[J]. Computer Applications and Software, 2006, 23(6): 127-129. (in Chinese)

[责任编辑:严海琳]