第38卷 第17期
Vol.38 No.17

计 算 机 工 程
Computer Engineering

2012年9月
September 2012

• 安全技术 •

文章编号：1000—3428(2012)17—0152—05 文献标识码：A 中图分类号：TP393.08

基于交易节点分类管理的网络安全模型

王海晟[1,2]，桂小林[1]，王海晨[3]

(1. 西安交通大学电子与信息工程学院，西安 710049；2. 西安理工大学计算机科学与工程学院，西安 710048；
3. 长安大学信息工程学院，西安 710064)

摘 要：为确保对等网络节点交互的安全性，提出一种基于交易节点分类管理的网络安全模型。将失败的交易分为严重失败与一般不满意进行分类统计，以便更准确及时地检测恶意节点。在节点的直接交易过程中，根据交易历史记录，使用支持向量机分类器将网络中的节点划分为可信任节点、陌生节点和恶意节点，分别建立可信任节点列表与恶意节点列表，限制恶意节点的交易及反馈推荐行为。在反馈推荐意见统计表的基础上，利用Bayesian分类器对被评价节点进行分类，根据不同的可信度将可信任节点和陌生节点的反馈意见进行综合，再通过Bayesian估计调整节点的可信度。实验结果表明，与已有的安全模型相比，该模型对恶意行为具有更高的检测率，且交易成功率更高。

关键词：安全模型；对等网络；节点分类管理；支持向量机分类器；Bayesian分类器

Network Security Model Based on Classification Management of Trading Nodes

WANG Hai-sheng[1,2], GUI Xiao-lin[1], WANG Hai-chen[3]

(1. School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China;
2. School of Computer Science and Engineering, Xi'an University of Technology, Xi'an 710048, China;
3. School of Information Engineering, Chang'an University, Xi'an 710064, China)

【Abstract】To ensure the security of the transaction in P2P network, a new network security model based on classification management of trading nodes is proposed. Through classification statistics of failure events in the trade between the local node and other nodes, the trade failure events are divided into malicious attacks, bad quality and so on, so that malicious nodes can be detected and controlled timely and correctly. According to transaction history records, Support Vector Machine(SVM) classifier is used to divide trading nodes into trust nodes, strange nodes and malicious nodes. The trust node list and the malicious node list are established to exclude the malicious nodes from trading. According to the statistical data of feedbacks from the other nodes, Bayesian classifier is used for the classification of the evaluated nodes. The model dynamically counts the feedback behavior condition, divided the feedback behavior into the honest feedback, the malicious feedback and so on. Experimental results show that compared with the existing trust model, the model proposed can obtain higher examination rate over malicious acts and the higher transaction success rate.

【Key words】security model; P2P network; classification management of nodes; Support Vector Machine(SVM) classifier; Bayesian classifier

DOI: 10.3969/j.issn.1000-3428.2012.17.043

1 概述

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，避免遭遇有恶意的交互对象。现有的网络安全模型大多基于“信誉度”或“信任度”等概念，没有对节点之间交易失败的事件进行分类量化。本文提出了一种基于交易节点分类管理的网络安全模型。根据交易历史记录，使用支持向量机(Support Vector Machine, SVM)分类器[1-2]将网络中的节点划分为可信任节点、陌生节点、恶意节点等类型，使用Bayesian分类器[3-4]，依据其他节点的反馈推荐意见对被评价节点进行分类，Bayesian分类器在确定被评价节点类型的同时，分别计算该节点属于可信节点、陌生节点、恶意节点的概率[5-6]，从而实现对节点的分类管理与控制。

2 基于交易节点分类管理的安全管理模型

本文以对等文件共享应用为例来描述所提出的模型，模型具有良好的通用性，可以应用于其他的领域。

基金项目：国家自然科学基金资助项目(60873071)

作者简介：王海晟(1978－)，男，讲师、博士研究生、CCF会员，主研方向：网络安全，分布式网络；桂小林，教授、博士生导师；王海晨，副教授、博士

收稿日期：2011-10-17 **修回日期：**2011-12-16 **E-mail：**hswang@xaut.edu.cn

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[7-8]。

将失败的交易划分为两大类：严重失败与一般不满意。严重失败事件包括：下载了恶意攻击文件，大规模交易且质量严重不满意和恶意反馈推荐。一般不满意事件包括：小规模交易且质量不满意，下载速度太慢或中间离线，反馈推荐意见偏离等。

本文使用 SVM 根据网络中其他交易节点以往与本地节点进行交易的历史记录，把交易节点划分为可信任节点(类型标记为 Class_Trust 或 C_1)、恶意节点(类型标记为 Class_Virus 或 C_2)和陌生节点(类型标记为 Class_strange 或 C_3)3 种类型。可信任节点是与本地节点交易频繁、很少交易失败、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。

恶意节点是与本地节点的交易中多次出现严重失败事件的节点。对恶意节点建立恶意节点列表，今后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。发现恶意节点，将其记录到“恶意节点列表”中，每一次交易首先把恶意节点排除出去。

使用 Bayesian 分类器依据其他节点的反馈推荐意见确定被评价节点的类型，Bayesian 分类器在确定被评价节点类型的同时，分别计算出该节点属于可信任节点、陌生节点、恶意节点的概率。将其他节点对某个被评价节点的反馈推荐意见进行综合时，按照不同的可信度乘以 Bayesian 分类器计算出来的对应概率来综合可信任节点反馈的意见和陌生节点反馈的意见。

本文模型中，每当交易记录的时间段交替时或交易中出现了严重失败事件后，立即调用 SVM 分类器对当事节点进行检测，决定应该对当事节点作何处理(重新划分所属的节点类型)。

3　基于 SVM 的交易节点分类

支持向量机的原理[9]是用分类超平面将空间中 2 类样本点正确分离，即把正常节点(正样本)和恶意节点(负样本)正确分离，并取得最大边缘(正样本与负样本到超平面的最小距离)，该分类问题为一个有约束非线性规划问题：

若给定的样本集为$(\boldsymbol{x}_i,\ \boldsymbol{y}_i),\ i=1,2,\cdots,n,\ \boldsymbol{x}_i\in R,\ \boldsymbol{y}_i\in\{-1,+1\}$。存在一个超平面：$\boldsymbol{w}\cdot\boldsymbol{x}+b=0$，可以把样本点正确地分开，其中，“·”是点积；$\boldsymbol{w}$ 是 n 维向量；b 为偏移量。最优超平面通过解下面的二次优化问题来获得：

$$\min \Phi(\boldsymbol{w},b)=\frac{1}{2}\|\boldsymbol{w}\|^2$$
$$\text{s.t.}$$
$$\boldsymbol{y}_i(\boldsymbol{x}_i\cdot\boldsymbol{w}+b)-1\geqslant 0, i=1,2,\cdots,n \quad (1)$$

其中，$\|\boldsymbol{w}\|$是向量 $\boldsymbol{w}$ 的范数。

范数最小的、满足约束的 $\boldsymbol{w}$ 就是最优分类超平面的法向量。这是一个严格凸规划问题，按照最优化理论中凸二次规划的解法，把它转化为 Wolfe 对偶问题来求解：

$$\max W(\boldsymbol{\alpha})=\sum_{i=1}^{n}\alpha_i-\frac{1}{2}\sum_{i,j}^{n}\alpha_i\alpha_j\boldsymbol{y}_i\boldsymbol{y}_j\boldsymbol{x}_i\boldsymbol{x}_j$$
$$\text{s.t.}$$
$$\sum_{i=1}^{n}\alpha_i\boldsymbol{y}_i=0$$
$$\alpha_i\geqslant 0, i=1,2,\cdots,n \quad (2)$$

其中，α_i 是样本点 $\boldsymbol{x}_i$ 的 Lagrange 乘子。Kuhn-Tunker 条件定理指出，分类规则仅由恰好在超平面上的少数支持向量决定，而与其他样本无关。

利用 SVM 方法对节点进行分类，样本数据是节点间的交易历史记录，每条交易记录包括若干交易特征。选取那些最能够反映可信任节点、陌生节点与恶意节点的交易特征进行分类统计。本文选取的特征列分为 2 个部分：

(1)所有时间段内的统计数据(本文取最近 20 个时间段)。

(2)最近 2 个时间段内的统计数据。

截取交易历史记录表中的部分内容说明如下：设某个节点 ei 其特征向量为 $\boldsymbol{X}_{ei}=(\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_n)$，其中，$\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_n$ 分别是节点 i 对应 $\boldsymbol{X}_1,\boldsymbol{X}_2,\cdots,\boldsymbol{X}_n$ 特征项的取值。$\boldsymbol{X}_1,\boldsymbol{X}_2,\cdots,\boldsymbol{X}_n$ 特征项对应于节点交易记录表中的各列，如表 1 所示。

表 1　节点交易记录表(训练数据集截取)

ID	最近 20 个时间段内的统计数据				最近 2 个时间段内的统计数据					节点类型
	X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8	X_9	C_i
1050-625	256	5	3	6	0	3	0	5	1	C_3

特征列的含义如下：

X_1：所有时间段内该节点与本地节点交易的总次数。

X_2：所有时间段内该节点与本地节点在交易中被检测到的恶意攻击的总次数。

X_3：所有时间段内该节点与本地节点在交易中被检测到的欺诈交易的总次数。

X_4：所有时间段内该节点与本地节点在交易中被检测到的恶意反馈总次数。

X_5：最近 2 个时间段内该节点与本地节点在交易中被检测到的恶意攻击的次数。

X_6：最近 2 个时间段内该节点与本地节点在交易中被检测到的欺诈交易的次数。

X_7：最近 2 个时间段内该节点与本地节点在交易中被检测到的恶意反馈总次数。

X_8：最近 2 个时间段内该节点与本地节点在交易中被检测到的其他交易失败的次数。

X_9：最近时间段内交易的失败率，$X_9=n_f/n$，其中，n 是最近时间段内本地节点与该节点交易的总次数；nf 是本

地节点与该节点交易失败的总次数。

不满意事件门限值：针对最近时间段、最近 2 个时间段、最近 3 个时间段和所有时间段，分别设置不满意事件门限值。以所有时间段内的不满意事件门限值为例，定义如下：

本地节点与某一个节点交易中累计发生的恶意攻击次数(X_2)达到 m_a*时，判定该节点为恶意节点，m_a*为恶意攻击次数门限值。

本地节点与某节点交易中累计发生的大规模交易且质量不满意次数(X_3)达到 m_q*，或 X_2 与 X_3 之和达到 m_q*时，判定该节点为恶意节点，m_q*为质量不满意次数门限值。

本地节点接收到某一个节点反馈的推荐意见中累计发生的恶意反馈次数(X_4)达到 m_f*，或 X_2、X_3 与 X_4 之和达到 m_f*时，判定该节点为恶意节点，m_f*为反馈不满意次数门限值。

仿真实验中取 m_a*=4、m_q*=5、m_f*=6。

本文使用了 2 个分类器：第 1 个分类器 A 检测被测试样本是否为恶意节点；第 2 个分类器 B 检测被测试样本是否为可信节点。这 2 个分类器对样本选取了不同的特征列。对交易节点进行分类判断时，为了提高分类效率与准确度，采用如下判断规则：

计算并判定相关特征列是否达到了门限值：

$Uw=maxof(X_2/m_a^*,(X_2+X_3)/m_q^*,(X_2+X_3+X_4)/m_f^*)$

(1)如果 Uw 等于或大于 1，表明某一个特征列达到了不满意门限值，则判定该交易节点为恶意节点。

(2)如果 Uw 小于 1，调用 SVM 子程序进行分类判断。

实验训练样本包括 300 个交易节点。其中可信任节点 100 个；恶意节点 100 个；陌生节点 100 个。将训练集合分成 4 个大小相同的子集。其中，一个子集用于测试；其他 3 个子集用于对分类器进行训练。整个训练集中的每一个子集被预测一次，交叉验证的分类正确率达到 100%。随着系统的运行，不断完善训练样本。通过对不同的训练集学习归纳出 2 个分类器。

4 对反馈推荐意见的综合

4.1 基于推荐意见的被评价节点分类

在对等网络中，每个节点通常要对其他节点建立 2 种信任统计：一类是某个节点提供服务、进行交易的记录；另一类是该节点提供推荐的记录。反馈意见同样按照表 1 的格式给出相关的 1 行记录，包括：交易节点标识号 ID(即被推荐节点的 *ID*)，交易总次数(所有时间段内)X_1，所有时间段内恶意攻击总次数 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 X_8(下载速度太慢、反馈偏离)，最近时间段内交易失败率 X_9 和推荐的该服务提供者所属的节点类型标号。

经过整理后，所有可信任节点的反馈推荐意见构成了推荐意见表 *Table_T*。把 *Table_T* 中的每一列按列相加(剔除某些特征列，比如 X_9)，得到被评价节点与所有可信任节点的交易情况统计，这也是按照表 1 的格式给出的 1 行记录，依据这一记录，使用 Bayesian 分类器可以对被评价节点进行分类。

同样，所有陌生节点的反馈推荐意见构成了推荐意见表 *Table_S*。把 *Table_S* 中的每一列按列相加(同样剔除某些特征列)，得到被评价节点与所有陌生节点的交易情况统计，这也是按照表 1 的格式给出的 1 行记录，依据这一记录，可以使用 Bayesian 分类器[10-11]对被评价的节点进行分类。

Bayesian 分类器在确定被评价节点类型的同时，分别计算出被评价节点属于可信节点、陌生节点、恶意节点的概率。将其他节点对某个被评价节点的反馈推荐意见进行综合时要使用这些概率。

通过对训练集的学习，归纳出 Bayesian 分类器，用于对需要分类的对象进行分类。

设某个节点 *ei* 的特征向量为：$\boldsymbol{X}_{ei}=(x_1, x_2,\cdots, x_n)$，其中，$x_1,x_2,\cdots,x_n$ 分别是节点 *ei* 对应 $X_1,X_2,\cdots,X_n$ 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)。每个特征列中又划分为几个区间，比如：所有时间段内恶意攻击总次数 X_2 划分为 $X_2\geqslant 4$、$4>X_2\geqslant 3$、$3>X_2\geqslant 1$ 和 $X_2=0$ 等区间。

设有 m 个类 $C_1,C_2,\cdots,C_m$，给定一个未知的数据样本 $\boldsymbol{X}_{ei}$(即没有类标号)，分类法将预测 $\boldsymbol{X}_{ei}$ 属于具有最大后验概率的类。朴素 Bayesian 分类将未知的样本分配给类 C_i，当且仅当：

$$P(C_i \mid \boldsymbol{X}_{ei}) > P(C_j \mid \boldsymbol{X}_{ei}), 1\leqslant j\leqslant m, j\neq i \tag{3}$$

C_i 是具有最大后验概率的类。根据 Bayesian 定理，后验概率使用式(4)计算：

$$P(C_i|\boldsymbol{X}_{ei})=\frac{P(\boldsymbol{X}_{ei}\mid C_i)P(C_i)}{P(X)} \tag{4}$$

使用 Bayesian 假设，即类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：

$$P(\boldsymbol{X}_{ei}\mid C_i)=\prod_{k=1}^{n}P(X_k|C_i) \tag{5}$$

概率 $P(X_1|C_i),P(X_2|C_i),\cdots,P(X_n|C_i)$可以由训练样本获得。$P(X_k\mid C_i)=S_{ik}/S_i$，其中，$S_{ik}$ 是在属性 X_k 上具有值 x_k 的类 C_i 的样本数；S_i 是类标号为 C_i 的训练样本数。

$$P(X)=\sum_{i=1}^{m}P(\boldsymbol{X}_{ei}\mid C_i)P(C_i) \tag{6}$$

Bayesian 分类器的初始训练样本包括 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(同样剔除某些特征列)，得到每个节点与网络中其他节点交易情况统计。使用这 120 个统计记录，对分类器进行训练。其中推荐结论为可信任节点的 40 份，为恶意节点 40 份，陌生节点 40 份。随着系统运行，不断完善训练样本。

利用 Bayesian 分类器，根据所有可信任节点的反馈推荐意见构成的推荐意见表 *Table_T*，得到一个对被考察的节点的包括 3 个概率结果数据的评价意见 ***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)，即：

$$\boldsymbol{Prob\_T}(P_t(C_{\text{trust}}|\boldsymbol{X}_{ei}),\ P_t(C_{\text{stranger}}|\boldsymbol{X}_{ei}),\ P_t(C_{\text{virus}}|\boldsymbol{X}_{ei}))$$

根据所有陌生节点的反馈推荐意见构成的推荐意见表 *Table_S*，得到另一个对被考察的节点的评价意见：

$$\boldsymbol{Prob\_S}(P_s(C_{\text{trust}}|\boldsymbol{X}_{ei}),\ P_s(C_{\text{stranger}}|\boldsymbol{X}_{ei}),P_s(C_{\text{virus}}|\boldsymbol{X}_{ei}))$$

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

$$\begin{aligned}\boldsymbol{Prob\_G}(&0.65P_t(C_{\text{trust}}|\boldsymbol{X}_{ei})+0.35P_s(C_{\text{trust}}|\boldsymbol{X}_{ei}),\\ &0.65P_t(C_{\text{stranger}}|\boldsymbol{X}_{ei})+0.35P_s(C_{\text{stranger}}|\boldsymbol{X}_{ei}),\\ &0.65P_t(C_{\text{virus}}|\boldsymbol{X}_{ei})+0.35P_s(C_{\text{virus}}|\boldsymbol{X}_{ei}))\end{aligned}$$

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。

如果被评价节点被分类为恶意节点，则拒绝与其交易，并且把该节点列入恶意节点列表之内。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，才能划分为可信任节点，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。

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，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 次推荐颠倒时，此次及之后的每一次都判定为恶意推荐。对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。

4.2　可信任节点与陌生节点的可信度调整

上面可信任节点的可信度取为 0.65；陌生节点的可信度取为 0.35，下面对这 2 个可信度进行调整。采用 Bayesian 估计，依据实验数据来调整可信任节点与陌生节点的可信度。随机选取 n 个交易节点，随机变量 $\boldsymbol{X}$ 表示这 n 个交易节点中可信节点向量，$\boldsymbol{X}=(\boldsymbol{x}_1,\ \boldsymbol{x}_2,\cdots,\ \boldsymbol{x}_n)$。$\theta$ 表示这 n 个交易节点中可信节点的概率，θ 的先验分布函数为 $\pi(\theta)$。

在给定了实验结果数据 $\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_n$ 的条件下，θ 的条件分布为 θ 的后验分布：

$$\pi(\theta\,|\,\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_n)=\frac{P(\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_n,\theta)}{P(\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_n)}=\frac{P(\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_n\,|\,\theta)\pi(\theta)}{\int P(\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_n\,|\,\theta)\pi(\theta)\mathrm{d}\theta}$$

假设一次实验中，选取了 3 个服务提供者请求其他节点进行推荐。可信节点对这 3 个节点的反馈的意见平均为：

$P_s(C_{\text{trust}}|\boldsymbol{X}_{ei})=0.9$

陌生节点对这 3 个节点的反馈的意见平均为：

$P_s(C_{\text{trust}}|\boldsymbol{X}_{ei})=0.8$

θ_1 表示认为这一组中的节点属于可信节点的概率为 0.9，即：

$\theta_1= P_s(C_{\text{trust}}|\boldsymbol{X}_{ei})=0.9$

θ_2 表示认为这组中的节点属于可信节点的概率为 0.8，即：

$\theta_2= P_s(C_{\text{trust}}|\boldsymbol{X}_{ei})=0.8$

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。可信任节点对该服务提供者的推荐意见的可信度取为 0.65；陌生节点对该服务提供者的推荐意见的可信度取为 0.35。即 θ 的先验分布为：

$\pi(\theta=\theta_1)=0.65$

$\pi(\theta=\theta_2)=0.35$

事件 A：本地节点与这 3 个节点进行一段时间的交易后，确定它们都达到了可信节点的标准，即都属于可信任节点。

根据事件 A，条件概率 $P(A|\theta_1)$和 $P(A|\theta_2)$由二项分布计算得到：

$P(A|\theta_1)=0.9^3=0.729$

$P(A|\theta_2)=0.8^3=0.512$

由全概率公式可算得：

$p(A)= P(A|\theta_1)\pi(\theta_1)+ P(A|\theta_2)\pi(\theta_2)=$

$0.729\times0.65+0.512\times0.35= 0.653$

由后验分布公式可求得：

$\pi(\theta_1|A)= P(A|\theta_1)\pi(\theta_1)/P(A)=0.474/0.653=0.73$

$\pi(\theta_2|A)= P(A|\theta_2)\pi(\theta_2)/P(A)=0.179/0.653=0.27$

因为后验分布综合了先验概率分布和实践结果，所以比先验概率分布更贴近实际，可以把可信任节点对服务提供者的推荐意见的可信度取为 0.73；陌生节点对服务提供者的推荐意见的可信度取为 0.27。将当前得到的后验分布作为先验分布再次计算验证，结果将更贴近实际。

采取以时间段为先验概率的调整周期。在一个时间段内对多次实验验证获得的后验分布取其平均值作为下一时间段的先验分布。

5　仿真及结果分析

通过在 PeerSim 平台上集成 SVM 分类器和 Bayesian 分类器，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 20 个以上的节点进行交互，一旦发生严重失败事件，立即更新相应的交易记录表，并调用 SVM 分类器，判断由于这一严重失败事件，该节点是否应该重新分类。如果检测出恶意节点，立即添加到恶意节点列表。需要与陌生节点进行交易时，先请求其他节点对该陌生节点进行推荐，调用 Bayes 分类器对推荐意见进行综合，确定能否与该陌生节点进行

交易。本文基于节点分类控制的安全模型其功能就是帮助用户选择正确的交易对象，屏蔽恶意节点。用文件服务的成功率和恶意反馈行为的检测率反映安全模型的性能。

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 β=20%，仿真实验初始的成功率应该为 1－20%=80%左右。

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 2 种配置：(1)对交易节点进行分类控制的网络安全模型(本文模型)：系统构建了 SVM 分类器，建立了可信任邻居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)基于高信誉度优先选择的 EigenTrust 模型(比较模型)：没有对不满意行为进行分类管理，仅建立了交互节点历史记录，按节点的信任度从高到低选择文件提供者。

图 1、图 2 是恶意节点的比例分别为总节点数的 20%与 30%时 2 种模型的文件服务成功率比较。由结果可知，开始时 2 种模型的性能差距不大，但随着迭代次数的增加，对交易节点进行分类控制的网络安全模型显示出更高的成功率。

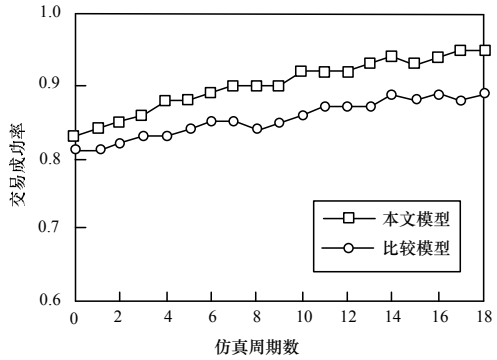

图 1 β=20%时 2 种模型的交易成功率比较

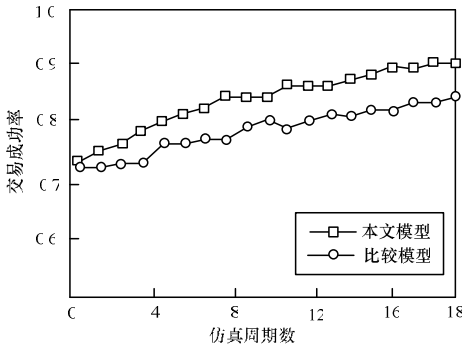

图 2 β=30%时 2 种模型的交易成功率比较

图 3、图 4 是恶意节点的比例分别为总节点数的 20%与 30%时 2 种模型的恶意节点检测率比较。仿真开始时 2 种模型对恶意节点的检测率都从 0 开始，随着仿真次数的增加，对交易节点进行分类控制的网络安全模型显示出更高的恶意节点检测率。

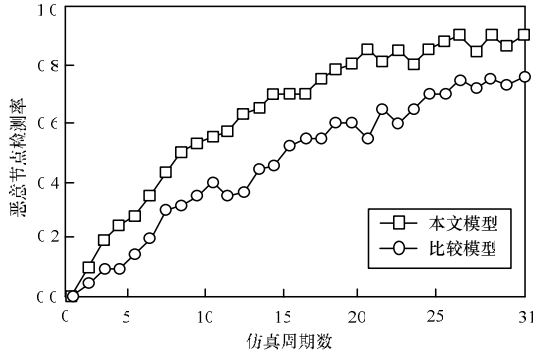

图 3 β=20%时 2 种模型的恶意节点检测率比较

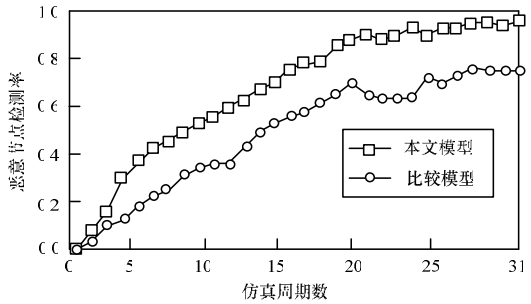

图 4 β=30%时 2 种模型的恶意节点检测率比较

6 结束语

本文模型摒弃了局部信任度与全局信任度等概念，在对不满意事件进行分类统计与量化的基础上，对交易节点进行分类，建立恶意节点黑名单，分类管理，分类控制。模型的特点是根据节点间的交易历史记录，使用 SVM 分类器把恶意节点检测出来，对恶意节点进行控制。使用 Bayesian 分类器把节点反馈的意见综合起来，确定被评价节点的类型，同时检测提出推荐意见者的行为。实验结果表明，与已有的安全模型相比，本文模型可以获得对恶意行为更高的检测率，具有更高的交易成功率。本文以对等网络为研究环境，如何在云计算等其他环境下应用该模型是下一步工作的重点。

参考文献

[1] Kamvar S, Schlosser M, Garcia-Molina H. The EigenTrust Algorithm for Reputation Management in P2P Networks[C]//Proc. of the 12th International World Wide Web Conference. Budapest, Hungary: [s. n.], 2003: 640-651.

[2] Hou Mengshu, Lu Xianliang, Zhou Xu, et al. A Trust Model of P2P System Based on Confirmation Theory[J]. Operating Systems Review, 2005, 39(1): 56-62.

[3] Li Xiaoyong, Gui Xiaolin. Research on Adaptive Prediction Model of Dynamic Trust Relationship in Open Distributed Systems[J]. Journal of Computational Information Systems, 2008, 4(4): 1427-1434.

(下转第 161 页)