

基于信任算法的分布式农产品交易系统设计

章程 郭曦 田芳

华中农业大学信息学院, 武汉 430070

摘要 针对分布式农产品交易系统里的主机和网络通信容易受到安全威胁的现状, 提出一种基于信任的安全算法。首先, 使用移动代理对用户交易记录进行综合统计并计算出行为信任值; 然后对用户反馈进行分析筛选, 计算出推荐信任值; 最后对各种信任值进行分析, 得出综合信任值。使用该算法的分布式农产品交易系统运行正常, 能较好地保障网络交易安全。

关键词 分布式系统; 农产品交易; 移动代理; 信任值; 信任算法

中图分类号 TP 397.07 **文献标识码** A **文章编号** 1000-2421(2016)06-0092-06

加强农产品电子商务平台的建设, 健全农产品交易体系在农业信息化中具有重要作用^[1]。1999年, 广西建立了我国第一个大宗农产品电子交易平台^[2], 截至目前, 全国已有一百多家类似的平台。在农产品交易中, 为了找到所需农产品, 顾客通常不得不浏览若干个网站进行选择, 然后从中找出适合自己的且性价比较高的农产品, 最后进行订购, 上述购物过程都需要客户在线进行操作, 但是当电子商务系统的应用量越来越大时, 这种在线操作的代价也将越来越大^[3]。一种新的分布式计算模型—移动 Agent (mobile agent) 近年来引起研究人员的广泛关注并被引入到电子商务领域中^[4]。移动 Agent 是一段可执行的程序, 它能够携带其代码和状态自主地从网络中的一个节点移动到另一个节点上运行, 寻找合适的计算资源和信息资源, 完成特定的任务。移动 Agent 的基本特性是自主性和移动性, 其基本目标是减少网络传输和实现异步交互, 因而被认为是未来的主流分布计算模式^[5]。移动 Agent 在云环境^[6]和大型分布式系统上具有很强的适应性和优势, 这使得移动 Agent 在农产品电子商务的应用上前景广阔。

随着电子商务的快速发展, 各种网络欺诈层出不穷, 信任问题逐渐成为阻碍电子商务进一步发展的重要障碍。目前, 许多大型电子商务平台都建立了自己的信任评价体系^[7], 如亚马逊和淘宝等, 但这

些评价体系相对简单, 且局限于单一平台。移动 Agent 的主动性和移动性可以使它在多个节点、不同平台间自主运行, 可以实现农产品信息的智能发现、双方自动协商、安全的交易管理等, 更加适应农产品电子商务的进一步发展的需要。现在, 移动 Agent 已经在电子商务、分布式计算等领域中得到日益广泛的应用, 但是移动 Agent 的安全性问题一直难以很好地解决。在当前的环境下如何使用信任算法更好地去保护移动 Agent 的安全已成为热点课题之一^[8]。

1 材料与方法

移动 Agent 系统中信任关系^[9-10]的建立一般有 2 种方法: 一是主机记录与自身交易主机的相关信任信息, 通过信任信息来计算信任值, 建立信任关系。如果信任信息不够, 可以通过主机间的交互, 在不同主机之间搜集信任信息, 然后通过信任信息, 主机自己建立信任关系。另一种方法是通过可信的第三方如信任中心来建立信任关系, 也就是建立一个所有主机都信任的信任中心。信任中心对信任信息进行记录、更新、计算, 并进行维护, 主机需要得到信任信息时, 可以从信任中心申请。其中, 第 1 种方法每个主机自身都要维持一个自身的信任数据库, 而且需要不断更新。而第 2 种方法通常是由一个信任中心来建立信任关系, 虽然简单一些, 但并不适合于

收稿日期: 2016-06-07

基金项目: 国家自然科学基金项目(61502194); 中央高校基本科研业务费专项(2662015JC010)

章程, 博士研究生, 讲师。研究方向: 电子商务、生物信息。E-mail: sameboy@mail.hzau.edu.cn

通信作者: 田芳, 讲师。研究方向: 计算机网络、生物信息。E-mail: fangzhihai_2003@mail.hzau.edu.cn

移动代理的计算环境。移动代理中的信任关系通常是使用第 1 种方法来实现,本研究讨论的也是这种情况。在本信任机制中,一个主机和信任有关的主要属性有:行为信任值、推荐信任值、被推荐次数、恶意行为次数。行为信任值是指在代理系统中,主机在经过和其他主机进行交互、被主机记录下来、通过一定的计算获得的信任值。这个信任值是和主机在移动 Agent 系统中的善意或恶意的行为直接相关的,所以称为行为信任值。推荐信任值是指信任值达到一定标准的主机,对其他主机进行推荐,被推荐主机经主机计算获得的信任值。显然,推荐信任值在信任方面的可信程度比不上行为信任值。在本信任机制中,判断主机信任程度时,取行为信任值和推荐信任值中较高的一个,依据信任值,把主机信任程度分为 5 个等级,从低到高位依次为:高恶意主机、低恶意主机、一般主机、低信任主机、高信任主机。

推荐行为只能由高信任主机作出,而高恶意主机则不允许被推荐。为了避免主机信任值“虚高”,本信任机制规定推荐信任值的上限为达到低信任主机所需信任值的下限,达到这个限度之后即使还有其他主机推荐,其推荐信任值也不会提高。推荐信任值可以使一个低恶意主机或一般主机更快地加入到商业活动中来,因此,推荐信任值是行为信任值的一个补充。在 2 个信任值中,行为信任值更为重要。推荐信任值虽然有上限的限制,但是它对行为信任值不高的主机意义重大,因为在推荐的时候必须谨慎,只能由高信任主机做出,在到达上限之前,每次推荐都会使推荐信任值有一定的上升。在达到上限之后,虽然不再上升,但被推荐次数也可为其他主机决定交易对象时提供参考。

1.1 行为信任值的计算

在 1 次成功的交易中,代理源主机 X 发出的代理要在多台主机(如主机 Y)之间搜集信息,然后与其中 1 台主机 Z 进行交易。显然,这两个阶段的重要性并不一样,但这两个阶段都是交易的组成部分,因此,信任值计算的时候,必须都将其考虑在内。这样才能比较好的反映一个主机的行为信任值。近一段时间来,主机的交易活动和交易评价显然更有参考价值,所以在计算行为信任值的时候,需要对近期的行为进行评价,以便交易主机参考。近期行为信任值如公式(1):

$$T_{t(Y|X)} = \frac{\sum_{i=1}^g m_{xy\Delta t}^i \times e_{xy\Delta t}^i}{\sum_{i=1}^g m_{xy\Delta t}^i + \sum_{j=1}^b m_{xy\Delta t}^j} \quad (1)$$

$T_{t(Y|X)}$ 表示最近一段时间内主机的近期行为信任值,近期行为信任值主要是对主机最近的交易活动进行评价,使交易参与者能比较好地把握主机最近的交易走势,更好地做出交易决策。 $m_{xy\Delta t}^i$ 表示最近一段时间内第 i 次交易的金额, $e_{xy\Delta t}^i$ 表示最近一段时间内第 i 次交易的评价, $0 \leq e_{xy\Delta t}^i \leq 1$ 。

近期行为信任值只能表示主机近期的行为,2 个主机经过长时间的交易活动,有时候主机可能存在恶意行为,或者存在一些交易上的欺诈,不管是恶意行为还是正常的交易行为,在计算主机信任值的时候都必须考虑到,对交易活动的整体评价需要用长期行为信任值如公式(2)来表示:

$$T_{a(Y|X)} = \alpha \frac{l_g}{l_g + l_b} + \beta \frac{m_g}{m_g + m_b} + \gamma \frac{\sum_{i=1}^g m_{xy}^i \times e_{xy}^i}{\sum_{i=1}^g m_{xy}^i + \sum_{j=1}^b m_{xy}^j} \quad (2)$$

$T_{a(Y|X)}$ 表示主机 Y 对于主机 X 的长期行为信任值, l_g 表示正常的提供数据的次数, l_b 表示恶意的提供数据的次数, m_g 表示正常的交易次数, m_b 表示恶意的交易次数, m_{xy}^i 表示第 i 次交易的金额, e_{xy}^i 表示第 i 次交易的评价, $0 \leq e_{xy}^i \leq 1$, $\alpha + \beta + \gamma = 1$ 。

在社会活动中,信任需要长年累月的善意或正常交互活动的积累才能慢慢的产生。信任的积累是缓慢的,但是信任的丧失却是非常快速的,可能只需要 1~2 次恶意的活动,以前积累了很长时间的信任就会丧失殆尽。信任的累积和丧失的速度是不对等的。对于主机而言,需要谨慎的对待每次交易,因为恶意的欺诈后果是非常严重的,为了加大对恶意活动的惩罚,加入惩罚参数 δ , $\delta \geq 1$ 。公式(1)和(2)相应的变为公式(3)和(4):

$$T_{t(Y|X)} = \frac{\sum_{i=1}^g m_{xy\Delta t}^i \times e_{xy\Delta t}^i}{\sum_{i=1}^g m_{xy\Delta t}^i + \delta \sum_{j=1}^b m_{xy\Delta t}^j} \quad (3)$$

$$T_{a(Y|X)} = \alpha \frac{l_g}{l_g + \delta \times l_b} + \beta \frac{m_g}{m_g + \delta \times m_b} + \gamma \frac{\sum_{i=1}^g m_{xy}^i \times e_{xy}^i}{\sum_{i=1}^g m_{xy}^i + \delta \times \sum_{j=1}^b m_{xy}^j} \quad (4)$$

加入惩罚参数 δ 后,恶意活动所降低的信任值将会超过正常交易所获得的信任值,而持续的恶意活动会使惩罚参数变大,信任值的降低速度将会更快。惩罚参数的取值不能随意,需要考虑到多种情

况。如果取值过低,对恶意行为的惩罚力度也就不够,恶意主机可能进行多次恶意活动之后,其行为信任值才会降到一个比较低的程度,如果取得过高,一个主机可能只进行了 1 次恶意活动,就被降得很低,也不符合要求。

1.2 推荐信任值的计算

在计算推荐信任值之前,需要对搜集到的信息进行分析甄别,计算搜集数据的标准方差,如果搜集数据与均值及标准方差相差太远,则不予采用。搜集到的近期和长期行为信任值的均值如公式(5)和(6)为:

$$a_1 = \frac{\sum_{i=1}^d T_{t(Y|Z_i)}}{d} \quad (5)$$

$$a_2 = \frac{\sum_{i=1}^d T_{a(Y|Z_i)}}{d} \quad (6)$$

近期与长期行为信任值的方差可以通过公式(7)和(8)计算:

$$c_1^2 = \frac{\sum_{i=1}^d (T_{t(Y|Z_i)} - a_1)^2}{d} \quad (7)$$

$$c_2^2 = \frac{\sum_{i=1}^d (T_{a(Y|Z_i)} - a_2)^2}{d} \quad (8)$$

根据公式(5)~(8)计算出的 a_1 、 a_2 、 c_1 、 c_2 等 4 个值对所搜集到的行为信任值进行甄别。如果从主机 Z_i 上搜集到的近期行为信任值 $T_{t(Y|Z_i)}$ 不满足 $a_1 - c_1 \leq T_{t(Y|Z_i)} \leq a_1 + c_1$,则放弃搜集到的数据。同样,如果从主机 Z_i 上搜集到的长期行为信任值 $T_{a(Y|Z_i)}$ 不满足 $a_2 - c_2 \leq T_{a(Y|Z_i)} \leq a_2 + c_2$,也要放弃搜集到的长期行为信任值。搜集到的信任值如果偏差太大,在计算推荐信任值的时候会使得推荐信任值的波动很大,不能符合信任的真实情况。而且在网络中总存在一些不真实的信息,这些信息可能是对目标主机的诋毁或者故意拔高,不管怎样这些信息的存在都会使得信任值的计算出现偏差。即使有些信任值是真实的,但是由于与目标主机交互过少,从而计算出的信任值偏差太大,这样的信任值在计算推荐信任值的时候也不能采用。

经过筛选后,搜集到的对目标主机 Y 的信任信息应该还是比较可靠的。如果主机 Z 对主机 Y 的信任度越高,那么计算出来的主机 Y 的推荐信任值也就越高,如果信任度很低,那么计算出来的推荐信任值也就越低。另外,交易金额对于信任值的意义也很大,如果两者之间的交易金额很大,那么这个信任

值的可信度也应该越高,它在推荐信任值中占的比重也应该越大,反之亦然。计算推荐信任值的时候还应该考虑到交易双方的交易次数问题,交易次数越多,所搜集到的信任值的可信度也就越高。

推荐信任值也分为近期推荐信任值和长期推荐信任值。近期推荐信任的计算用公式(9):

$$T_{r(Y)} = \frac{\sum_{i=1}^{d_1} T_{t(Y|Z_i)} \times m^i}{\sum_{i=1}^{d_1} m^i} \quad (9)$$

长期推荐信任值用公式(10)计算:

$$T_{r(Y)} = \frac{\sum_{i=1}^{d_2} T_{a(Y|Z_i)} \times m^i}{\sum_{i=1}^{d_2} m^i} \quad (10)$$

其中 m^i 是指主机 Y 与主机 Z 交易金额的总和, $T_{t(Y|Z_i)}$ 是指主机 Z_i 上主机 Y 的近期行为信任值。 $T_{a(Y|Z_i)}$ 是指主机 Z_i 上主机 Y 的长期行为信任值。

1.3 综合信任值的计算

主机 X 和主机 Y 进行交易时,信任值是决定交易是否进行的一个非常重要的因素。每个主机都想和信任值比较高的主机进行交易,与信任值高的主机进行交易意味着交易更加安全可靠,信任值低的主机意味着高的风险,这是所有主机都不愿意遇到的。

综合行为信任值和综合推荐信任值由公式(11)和(12)计算:

$$T_{(Y|X)} = \epsilon \times T_{t(Y|X)} + \varphi \times T_{a(Y|X)} \quad (11)$$

$$T_{r(Y)} = \epsilon \times T_{r(Y)} + \varphi \times T_{r(Y)} \quad (12)$$

其中 $\epsilon + \varphi = 1$,综合信任值取综合行为信任值和综合推荐信任值中小的一个,算法如公式(13)所示:

$$T_Y = \min(T_{(Y|X)}, T_{r(Y)}) \quad (13)$$

2 结果与分析

2.1 农产品交易系统结构设计

该系统是基于 IBM 公司提供的 Aglet 的 API 开发而成,整个系统采用 B-S-S 体系结构^[11],用户通过浏览器登录 ASP 服务器进行购买活动,ASP 是一个为用户提供购买移动代理来执行购买活动的代理平台。用户客户端和 ASP 服务器之间使用的是传统的 B-S 模式。商家拥有自己的销售代理平台。同时,商家必须在 MMSP 上进行注册登记,MMSP 是一个静止的代理服务器,MMSP 同时还要提供信任管理的功能。ASP 服务器派出的购买代理

依次访问对应的商家服务器平台,根据用户提出的需求完成整个购买活动。系统的结构如图 1 所示。

1)ASP 服务器。用户登录 ASP 服务器,为自己创建一个购买 Agent,并提供购买农产品的信息和购买策略。主 Agent 停留在 ASP 平台,消费者输入需要购买的农产品详细情况,主 Agent 接收到信息后,创建相应的搜索子 Agent,并将搜索子 Agent

派遣到选定好的商家服务器搜集详细农产品信息。搜索子 Agent 首先访问 EMSP 服务器,获得商家 Agent 平台的信息。信息返回后,主 Agent 根据信任管理 Agent 的评价和生成结果生成并派出多个谈判 Agent,谈判不论成功或失败都返回 ASP 服务器。在所有的谈判子 Agent 返回后,根据返回的信息选择最佳的交易对象,生成并派发交易 Agent。

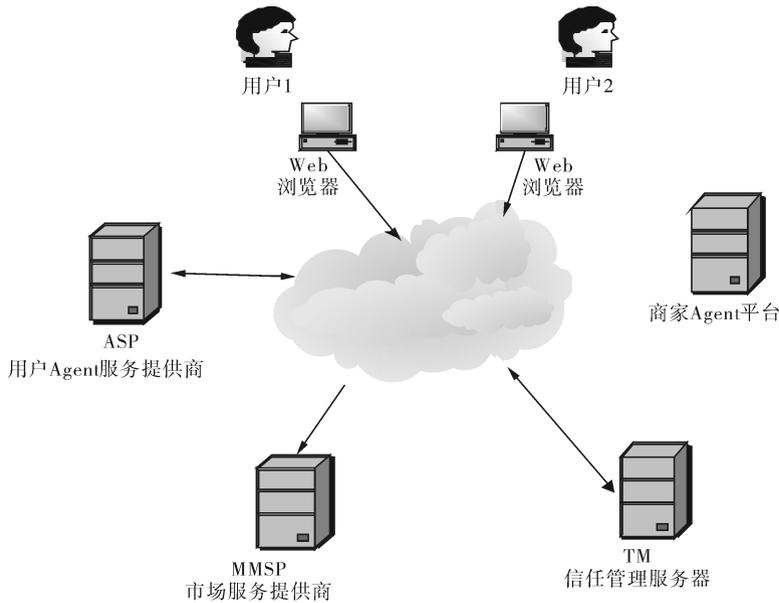


图 1 系统结构

Fig.1 Structure of system

2)MMS 服务器。MMS 服务器是整个电子市场的管理者,它的功能主要有:(1)管理商家 Agent 平台和 ASP,接受商家的注册并给予 1 个唯一的 ID 号,登记商家的农产品信息同时将其录入农产品数据库。(2)接受搜索 Agent 对所需农产品信息的查询,告知相关的商家 Agent 平台的地址。(3)记录用户对商家的评价。

3)TM 信任管理服务器。功能主要是计算商家的信任值,根据信任值判断该商家是否值得信任,在交易后,接收用户对商家的评价,并把相关数据保存到信任评估数据库。

4)商家 Agent 平台。商家 Agent 平台是商家和用户谈判和交易的场所。商家 Agent 系统包括主 Agent、谈判 Agent 和交易 Agent。主 Agent:负责接待到访的各个购买代理的子代理。根据不同的子代理提供不同的服务。谈判 Agent:根据相关策略与对方的谈判 Agent 进行谈判。交易 Agent:与对方的交易 Agent,通过可信任认证中心或电子银行等第三方机构进行安全交易。该农产品交易系统

的工作流程如图 2 所示。

用户通过浏览器登陆 ASP 服务器,输入所需农产品信息,ASP 服务器为用户生成交易代理,其中主代理驻留在 ASP 服务器内。搜索子代理从 MMS 获得商家列表,信任评估子代理对商家列表里的商家的信任值进行评估,评估时需要从 TM 获得商家的信任资料。评估结束后选择信任值较高的商家进行协商,协商后也需考虑到信任值,根据信任值提出谈判策略。谈判结束后,谈判子代理返回,对谈判结果进行评估,从中选择 1 个满足用户要求的商家进行交易。交易结束之后,用户对本次交易进行评价,MMS 记录本次交易数据和评价。同时, TM 服务器根据本次交易结果重新计算信任值,把相关数据存储到数据库中。

2.2 信任管理的设计

位于 TM 服务器上的信任管理模块的主要功能是管理相关的信任信息并计算消费者与商家之间的信任关系。信任管理代理由 3 个子模块组成:数据收集子模块、信任评估子模块、交易评价子模块。

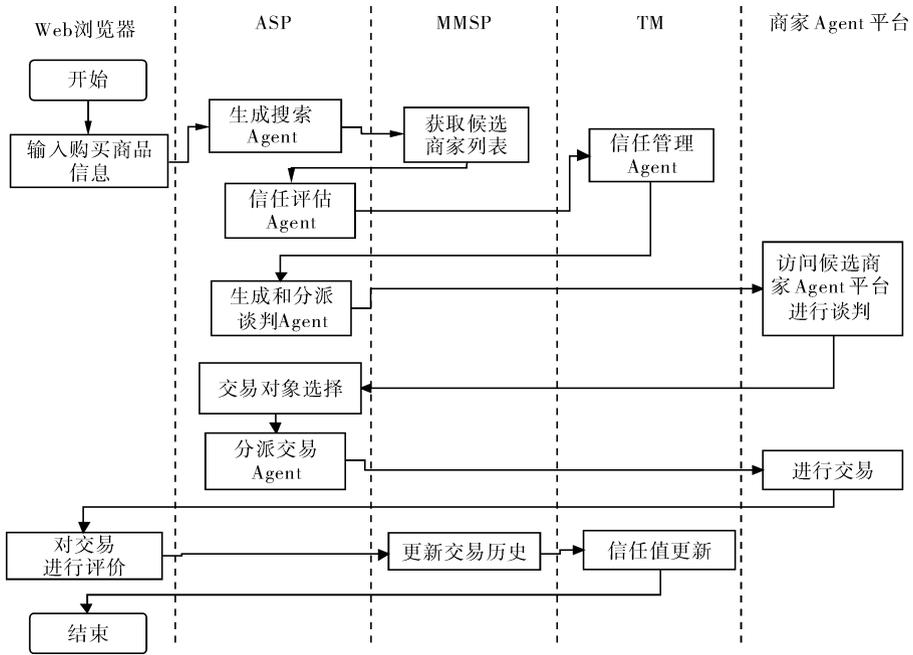


图 2 系统工作流程

Fig.2 System work flow

数据收集子模块从 MMSP 服务器上上和 ASP 的用户中收集信任相关信息,并把搜集到的信息存入信任信息的相关数据库。信任评估模块是信任管理模块中的最主要的模块,该模块需要对搜集到的数据进行评估计算,实现信任机制中的数学算法公式。信任评估模块从相关数据库中读取信任相关的信息数据,然后对获取的数据进行计算,得到商家的相关信任值,根据信任值做出决策,同时对信任信息数据库中的数据进行更新。交易评价模块在交易结束后,根据交易活动执行的结果,对交易对象进行评价,计算交易对象本次交易的信任相关数据,对数据进行更新,把结果保存到信任信息数据库中。信任管理模块的结构如图 3 所示。

3 讨论

本系统是一个分布式的农产品交易系统,系统使用移动 Agent 技术,通过搜索、谈判、交易 Agent 实现了在分布式环境中自主的在不同网络商家平台之间收集信息并进行谈判和交易的功能。为了保障本农产品交易系统的安全,在移动 Agent 中引入了信任的机制,把信任机制和传统的移动代理进行结合来保护移动 Agent 系统的安全。在信任机制中使用了 2 种信任值,其中以行为信任值为主,推荐信任值为辅,既能够反映主机在交易活动中的各种行为对交易的影响,也能反映主机用户的社会信任度,能比较好地对信任进行综合衡量,在提高了系统安全性的基础上,也使信任机制更加灵活和人性化。提出了关于行为信任值、推荐信任值、综合信任值的计算公式。把信任值分为近期和长期 2 种,近期信任值可以体现主机最近的交易动向,长期信任值则是主机交易以来的总体表现。对奖惩机制进行了设计,信任值会随着用户对移动代理系统的使用情况而变化。对信任机制实现的过程和实现的方法进行了说明,给出了信任评估的流程,提出了信任信息的存储结构。本农产品交易系统运行正常,能较好地保障交易安全。本系统在信任安全和欺诈方面还存在不足,在以后的工作中需要改进。

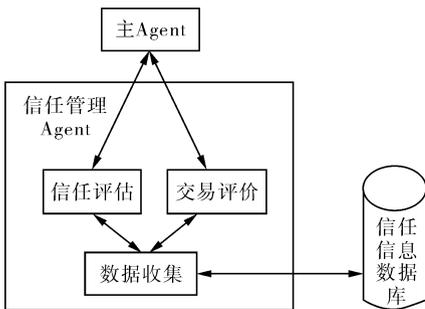


图 3 信任管理 Agent 的模块结构图

Fig.3 Module structure of trust management Agent

致 谢:感谢在华中科技大学计算机科学与技术学院攻读硕士学位期间甘早斌副教授及其团队给予的指导与帮助。

参 考 文 献

- [1] 崔雪冬.完善农产品流通信息服务体系的对策探讨[J].农业经济,2012(6):117-119.
- [2] 乔银.基于网络组织的大宗农产品电子交易平台建设研究[D].合肥:安徽财经大学,2015.
- [3] 王刊良.基于分类的企业电子商务模式创新方法[J].系统工程理论与实践,2003,23(3):18-23.
- [4] 李发英,于芳.基于移动代理的信息检索系统的设计与实现[J].湘南学院学报,2015,36(5):39-43.
- [5] TAO X P,LI J.Mobile agent;one of the main paradigms of future distributed computing[J].Computer science,1999,26(20):1-6.
- [6] 柳兴,袁超伟,杨震,等.移动云计算中基于移动代理的用户切换与接入控制[J].北京邮电大学学报,2014,37(2):88-92.
- [7] 柴梦竹.基于信任管理的农产品交易平台的设计与实现[D].广州:中山大学,2012.
- [8] MAYER R C,DAVIS J H.An integrative model of organizational trust[J].Academy of management review,1995,20(3):709-734.
- [9] 徐小龙,王汝传.移动 Agent 安全机制的研究[J].计算机工程与应用,2004,22(6):56-64.
- [10] 田慧蓉.P2P 网络信任模型与激励机制的研究[D].北京:北京邮电大学,2006
- [11] 李亦婕.基于移动代理的电子商务系统的信任模型研究[D].武汉:华中科技大学,2008.

Designing trading system of distributed agricultural products based on trust algorithm

ZHANG Cheng GUO Xi TIAN Fang

College of Informatics, Huazhong Agricultural University, Wuhan 430070, China

Abstract A security algorithm based on trust is proposed to deal with the security threats of host and network communication in trading system of distributed agricultural products. First, mobile agents are used to conduct a comprehensive statistical calculation of the user transaction records to calculate the behavior trust value. Then, the user feedback is analyzed and selected to calculate the recommended trust value. Finally, a variety of trust value is analyzed and the comprehensive trust value is obtained. The trading system of distributed agricultural products established is running correctly and can ensure the security of network transactions.

Keywords distributed system; agricultural products trade; mobile agent; trust value; trust algorithm

(责任编辑:陆文昌)