Journal of Computer Applications
计算机应用,2013,33(12):3437 -3440
ISSN 1001-9081
CODEN JYIIDU
2013-12-01
http://www.joca.cn

文章编号:1001-9081(2013)12-3437-04
doi:10.11772/j.issn.1001-9081.2013.12.3437

隐私保护的一站多表跨多表频繁项集挖掘

林　瑞,钟　诚*,华　蓓
(广西大学 计算机与电子信息学院,南宁 530004)
(*通信作者电子邮箱 chzhong@gxu.edu.cn)

摘　要:从多方合作挖掘分布存储在不同计算站点上多个数据库表而不泄露各方原始数据信息的目的出发,对于每个站点拥有多个数据表的分布式计算环境,基于三方安全协议,运用生成随机数扰乱方法,采取各站点并行挖掘频繁项集,将站点间各表数据公共连接属性作等值连接,以安全协议计算全局站间跨表频繁项集支持数的策略,提出了一站多表的3站点跨多表频繁项集挖掘隐私保护算法。实验结果表明,该算法在高效地联合挖掘出跨多表频繁项集的同时保护了各站点的敏感信息。

关键词:跨表挖掘;频繁项集;并行挖掘;隐私保护;多方安全协议
中图分类号:TP311.13　　**文献标志码**:A

One-site multi-table and cross multi-table frequent item sets mining with privacy preserving

LIN Rui, ZHONG Cheng*, HUA Bei
(*School of Computer, Electronics and Information, Guangxi University, Nanning Guangxi 530004, China*)

Abstract: To achieve the goal that personal and original information is not disclosed to each other when several parties cooperatively mine several data tables at different computational sites, based on secure triple-party protocol, a triple-site cross multi-table frequent item sets mining algorithm with privacy preserving was proposed in distributed environment with multiple tables at each site. The proposed algorithm disturbed data by generating random numbers, mined frequent item sets of inter-site in parallel, and linked the data with equal-value by common link attribution of the tables among the sites and applied secure protocol to compute the global support of inter-site cross-table frequent item sets. The experimental results show that the proposed algorithm is efficient, and it can not only mine the cross multi-table frequent item sets, but also preserve the private data at each site.

Key words: cross multi-table mining; frequent item set; parallel mining; privacy preserving; secure multi-party protocol

0　引言

数据挖掘中的隐私保护技术既能高效地挖掘出有用知识又能保护数据中的隐私信息不被泄露。文献[1]较早研究了垂直划分数据格式的关联规则挖掘隐私保护问题。文献[2]重点讨论了数据挖掘隐私保护技术中的安全点乘计算算法。文献[3]通过计算事务序列事务组的影响权值,选取对非敏感序列模式影响最小的事务序列事务组进行清洗,以使得在确保隐藏敏感序列模式的同时,尽量减少对非敏感模式集的影响,提出一种基于数据清洗的具有更好稳定性的敏感序列模式隐藏算法。文献[4]探讨分布式环境下连续模式挖掘隐私保护机制,提出了一个安全的长序列模式挖掘优化算法。对于不完整的原始数据,传统的基于抑制和泛化的算法会导致大量信息丢失。文献[5]将数据表中缺失值看作正常值处理,从而大大减少正被抑制的记录数量,提出一个适用于单敏感属性的保持更多信息的线性时间复杂度的不完整原始数据分类隐私保护算法。文献[6]采取无需事先预置安全度阈值,在一个合理的数据安全度区间内随机选取等距变换角度的方法,使得数据集经过等距变换后保持在空间中的距离不变,给出一种聚类数据挖掘的数据预处理算法,该算法完成数据等距变换的同时能够较好地保护敏感信息。文献[7]针对数据水平分布环境,采取分拆方法,在给出基于随机站点重排策略的多方安全求和计算协议的基础上,设计了一个隐私保护分布式序列模式挖掘算法,该算法在半诚实模型下可以保护局部站点信息安全,具有防站点串谋能力。文献[8]使用连接聚合查询技术完成多个私有数据表信息的连接共享,通过使用安全框架协议计算私有数据表随机和方法,实现了在私有数据表之间安全地交换其随机和信息。文献[9]指出,在多方安全计算中,需要考虑参与协议的多方知识联合的获取问题,同时要确保数据的保密性没有被减弱。因此,研究多方安全挖掘数据问题非常具有吸引力。文献[10]给出将跨两表频繁项集挖掘方法扩展到跨3表频繁项集挖掘方法的技术,以3表频繁项集的公共属性记数集作为三方安全协议的参数,实现了跨3表频繁项集挖掘的隐私保护。在云计算环境中,用户的敏感数据存储在云数据中心远程服务器中,这些数据不由拥有者本身管理与控制,研究如何存储、处理和访问不同类型的隐私数据是一个十分重要的云计算安全问题[11]。在云计算中,不同可信领域的参与者不希望泄露其隐私数据集,文献[12]提出了一个云计算中适应处理多方设置、任意划分数据的BP神经网络学习隐私保护算法。在用户具有有

收稿日期:2013-08-05;**修回日期**:2013-00-00。　**基金项目**:广西自然科学基金资助项目(2011GXNSFA018152)。
作者简介:林瑞(1985 -),男,广西南宁人,硕士,主要研究方向:网络信息安全;　钟诚(1964 -),男,广西桂平人,教授,博士生导师,博士,CCF高级会员,主要研究方向:并行分布计算、网络信息安全;　华蓓(1972 -),女,江苏无锡人,讲师,硕士,CCF会员,主研究方向:网络信息安全、数据挖掘。

限资源或者有限专业知识的云数据存储系统中,文献[13]提出一个文件拥有者利用含有噪声数据的关键词在私钥加密的远程数据中进行容错查找的通用框架和实现隐私保护的查找模式。通过使用敏感性参数化云数据库属性的父类会员已经利用加密和关系隐私保护操作修改数据库模式,文献[14]提出了一个保护云用户数据隐私的基于数据库模式再设计和云元数据动态重构的架构。

目前,分布式计算环境下一站多表跨多表频繁项集挖掘隐私保护研究成果极少。本文的主要工作是:对于各站点拥有多数据表的分布式计算环境,基于三方安全协议,运用生成随机数扰乱方法,采取各站点并行挖掘频繁项集,将站点间各表数据公共连接属性作等值连接,以安全协议计算全局站点间跨表频繁项集支持数的策略,提出一站多表的 3 站点跨多表频繁项集挖掘隐私保护算法。

1 相关知识

定义 1 多方安全计算。拥有秘密输入的 k 方,希望用各自的秘密输入共同计算一个函数,计算要求每方都能得到正确输出,且每方只能获知他们各自的输出[15]。

定义 2 设有一站点 S_1,其拥有 p 个数据表(R_{11}, R_{12},…, R_{1p}),T_{11}, T_{12},…, T_{1p} 为 p 个表的站内公共连接属性,n_p 为 $T_{11} \cap T_{12} \cap \cdots \cap T_{1p}$ 公共元组个数,p 个表按站内公共连接属性连接后,站内连接表 $R_{11} \rhd\lhd R_{12} \rhd\lhd \cdots \rhd\lhd R_{1p}$ 大小 $JoinS_1 = \sum_{i=1}^{n_p} a_{i1}.sum \times a_{i2}.sum \times \cdots \times a_{ip}.sum$,其中 $a_{i1} \in T_{11}$, $a_{i2} \in T_{12}$,…,$a_{ip} \in T_{1p}$,$a_{i1}.sum$, $a_{i2}.sum$,…, $a_{ip}.sum$ 分别为 a_{i1},a_{i2},…,a_{ip} 元素的个数之和。

定义 3 设有 3 个站点 S_1、S_2 和 S_3,S_1 拥有 p 个数据表(R_{11}, R_{12},…,R_{1p}),S_2 拥有 q 个数据表(R_{21},R_{22},…,R_{2q}),S_3 拥有 r 个数据表(R_{31},R_{32},…,R_{3r}),在 3 个站点挖掘出各自站内的跨表频繁项集后,从站内跨表频繁项集找出站间的公共连接属性,C_1,C_2 和 C_3 分别为此 3 个站点的公共连接属性,n 为 $C_1 \cap C_2 \cap C_3$ 公共元组的个数,3 个站点按站间公共连接属性 C_1、C_2、C_3 连接后,全局站间连接表大小 $Joinsize = \sum_{i=1}^{n} u_i.sum \times v_i.sum \times w_i.sum$,其中 $u_i \in C_1$, $v_i \in C_2$, $w_i \in C_3$, $u_i.sum$, $v_i.sum$ 和 $w_i.sum$ 分别为 u_i,v_i 和 w_i 元素的个数之和。

定义 4 设有 3 个站点 S_1、S_2 和 S_3,3 个站点站内跨表频繁项集对应的公共连接属性记数集分别为 m_1、m_2 和 m_3,将 m_1、m_2 和 m_3 作为三方安全协议 protocal 的输入计算参数,若三方安全协议输出结果满足 protocal(m_1,m_2,m_3) $\geqslant Joinsize \times minsup$,则由记数集 m_1、m_2 和 m_3 对应的站内跨表频繁项集生成的站间跨表候选频繁项集作为隐私保护的站间跨表频繁项集。

2 隐私保护的一站多表跨多表频繁项集挖掘

一站多表的 3 站点跨多表频繁项集挖掘隐私保护算法的思想:从站内多个表中首先确定一个主表,其余为从表,由于同属一个站点的多个表不存在私有数据泄露的问题,所以站内跨表候选频繁项集支持数不需要安全协议参与计算,直接以站内各表的频繁项集对应的公共属性记数集作乘积操作;站间跨表频繁项集挖掘的数据传送及计算操作涉及到不同的数据拥有者(站点),将各站点间公共连接属性作等值连接,结合三方安全协议参与对站间跨表候选频繁项集的支持数计算,在能够有效保护站点间支持数计算安全的条件下,合作挖掘出一站多表的跨表频繁项集。

算法 1 一站多表的 3 站点跨多表频繁项集挖掘隐私保护算法。

1)3 个站点独立扫描各自站内的数据库,找出数据库中多个表存在有内在关联的公共连接属性,统计出其记数集,求出站内连接表大小 $JoinS_i(i = 1,2,3)$。

2)对站内的各表挖掘出频繁 1-项集,在站内各表的公共连接属性作等值连接判断操作后,合作计算由各表的频繁 1-项集生成站内跨表频繁项集。

3)3 个站点间相互传送站内跨表频繁项集及对应的公共连接属性集。

4)选择其中两个站点,以站间公共连接属性作等值连接,生成两站点站间跨表候选频繁项集,采用三方安全协议,将两站点站间跨表候选频繁项集投影在其站内跨表频繁项集对应的公共连接属性记数集,以及第 3 个站点全部站内跨表频繁项集对应的公共连接属性记数集参与安全协议支持数的计算,运用生成随机数扰乱方法,依照三方安全协议计算出的结果,判断得出两站点站间跨表频繁项集。

5)在步骤 4)得出的两站点站间跨表频繁项集结果下,在相应的两站点内剪枝出参与挖掘全局 3 站点站间跨表频繁项集的站内跨表频繁项集及对应的公共连接属性集。

6)利用步骤 5)的剪枝结果,联合剩余的第 3 个站点的站内跨表频繁项集及对应的公共连接属性集,在 3 站点共有的连接属性等值连接下,生成 3 站点站间跨表候选频繁项集,进一步以三方安全协议计算其支持数,保持 3 个站点各自拥有的站内跨表频繁项集对应的公共连接属性记数集在合作计算中作为一个安全因子,3 个站点互不能推测获悉其值,最后确保生成 3 站点站间跨表频繁项集的同时,隐私安全得到有效保护。

算法 1 的步骤 1)和 2)在 3 个站点内部可并行执行,以提高算法的运行效率;步骤 3)分布式站点数据的发送和接收花费较大的通信开销;步骤 4)~6)采用三方安全协议参与站点间跨表候选频繁项集支持数的计算,运用生成随机数扰乱方法,使不同站点的敏感数据不泄露给其他方。算法是以各站点站内数据跨表频繁项集挖掘并行的执行,站间数据频繁项集以三方安全协议计算其支持数挖掘的安全策略,执行隐私保护一站多表式的 3 站点跨多表频繁项集挖掘的过程。

算法 1 拥有 3 个站点 S_1、S_2 和 S_3,S_1 拥有 p 个数据表(R_{11}, R_{12},…,R_{1p}),S_2 拥有 q 个数据表(R_{21},R_{22},…,R_{2q}),S_3 拥有 r 个数据表(R_{31},R_{32},…,R_{3r}),全局站间跨多表候选频繁项集由各站点站内跨表频繁项集生成,站点 S_i 内跨表频繁项集在数据表 R_{ij} 中的投影项集大小为 $|C_{ij}|$,数据表 R_{ij} 大小为 N_{ij},算法的计算开销集中在站内和站间挖掘频繁项集过程中,算法时间复杂度为 $O\left(\sum_{i=1}^{p}(|C_{1i}| \cdot N_{1i}) + \sum_{j=1}^{q}(|C_{2j}| \cdot N_{2j}) + \sum_{k=1}^{r}(|C_{3k}| \cdot N_{3k})\right)$。

3　实验分析

实验硬件环境为采用 100 Mb/s 以太网连接 4 台计算机(站点)构成分布式计算环境,其中第 1 台机器主频 2.70 GHz、内存容量 2.00 GB,第 2 台机器主频 2.69 GHz、内存容量 2.00 GB,第 3 台机器主频 3.0 GHz、内存容量 512 MB,第 4 台机器主频 2.99 GHz、内存容量 512 MB;设置其中 1 个站点为半可信服务方,3 个站点(设为 A、B、C)为独立计算站点。算法采用 Java 语言编程实现,在 Windows XP 操作系统和 SQL Server 2008 数据库支持下运行。实验测试数据采用 PKDD'99 Discovery Challenge 金融数据库中的数据表(http://lisp.vse.cz/pkdd99/Challenge/chall.htm)。

原始 PKDD'99 Discovery Challenge 金融数据库共包含有 8 个数据表,其中满足本文实验条件的数据表有 5 个,分别为 account 表、loan 表、order 表、disp 表和 trans 表。把 account 表和 loan 表分配到 A 站点,order 表和 disp 表分配到 B 站点,C 站点独自拥有 trans 表;在 A 站点以 account 表为主表、loan 表为从表,在 B 站点以 order 表为主表、disp 表为从表,C 站点以 trans 表为主表。3 个站点 A、B 和 C 在站内及站间挖掘跨表频繁项集以属性 account_id 作为 5 个表的公共连接属性。

本文测试一站多表的 3 站点跨 5 表频繁项集挖掘隐私保护算法(简记为算法 MTCMPP)在确保 3 个站点隐私信息安全前提下的运行效率。

图 1 给出了站点 A 中 account 表记录数为 900、loan 表记录数为 600,站点 B 中 order 表记录数为 1 200、disp 表记录数为 500,站点 C 中 trans 表记录数为 500,对于不同的最小支持度 *minsup*, MTCMPP 算法的运行时间。

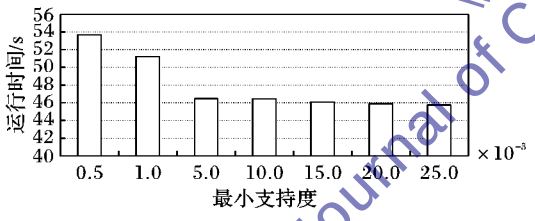

图 1　不同最小支持度下算法 MTCMPP 的运行时间

图 1 的实验结果表明:随着最小支持度的增大,MTCMPP 算法所需的运行时间逐渐减少,算法具有较好的执行效率。这是因为随着最小支持度的增大,3 个站点生成的频繁项集数量在减少,站点间需要传送的站内频繁项集通信开销减少,同时参与三方安全协议计算的参数数量也相应减少,需要运行三方安全协议的次数变少,从而使得 MTCMPP 算法的运行速度加快。

当最小支持度为 0.001,A 站点中 account 表记录数为 4 500、loan 表记录数为 682,B 站点中 disp 表记录数为 5 369,C 站点中 trans 表记录数为 5 000,在 B 站点主表 order 表记录数变化时,图 2 给出了 MTCMPP 算法的运行时间,图 3 给出了 MTCMPP 算法运行时站点连接表大小变化的情况。

从图 2 中可以看到:MTCMPP 算法的运行时间随着 B 站点主表 order 表记录数的增加而增加。这是因为随着 order 表记录数的增加,B 站点内公共连接属性 account_id 数目相应增加,B 站点内主表和从表联合计算站内连接表大小的开销时间变大。对于 3 站点计算 5 表的连接表大小开销增加更为明显,这是因为满足 5 表连接条件的参与三方安全协议计算的参数数量变大,执行三方安全协议的轮数增多,计算消耗时间随之增加。另一方面,生成的站内和站间跨表频繁项集数也相应增多,增加了挖掘时间。

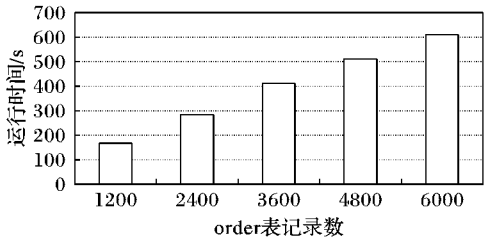

图 2　order 表记录数变化时 MTCMPP 算法的运行时间

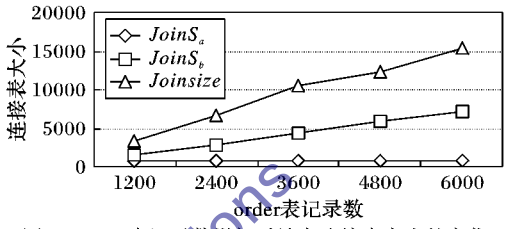

图 3　order 表记录数增加时站点连接表大小的变化

图 3 的实验结果表明:随着 order 表记录数的增加,A 站点站内连接表大小 $JoinS_a$ 变化没有产生影响,B 站点站内连接表大小 $JoinS_b$ 则相应增加,全局 3 站点站间跨 5 表连接表大小 *Joinsize* 增加幅度较大。这说明当构筑全局站间连接表大小、在站间挖掘跨表频繁项集数据时,order 表数据对调节挖掘出站间跨表频繁项集结果起到决定性影响。而需要表明的是,连接表大小为判断生成跨表频繁项集条件的一个决定性参数,在最小支持数固定的条件下,连接表大小越大,要满足条件:不小于 *Joinsize*(或 $JoinS_a$ 或 $JoinS_b$) × *minsup* 结果的跨表候选项集支持数就要越大,所以站间(或站内)连接表大小变化,对于生成跨表频繁项集数目以及站间执行三方安全协议次数具有很大的影响,从而影响算法所需的运行时间。

当最小支持度为 0.001,A 站点中 account 表记录数为 4 500、loan 表记录数为 682,B 站点中 order 表记录数为 6 471、disp 表记录数为 5 369,C 站点 trans 表记录数变化时,图 4 给出了 MTCMPP 算法的运行时间,图 5 给出了 MTCMPP 算法运行时站点连接表大小变化的情况。

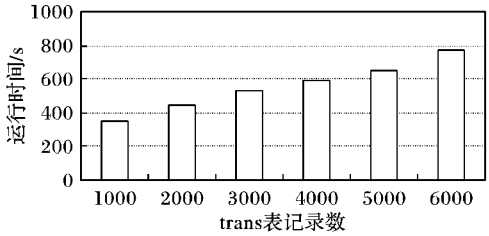

图 4　trans 表记录数变化时 MTCMPP 算法的运行时间

图 4 的实验结果表明:MTCMPP 算法的运行时间随着 C 站点 trans 表记录数的增加而增加。

从图 5 可以看到:随着 C 站点 trans 表记录数的增加,对 A 站点站内连接表大小 $JoinS_a$ 和 B 站点站内连接表大小 $JoinS_b$ 变化不产生影响,对全局 3 站点站间跨 5 表连接表大小 *Joinsize* 变化呈亚线性增长,这也说明了 C 站点 trans 表数据对于构筑全局站间连接表大小、调节挖掘出站间跨表频繁项集结果影响大。

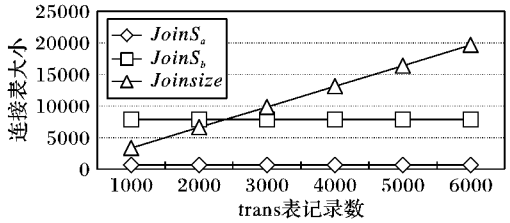

图 5 trans 表记录数变化时站点连接表大小的趋势

本文给出的 MTCMPP 算法执行三方安全协议计算站间跨表项集支持数,使得三方中的任何一方都不能获知其他两方的敏感数据,确保 3 站点间隐私信息得到安全保护,并且高效地挖掘出一站多表 3 站点跨 5 表的频繁项集结果。

4 结语

已有的隐私保护频繁项集挖掘算法不能满足多个数据表分布在不同计算站点上的多方安全联合获取知识的需求。对于每个站点拥有多个数据表的分布式计算环境,基于三方安全协议,采用随机数扰乱方法,本文设计实现了一站多表的 3 站点跨多表频繁项集挖掘隐私保护算法,该算法高效并且能够保护各方私有数据的安全。下一步将研究算法效率和隐私保护没有受到减弱的同时,将算法扩展到拥有更多参与方的情形。

参考文献:

[1] VAIDYA J, CLIFTON C. Privacy preserving association rule mining in vertically partitioned data [C]// KDD'02: Proceedings of the 8th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. New York: ACM, 2002: 639 – 644.

[2] GOETHALS B, LAUR S, LIPMAA H, *et al*. On private scalar product computation for privacy-preserving data mining [C]// ICISC'04: Proceedings of the 7th Annual International Conference in Information Security and Cryptology, LNCS 3506. Berlin: Springer-Verlag, 2004: 104 – 120.

[3] 华蓓, 钟诚, 黄肇明, 等. 通过计算影响权值实现敏感序列模式隐藏[J]. 小型微型计算机系统, 2010, 31(8): 1647 – 1651.

[4] GONG Q Y, LUO J Z, YANG M. AIM: a new privacy preservation algorithm for incomplete microdata based on anatomy [C]// Proceedings of the 7th International Conference on Pervasive Computing and Applications (ICPCA) and the 4th Symposium on Web Society, LNCS 7719. Berlin: Springer-Verlag, 2013: 194 – 208.

[5] GORAWSKI M, JURECZEK P. Optimization of privacy preserving mechanisms in mining continuous patterns [C]// Proceedings of the 8th International Conference on Dependability and Complex Systems, AISC 224. Berlin: Springer- Verlag, 2013: 183 – 194.

[6] 贡晓静, 钟诚, 华蓓. 基于等距变换的聚类挖掘敏感信息保护方法[J]. 计算机工程, 2011, 37(19): 122 – 125.

[7] HUA B, ZHONG C, YANG L, *et al*. Collusion-resistance privacy-preserving distributed sequential pattern mining [J]. International Journal of Advancements in Computing Technology, 2012, 4(21): 204 – 212.

[8] SHE R, WANG K, FU A W, *et al*. Computing join aggregates over private tables [C]// Proceedings of 9th International Conference on Data Warehousing and Knowledge Discovery, LNCS 4654. Berlin: Springer- Verlag, 2007: 78 – 88.

[9] DU W. A study of several specific secure two-party computation problems [D]. West Lafayette, Indiana: Purdue University, 2001: 1 – 159.

[10] 林瑞, 钟诚, 李效鲁. 隐私保护的跨多表频繁项集挖掘[J]. 计算机工程与应用, 2012, 48(2): 66 – 68.

[11] JANGRA A, BALA R. PASA: privacy-aware security algorithm for cloud computing [C]// Proceedings of the International Symposium on Intelligent Informatics, AISC 182. Berlin: Springer-Verlag, 2013: 487 – 497.

[12] YUAN J W, YU S C. Privacy preserving back-propagation learning made practical with cloud computing [C]// Proceedings of the 8th International Conference on Security and Privacy in Communication Networks, LNICST 106. Berlin: Springer-Verlag, 2012: 292 – 309.

[13] PANG X Q, YANG B, HUANG Q. Privacy-preserving noisy keyword search in cloud computing [C]// Proceedings of the 33rd International Conference on Information Systems, LNCS 7618. Berlin: Springer-Verlag, 2012: 154 – 166.

[14] WAQAR A, RAZA A, ABBAS H, *et al*. A framework for preservation of cloud users' data privacy using dynamic reconstruction of metadata [J]. Journal of Network and Computer Applications, 2013, 36(1): 235 – 248.

[15] CANETTI R, FEIGE U, GOLDREICH O, *et al*. Adaptively secure multi-party computation [C]// STOC '96: Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing. New York: ACM, 1996: 639 – 648.

(上接第 3427 页)

[5] FOX A, KICIMAN E, PATTERSON D A. Combining statistical monitoring and predictable recovery for self-management [C]// WOSS '04: Proceedings of the 1st ACM SIGSOFT Workshop on Self-managed Systems. New York: ACM, 2004: 49 – 53.

[6] 朱友文, 黄刘生, 陈国良, 等. 分布式计算环境下的动态可信度评估模型[J]. 计算机学报, 2011, 34(1): 55 – 64.

[7] BARR M, WELLS C. Category theory for computing science [M]. Upper Saddle River: Prentice Hall, 1990.

[8] 侯金奎, 万建成, 杨潇, 等. 构件式体系结构模型映射的形式化语义[J]. 计算机研究与发展, 2009, 46(2): 310 – 320.

[9] 侯金奎. 支持模型驱动开发的体系结构形式化语义与转换一致性研究[D]. 济南: 山东大学, 2008.

[10] 王占杰, 刘晶晶. 基于多 Agent 的分布式多目标任务调度机制研究[J]. 大连理工大学学报, 2011, 51(5): 755 – 760.

[11] 郑宇军, 陈胜勇, 凌海风, 等. 多 Agent 主从粒子群分布式计算框架[J]. 软件学报, 2012, 23(11): 3000 – 3008.

[12] 孙知信, 宫婧, 程媛, 等. 基于移动 Agent 的分布式仿真系统体系结构研究[J]. 计算机集成制造系统, 2006, 12(3): 95 – 400.

[13] JAISANKAR N, SARAVANAN R, SWAMY K D. Intelligent intrusion detection system framework using mobile Agents [J]. International Journal of Network Security & Its Applications, 2009, 1(2): 73 – 74.

[14] BERNARDO M, CIANCARINI P, DONATIELLO L. Architecting families of software systems with process algebras [J]. ACM Transactions on Software Engineering and Methodology, 2002, 11(4): 386 – 426.

[15] 曹木亮, 吴智铭. PI 网的强互模拟等价[J]. 计算机学报, 2005, 28(1): 1 – 8.

[16] 徐小龙, 程春玲, 熊婧夷. 基于 multi-Agent 的云端计算融合模型的研究[J]. 通信学报, 2010, 31(10): 203 – 211.

[17] ATTIYA H, WELCH J. 分布式计算[M]. 2 版. 骆志刚, 黄朝晖, 黄旭慧, 译. 北京: 电子工业出版社, 2008.