使用粗糙集与Bayes分类器的P2P网络安全管理机制

王海晟[1,2] 王海晨[3] 桂小林[2]
(西安理工大学计算机学院 西安 710048)[1] (西安交通大学电信学院 西安 710049)[2]
(长安大学信息工程学院 西安 710064)[3]

摘 要 提出一种使用粗糙集与Bayes分类器的P2P网络安全管理机制。该模型放弃了局部信任度与全局信任度等概念,对不满意事件进行分类统计,对交易节点进行分类控制。创新之处有:1)通过对节点彼此之间进行交易发生的不满意事件按照交易失败的类型、损害的严重程度、交易规模的大小等情况进行分类与量化,将交易失败事件区分为恶意攻击、大规模交易且质量不满意等类型。2)使用粗糙集分类器与Bayes分类器,将对等网络中的节点划分为可信任节点、陌生节点、恶意节点等不同的类型;建立信任节点列表与恶意节点列表;交易时将恶意节点排除在外。3)建立了反馈控制机制,使用粗糙集分类器与Bayes分类器根据节点反馈推荐的意见对被评价节点进行分类、做出评价,同时监测提出评价的节点是否有恶意行为,将反馈行为划分为诚实反馈、恶意反馈等。实验表明,与已有的安全模型相比,提出的安全管理机制对恶意行为具有更高的检测率、更满意的交易成功率以及更好的反馈信息综合能力。

关键词 安全模型,对等网络,粗糙集,贝叶斯分类器,仿真
中图法分类号 TP309 **文献标识码** A

New P2P Network Security Mechanism Based on the Rough Set and the Bayes Classifier

WANG Hai-sheng[1,2] WANG Hai-chen[3] GUI Xiao-lin[2]
(Department of Computer Science and Technology, Xi'an University of Thecnology, Xi'an 710048, China)[1]
(Department of Computer Science and Technology, Xi'an Jiaotong University, Xi'an 710049, China)[2]
(School of Information Engineering, Chang'an University, Xi'an 710064, China)[3]

Abstract A new security management mechanism based on the classification control of trade nodes was proposed. The model gives over the concepts of local trust and global trust and takes the classification control of trade nodes. This paper's innovation is as follows: 1) Through classification and quantification of failure events in trade between nodes, according to the severity of damage and the size of the trade, the trade failure events are divided into malicious attacks, bad quality and so on. 2) The rough set classifier and Bayes classifier are used and the nodes are divided into trust nodes, strange nodes and malicious nodes in a peer-to-peer network. The trust node list and the malicious node list are built. The malicious nodes are excluded from trading. 3) The rough set classifier and Bayes classifier are used to integrate the feedback recommendation and to decide the type of the recommended node. The feedback behaviors are divided into the honest feedback, the malicious feedback and so on. The experiment indicates that compared with the existing trust model, the model may obtain higher examination rate over malicious acts with the higher transaction success ratio, and has the better feedback information synthesizing capacity.

Keywords Security model, Peer-to-peer network, Rough set, Bayes classifier, Simulation experiment

1 引言

随着计算机网络技术的发展,分布式计算技术得到了广泛的应用。分布式网络计算环境已经显现出社会性的社交网络的特点,节点间的信任问题已变得日益突出。个体在彼此的交往过程中,总是希望选择可信任的对象,但更多的想法是避免遭遇有恶意的交互对象[1]。在社会关系网络中,为应对这样的情况,例如银行系统通常对恶意、严重不诚信的客户建立档案,应对产生不满意结果的行为进行控制。

本文提出了一种基于对交易节点进行分类控制的实用网络安全管理机制。该模型通过对节点彼此之间交易的不满意事件按照交易失败的类型、损害的严重程度、交易规模的大小等情况进行分类与量化。模型放弃了局部信任度与全局信任度等概念;对不满意事件进行分类统计,对交易节点进行分类管理与控制。

模型的重点是根据节点间的交易历史记录,结合使用粗糙集分类器和Bayes分类器将恶意节点检测出来,并对恶意节点进行控制,以在交易中避免遭遇有恶意的交互对象。根

到稿日期:2011-11-07 返修日期:2012-03-07 本文受国家自然科学基金(60873071)资助。
王海晟(1978—),男,博士生,讲师,CCF会员,主要研究领域为分布式网络计算,E-mail:hswang@xaut.edu.cn;王海晨(1969—),男,副教授,主要研究领域为计算机体系结构、并行计算;桂小林(1966—),男,教授,博士生导师,主要研究领域为网络计算、动态信任管理理论。

据节点间的交易历史记录，采用粗糙集分类器和 Bayes 分类器将对等网络中的节点划分为可信任节点、陌生节点、恶意节点等不同的类型。建立信任节点列表与恶意节点列表。交易时将恶意节点排除在外，不仅本地节点不与检测出的恶意节点交易，且将相关信息通知可信任邻居节点。

通过反馈控制机制动态统计节点的反馈推荐行为的状态，将反馈行为划分为诚实反馈、恶意反馈等情况[2,3]，采用粗糙集分类器和 Bayes 分类器根据节点反馈推荐的意见对被评价节点进行分类，提高了安全模型的动态适应能力。

本文第 2 节介绍相关工作；第 3 节给出新的安全管理机制的表述；第 4 节通过仿真实验分析新模型的各种性能；最后总结下一步工作的重点。

2 相关工作

在对等网络环境下，各节点彼此直接连接，交换数据和提供服务，具有匿名性、动态性和开放性等特性。在此环境下存在恶意用户或自私用户，存在大量安全隐患或自私的行为。如何规避不良用户带来的安全风险是分布式网络研究的关键课题。目前已提出的解决方式集中在信任与信誉机制研究方面。

采取信任机制的基本思想是根据交易的历史记录和相互的推荐信息计算出各主体相应的信任度，各主体均以此作为选择交易对象时的参考。

目前已提出的安全模型与算法包括以下几类：

(1)EigenTrust 算法和 PowerTrust 算法

将全局信任值进行归一化处理，由直接信任来计算全局信任值的 EigenTrust 算法认为直接信任值越高的节点推荐的信任值越可信，在计算全局信任时给予的权重越大[4]。

PowerTrust 算法对 EigenTrust 算法进行了改进：它肯定了可信任节点集合与 Power 节点的存在[5]。但它没有考虑交易量大小的作用，这使得恶意用户能以小额交易积累信任，在大额交易上进行欺骗，它也没有考虑对恶意行为的惩罚。

(2)PeerTrust 算法

PeerTrust 算法使用反馈评价来计算节点的直接信任值[6]，考虑到了以下 4 个因素：(1)反馈评价，这是计算信任值的基本元素；(2)交易的数量；(3)提供反馈评价的节点的可信度；(4)与交易相关的其它因素。

PeerTrust 算法具有以下缺点：(1)没有考虑到对恶意行为的惩处；(2)未考虑到计算的收敛速度；(3)在大规模环境下评价信息相对较为稀疏，利用相似性计算可信度会有很大的误差。

(3)采取模糊计算来计算信任值的算法[7-9]

例如 K-ranks 模型和直接信任树(DTT)模型，它们借鉴信任不确定的特性来处理不确定的评价；每轮交易后，算法动态调整推荐主体的可信性。这些算法考虑了对恶意推荐的惩罚，并给出了基于模糊逻辑的推理过程。

以上的模型都致力于节点的信誉度计算上，包括直接信任度、全局信任度，以便选择信誉度高的节点进行交易，达到抵制系统中恶意或不良行为的目的。但是这些模型对交易失败的事件、系统中恶意或不良的行为都没有进行分类研究，没有把交易失败事件按照交易失败的类型、损害的严重程度等进行分类细化统计。

3 基于粗糙集分类器与贝叶斯分类器的 P2P 网络安全管理机制

本文的模型以对等文件共享应用为例来描述所提出的算法，算法具有良好的通用性，可以应用于其他的领域。在文件共享应用中，每个节点要担任两种角色，其一是文件提供者，即向其它节点提供文件；其二是文件使用者，即使用其它节点提供的文件[10-12]。

在基于文件共享系统的对等交互应用中，节点为获取期望的文件，通常通过搜索功能向对等网络中的其他节点发出请求。大多数情况下，该节点会得到一个能够提供所需文件内容的提供者列表。表中包含正常节点，也可能包含恶意节点。若偶然选择了恶意节点并使用它提供的虚假或不良的文件，用户将浪费时间和精力，甚至对自己的计算机系统造成损害。

本文基于 Bayes 模型构建了安全管理模型。若发现恶意节点，将其记录到“恶意节点列表”中。根据交易历史，建立“可信任节点列表”(交易频繁、不良记录很少的节点)。建立“可信任邻居节点列表”，它们相互信任，相互之间共享“恶意节点列表”和“可信任节点列表”[13,14]。

对恶意节点的监测包括对提供文件的服务质量，还包括对提供反馈推荐意见的服务质量。既要监测提供文件服务时的恶意行为，还要监测对其他节点提供评价意见时的恶意行为。既要聚合其他节点的反馈推荐意见，对被推荐节点做出评价，还要监测提出评价的节点是否有恶意行为。

3.1 使用 Bayes 分类器对交易节点进行分类

本文使用贝叶斯分类器把发生过交易的节点根据交易历史记录进行分类。贝叶斯分类属于非规则分类，通过对训练样本集学习，归纳出分类器，利用分类器对需要分类的对象进行分类。贝叶斯分类并不是将某个对象绝对地指派给某一类，而是通过计算得出属于某一类的概率，具有最大概率的类便是该对象所属的类。

节点划分为可信任节点、陌生节点(不确定节点)和恶意节点 3 个类型。可信任节点是交易频繁、交易很少失败、没有恶意攻击记录、相互信任的节点。在可信任节点中，那些最熟悉的、相互了解的节点保持为“可信任邻居节点”，这些节点之间共享可信任节点列表、恶意节点列表等信息。

假定分类器考虑的是定义在实例空间 X 上的有限的分类假设空间 H，寻找某个目标函数 $c:X\rightarrow\{0,1\}$，若给定实例序列为$\langle\langle x_1,d_1,\rangle\cdots\langle x_m,d_m\rangle\rangle$，其中 x_i 为 X 中的某个实例，d_i 为 x_i 的目标函数值，则有 $d_i=c(x_i)$。

分类器考虑候选分类假设集合 H 并在其中寻找当给定数据集 D 时可能性最大的分类假设 $h\in H$。这样具有最大可能性的假设被称为极大后验(maximum a posteriori，MAP)假设。确定 MAP 假设的方法是用贝叶斯公式计算每个候选假设的后验概率。当下式成立时，称 h_{MAP} 为 MAP 假设：

$$h_{MAP}\equiv\underset{h\in H}{\operatorname{argmax}}P(h|D)=\underset{h\in H}{\operatorname{argmax}}\frac{P(D|h)P(h)}{P(D)} \tag{1}$$

某个待分类节点 ei 的特征向量为：$X_{ei}=(x_1,x_2,\cdots,x_n)$，其中 $x_1,x_2,\cdots,x_n$ 分别是节点 ei 对应于 $X_1,X_2,\cdots,X_n$ 特征项的取值。$X_1,X_2,\cdots,X_n$ 特征项对应于“节点交易记录表”中的各列(见表 1)，特征列含义说明见表 2。

表 1　节点交易记录表(训练数据集截取)

ID	所有时间段				最近时间段			节点类型
	X_1	X_2	X_3	X_4	X_5	…	X_9	C_i
103								

表 2　特征列含义说明

	含义
X_1	与本地节点交易的总次数(包括所有的时间段) 在运行开始阶段,划分为 $X_1 \geqslant 100$、$100 > X_1 \geqslant 50$、$50 > X_1 \geqslant 20$ 和 $20 > X_1$ 等区间,随着运行时间的增加,节点之间交易次数不断增加,可以重新划分区间。
X_2	所有时间段内、该节点与本地节点交易中发生的恶意攻击的总次数。划分为 $X_2 \geqslant 4$ 、$X_2 = 3$、$3 > X_2 \geqslant 1$ 和 $X_2 = 0$ 等区间。
X_3	所有时间段内、该节点与本地节点交易中发生的大规模交易、质量严重不合格的总次数。划分为 $X_3 \geqslant 5$ 、$5 > X_3 \geqslant 3$、$3 > X_3 \geqslant 1$ 和 $X_3 = 0$ 等区间。
X_4	所有时间段内、该节点给本地节点反馈推荐中发生的恶意反馈总次数。划分为 $X_4 \geqslant 6$ 、$6 > X_4 \geqslant 4$、$4 > X_4 \geqslant 1$ 和 $X_4 = 0$ 等区间。
X_5	最近时间段内该节点与本地节点交易中发生的恶意攻击的次数。划分为 $X_5 \geqslant 3$、$X_5 = 2$、$X_5 = 1$、$X_5 = 0$ 等区间。
X_6	最近时间段内、该节点与本地节点交易中发生大规模交易、质量严重不合格的次数。划分为 $X_6 \geqslant 4$、$X_6 = 3$、$3 > X_6 \geqslant 1$、$X_6 = 0$ 等区间。
X_7	最近时间段内该节点给本地节点反馈推荐中发生恶意反馈总次数。划分为 $X_7 \geqslant 5$、$5 > X_7 \geqslant 3$、$3 > X_7 \geqslant 1$、$X_7 = 0$ 等区间。
X_8	最近时间段内该节点与本地节点交易中发生的其他交易失败的次数。包括:下载速度低下、反馈偏离等。
X_9	在最近时间段内交易的失败率 $X_9 = n_f / n$ n 是最近时间段内本地节点与该节点交易的总次数;n_f 是交易失败的总次数。

设有 m 个类 $C_1, C_2, \cdots, C_m$。给定一个未知的数据样本 X_a(即等待分类的样本),分类器将预测 X_a 属于具有最高后验概率的类。贝叶斯分类器将未知的样本分配给类 C_i,当且仅当

$$P(C_i \mid X_a) > P(C_j \mid X_a), 1 \leqslant j \leqslant m, j \neq i \tag{2}$$

式中,C_i 是具有最大后验概率的类。根据式(1),后验概率:

$$P(C_i \mid X_a) = \frac{P(X_a \mid C_i) P(C_i)}{P(X)} \tag{3}$$

给定具有多个特征列的数据集,计算 $P(X_a \mid C_i)$ 的开销可能非常大。为降低计算开销,使用贝叶斯假设,即条件独立的朴素假定。假定属性值相互条件独立,即在属性间不存在依赖关系。这样,

$$P(X_a \mid C_i) = \prod_{k=1}^{n} p(x_i \mid C_i) \tag{4}$$

概率 $P(X_1 \mid C_1), P(X_2 \mid C_2), \cdots, P(X_n \mid C_n)$ 可由训练样本获得。$P(X_k \mid C_i) = S_{ik} / S_i$,其中 S_i 是训练样本中类别号为 C_i 的训练样本数,S_{ik} 是在属性 X_k 上具有值 x_k 并且类别号为 C_i 的样本数。

$$P(X) = \sum_{i=1}^{m} p(X_a \mid C_i) P(C_i) \tag{5}$$

计算给定类别 C_i 中节点的特征项 X_j 的第 k 区间 X_{jk} 的条件概率时,为避免出现零概率,加入了平滑因子,其估计由式(6)给出:

$$P(X_{ik} \mid C_i) = \frac{(s_{ik})_i + 1}{s_i + 2} \tag{6}$$

为对未知样本 X_a 分类,对每个类 C_i,计算 $P(X_a \mid C_i) P(C_i)$;样本 X_a 被指派到得到 $P(X_a \mid C_i) P(C_i)$ 最大的类 C_i。

本文 C_i 取值为可信任节点、陌生节点和恶意节点 3 个类型。可信任节点集合用 *Ctrust* 表示;恶意节点集合用 *Cvirus* 表示;陌生节点集合用 *Cstranger* 表示。采用符合归一化要求的式(3)进行计算,保证:

$$\sum_{i=0}^{m} P(C_i \parallel X_a) = 1$$

即归一化处理:

$$P(Ctrust \mid X_a) + P(Cstanger \mid X_a) + P(Cvirus) = 1$$

取最近 30 个时间段的记录作为"所有时间段"的记录。

本文实验初始训练样本包括 120 个交易节点。其中可信任节点 30 个,恶意节点 30 个,陌生节点 60 个。随着系统运行,不断完善训练样本。目前使用的训练样本,已经经过仿真实验进行过多次完善。样本中体现对可信任节点、陌生节点和恶意节点的定义。通过对训练集学习而归纳出分类器,本系统中称这个分类器为"Bayes 分类器 A"。

3.2　结合使用粗糙集分类器与贝叶斯分类器完成对节点的分类

粗糙集理论是一种处理模糊性和不精确性问题的新型数学工具,能够在保留关键信息的前提下对知识进行处理,并求得知识的最小表达。

四元组 $S=(U, A, V, f)$ 为一个知识表达系统,其中,U 为对象的有限集合,称为论域;A 为非空有限集,称为属性集合;V 为属性 A 的值域;$f: U \times A \to V$ 是一个信息函数,U 中任一元素其属性 A 取值 a 时,a 在 V 中有唯一确定值。

令 R 为一族等价关系,$r \in R$,如果 $ind(R) = ind(R - \{r\})$,即属性集 R 对于对象集 U 的分类与属性集 $R - \{r\}$ 对于 U 的分类相同,则称 r 为 R 中冗余;否则 r 为 R 中必要。若存在 $Q = P - r$,$Q \subseteq P$,Q 是独立的,满足 $ind(Q) = ind(P)$,则称 Q 为 P 的一个约简,用 $red(P)$ 表示。

一族等价关系 P 可能有多个约简,全部约简的交集定义为 P 的核,记为 $core(P)$,$core(P) = \cap red(P)$。约简是在不丢失信息的前提下,能够与原信息系统表达同样知识的最小条件属性集,它是保持信息系统的相同分类能力的最简形式,通过知识约简导出问题的分类规则。

本文的创新之处在于:结合使用粗糙集分类器与贝叶斯分类器来完成对节点的分类。

一方面使用粗糙集分类器对节点进行分类,存在一定的错误率与不可识别的情况;另一方面,贝叶斯分类中所有的属性都起作用,并不是一个或几个属性决定分类,而是所有属性都参与分类,但是对节点进行分类时,经常有仅仅根据 1 个或 2 个属性来确定节点的分类情况。比如:如果节点的交易记录中,所有时间段内恶意攻击次数(X_2)大于或等于 4 时,就独立确定该节点为恶意节点,不必考虑其它属性的取值情况。

使用对 Bayes 分类器进行训练时用过的、相同的训练样例集,不需要提供训练集以外的任何先验信息,粗糙集分类器就可以生成精确的、可检查的分类规则(包括仅仅根据 1 个或 2 个属性来确定节点分类的判断规则),并且可以根据这些规则进行分类。

结合使用粗糙集分类器与贝叶斯分类器来完成对节点的分类提高了分类准确度与分类效率。处理流程描述如下:

1)使用在 3.1 节描述的、对 Bayes 分类器 A 进行训练时使用的 120 个样本集(这含有 120 个记录的交易记录表就是一个决策表),对粗糙集分类器进行训练,通过离散化、属性约简、属性值约简导出精确而又易于检查和证实的分类规则。

2)选择、保留部分分类规则,按照如下要求:

a)只选择、保留可信度为 100%的分类规则;

b)只选择、保留决策属性值对应于"恶意节点"的分类规则;

c)只选择、保留仅包含1个条件属性或2个条件属性的分类规则，比如：IF(所有时间段内恶意攻击次数(X_2)≥4) THEN(该节点分类为恶意节点)；或者 IF(所有时间段内恶意攻击次数(X_2)=3 AND 所有时间段内恶意反馈次数(X_4)=3) THEN(该节点分类为恶意节点)等等。

3)仅当训练样本集改变时，重新生成与选择保留分类规则；

4)对交易节点进行分类判断时：

a)首先调用"粗糙集分类器"，使用选择保留的分类规则对"待分类节点"进行分类，如果分类成功，则该节点被判断为恶意节点，并且设置属于恶意节点的概率 $P(Cvirus|X_a)=100\%$；

b)如果使用"粗糙集分类器"分类不成功，不能识别，则调用"Bayes 分类器 "，分别计算该节点属于可信节点的概率 $P(Ctrust|X_a)$、属于陌生节点的概率 $Pt(Cstranger|X_a)$和属于恶意节点的概率 $P(Cvirus|X_a)$。

定义 1(恶意节点)　归一化处理后，$P(Cvirus|X_a)>0.7$，即属于"恶意节点类"的概率大于70%的节点被认定为恶意节点。节点属于"恶意节点类"的概率大于属于其他类型的概率，但小于70%，该节点划分为"准恶意节点"。

定义 2(可信任节点)　归一化处理后，$P(C\ \text{trust}|X_a)>0.7$，即属于"可信任节点类"的概率大于70%的节点被认定为可信任节点。节点属于"可信任节点类"的概率大于属于其他类型的概率，但小于70%，则节点划分为"准可信任节点"。

贝叶斯分类器把未知样本 X_a 指派到其后验概率 $P(X_a|C_i)P(C_i)$最大的类 C_i；本文强制仅把 $P(Cvirus|X_a)>0.7$ 的节点划分为恶意节点；仅把 $P(Ctrust|X_a)>0.7$ 的节点划分为可信任节点。

对恶意节点建立恶意节点列表，在若干时间段内不与这些节点发生交易，拒绝接收这些节点的反馈推荐意见。对"准恶意节点"建立准恶意节点列表，在若干时间段内不与这些节点发生交易，对这些节点的反馈推荐意见与陌生节点的反馈推荐意见同样处理。对"准可信任节点"建立准可信任节点列表，可以与这些节点进行交易，对这些节点的反馈推荐意见与陌生节点的反馈推荐意见同样处理。当本地节点向其它节点给出推荐意见时，对"准恶意节点"和"准可信任节点"都按照陌生节点进行推荐。

3.3　对反馈推荐意见进行综合

当本地节点对一个服务提供者缺少交易记录数据时，首先在与自己共享信息的可信任邻居节点之间提供的可信任节点列表、恶意节点列表内搜索，仍然得不到相关信息时，可以提请别的节点对该服务提供者给出推荐意见。每个节点都保持一个可信任节点列表和一个受控制的恶意节点列表。节点收到其它节点反馈回来的对指定服务提供者的评价后，进行综合，达到去伪存真的效果。不采纳在受控制的恶意节点列表中的恶意节点的反馈意见，按照不同的可信度来综合可信任节点反馈的意见和陌生节点反馈的意见。采用 Bayes 估计来确定和调整可信任节点的可信度和陌生节点的可信度。根据综合的结果决定是否与该服务提供者进行交易[15,16]。

3.3.1　使用粗糙集分类器和 Bayes 分类器对被评价节点进行分类

反馈意见同样按表1的格式给出相关的1行记录，包括：交易节点标识号 ID(这里的交易节点标识号 ID 即被推荐节点的 ID)、所有时间段内与被推荐节点的交易总次数 X_1、所有时间段内发生的恶意攻击总次数 X_2、质量严重不满意总次数 X_3、恶意反馈推荐次数 X_4、最近时间段内恶意攻击次数 X_5、质量严重不满意次数 X_6、恶意反馈推荐次数 X_7、其他交易失败次数(下载速度太低、反馈偏离)X_8、最近时间段内交易失败率 X_9 和推荐的该被推荐节点所属的节点类型标号。

通过对由反馈推荐意见表综合而成的训练样例集学习而归纳出分类器，本系统中称这2个分类器为"粗糙集分类器 B"和"Bayes 分类器 B"。实验初始训练样本包括120份推荐意见表(包括可信任节点与陌生节点的推荐意见)。把每一个推荐表中的每一列按列相加(剔除某些特征列，比如：最近时间段内交易失败率 X_9)，得到120个按照表1的格式给出的记录。使用这120个统计记录，分别对分类器进行训练，归纳出2个分类器。其中推荐结论为可信任节点的有40份，为恶意节点的有40份，陌生节点40份。随着系统运行，不断完善训练样本。

对反馈推荐意见进行综合的步骤为：

经过整理后，所有接收到的可信任节点的反馈推荐意见构成了推荐意见表 Table_T；把表 Table_T 中的每一列按列相加(剔除某些特征列，比如：最近时间段内交易失败率 X_9)，得到被评价节点与所有接收到的可信任节点的交易情况统计，进行规范化处理，这也是按照表1的格式给出的1行记录 Record_T，依据这一记录，使用粗糙集分类器和 Bayes 分类器可以对被评价节点进行分类。

同样，所有接收到的陌生节点的反馈推荐意见构成了推荐意见表 Table_S；把表 Table_S 中的每一列按列相加(同样剔除某些特征列，比如：最近时间段内交易失败率 X_9)，得到被评价节点与所有接收到的陌生节点的交易情况统计，进行规范化处理，这也是按照表1的格式给出的1行记录 Record_S，依据这一记录，也可以使用粗糙集分类器和 Bayes 分类器对被评价节点进行分类。

根据接收到的所有可信任节点的反馈推荐意见构成的推荐意见 Record_T，使用"粗糙集分类器 B"和"Bayes 分类器 B"，得到一个对被评价节点的包括3个概率结果数据的评价意见 Prob_T：

$Prob\_T$(属于可信任节点的概率，属于陌生节点的概率，属于恶意节点的概率)$=Prob\_T(Pt(Ctrust|X_a), Pt(Cstranger|X_a), Pt(Cvirus|X_a))$。

根据所有陌生节点的反馈推荐意见构成的推荐意见 $Record\_S$，使用"粗糙集分类器 B"和"Bayes 分类器 B"，得到另一个对被评价节点的评价意见 $Prob\_S(Ps(Ctrust|X_a), Ps(Cstranger|X_a), Ps(Cvirus|X_a))$。

根据经验，可信任节点的推荐意见的可信度高于陌生节点的推荐意见的可信度。在开始时，可信任节点对该被评价节点的推荐意见的可信度取为0.65；陌生节点对该被评价节点的推荐意见的可信度取为0.35 。对该被评价节点综合的评价意见 Prob__G(包括3个概率数据)为：

$$Prob\_G(0.65*Pt(Ctrust|X_a)+0.35*Ps(Ctrust|X_a),\ 0.65*Pt(Cstranger|X_a)+0.35*Ps(Cstranger|X_a),\ 0.65*Pt(Cvirus|X_a)+0.35*Ps(Cvirus|X_a))$$

综合评价结果：在综合评价意见 Prob_G 中，具有最大概率的类，就是该被评价节点所属的类。

如果该被评价节点被分类为恶意节点，则拒绝与其交易，并且把该被评价节点列入受控制的恶意节点列表之内。如果分类为可信任节点，则可以优先与其交易，但是不把该被评价节点列入可信任节点列表之内。只有在与本地节点进行足够多的交易之后，根据与本地节点的交易记录，才可能将其划分为可信任节点，并且列入可信任节点列表之内。如果分类为陌生节点，则可以根据概率数据的排序，酌情与其交易。

3.3.2 对提出评价意见的节点进行监测

以当前分类器给出的分类结果为标准，对每个给出反馈推荐意见的节点的反馈行为进行评价。如果分类结果与推荐意见一致，评价为诚实推荐；如果分类结果与推荐意见相反，比如分类器分类结果为可信节点，而推荐意见为恶意节点，或者分类器分类结果为恶意节点，而推荐意见为可信节点，评价为推荐颠倒。在一个时间段内出现 1 次或 2 次推荐颠倒，判定为推荐偏离；出现第 3 次(或 3 次以上)推荐颠倒，每次都判定为恶意推荐。将每个节点的反馈行为的评价结果记录到节点交易记录表中。

4 仿真及其结果分析

仿真实验的目的就是要将“使用粗糙集与 Bayes 分类器的 P2P 网络安全管理机制”(本文模型)与“基于局部信任度和全局信任度的 P2P 网络信任管理机制”(比较模型)进行比较，从多个角度评估本文模型在解决实际问题时的效果。本文通过在 PeerSim 平台上集成粗糙集分类器和贝叶斯分类器[17,18]，实现了一个模拟对等网络环境来对本文的相关模型及其算法进行性能分析。仿真实验中，对等网络的规模为 800 个节点，在每个仿真周期中每个节点至少与 40 个以上的节点进行交互，共进行了 2 个类型的仿真实验。

安全管理的一个主要功能是对节点各种恶意行为的检测。用文件服务的成功率和恶意反馈行为的检测率来反映安全模型的能力。文件服务的成功率反映了系统对节点在提供文件下载服务时的恶意攻击或提供虚假文件等行为时的检测与抵御能力，而恶意反馈行为的检测率主要反映了系统对节点在提供反馈评价意见时的恶意行为的检测能力。

设在节点交互过程中某个时刻 t 检测到提供文件服务的总次数为 $S(t)$，提供文件服务成功的次数为 $N(t)$，则文件服务的成功率($SR(t)$)定义为：$SR(t)=N(t)/S(t)$。系统初始设定的恶意节点所占的百分比为 β，该值直接影响仿真实验初始的成功率。如果 $\beta=20\%$，仿真实验初始的成功率应该为 $1-20\%=80\%$左右；随着系统对恶意节点的检测与控制，文件服务的成功率从 80%不断提高。

设节点在收集聚合其他节点的反馈评价意见时，某个时刻 t 收到反馈意见的总数为 $Fs(t)$，检测到恶意反馈意见数为 $Fm(t)$，并且系统初始设定的恶意反馈节点所占的百分比为 β，则恶意反馈行为的检测率 $Fr(t)$定义为：$Fr(t)=Fm(t)/Fs(t)/\beta$。

在实验中有两种配置：

1)使用粗糙集与 Bayes 分类器的 P2P 网络安全管理机制(本文模型)：使用分类器对节点进行分类，建立了可信任节点列表和恶意节点列表。选择文件提供者时排除了检测出来的恶意节点。

2)基于局部信任度和全局信任度的 P2P 网络信任管理机制的 EigenTrust 算法模型(比较模型)：没有对节点进行分类管理，对不满意行为没有进行分类统计，仅建立了节点交易历史记录，按照节点的信任度从高到低选择文件提供者。

以下是结果分析。

1) 图 1、图 2 是恶意节点的比例分别为总节点数的 20%与 30%时的文件服务成功率统计。从图上可看到，开始时两种算法的性能差距不大，但随着迭代次数的增加，本文模型显示出更高的成功率。

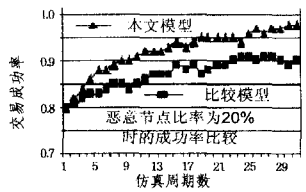

图 1 文件服务成功率 $SR(t)$比较 $\beta=0.2$

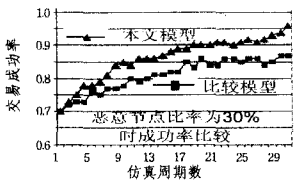

图 2 文件服务成功率 $SR(t)$比较 $\beta=0.3$

2)图 3、图 4 是恶意节点的比例分别为总节点数的 20%与 30%时的恶意反馈检测率统计。仿真开始时两种模型对恶意反馈的检测率都从 0 开始，随着仿真次数的增加，本文模型显示出更高的对于恶意反馈的检测率。

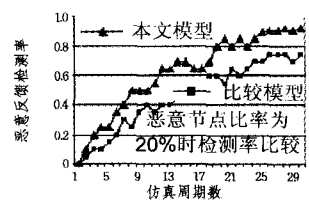

图 3 恶意反馈检测率 $Fr(t)$比较 $\beta=0.2$

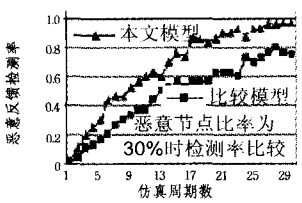

图 4 恶意反馈检测率 $Fr(t)$比较 $\beta=0.3$

结束语 本文两次结合使用粗糙集分类器与 Bayes 分类器，第一次依据节点的交易历史记录，对节点进行分类。第二次依据反馈推荐意见综合表，对被推荐节点进行分类。对节点分类的目的就是要分类管理。通过对恶意节点的识别与控制，提高了 P2P 网络环境的安全性能，提高了节点之间交易的成功率。实验表明，与已有的安全模型相比，本模型可以获得对恶意行为的更高的检测率，具有更高的交易成功率、更稳健的动态适应能力。本文是以对等网络为研究环境的，而如何在云计算等其它环境下应用本文提出的模型是我们下一步工作的重点。

参 考 文 献

[1] Li J T, Wang X P, Chen Y Q. A reputation management framework based on global trust model for P2P systems[C]// ICCS '06 Proceedings of the 6th International Conference on Computational Science-Volume Part I. Hong Kong, China: Springer Verlag, 2006: 896-899

[2] Li Xiao-yong, Gui Xiao-Lin, Zhao Juan. Novel Scalable Aggregation Algorithm of Feedback Trust Information[J]. Journal of Xi'an Jiaotong University, 2007, 41(8): 142-146

[3] 任艳，任平安，吴振强，等. 移动 P2P 网络中的多粒度信任模型[J]. 计算机工程与应用，2009，45(6)

(下转第 54 页)

出的影响力值排名前 10 的用户列表。

表 1　论坛静态网络图分析结果

UserId	Out-degree	Outgoing-clustering	Influence-value
历尽风雨见彩虹	59	0.98	44.50
财经小散	52	0.85	39.21
fcdsrgggggggg	50	0.78	37.70
frgtgt	48	0.74	36.19
云天梦	45	0.89	33.97
渐行渐远渐无言	41	0.75	30.94
俺 Q1395278391	40	0.87	30.22
飘飞的雪泥	38	0.72	28.68
2410897114hdd	37	0.72	27.93
伊凡童心	22	0.43	16.61

依据选用 Top $n=10$ 的算法对 12 个潜在意见领袖组成的集合相互进行匹配，获取的用户分别为：历尽风雨见彩虹，云天梦，俺 Q1395278391(它们在网络图中的位置用矩形块标识)。并将以上 12 个集合与表 1 中的结果进行 Jaccard 系数计算，将得到的相似度值建立如图 8 所示的相似度变化图。从图中可以发现，不仅各个时间步长上的相似度值低于 1，相邻步长的相似度值垂直变化也比较快。

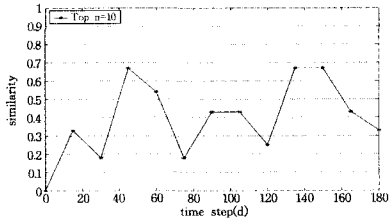

图 8　相似度变化图

以上实验结果说明，网络中用户的影响力随着时间的推移是动态变化的。同时也可以看出，由于噪声干扰的存在，相邻时间窗口内的识别结果存在偏差。但是，总体来看，相对于传统的基于静态网络图的论坛意见领袖发现方法，本文提出的算法不仅可以有效和准确地识别在某一短时间周期内变化的论坛意见领袖，而且可以将某一较长时间周期分割成不同的时间窗口，通过不同时间窗口内识别结果的相互匹配，较准确地发现该时间周期内的意见领袖。

结束语　在对网络论坛中意见领袖的识别研究中，本文提出了一个基于时间变化图的网络论坛意见领袖识别算法。实验表明，该算法与传统的基于静态网络图的识别方法相比，可以更准确地识别随时间的推移而变化的论坛意见领袖。

将来的工作主要包括：(1)将本文提出的算法中的网络论坛图的进化分割在数据的短期变化上，在降低噪声干扰的同时仍确保捕捉数据统计特性上的动向；(2)探讨结合多个时间窗口内的数据来计算在单个时间窗口的特征参数，使得所求特征参数随时间推移而平稳地变化，从而产生稳定的意见领袖识别结果。

参 考 文 献

[1] Hon Wai Lam, Chen Wu. Finding Influential eBay Buyers for Viral Marketing-A Conceptual Model of BuyerRank[C]// Proceedings of IEEE Conference on Commerce and Enterprise Computing. IEEE, 2009: 778-785

[2] Tang Xu-ning, Yang C C. Identifing influential users in an online healthcare social network[C]// Proc. IEEE Int. Conf. on Intelligence and Security Informatics, 2010 (ISI '10). May 2010: 43-48

[3] Bodendorf F, Kaiser C. Detecting Opinion Leaders and Trends in Online Communities[C]// 2010 Fourth International Conference on Digital Society. 2010: 124-129

[4] Rad A A, Benyoucef M. Towards Detecting Influential Users in Social Networks[C]// MCETECH 2011, LNBIP 78. 2011: 227-240

[5] Chen You, Cheng Xue-qi, Yang Sen. Finding High Quality Threads in Web Forums[J]. Journal of Software, 2011, 22(8): 1785-1804

[6] Casteigts A, Flocchini P, Quattrociocchi W, et al. Time-varying graphs and dynamic networks[R]. University of Carleton, 2010

[7] Esslimani I, Brun A, Boyer A. Detecting Leaders in Behavioral Networks[C]// 2010 International Conference on Advances in Social Networks Analysis and Mining. 2010: 281-285

[8] Zhou H. Scaling exponents and clustering coefficients of a growing random network[D]. Physical Review E 66. 2002

(上接第 32 页)

[4] Hou Meng-shu, Lu Xian-liang, Zhou Xu, et al. A trust model of P2P system based on confirmation theory [J]. Operating Systems Review, 2005, 39(1): 56-62

[5] Tian Chun-qi, Zou Shi-hong, Tian Hui-rong. A New Trust Model Based on Reputation and Risk Evaluation[J]. Journal of Electronics & Information Technology, 2007, 29(7): 1628-1632

[6] Li Xiong, Ling Liu. Peer Trust- supporting reputation-based trust for peer-to-peer election communities[J]. IEEE transactions on Knowledge and Data Engineering, 2004, 16(7): 843- 857

[7] Song S, Hwang K, Zhou R. Trusted P2P transactions with fuzzy reputation aggregation[J]. IEEE Internet Computing, 2005(6)

[8] Song Shan-shan, Huang Kai, Zhou Run-fang. Trusted P2P transactions with fuzzy reputation aggregation [J]. Internet Computing. 2005, 9(6): 24-34

[9] Altman J. PKI security for JXTA overlay networks[R]. TR-12-03-06. Palo Alto: Sun Microsystem, 2003

[10] 鲍翊平，姚莉，张维明，等. 对等网中基于种群进化的信誉模型[J]. 计算机科学，2011，38(1)：54-56

[11] Dou W, Wang H M, Jia Y, et al. A recommendation-based peer-to-peer trust model[J]. Journal of Software, 2004, 15(4): 571-583

[12] Zhang Q, Zhang X, Wen X Z, et al. Construction of peer-to-peer multiple-grain trust model[J]. Journal of Software, 2006, 17(1): 96-107

[13] Tian H, Zou S, Wang W. A Hierarchical reputation model for P2P networks[J]. Journal of Electronics and Information Technology, 2007(11)

[14] Swamynathan G, Zhao B Y, Almeroth K C. Decoupling service and feedback trust in a peer-to-peer reputation system[C]// Parallel and Distributed Processing and Applications Workshop 2005. Lecture Notes on Computer Science 3759, 2005: 82-90

[15] 封孝生，王桢文，黎湘运. P2P 中基于信任和属性的访问控制[J]. 计算机科学，2011，38(2)：28-31，41

[16] 黄骏虎，虞慧群. 一种基于信誉的 P2P 的评价模型[J]. 计算机科学，2011，38(Z10)：331-335

[17] 胡建理，吴泉源，周斌. P2P 环境下基于信誉的信任模型研究[J]. 计算机科学，2009，36(9)：1-6

[18] 杨超，刘念祖. P2P 环境下基于声誉的信任模型[J]. 计算机科学，2011，38(3)：131-135