基于用户及其行为社会属性的信任测度模型

陆 悠[1,2] 华 泽[1] 盛 浩[1,3] 奚雪峰[1]
(苏州科技学院电子与信息工程学院 苏州 215011)[1] (东南大学计算机科学与工程学院 南京 211189)[2]
(北京航空航天大学仪器科学与光电工程学院 北京 100191)[3]

摘 要 信任测度是信任机制的核心和基础,现有的信任机制面临着恶意用户操纵信誉的安全威胁。基于用户及其行为社会属性的信任测度模型对传统的信任机制进行了扩充,引入用户及其行为所映射的本质特性即社会属性来描述和分析恶意用户及其行为的特征,在信任测度过程中增加信誉评审过程来修正对信任测度的攻击,从而保证了分布式环境中的信任测度的可信性。模拟实验表明,该信任测度模型能有效地应对恶意用户对信誉的操纵攻击。

关键词 用户行为,信任测度,信任机制
中图法分类号 TP393 **文献标识码** A

Trust Measuring Model Based on Social Factors of Users and their Behavior

LU You[1,2] HUA Ze[1] SHENG Hao[1,3] XI Xue-feng[1]
(School of Electronical and Information Engineering, Suzhou University of Science and Technology, Suzhou 215011, China)[1]
(School of Computer Science and Engineering, Southeast University, Nanjing 211189, China)[2]
(School of Instrumentation Science and Optoelectronics Engineering, Beihang University, Beijing 100191, China)[3]

Abstract Trust measure is the basis of trust mechanism. Now the trust mechanism is facing the threat that malicious users manipulate the reputation. The trust measure model based on the social factors of users and their behavior expands the traditional trust mechanism. It describes and analyses the characters of malicious users and their behavior by the social factor, which reflects the essential of user and behavior. This model also adds the audit process in order to correct the reputation under the attack, so it can guarantee the credibility of trust measure in distributed Environment. Simulation experiments show that this model can effectively react to the reputation manipulation attack by the malicious users.

Keywords User behavior, Trust measure, Trust mechanism

1 引言

随着大规模、多用户的分布式应用(如网格、P2P、电子商务等)的普及,信任机制作为确保用户与服务可信性的一种重要机制得到了重视和普及[1-4]。但信任机制也面临着安全威胁,其中最为突出的是恶意用户对信誉的操纵,根据文献[1-4],操纵行为可分类如下:从操纵目的来看,可以分为对信誉的提升洗刷(Washing)行为、降低诋毁(Slandering)行为以及周期性的摇摆行为;从参与操纵的用户数量来看,可以分为单独操纵和团体操纵;而恶意用户团体的构成则可以分为 Sybil 团体和真实团体(Sybil 团体中的成员通常是由一个或少数几个真实用户创建的大量虚假账号或一次性的新用户账号构成,而真实团体中的成员则都是系统中的真实用户)。面对这些威胁,已有的工作分别使用不同的方法加以应对,例如文献[3]基于数据分析认为用户信誉评价的正常分布模式呈 Heavy Tail 分布,并给出过滤异常评价的算法。类似的工作还有文献[5-7],但这些工作在信誉评价数量较少或恶意用户较多的场景中无法有效工作;文献[8-10]则将信誉评价与评价者本身的可信程度挂钩并加以处理,但这些方法不能处理 Sybil 攻击,也不能应对摇摆攻击方法;文献[11,12]提出使用唯一的 ID 来标识用户,并增加注册新用户的难度等,但这类方法只能用来应对 Sybil 攻击;文献[13]提出在信任测度时采用"慢升快降"的方法;文献[14]引入用户行为历史作为信誉测度的重要因素来增加摇摆的难度;文献[15]也提出在信任测度时引入时间帧和近期、长期、累积滥用信任以及反馈可信度等多个因素,但这些手段仅仅针对摇摆行为,且会导致对正常的新用户较为排斥的"冷启动"缺陷。

由此可见,如何应对恶意用户对信誉或信任测度的操纵是一个有待解决的紧迫问题。本文试图找出一个新思路,即信任机制中的用户及其行为是现实世界的人及其行为的映射,具备社会属性,因此引入社会属性来描述和分析恶意用户及其行为的特征,随后通过基于逻辑推理的信誉评审来处理恶意用户及其行为,从而设计一个能够应对这些信誉操纵威胁的信誉评审机制,由此提出了一种基于用户及其行为社会

到稿日期:2012-03-31 返修日期:2012-07-05 本文受国家高技术研究发展计划(863 计划)(2010AA122202),建设部科学技术项目(2010-K9-40),苏州市工业应用基础研究项目(SYJG0929)资助。
陆 悠(1977—),男,博士生,讲师,主要研究方向为网络应用及安全、用户行为控制,E-mail:luyou.china@gmail.com;华 泽 女,副教授;盛 浩 男,博士,副教授;奚雪峰 男,讲师。

属性的信任测度模型，其主要致力于应对：1）Sybil 攻击，即 Sybil 团体对目标进行洗刷或诋毁攻击；2）Group 攻击，即真实团体对目标进行洗刷或诋毁攻击；3）摇摆等针对信任测度的攻击行为。实验结果表明，与传统信任机制相比，本文的信任测度模型能够很好地应对恶意用户对信誉的操纵攻击。

本文第 2 节介绍信任测度模型的框架设计；第 3 节介绍用户及其行为的社会属性以及分析方法；第 4 节给出信誉评审机制的具体设计；第 5 节对评审机制的效果进行模拟实验验证；最后是结论。

2 模型框架

信任代表一个用户在自身知识和经验基础上对其他用户的判断[1-4]。其量化过程是对用户交互中给予的评价进行处理的过程，处理的结果即信誉。信任机制的应用是有其背景的，通常为一个不是完全开放的分布式应用环境，用户需要通过一定的步骤（例如注册）才被允许进入系统，从而具备诸如 ID、注册时间、偏好等数据，随后每个用户交互后互相给予评价，该过程即用户的行为。在该环境中，用户及其行为具有可以从社会、经济等层面上观察并理解到的特征，这些特征即构成用户及其行为的社会属性。

由于社会属性可以从现实意义上去理解，恶意用户及其行为的特征在现实中较易被发现和描述，比如 Sybil 攻击出于成本和时间考虑，相关账号都有相近的注册时间及注册信息（例如默认值），因而电子商务环境中定义大量新注册的账号在短时间内给予某个用户较低的评价为一种攻击（例 1）；又如 Group 攻击往往是在相近的时间阶段对相同的用户做出同类型的评价，摇摆行为往往会重复类似的交互对象及评价等。因此本文将社会属性引入信任测度模型中来对用户及其行为进行描述和分析，将结果用于信任测度的评审，以此应对信誉操纵的攻击。例如对例 1，可抽取注册时间、注册信息、交互对象、评价值作为特征，分别对所有用户的数据进行采样并聚类，聚类结果是在这些特征值上有相同特征且达到较多数量的用户群体，视情况还可进一步遴选聚类结果（如只选取负面评价对应的结果）。最后定义一条规则，即同时满足上述特征（即在上述群体的归类情况雷同）者可能属于恶意用户团体，其评价需要进行评审处理。因此，基于上述用户及其行为社会属性的信任测度模型框架可设计如图 1 所示。

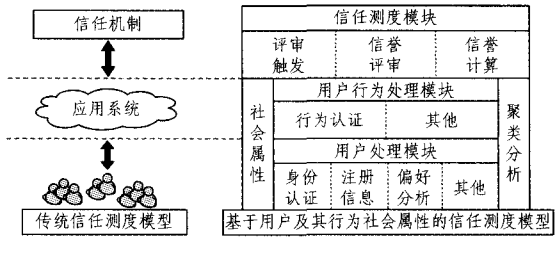


图 1 基于用户及其行为社会属性的信任测度模型框架

框架主要分为 3 个模块，用户处理模块处理用户本身信息，用户行为模块则处理用户之间交互行为的信息，两个模块都建立在基于社会属性的聚类分析基础之上，信任测度模块则负责信誉的评审与计算。与传统信任测度模型中信誉计算与用户本身以及用户交互等信息相互脱离的情况不同，本文的信任测度模型将用户及其行为的特性用社会属性进行刻画与分析，并将其应用于信誉评审，从而能更好地应对恶意用户及其行为。

框架的运行流程设计如下：

1. 描述恶意用户及其行为特征。

2. 监控用户本身以及交互行为信息，根据条件触发信誉评审机制。

3. 每当评审机制被触发，则：

a）根据恶意特征对应的社会属性选取指标，对用户及其行为的社会属性数据采样；

b）对样本进行数据分析，根据分析结果对相关用户的信誉进行评审。

4. 评审结束，更新用户信誉，回到步骤 2，如果发现新的恶意用户及其行为特征，则回到步骤 1。

3 用户及其行为的社会属性与分析方法

3.1 社会属性及其定义

本文用 R 来表示信誉，其由用户之间的相互评价（voting）计算而得，评价取值区间为$[-1,1]$，负值表示负面的评价，其值越低表示主体对客体越不满意，正值则相反。使用行为历史（Action History），$IH_{start,end}\{action_1, action_2, \cdots, action_n\}$则表示用户 I 与其他用户的交互，$action(Is, Io, voting)$ 表示一次具体交互，Is 表示交互中的主体，Io 表示客体。而社会属性是人们可以从社会、经济等现实意义上去解释的特征值，其定义为：

定义 1（社会属性） 系统中的用户及其行为所具备的可以从社会、经济现实意义上去理解的特征值。根据特征基于用户还是基于行为可将社会属性分为以下两种类别。

定义 2（用户的社会属性） 即用来描述用户本身特征的社会属性 $I=\{i_1, i_2, \cdots, i_n, preference\}$，其中每个分量 i_i 都可以代表一个实际的社会属性，例如用户名称、注册时间地点、用户近期行为活跃程度、自注册至今的整体活跃程度等等。而 $preference$ 则为用户的偏好向量，即主体较为偏向于与哪类客体交互。

定义 3（行为的社会属性） 可以用向量来表示行为的社会属性，即 $A=\{a_1, a_2 \cdots a_n\}$，每一个分量 a_i 表示一个实际的社会属性，例如主体 ID、客体 ID、评价值、评价类型（正评价、负评价）、主体付出的代价（比如购买商品的出价、客体对主体的信誉要求等）、客体的成本、主体的行为历史等等。

3.2 基于社会属性的恶意用户判断条件

根据用户及其行为的社会属性，可以有效地判断恶意用户及其行为。由于恶意行为最终是由恶意用户来完成的。因此两者可以归结为恶意用户，最终基于恶意用户对信誉进行设计。因此给出恶意用户的定义如下：首先设 $f_{cluster}(Att_1, Att_2, Att_3, \cdots)=\{User_{set1}, User_{set2}, \cdots, User_{setN}\}$ 为根据用户或行为的社会属性 Att_i 对相关的所有用户进行聚类的函数，其中 $User_{seti}=\{number, C_1, C_2, \cdots\}$ 为聚类之后每一个用户类别的特征值集合，$number$ 为集合中用户的数量，$C_1, C_2, \cdots$ 为对应属性的聚类中心值。于是可以根据用户类别特征值是否满足一定条件来对恶意用户进行判断，判断条件可以用向量 $\{Attribute, Rule\}$ 表示，其中 $Attribute=\{Att_1, Att_2, Att_3, \cdots\}$ 为恶意用户或恶意行为的特征属性，可以从用户或行为的社

会属性中选取，$Rule=\{t_1,t_2,\cdots\}$为一系列阈值范围，则针对 $Attribute$ 特征属性对所有用户进行聚类的结果为 $f_{cluster}(Att_1,Att_2,Att_3,\cdots)=\{User_{set1},User_{set2},\cdots,User_{setN}\}$，$User_{seti}$ 为恶意用户的条件为：$User_{seti}=\{number,C_1,C_2,\cdots\}$，同时满足 $number\in t_1$，$C_1\in t_2\cdots$所有阈值范围。

例如可以给出 Sybil 恶意用户的判断条件为：Sybil{注册时间，用户近期行为活跃程度，整体活跃程度，注册时间间隔不超过一天，集合内近期活跃程度差异不超过一个较小阈值，整体活跃程度较低，整体活跃程度差异不超过一个较小阈值}，即找出在很短时间内注册并在过去较短时间内活跃程度比较一致、整体活跃程度较为一致且普遍较低的用户集合，该集合中的用户为 Sybil 用户的可能性最大。

Group 攻击的判断条件则可以在 Sybil 条件的基础上进一步增加新的条件，表示为：$Group$｛行为历史中的客体集合，评价类型，主体代价，行为历史中客体集合差异不超过一个较小阈值，评价类型同为负评价，主体代价较小且差异不超过一个较小阈值，即满足 Sybil 条件的用户中，如果他们在过去的交互历史中都与相同的客体以较小的代价进行交互，并都给予负面的评价，则这些用户进行 Group 攻击的可能性最大。

33.3 基于社会属性的用户及其行为分析

根据恶意用户的判断条件可以对实际的用户及行为数据进行分析，分析流程可以用图 2 描述。

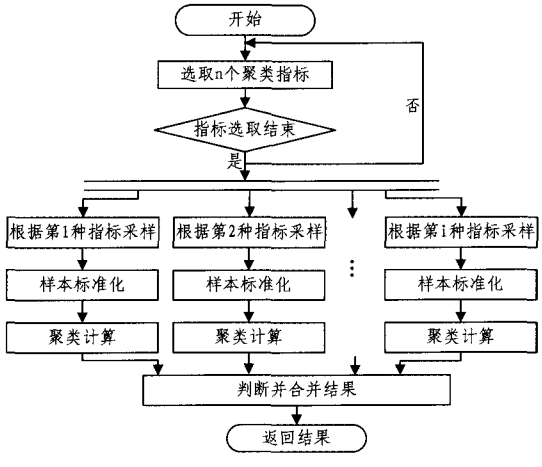


图 2 针对社会属性的用户及其行为聚类分析流程

4 基于社会属性的信誉评审及信任测度

4.1 审计触发机制

信誉评审根据恶意用户判断条件对用户及其行为数据进行聚类分析之后，对符合特征条件的相关用户的信任测度值即信誉进行处理，以消除恶意攻击的影响。由于聚类计算往往开销较大，不可能进行实时审计，因此只能根据实际情况触发，借鉴实际生活经验，可以将同时时间以及信誉变化程度作为触发评审的条件。

基于时间的触发机制：定义一个时间周期 T，在这个时间周期内通常用户可以完成若干次交互。每个周期结束时触发评审。

基于信誉变化程度的触发机制：即用户信誉的变化达到何种程度会触发评审，若以 0.25 为单位将区间分为 8 个间隔，其分布如表 1 所列。

表 1 信誉变化程度区间表

时间间隔	1	2	3	4
信誉值	[−1, −0.75)	[−0.75, −0.5)	[−0.5, −0.25)	[−0.25,0)
时间间隔	5	6	7	8
信誉值	[0,0.25)	[0.25,0.5)	[0.5,0.75)	[0.75,1]

4.2 信誉评审算法

在满足触发条件后，需要根据恶意用户及其行为特征以及用户及其行为分析结果来对相关用户的信任测度进行处理。本文使用系统决策表(System Decision Table，SDT)，根据逻辑推理规则来进行相关的处理工作。

定义 4(系统决策表) 系统决策表中每一行都代表一条决策规则。决策规则 r 是第 3.2 节所描述的现实意义上的恶意用户及其行为特征的形式化描述，是形如：if $x_1\wedge x_2\wedge\cdots\wedge x_n$ then d 的一条推理规则，其中 x_i 表示条件，为参与交互的用户 i 以及用户 j 各自对聚类形成的不同类别的归属情况，d 则为决策，一般为一个调整数值 τ，将所有规则进行汇总则得到系统决策表，表中条件列表$\{Condition_1,Condition_2,\cdots,Condition_n\}$为所有规则所用到的条件总和，形式如表 2 所列。

表 2 系统决策表

规则	条件1	条件2	…	…	条件n	调整值
$Rule_1$	$C_{1,1}$	$C_{1,a}$	…	…	$C_{1,m}$	d_1
$Rule_2$	$C_{2,1}$	$C_{2,a}$	…	…	$C_{2,m}$	d_2
…	…	…	…	…	…	…
$Rule_i$	$C_{i,1}$	$C_{i,a}$	…	…	$C_{i,m}$	d_i
…	…	…	…	…	…	…
$Rule_n$	$C_{n,1}$	$C_{n,a}$	…	…	$C_{n,m}$	d_n

根据系统决策表进行信誉评审的算法如下。

算法 1 信誉评审算法

算法准备阶段：首先使用第 3.2 节所述分析方法对引发触发机制的用户及其行为进行分析，并形成系统决策表。

步骤 1 从信誉计算流程中已经记录的交互用户集合 User 中提取一个未被评审过的用户 u，根据系统决策表收集其社会属性值、对聚类结果的归属情况以及客体的社会属性，形成向量 result$\{C_1,C_2,\cdots,C_n\}$

步骤 2 将向量 result 遍历系统决策表进行决策，并将结果进行累加，得到调整参数 τ。

步骤 3 根据调整参数，将主体 u 对客体的评价调整为 $e'=e*\tau$。

步骤 4 检查是否还有未被评审过的用户，如果有，则转回步骤 1，否则评审结束。

从算法 1 可以看出，其准备部分是大量的聚类计算，时空复杂度等价于聚类算法的时空复杂度(根据算法的不同，由 O(n)到 O($n2$)不等)，但恶意用户及其行为特征发现后只需根据触发机制定期针对用户行为进行聚类。而决策本身，对每一个待评审的用户而言，若与其交互的用户数量为 n，系统决策表规模为 m，则算法的时间复杂度为 O($m*n$)，如果系统决策表规模能保持在一定范围内(至少不与用户数量在一个数量级别上)，则可将其视为线性的算法。

4.3 基于信誉评审的信任测度

在信誉评审基础上，用户的信誉的计算流程为基于触发机制的周期性的迭代模型，其流程图如图 3 所示。

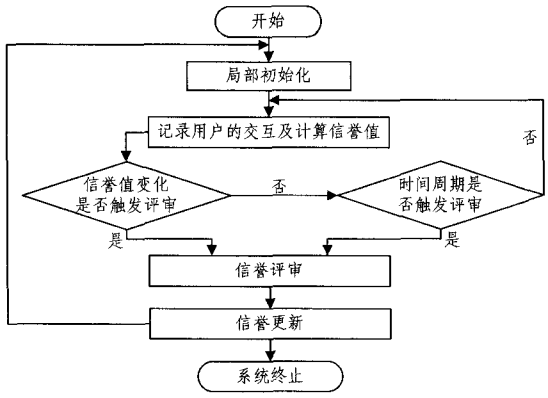


图 3　信誉计算模型流程图

局部初始化：将系统当前时间定义为时间坐标原点，并将用户当前的信誉值置为 R_{long}。

记录用户交互及计算信誉值：记录从时间坐标原点开始的所有与当前用户进行交互的用户及其行为，另外计算用户信誉值，其计算公式为：$R_{recent}=\frac{\sum_{t=0}^{T}(\frac{\sum_{i=1}^{N}e_{ij}}{N})}{n}$，其中 e_{ij} 表示与当前用户 i 交互的用户 j 所给予 i 的反馈值，与 i 用户交互的用户总数为 N。

针对 R_{recent} 进行的信誉评审根据触发机制启动，评审后其值为 R'_{recent}。

信誉更新：评审后的信誉值以及局部初始化中的信誉按公式 $R=(1-\alpha)*R_{long}+\alpha*R'_{recent}$ 对用户信誉进行更新，其中 α 为权重因子。

5　实验与分析

5.1　实验方法描述

模拟实验是目前应用较为广泛的针对信誉及信任机制等相关研究的评测方法。本文在一个模拟电子商务系统中部署信任测度模型，并对不使用评审的信任测度模型[1]、文献[2]中基于 Heavy Tail 的信任测度模型和本文的信任测度模型进行比较。实验参数如表 3 所列。

表 3　实验参数表

参数	取值	描述
N0	1000,1200,1500	环境中用户总数
N1	由具体实验内容确定	恶意用户数量
α	0.5,0.6	近期信誉权重

分别设计如下场景：

场景 1　注册大量的新用户，在一段时间内对一个目标用户进行 Sybil 攻击；

场景 2　多名实际用户结成恶意团伙，在一段时间内合作对目标用户进行 Group 攻击；

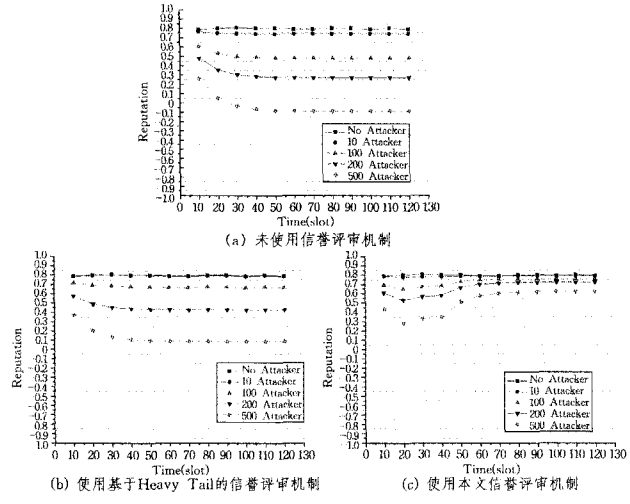
场景 3　某用户进行恶意行为后，借助 Group 洗刷来重新提升自己的信誉，再重复恶意行为的摇摆行为。

Sybil 和 Group 的判断条件如第 3.2 节所述，摇摆行为的判断条件则可在 Group 条件基础上进行修改。

实验的软硬件环境为：联想 T400 服（奔腾 2.2GCPU，2G 内存），Redhat Linux 9.0 版本，Oracle9i 数据库等。实验软件采用多 Agent 仿真软件 Netlogo，并按如上不同场景的用户行为策略仿真用户行为，以获得动态的用户行为数据，而正常用户的静态社会属性通过在学校 bbs 注册用户资料中随机抽取（ID 名、注册时间和 ip 地址）获得，恶意用户的社会属性则通过人工模仿 sybil 用户的特性注册相应的虚假用户信息来获得。聚类分析采用基于层次法的聚类算法 Birch 算法。

5.2　实验结果分析

首先验证场景 1，设有一个目标用户 A，其余用户作为主体与其交互，每 10 个间隔（slot）内其交互与否的概率在 20%，主体 A 的表现为正面的，因此正常的用户对其评价在 0.8 左右波动（随机赋值，赋值分布呈中心为 0.8 的正态分布，下同）。现分别注册 10、100、200 和 500 个 Sybil 用户，每 10 个时间间隔以 50%的概率密集与 A 交互且给予 A 的负面评价在−0.8 左右波动，未被攻击时 A 的信誉为 0.8，验证结果如图 4 所示。



(a) 未使用信誉评审机制

(b) 使用基于Heavy Tail的信誉评审机制

(c) 使用本文信誉评审机制

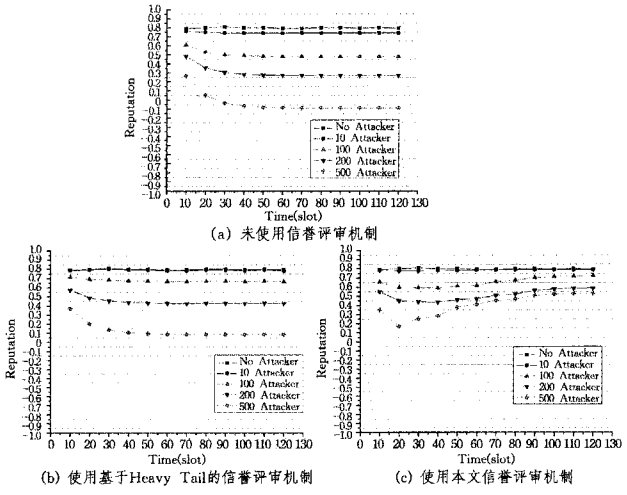
图 4　场景 1 实验结果

随着攻击者数量的增多，受到攻击的用户的信誉在第 1 个 10 个时间间隔后的初始值下降幅度较大（5%，24%、39.8%和 66.8%），随着攻击的持续，目标的信誉继续下降，直到经过 4～5 次 10 个时间间隔后信誉会维持到一个比较稳定的值（下降 5%、40%、66.2%、111%）。采取基于 Heavy Tail 的信誉处理方法使用户的信誉下降趋势得到一定的遏制，尤其是攻击者占用户比例较少（如占 1%和 10%）时，效果较为明显（最终下降大约 3%，15%）；但当攻击者占用户比例较多（20%和 50%）时；其效果不明显（最终下降大约 48%，80%）。而采用本文所述的信誉评审机制能够较好地发现并修正虚假的评价，受攻击的用户信誉初值下降幅度为 1.78%、13.4%、24%和 46.2%，而稳定状态的信誉比正常的值仅下降 1%、4.9%、9.6%和 22.3%，极大地缓解了攻击者造成的危害。

验证场景 2　同场景 1，但选择正常用户中 10、100、200 和 500 个用户每 10 个时间间隔以 100%的概率密集与目标 A 额外交互，10 个时间间隔给予 A 的负面评价在−0.8 左右波动，比较结果如图 5 所示。

从图 5 可看出，场景 2 中未使用信誉评审机制和使用基于 Heavy Tail 的信誉评审机制的结果与场景 1 类似；而本文的评审机制在攻击的初期对攻击的修正作用则弱于场景 1，受攻击的用户信誉初值下降幅度为 3.12%、18.1%、30.2%和 55.8%，猜测这是由于实际用户的聚类特征不如新用户明显。而随着攻击的持续，恶意用户在行为方面的聚类特征将

会逐渐突出，因此可以修正目标的信誉回升并稳定在一个较高的值，稳定状态的信誉比正常的值仅下降 1.3%、8.1%、25.1%和 32.1%，虽然较场景 1 有所减弱，但本文的评审机制仍可以有效缓解对目标的攻击。



(a) 未使用信誉评审机制

(b) 使用基于Heavy Tail的信誉评审机制

(c) 使用本文信誉评审机制

图 5 场景 2 实验结果

验证场景 3 设有目标用户 A，以 30 个时间间隔为周期，第 1、2 个时间周期主体 A 的表现为正面的，其后 1 个时间周期进行恶意行为，再使用 10 个新用户和 10 个普通用户在 20 个时间间隔与 A 交互，给予 A 正面评价，随后 A 又重新进行摇摆，以此往复，以 A 作为测量目标，比较结果如图 6 所示。

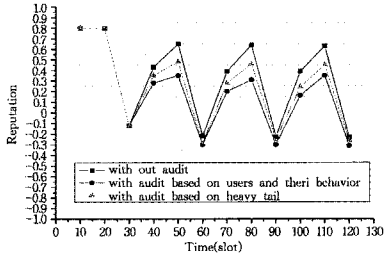


图 6 场景 3 实验结果

从图 6 可以看出，对于用户的摇摆行为，由于评审机制能够将参与洗刷的虚假节点和恶意团伙节点的评价加以剔除，因此相较于无评审机制以及基于 Heavy Tail 的评审机制而言，无评审机制的摇摆行为较为明显，摇摆幅度大且稳定，基于 Heavy Tail 的评审机制能够减弱一部分摇摆的幅度。而本文的评审机制随着用户摇摆行为的持续，其行为特征能够被识别而修正，因此能减缓用户在恶意行为之后推高信誉的程度和速度。但由于用户 A 本身在非恶意行为的周期里的确能获得较好的评价，因此信誉的波动仍然存在。

结束语 本文提出的信任测度模型引入了用户及其行为社会属性，以描述和分析恶意用户及其行为特征，在信任测度过程中增加了基于逻辑推理的信誉评审机制，以此修正用户的信任测度来应对恶意用户团伙的攻击。与传统信任机制的信任测度方法相比，本文的信任测度模型能够很好地应对有较多恶意用户环境下的信誉安全问题。在将来的工作中，一方面要设计更高效的数据分析算法；另一方面要在恶意行为特征规则方面进一步展开研究。

参 考 文 献

[1] Hoffman K, Zage D, Nita-Rotaru C. A Survey of Attack and Defense Techniques for Reputation Systems[J]. ACM Computing Surveys (CSUR), 2009, 42(1)

[2] Whitby A, Jøsang A, Indulska J. Filtering out unfair ratings in Bayesian reputation systems[J]. Icfain J. Manage. Res, 2005, 2(4): 48-64

[3] Chatterjee K, de Alfaro L, Pye I. Robust Content-Driven Reputation[C]// AISec '08 Proceedings of the 1st ACM workshop on Workshop on AISec. 2008

[4] Azzedin F, Khwaja S. Towards Trustworthy Peer-To-Peer Environments: An Appraisal Analysis Approach[J]. Journal of Next Generation Information Technology, 2010, 1(1)

[5] Feng Qin-yuan, Sun Y L, et al. Voting Systems with Trust Mechanisms in Cyberspace: Vulnerabilities and Defenses[J]. IEEE Transaction on Knowledge and Data Engineering, 2010, 22(12): 1766-1780

[6] Wang Yu-feng, Nakao A, Vasilakos A V. Doubleface: Robust Reputation Ranking Based on Link Analysis in P2P Networks [J]. Cybernetics and Systems: An International Journal, 2010, 41(2): 167-189

[7] Wang Xiao-feng, Liu Ling, Su Jin-shu. RLM: A General Model for Trust Representation and Aggregation[J]. IEEE Transactions on Services Computing, 2010(12)

[8] Xiong L, Liu L. Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities[J]. IEEE Trans. Knowl. Data Eng, 2004, 16(7): 843-857

[9] Yu Hai-feng, Shi Chen-wei, Kaminsky M, et al. DSybil: Optimal Sybil-Resistance for Recommendation Systems[C]// IEEE Symposium on Security and Privacy. 2009

[10] Seibert J, Sun Xin, Nita-Rotaru C, et al. Towards Securing Data Delivery in Peer-to-Peer Streaming[C]// Communication Systems and Networks (COMSNETS), 2010 Second International Conference. Jan. 2010: 1-10

[11] Ham M, Agha G. ARA: a robust audit to prevent free-riding in P2P networks[C]// Peer-to-Peer Computing, 2005 (P2P 2005), Fifth IEEE International Conference. 2005: 125-132

[12] Douceur J R. The Sybil attack[C]// Proceedings for the 1st International Workshop on Peer-to-Peer Systems. (IPTPS) Springer Berlin/Heidelberg, 2002: 251-260

[13] Bazzi R A, Konjevod G. On the establishment of distinct identities in overlay net- works[C]// PODC '05: Proceedings of the twenty-fourth annual ACM symposium on Principles of distributed computing. New York: ACM Press, 2005

[14] Aringhieri R, Damiani E, Vimercati S D C D, et al. Fuzzy techniques for trust and reputation management in anonymous peer-to-peer systems[J]. J. Am. Soc. Inf. Sci. Technol., 2006, 57(4): 528-537

[15] 常俊胜，王怀民，尹刚. DyTrust：一种 P2P 系统中基于时间帧的动态信任模型[J]. 计算机学报，2006，29(8)：1301-1307

[16] Sirivianos M, Kim K, Yang Xiao-wei. SocialFilter: Introducing Social Trust to Collaborative SpamMitigation[C]// USENIX CollSec. 2010

[17] Liu Qing-min. Information Acquisition and Reputation Dynamics [J]. The Review of Economic Studies, 2011, 78(2)

[18] 李小勇，桂小林. 可信网络中基于多维决策属性的信任量化模型[J]. 计算机学报，2009，32(3)：405-416