RulerRep：一种基于偏离度的过滤不实评价新方法

单明辉[1),2)] 贡佳炜[1),2)] 牛尔力[1),2)] 陈 君[2)] 倪 宏[2)]

[1)]（中国科学院研究生院 北京 100190）

[2)]（中国科学院声学研究所国家网络新媒体工程技术研究中心 北京 100190）

摘 要 信誉系统在解决开放网络环境中的信任问题时，较传统技术具有明显优势.然而不实评价的存在严重降低了信誉系统的可用性.文中提出一种基于偏离度的不实评价过滤方法：RulerRep.该方法以用户自身与服务提供者的直接经验为标尺，度量评价者的评价准确性，并以该评价准确性定义评价者的平均偏离度.在融合多个评价以计算服务提供者信誉的过程中，用该平均偏离度导出其评价的权重，使得平均偏离度大的节点的意见权重较小，从而达到过滤不实评价的效果.最后，以平均均方误差为指标，在实验仿真中与 TRAVOS 算法和没有使用过滤技术的 Beta Reputation 系统进行了性能对比.实验结果表明，在 50%与 100%的评价者均为恶意节点的情况下，RulerRep 仍显示出接近理论最优过滤的性能，并大幅优于同类技术.

关键词 信誉；偏离度；过滤不实评价；信任；RulerRep

中图法分类号 TP309 **DOI 号**：10.3724/SP.J.1016.2010.01226

RulerRep：Filtering out Inaccurate Ratings in Reputation Systems Based on Departure Degree

SHAN Ming-Hui[1),2)] GONG Jia-Wei[1),2)] NIU Er-Li[1),2)] CHEN Jun[2)] NI Hong[2)]

[1)]（*Graduate University of Chinese Academy of Sciences, Beijing* 100190）

[2)]（*National Network New Media Engineering Research Center, Institute of Acoustics, Chinese Academy of Sciences, Beijing* 100190）

Abstract Compared with conventional techniques, reputation systems are more capable of dealing with trust in an open environment. But unfair ratings in reputation systems would slow down the system's availability. To filter out unfair ratings, this paper proposes a new model, RulerRep. In this model, to measure the accuracy of a rator's history ratings, the authors use the service requester's interaction experience with other service providers as a rule, which is defined as the rator's departure degree. Then, when ratings from all rators are merged to calculate an unfamiliar service provider's reputation, each rating's weight is derived from the source rator's departure degree, namely the weight would be small if corresponding rator has a big departure degree. By using this method, the impact of the unfair ratings can be minimized. In simulations, RulerRep is compared with Beta Reputation system (with no unfair-rating-filtering techniques) and TRAVOS. The results show that, in environments where 50% and 100% of the rators are malicious rators, RulerRep has a good performance which is very close to that of the theoretical best filtering and also much better than that of using similar unfair-rating-filtering techniques.

Keywords reputation; departure degree; unfair rating filtering; trust; RulerRep

收稿日期：2007-08-12；最终修改稿收到日期：2009-03-31.本课题得到国家“八六三”高技术研究发展计划项目基金（2008AA01A317）、中国科学院知识创新工程领域前沿项目资助.**单明辉**，男，1981 年生，博士研究生，主要研究方向为分布式网络、数字版权管理. E-mail：shanminghui@gmail.com. **贡佳炜**（通信作者），男，1983 年生，博士研究生，主要研究方向为宽带通信. E-mail：gongjw@dsp.ac.cn. **牛尔力**，男，1981 年生，博士研究生，主要研究方向为网络与信息安全. **陈 君**，女，1977 年生，助理研究员，主要研究方向为宽带通信与信息安全. **倪 宏**，男，1964 年生，研究员，博士生导师，主要研究领域为宽带多媒体通信.

1 引　言

传统的基于策略的信任管理系统以认证、授权技术为核心,主要用来解决将合法的资源与不合法的使用者隔离的问题.而基于信誉的信任管理系统由于更易于处理动态、开放环境中的信任关系,因此更适用于分布式网络环境中;同时其更适于解决把合法的使用者与不合法的资源隔离开的问题,因此逐渐发展成为一种新的信任处理机制.

信誉(Reputation,也称声望),是指一个集体对一个个体的某种特性的一般评价[1].一般认为实体的信誉依赖于其在系统中的行为表现,并由其它节点的评价聚合而成.信誉系统的基本原理可描述为:当服务请求者需要计算某服务提供者的某种属性值、而本地又没有该提供者足够的信息时,该请求者向网络中其它节点发送询问请求,其它节点基于其与该服务提供者的交互历史返回评价(也称推荐),则请求者可通过返回的评价信息计算出该服务提供者的该属性值,从而可为进一步是否选用其服务的决策提供依据.

信誉系统,按其技术不同可分为简单平均模型、贝叶斯模型、离散信任模型、基于证据理论模型、模糊模型、流式模型等.国内外学者近年来提出了多种信誉系统,其中较具代表性的有文献[2-12].其中,Jøsang 提出的 Beta Reputation[2] 是基于贝叶斯概率理论信誉系统中的代表,该系统适用于交互结果可用二值(好、坏)描述的场景.

信誉系统现已广泛应用于在线贸易的商家评定、P2P 文件传输的上传节点选择、网格计算等多个领域.但目前信誉系统仍面临着多种攻击,如 Free riding 现象、评价的正向偏移、不实评价(虚夸,诋毁)、身份变更、节点品质随时间变化、辨识身份区分服务、评价量奇大等[1].其中,对不实评价过滤的研究是其中的一个热点.

不实评价,指的是评价者在对某服务提供者进行评价时,做出了与事实不符的评价,从而达到其私利目的,如虚夸和诋毁等.前者指评价者做出比真实值更好的评价以抬高服务提供者信誉,后者指评价者做出比真实值更差的评价以降低服务提供者信誉.不实评价的存在,使得对服务提供者的信誉值计算准确度大大降低,从而降低了信誉系统的可用性.

国内外学者针对不实评价的过滤提出了多种解决方法,按其技术体系主要可分为内生式和外生式[1]两类,内生式指利用一组评价自身的统计信息识别不实评价,该类方法主要采用聚类的技术,典型代表技术有文献[4-5,7];外生式指借助于外部的信息,如评价者的信誉值,识别并过滤不实评价.一般而言,内生式和外生式方法可同时使用,从而进一步增强过滤效果,提高计算的准确度.

在外生式过滤不实评价的方法中,典型的外生式过滤不实评价的方法有文献[5-6,11],文献[6]提出了一种基于证据理论的信誉系统,其过滤不实评价的主要思想为每次交互后根据公式 $w_i^{j+1}=\theta_i \cdot w_i^j$ 调整权重 w_i,若交互结果与推荐者的推荐值相差较大,则 θ 较小,反之 θ 较大.该方法某些参数没有给出计算方法,需要依赖主观决定.文献[5]综合运用了内生式和外生式方法构造了一个适用于网络书评的信誉系统.在该系统所采用的外生式方法中,评价者权重的确定综合考虑了评价本身的信息和读者对评价的评价,因此要求读者对评价进行评价这种额外操作.文献[11]提出了一种基于 Beta Reputation 的不实评价过滤方法,其主要思想与本文类似,都是利用评价者的评价与本节点的直接经验之间的差异大小,对评价者的评价进行调整.但 Travos 方法需要将评价的值域空间平均分成多个段,分段的数目对性能会有严重影响;另一方面由于每次评价只能使用一个段内的数据,从而增加了所需的历史评价数目.

本文提出了一种应用于 Beta Reputation 系统的、基于评价偏离度的不实评价过滤方法:RulerRep.该方法的主要思想为:以服务请求者与服务提供者的交互经验为标尺,以评价者对同一服务提供者的评价与该标尺的差异大小,度量该评价者在评价活动中的准确性,以此定义评价者的平均偏离度.在融合多个评价以估算服务提供者信誉的过程中,利用该平均偏离度对各个评价者的意见分配不同的权重,使得平均偏离度大的节点的意见权重较小,从而大幅降低恶意节点的影响,有效过滤不实评价.实验结果表明,在 50%与 100%的评价者均为恶意节点的情况下,RulerRep 仍显示出接近最优过滤的性能,并大幅优于 Travos.

本文第 1 节为前言,介绍信誉系统以及过滤不实评价的研究现状;第 2 节介绍 Beta Reputation 系统;第 3 节详细描述 RulerRep 的算法;第 4 节是实验仿真与数据分析;第 5 节对全文进行总结并提出下一步工作的方向.

2 Beta 信誉系统

2.1 定义与说明

根据一次服务结果值域的不同，信誉系统可分为基于二值的、基于多值离散域的和基于连续域的.本文所述系统为基于二值，即服务结果可用好、坏二值表示.因此服务提供者的信誉值可定义为其提供好服务的概率 P，而信誉系统的目标就是利用评价信息尽量精确地估计 P 的值.

在一个信誉系统中，节点可分为 3 种：服务提供者(provider)、评价者(rator)和用户(user).

Provider：表示为 pro_i，i 为节点编号，下同.该类节点可向 rator 和 user 节点提供某种服务或资源，如文件下载、流媒体播放等.

Rator：表示为 $rator_i$.该类节点既可向 provider 节点申请并享用服务、并记录服务结果，又可向 user 提供其与 provider 的交互历史及结果，作为其对该 provider 的评价(rating).$rator_i$ 对 pro_j 的评价定义为二元组$\langle good_{ij}, bad_{ij}\rangle$，用 r_{ij} 表示.其中，$good_{ij}$ 代表 $rator_i$ 与 pro_j 交互历史中成功的次数，bad_{ij} 代表失败的次数.

User：表示为 $user_i$.该类节点可向 provider 申请服务，并记录服务结果；又可向 rator 索取其对某一 provider 的评价，以计算该 provider 的信誉值.

在实际系统中，同一个节点往往兼具 rator 和 user 身份(如 user 本身也可给出对某一 provider 的评价)，实际取何种身份依赖于该节点在该次交互过程中所起的作用，可根据上下文区分.

2.2 信誉计算

Jøsang 等提出了一种基于二值的信誉系统[2]，用贝叶斯理论计算节点的信誉值，其主要思想描述如下：

假设 pro_j 提供好服务的概率是 P_j.节点 i 与之经过若干次交互后，交互历史可以用$\langle good_{ij}, bad_{ij}\rangle$二元组表示.利用贝叶斯估计方法，根据同等无知原则，由交互历史$\langle good_{ij}, bad_{ij}\rangle$得出的 P_j 的概率密度函数为 Beta 分布的形式[12]：

$$f(P_j|\alpha_{ij},\beta_{ij})=\frac{\Gamma(\alpha_{ij}+\beta_{ij})}{\Gamma(\alpha_{ij})\Gamma(\beta_{ij})}P_j^{\alpha_{ij}-1}(1-P_j)^{\beta_{ij}-1}$$

$$0\leq P_j\leq 1,\ \alpha_{ij}=good_{ij}+1,\ \beta_{ij}=bad_{ij}+1 \quad (1)$$

其中，$\Gamma(\cdot)$代表 Gama 函数：

$$\Gamma(z)=\int_0^{+\infty}\mathrm{e}^{-t}t^{z-1}\mathrm{d}t.$$

由式(1)求 P_j 的期望，即得 P_j 的贝叶斯估计值 $\hat{P}_{ij}$：

$$\hat{P}_{ij}=\int_{P_j=0}^{1}f(P_j|\alpha_{ij},\beta_{ij})P_j\mathrm{d}P_j=\frac{\alpha_{ij}}{\alpha_{ij}+\beta_{ij}}$$

$$=\frac{good_{ij}+1}{good_{ij}+bad_{ij}+2} \quad (2)$$

则 $\hat{P}_{ij}$ 即可作为节点 i 计算出的 pro_j 的信誉值.

对于某一待考察 provider 节点 pro_j，大多数情况下 $user_i$ 自身没有足够的直接经验，因此需要利用来源于系统中其它节点的间接经验，对 pro_j 的信誉值进行估算.此时，$user_i$ 先向邻近的 rator 查询其对 pro_j 的评价(设该邻近 rator 节点集合为 R_i)，获得形式为$\langle good_{kj}, bad_{kj}\rangle$的评价 r_{kj}.要将 user 自身的直接经验与来自多个 rator 的评价$\{r_{kj}\}$融合，则只要把各个 rator 的评价按照下述公式相加，即可得出融合后总的经验$\langle GOOD_{ij}, BAD_{ij}\rangle$.

$$GOOD_{ij}=good_{ij}+\sum_{rator_k\in R_i}good_{kj},$$

$$BAD_{ij}=bad_{ij}+\sum_{rator_k\in R_i}bad_{kj} \quad (3)$$

由总的评价$\langle GOOD_{ij}, BAD_{ij}\rangle$，根据式(2)，$user_i$ 即可计算出 pro_j 的信誉值 $\hat{P}_{ij}$.

在实际系统中，为处理节点品质随时间变化的情况，通常会降低较早交互经验的权重，常用的技术有在评价上乘一个指数时间衰减因子和加时间窗两种.由于该技术并非本文重点，为降低描述复杂性，本文假设节点的品质是不随时间变化的.另外，本文不涉及信任网络的建立，$user_i$ 构造集合 R_i 的方式并非本文重点，因此本文假设该集合 R_i 已经建立完毕.

从上述过程可以看出，Beta Reputation 系统将所有的节点默认视为可信节点.因而恶意 rator 节点可通过报告错误的交互经验对系统发起攻击.设某一恶意节点 $rator_x$ 对 pro_j 的评价 r_{xj} 为$\langle good_{xj}, bad_{xj}\rangle$，则当 $good_{xj}+bad_{xj}$ 较大时，根据式(2)和(3)计算出的信誉值 $\hat{P}_{ij}$ 将受 r_{xj} 的严重影响.这样，恶意节点即可依据自己的喜好而肆意影响网络中其它节点的信誉值，从而破坏系统的可用性、可靠性.下面即介绍一种过滤不实评价的方法，可有效抵御恶意评价节点的攻击.

3 RulerRep 算法

3.1 基本思想

将 $rator_i$ 与 pro_j 的每一次交互视为 $rator_i$ 对 P_j

的一次观测.经过 N 次观测后,$rator_i$ 可根据观测的 N 个结果对 P_j 做出估计,这个估计过程我们称之为 $rator_i$ 对 P_j 的一次测量过程.若 $rator_i$ 属于良节点,则其测量结果中应该只有随机误差,且误差的大小仅与历史交互的次数 N 相关,N 越大,误差越小(严格意义上讲,误差也与 P_j 相关.本文忽略了 P_j 对误差的影响,以求得到简练的形式).以公式来表达,应有形式:

$$\hat{P}_{ij}=P_j+e(N) \tag{4}$$

其中,$e(N)$为随机变量:其均值为 0;方差随 N 增加而减小,当 N 趋于无穷时趋于 0.

当两个良 rator 节点 $rator_i$、$rator_j$ 均对同一个 provider 节点 pro_k 做出了测量时,根据式(4),其测量结果的差为

$$\begin{aligned}D_{ij,k}=\hat{P}\hat{P}_{ik}-\hat{P}_{jk}&=(P_k+e(N_{ik}))-(P_k+e(N_{jk}))\\&=e(N_{ik})-e(N_{jk})\end{aligned} \tag{5}$$

即其测量结果的差也为随机变量:其均值为 0;方差随 N_{ik}、N_{jk} 增大而减小,当 N_{ik}、N_{jk} 均趋于无穷时趋于 0.

可见,$D_{ij,k}$ 衡量了两个测量结果之间的距离.若 $rator_i$ 是良节点而 $rator_j$ 是恶意节点,则式(5)中随机变量 $D_{ij,k}$ 不再满足均值为 0、方差随 N 增大而趋于 0 的约束.因此,$user_i$ 可以通过 $D_{ij,k}$ 衡量与 $rator_j$ 之间的偏离程度:若偏离程度大,则说明 $rator_j$ 很可能是一个恶意评价节点,因此应给予其意见较小的权重;否则给予其意见较大权重.详细的过程描述如下.

3.2　偏离度与准确度

定义 1.　评价信誉.设 $rator_i$ 对 pro_k 有评价 $r_{ik}=\langle good_{ik},bad_{ik}\rangle$ 且 $N_{ik}=good_{ik}+bad_{ik}>0$,则评价信誉定义为通过单个评价 r_{ik} 直接得出的信誉估计值 $\hat{P}_{ik}$:

$$\hat{P}_{ik}=\frac{good_{ik}}{good_{ik}+bad_{ik}} \tag{6}$$

其值域为 $\hat{P}_{ik}\in[0,1]$.对于 $N_{ik}=0$ 的情况,由于是空评价,因此计算其评价信誉无实际意义.

式(6)是经过 N_{ik} 次实验后、对 P_k 的一种无偏估计[12].之所以这里选用该式而非式(2)的贝叶斯估计,是由于该信誉估计值是一个中间变量而非最终结果,需要在后面参与进一步计算;若采用式(2)的定义,会将“同等无知”原则运用多次,从而增加了先验概率的影响.实践表明,此处采用式(6)定义比式(2)效果要好.

评价信誉的值是一种估计,其估计准确程度随 N_{ik} 的增加而增加.为了表述该准确性,我们定义了评价信誉的准确度:

定义 2.　评价信誉的准确度.设评价信誉来源于 pro_k 对 $rator_i$ 提供的 $N_{ik}=good_{ik}+bad_{ik}$ 次服务,则评价信誉的准确度定义为

$$C_{\hat{P}_{ik}}=N_{ik}=good_{ik}+bad_{ik} \tag{7}$$

其值域为 $C_{\hat{P}_{ik}}\in[0,+\infty)$.

准确度具有两层物理含义:一方面它表征了计算评价值所依据的数据量的多少,另一方面,通过推导能够发现准确度与评价值的方差之间存在近似倒数关系,因篇幅原因,推导过程略去.这两层物理含义在后面的其它类型准确度中也存在.

定义 3.　评价的偏离度.若 $rator_i$ 与 $rator_j$ 各自独立给出了对 pro_k 的评价 r_{ik}、r_{jk},则定义这两个评价的偏离度为

$$D_{ij,k}=|\hat{P}_{ik}-\hat{P}_{jk}| \tag{8}$$

其值域为 $D_{ij,k}\in[0,1]$.

定义 4.　偏离度的准确度.若 $rator_i$ 与 $rator_j$ 各自独立给出了对 pro_k 的评价 r_{ik}、r_{jk},其偏离度为 $D_{ij,k}$,且 r_{ik}、r_{jk} 所依据的实验次数分别为 N_{ik}、N_{jk},则偏离度 $D_{ij,k}$ 的准确度定义为

$$C_{D_{ij,k}}=\frac{C_{\hat{P}_{ik}}C_{\hat{P}_{jk}}}{C_{\hat{P}_{ik}}+C_{\hat{P}_{jk}}} \tag{9}$$

其值域为 $C_{D_{ij,k}}\in[0,+\infty)$.从定义式可看出 $C_{D_{ij,k}}$ 小于 $C_{\hat{P}_{ik}}$ 和 $C_{\hat{P}_{jk}}$,即偏离度的准确度低于其所依据的任何一个评价信誉的准确度.

评价的偏离度刻画了两个评价之间的距离,而偏离度的准确度则描述了对于这种距离度量的准确程度.

设与节点 i 有交互历史的 provider 节点集合为 H_i,则节点 i 与节点 j 之间有共同交互历史的节点集合为 $H_{ij}=H_i\cap H_j$.

定义 5.　评价者的平均偏离度.以 $user_i$ 的经验为参照,则 $rator_j$ 平均偏离度定义为

$$D_{ij}=\frac{\sum\limits_{pro_k\in H_{ij}}D_{ij,k}C_{D_{ij,k}}}{\sum\limits_{pro_k\in H_{ij}}C_{D_{ij,k}}} \tag{10}$$

其值域为 $D_{ij}\in[0,1]$.

定义 6.　平均偏离度的准确度.以 $user_i$ 的经验为参照、$rator_j$ 的平均偏离度 D_{ij} 的准确度定义为

$$C_{D_{ij}}=\sum_{pro_k\in H_{ij}}C_{D_{ij,k}} \tag{11}$$

其值域为 $C_{D_{ij}}\in[0,+\infty)$.

平均偏离度描述了 $rator_j$ 与 $user_i$ 之间意见的一般偏离程度. 根据 3.1 节中的分析,$user_i$ 可根据该平均偏离度判定 $rator_j$ 是一个恶意节点的可能性. 平均偏离度的测量是根据 $user_i$、$rator_j$ 与共有的交互伙伴集合 H_{ij} 之间的历史交互结果,其交互次数越多,该测量越准确,因此可基于交互次数构造平均偏离度的准确度,来衡量这种准确性. 平均偏离度与平均偏离度的准确度组成的二元组 $\langle D_{ij}, C_{D_{ij}}\rangle$ 描述了 $user_i$ 对 $rator_j$ 品质的估计,其典型意义如下($user_i$ 自身为善意节点):

(1) 当 $C_{D_{ij}}$ 趋于无穷时:若 $rator_j$ 为善意节点,则 D_{ij} 趋于 0;若 $rator_j$ 为恶意节点,则 $D_{ij}>0$,其值越大,则说明 $rator_j$ 说谎的程度越大.

(2) 当 $C_{D_{ij}}$ 趋于 0 时:尽管 D_{ij} 有某一确定值,但由于其数据来源太少,该值没有使用价值.

(3) 当 $C_{D_{ij}}$ 为有限值时:对同样的 D_{ij},$C_{D_{ij}}$ 越大说明准确性越高;对同样的 $C_{D_{ij}}$,D_{ij} 越大说明节点越有可能是一个恶意节点.

因此,综合考虑平均偏离度与平均偏离度的准确度组成的二元组 $\langle D_{ij}, C_{D_{ij}}\rangle$,即可以确定 $user_i$ 对 $rator_j$ 的信任程度.

3.3 信誉计算

当 $user_i$ 需要计算 pro_j 的信誉时,$user_i$ 先向一组 rator 节点发出询问请求(设该组 rator 节点集合为 R_i);各 rator 节点返回对 pro_j 的评价后,$user_i$ 即依据 rator 的平均偏离度,对各个 rator 的评价进行修正,使得偏离度大的节点其意见权重较低. 具体方法如下:

首先,根据式(12),用 $C_{D_{ij}}$ 修正 D_{ij}. 式(12)表示实际采用的平均偏离度要根据平均偏离度的准确度做出调整:偏离度可能是由于测量中的随机误差导致的,而方差是衡量随机误差大小的指标,又因为平均偏离度的准确度和方差成近似倒数关系,因此利用式(12)能够尽量排除随机性的影响. 为保证一定的置信水平,要减去一个与准确性相关的值. θ_1 为经验参数,其取值对系统的影响如下:

(1) 若 $\theta_1>0$,表示把"该节点平均偏离度为 0"作为原假设:除非有足够的证据证明该节点偏离度不为 0,否则将该节点的偏离度视为 0. 此时,其取值影响识别恶意节点的误识率与漏识率:θ_1 越大,则误识率越小、漏识率越大;反之亦然. 根据实验结果,为取得较好的折衷性能,θ_1 取值一般在 1.5～2.5 之间,本文取 $\theta_1=2$.

(2) 若 $\theta_1=0$,则表示不依据可靠性来修正偏离度.

(3) 若 $\theta_1<0$,表示把"该节点平均偏离度大于 0"作为原假设;其它分析结果类似(1).

$$\hat{D}_{ik}=\max\left(D_{ik}-\frac{\theta_1}{\sqrt{C_{D_{ik}}}},0\right) \tag{12}$$

然后,根据调整后的平均偏离度,调整每个评价者的评价. 该调整方法应满足特性:

(1) 平均偏离度越大,其评价的权重越小.

(2) 偏离度每增加一定值,其权重也应下降一固定百分比. 即若两个评价者的平均偏离度分别为 D_1、D_2,评价的调整因子 $f(D)$ 应满足 $f(D_1)/f(D_2)=g(D_1-D_2)$.

因此构造调整公式如式(13). 其中,θ_2 为经验参数,其取值决定计算结果对偏离度的敏感程度:

(1) $\theta_2=0$,表示不依据偏离度来修正意见.

(2) $\theta_2>0$,越大表示系统对偏离度越敏感,同等偏离度的评价者其评价被折扣得越多. 根据仿真结果,经验参数 $\theta_2=40$ 时能够取得比较好的实验效果,因此本文取 $\theta_2=40$.

(3) θ_2 趋于正无穷,表示平均偏离度为 0 的节点的评价被无条件接受,其它的评价都被完全拒绝.

$$\begin{aligned} good_{kj}^{m}&=good_{kj}\cdot e^{-\theta_2\cdot\hat{D}_{ik}},\\ bad_{kj}^{m}&=bad_{kj}\cdot e^{-\theta_2\cdot\hat{D}_{ik}} \end{aligned} \tag{13}$$

根据式(12)、(13)得到修正意见 $\langle good_{kj}^{m}, bad_{kj}^{m}\rangle$ 后,pro_j 的信誉即可由式(2)、(3)计算,即

$$\begin{aligned} GOOD_{ij}&=good_{ij}+\sum_{rator_k\in R_i} good_{kj}^{m},\\ BAD_{ij}&=bad_{ij}+\sum_{rator_k\in R_i} bad_{kj}^{m} \end{aligned} \tag{14}$$

$user_i$ 对 pro_j 总的信誉估计值为

$$\hat{P}_{ij}^{a}=\frac{GOOD_{ij}+1}{GOOD_{ij}+BAD_{ij}+2} \tag{15}$$

4 仿真与比较分析

4.1 仿真环境说明

目前过滤不实评价性能较好的外生式技术为 Travos,因此本文选择 Travos 进行了对比(参照文献[11]设置,其值域划分为 5 个小区间),并选择相同环境下未使用任何过滤方法的基本 Beta Reputation 作为参照. 仿真环境中设有一个 user 节点,10 个 rator 节点,41 个 provider 节点. 其中,rator 节点分为良(fair)节点和恶意(unfair)节点,对 unfair 节点,我们分别仿真了以下几类:lying rator、noisy rator、badmouthing rator 和 bragging rator. 设 $rator_i$ 与 pro_j 节点的真实交互历史为 $\langle good_{ij}, bad_{ij}\rangle$,则 rator

向 user 报告的评价$\langle good'_{ij}, bad'_{ij}\rangle$将依 rator 身份的不同而有所差异:

Fair 节点:如实报告:

$$good'_{ij}=good_{ij},\ bad'_{ij}=bad_{ij}.$$

Lying 节点:报告与真实结果相反的经验:

$$good'_{ij}=bad_{ij},\ bad'_{ij}=good_{ij}.$$

Noisy 节点:在真实评价上增加一个随机值:

$$\rho=\begin{cases}1, & \dfrac{good_{ij}}{good_{ij}+bad_{ij}}+e>1\\ 0, & \dfrac{good_{ij}}{good_{ij}+bad_{ij}}+e<0\\ \dfrac{good_{ij}}{good_{ij}+bad_{ij}}+e, & \text{其它}\end{cases},$$

$$good'_{ij}=\rho\cdot(good_{ij}+bad_{ij}),$$

$$bad'_{ij}=good_{ij}+bad_{ij}-good'_{ij},$$

其中,e 是一个在$[-0.4, 0.4]$之间均匀分布的随机变量.

Badmouting 节点:对 provider 进行诋毁:

$$\Delta=\min\left(good_{ij}, \frac{1}{4}(good_{ij}+bad_{ij})\right),$$

$$good'_{ij}=good_{ij}-\Delta,\ bad'_{ij}=bad_{ij}+\Delta.$$

Bragging 节点:对 provider 进行虚夸:

$$\Delta=\min\left(bad_{ij}, \frac{1}{4}(good_{ij}+bad_{ij})\right),$$

$$good'_{ij}=good_{ij}+\Delta,\ bad'_{ij}=bad_{ij}-\Delta.$$

对 41 个 provider 节点,其提供好服务的真实概率 P_i在$[0,1]$区间内平均分布,分别设为$[0, 0.025, 0.05, \cdots, 0.975, 1]$. 设 user 通过信誉系统估算出的概率值为 $\hat{P}_i$,则信誉系统的性能可通过估算值与真实值之间的平均均方误差来衡量(N_P为 provider 节点个数):

$$\Phi=\frac{1}{N_P}\sum_{i=1}^{N_P}(P_i-\hat{P}_i)^2 \tag{16}$$

4.2　仿真流程

仿真系统的运行流程描述如下,其中 user 指特定的一个集中计算者,并不包括 rator. 流程中的步 7 之所以跳到步 2,主要是为了模拟真实环境,因为在真实环境中 user 在计算新的声望值前,并不知道在过去的一段时间内,整个系统内的 rator 是否发生过新的交易行为,因此 user 在每次计算新的声望值前需要实时向每个 rator 查询其对每个 provider 的评价,然后再根据自己的直接经验计算. 虽然对于本文所描述的特定仿真流程,每一次循环中步 2 和 3 的返回结果是一样的(除 noisy 结点外),因此循环步骤能够简化成直接跳到步 4,但为了保持和实际运行步骤的一致性,本文仍选择循环步骤跳到步 2.

1. 系统随机挑选一对 rator 与 provider 进行交互,共进行 $41\times10\times20=8200$ 次,即平均每个 rator 与每个 provider 之间进行 20 次交互,以产生 rator 与 provider 的交互历史. 初始化循环变量 $i=0$.

2. user 向每个 rator 查询其对每个 provider 的评价.

3. rator 以其与 provider 的交互历史记录数据为基础,按照 4.1 节中设定的行为方式,构造评价响应 user 的查询.

4. user 根据收到的评价,按照某一不实评价过滤方法,估计每个 provider 的信誉值.

5. 系统依据式(16)求得该次估计的平均均方误差 Φ_i.

6. user 与每个 provider 都进行一次交互,并保存交互结果;i++.

7. 如果 $i<40$,进入步 2.

8. 结束,输出每次的 Φ_i.

每次实验都将运行 20 次,并取平均值作为评测依据.

4.3　实验数据与分析

我们分别对 Beta Reputation(不使用任何过滤技术)、Travos 算法和 RulerRep 算法进行仿真,仿真效果以平均均方误差作为标准进行比较,并以平均均方误差为纵轴、user 与 provider 之间的交互次数为横轴作图. 实验分为两部分,第 1 部分实验侧重对比系统在善良环境(评价节点全为善意)和恶意环境(50%的评价节点是恶意节点)中的过滤性能;为了突出对比效果,该部分实验中 user 在计算信誉值时并不采用式(14),而是根据没有使用自身直接经验的式(17)以及式(15)来计算信誉值.

$$GOOD_{ij}=\sum_{rator_k\in R_i}good^m_{kj},$$

$$BAD_{ij}=\sum_{rator_k\in R_i}bad^m_{kj} \tag{17}$$

各次实验中,rator 节点的组成结构如表 1 所示,实验结果见图 1~图 5.

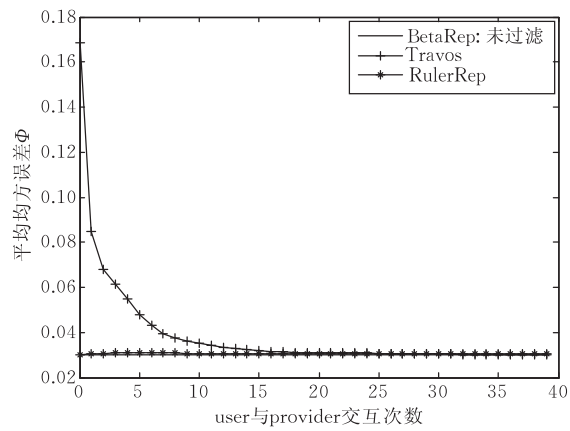

图 1　过滤算法对正常评价节点的影响

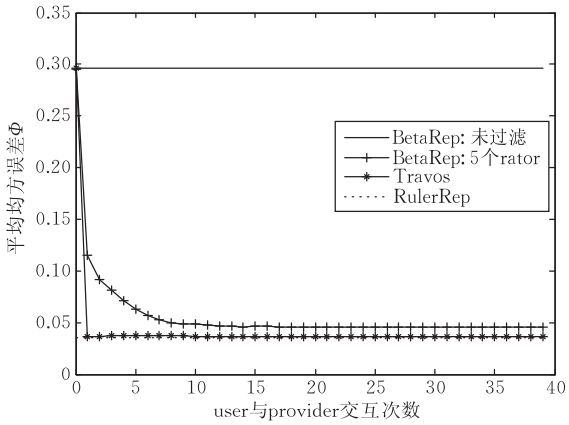

图 2 一半 rator 为 lying rator 时的过滤效果对比

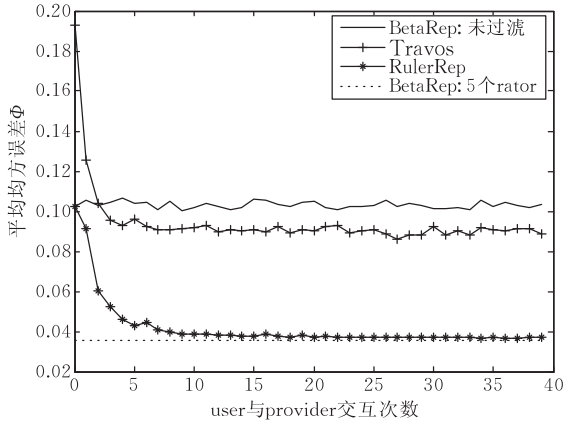

图 3 一半 rator 为 noisy rator 时的过滤效果对比

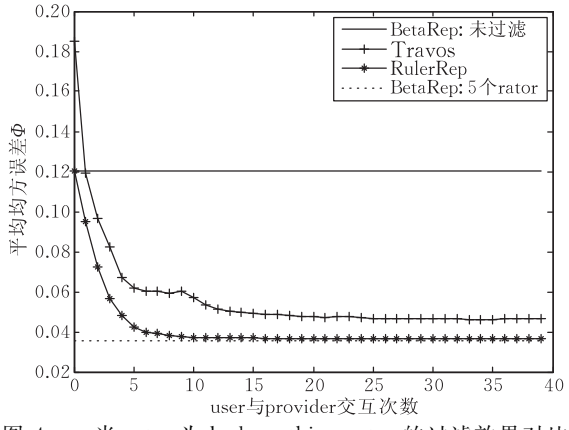

图 4 一半 rator 为 badmouthing rator 的过滤效果对比

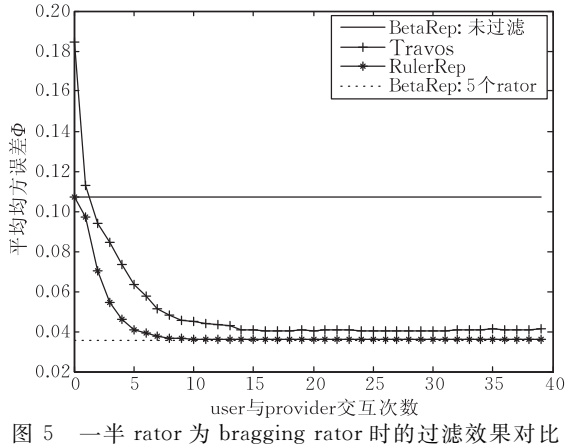

图 5 一半 rator 为 bragging rator 时的过滤效果对比

表 1 第 1 部分各次实验中的 rator 数目配置

类型	rator 数目				
	I	II	III	IV	V
fair	10	5	5	5	5
lying	0	5	0	0	0
noisy	0	0	5	0	0
badmouthing	0	0	0	5	0
bragging	0	0	0	0	5

一个好的不实评价过滤算法首先应该满足在良好系统环境中的可用性要求，即尽量小的误识(不是恶意节点却被识别成了恶意节点)率. 从图 1 中可以看出，当 10 个 rator 均为 fair rator 时，Beta Reputation 系统由于将所有 rator 都视为完全可信的，没有引入错误，可认为是理论最优值，其均方误差最小；而 RulerRep 系统的平均均方误差曲线基本与 Beta Reputation 的重合，可见 RulerRep 的过滤对 fair rator 节点基本无不良影响，即对恶意节点的误识率极小；在 Travos 系统中，当 user 与 provider 之间的交互次数较少时，因其无法检验 rator 是否值得信赖，因此将大部分 rator 的评价都错误地过滤掉了，随着 user 与 provider 间交互次数的增加，这种错误影响趋向于减小，直到交互次数达到 20 以后，其影响才基本消除.

图 2～图 5 分别对比了当存在各种类型的恶意节点时系统的过滤效果，并增加了去掉所有恶意节点、只有 5 个 fair rator 后的 Beta Reputation 系统(可视为最佳过滤结果)性能作为对比. 从图中可以看出，不使用过滤技术，计算出的信誉值与真实值之间的差异非常大，使得计算值几乎无使用价值，即恶意节点的存在能严重影响系统的可用性. Travos 与 RulerRep系统对不实评价的过滤效果均非常明显，可大幅提高系统的可用性，对二者相比较可以看出：

(1) 当 user 与 provider 之间的历史交互次数 N 足够多时(30～40)，二者对各种不实评价攻击均有明显过滤效果. 但 RulerRep 系统的平均均方误差普遍比最优值仅高 4%以内，而 Travos 系统的平均均方误差则比最优值大得多. 尤其对 noisy 型节点的攻击，其平均均方误差比最优值大 150%以上，因此可认为 Travos 系统对 noisy 型节点的过滤效果不佳. 其统计数据如表 2、表 3 所示.

表 2 N 较大时平均均方误差比不用过滤系统降低的平均百分比$(1-\Phi_x/\Phi_{\text{nofilter}})\cdot 100\%$，$x=\{\text{Travos}, \text{RulerRep}\}$

算法	降低的百分比			
	lying	noisy	badmouthing	bragging
Travos	84.6	12.65	61.39	61.9
RulerRep	87.68	64.2	69.56	66.27

表 3　N 较大时平均均方误差比理论最佳过滤系统升高的平均百分比($\Phi_x/\Phi_{best}-1)\cdot 100\%$, $x=\{$Travos, RulerRep$\}$

算法	升高的百分比			
	lying	noisy	badmouthing	bragging
Travos	28.24	153.22	30.48	14.42
RulerRep	2.59	3.78	2.87	1.3

(2) 当 user 与 provider 间的历史交互次数 N 较少时(1～10),RulerRep 比 Travos 的平均均方误差降低显著.其统计数据如表 4、表 5 所示.对于网络交易等应用而言,由于实际环境中 user 与 provider 间的历史交易次数较少,因此本项对比结果更具实际意义.

表 4　N 较小时平均均方误差比不用过滤系统降低的平均百分比($1-\Phi_x/\Phi_{nofilter})\cdot 100\%$, $x=\{$Travos, RulerRep$\}$

算法	降低的百分比			
	lying	noisy	badmouthing	bragging
Travos	77.07	5.84	39.72	36.78
RulerRep	87.47	51.94	57.9	53.73

表 5　N 较小时平均均方误差比理论最佳过滤系统升高的平均百分比($\Phi_x/\Phi_{best}-1)\cdot 100\%$, $x=\{$Travos, RulerRep$\}$

算法	升高的百分比			
	lying	noisy	badmouthing	bragging
Travos	90.94	172.94	103.7	89.87
RulerRep	4.37	39.31	42.26	38.98

在第 2 部分实验中,所有 rator 节点均为恶意节点,而 user 节点在计算 provider 节点信誉时将加入自身的直接经验.该部分主要对比 user 节点处于极端恶劣环境中时系统的鲁棒性能,并增加了去掉所有恶意节点后的 Beta Reputation 系统(可视为最佳过滤结果)进行对比.各次实验中,rator 节点数目如表 6 所示,实验结果见图 6～图 9.

表 6　第 2 部分各次实验中的 rator 数目配置

类型	rator 数目			
	I	II	III	IV
lying	10	0	0	0
noisy	0	10	0	0
badmouthing	0	0	10	0
bragging	0	0	0	10

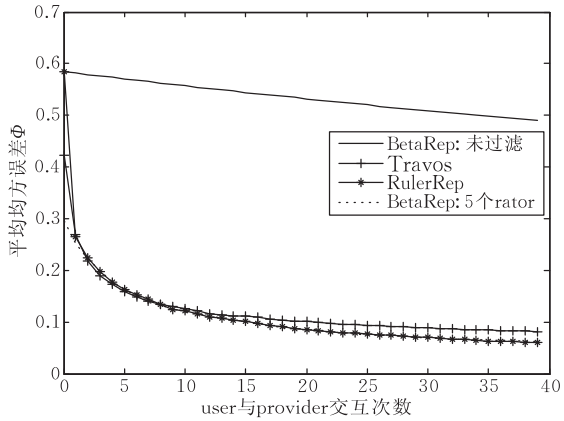

图 6　融合直接经验与 10 个 lying rators 的评价结果

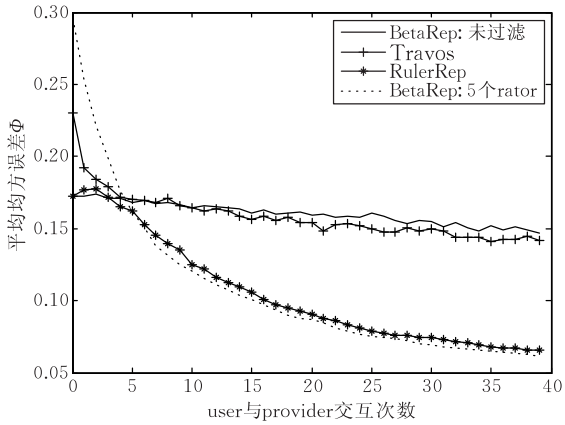

图 7　融合直接经验与 10 个 noisy rator 评价后的结果

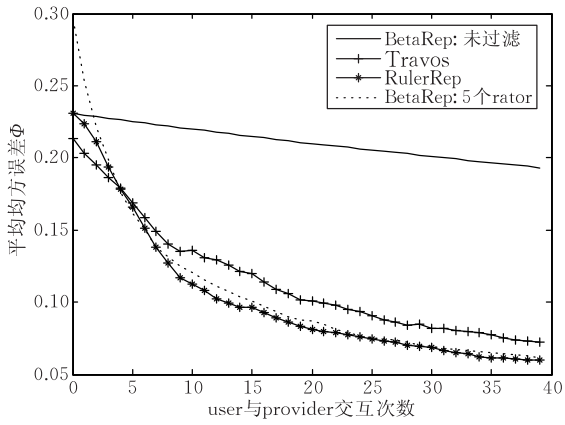

图 8　融合直接经验与 10 个 badmouthing rator 评价后的结果

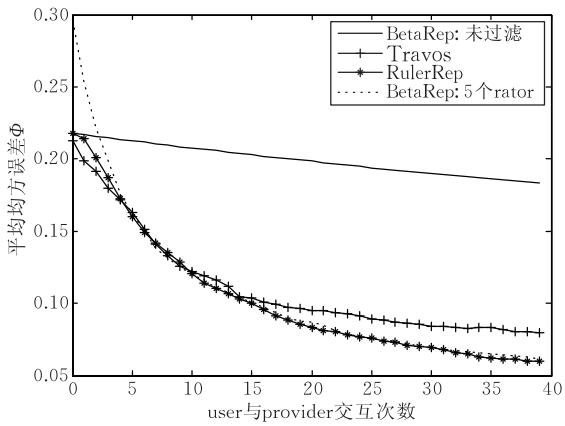

图 9　融合直接经验与 10 个 bragging rator 评价后的结果

从图 6～图 9 中可以看出,当 user 周围的 rator 都是恶意节点时,采用过滤系统仍然可以将不实评价的影响大幅降低.对比 Travos 与 RulerRep 的结果:(1) 在数据量较多时 RulerRep 表现出较为明显的优势,几乎与将所有恶意节点过滤掉的理论最优性能一致;而 Travos 仍有不可消除的误差.(2) 在应对 badmouthing 与 bragging 节点攻击时,在某些区段,RulerRep 的表现甚至超越将所有恶意节点都过滤掉的情况,其原因是由于随机误差.(3) 当 user 与 provider 间交互次数较少时,RulerRep 比 Travos

的优势不明显，在恶意节点为 badmouthing 和类型、且交易次数小于等于 3 时甚至略差；这是因为 RulerRep 在无数据情况下假定所有 rator 均为可信的，而 Travos 假定所有节点均为不可信的，因此在此极端恶劣情况下，Travos 的性能较优；Travos 的假设是以提高误识率的来降低漏识率，因此也导致了 Travos 在非极端恶意环境中的性能较差（参照第 1 部分实验，即使在 50％的结点均为恶意节点的次极端恶劣环境下，Travos 的这种假设也将转换为劣势）. 考虑到实际应用环境中，恶意节点的比例远比仿真环境中所设定的要低，因此 Travos 在这种特殊情况下（所有评价者均为恶意、恶意节点类型为 badmouthing 或 bragging、user 与 provider 的交互次数又恰小于等于 3 次）的略微相对优势可忽略不计.

RulerRep 方案比其它方案优的原因在于其侧重于消除信誉度量的一个重要误差：辨识力误差. 辨识力误差来源于对真实信任度辨识的客观能力不足或主观故意歪曲，并且无法像随机误差一样随着增加实验次数而减小. 而 RulerRep 提出的以平均偏离度和平均偏离度的准确度组成的二元组能够比较准确地度量辨识力误差，从而达到了比较好的实验效果.

5 结 论

信誉系统是分布式环境中解决信任问题的有效方法，然而目前信誉系统仍面临包括不实评价在内的多种攻击威胁. 本文提出了一种信誉系统中基于偏离度的过滤不实评价的新方法：RulerRep. 该方法属于外生式过滤方法，其主要思想为：以服务请求者与服务提供者的交互经验为标尺，用评价者对同一服务提供者的评价与该标尺的差异大小，度量该评价者的评价准确性，以此定义评价者的平均偏离度. 在融合多个评价以估算服务提供者信誉的过程中，利用该平均偏离度对各个评价者的评价分配不同的权重，使得平均偏离度大的节点的评价权重较小，从而大幅降低恶意节点的影响，有效过滤不实评价. 实验仿真结果表明，该方法可应对各种类型攻击，对不实评价的过滤接近最优过滤效果；同时对善意节点影响可忽略不计. 与现有同类系统相比，RulerRep 在对善意节点的影响、对各种恶意节点的过滤上，性能均有大幅提高，尤其适用于历史交互数据量较小的应用环境.

下一步的工作主要集中在：（1）研究 RulerRep 对各种类型、不同强度攻击的过滤效果，研究系统中经验参数对各种攻击过滤效果的影响.（2）研究 RulerRep 在多值离散域、连续域评价系统上的应用.（3）构造系统框架、研究与之配套的通讯协议，分析在网络环境下的通信、计算开销.（4）研究在无线传感器网络等节点资源极为有限的情况下的简化系统.

参 考 文 献

[1] Jøsang A, Ismail R, Boyd C. A survey of trust and reputation systems for online service provision. Decision Support Systems, 2007, 43(2): 618-644

[2] Jøsang A, Ismail R. The beta reputation system//Proceedings of the 15th Bled Electronic Commerce Conference, Bled, Slovenia, 2002

[3] Jøsang A. A logic for uncertain probabilities. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2001, 9(3): 279-311

[4] Dellarocas C. Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior//Proceedings of the 2nd ACM Conference on Electronic Commerce. Minneapolis, Minnesota, United States, 2000: 150-157

[5] Chen M, Singh J P. Computing and using reputations for internet ratings//Proceedings of the 3rd ACM Conference on Electronic Commerce. Tampa, Florida, USA, 2001: 154-162

[6] Yu B, Singh M. Detecting deception in reputation management//Proceedings of the 2nd International Joint Conference on Autonomous Agents and Multiagent Systems. Melbourne, Australia, 2003: 73-80

[7] Whitby A, Josang A, Indulska J. Filtering out unfair ratings in Bayesian reputation systems//Proceedings of the 7th International Workshop on Trust in Agent Societies. New York, USA, 2004

[8] Song S, Hwang K, Zhou R, Kwok Y-K. Trusted P2P transactions with fuzzy reputation aggregation. IEEE Internet Computing, 2005, 9(6): 24-34

[9] Kamvar S D, Schlosser M T, Garcia-Molina H. The EigenTrust algorithm for reputation management in P2P networks//Proceedings of the 12th International Conference on World Wide Web. Budapest, Hungary, 2003: 640-651

[10] Dou W, Wang H M, Jia Y, Zou P. A recommendation-based Peer-to-Peer trust model. Journal of Software, 2004, 15(4): 571-583(in Chinese)
(窦文，王怀民，贾焰，邹鹏. 构造基于推荐的 Peer-to-Peer 环境下的 Trust 模型. 软件学报，2004，15(4)：571-583)

[11] Teacy W T, Patel J, Jennings N R, Luck M. TRAVOS: Trust and reputation in the context of inaccurate information sources. Autonomous Agents and Multi-Agent Systems, 2006, 12(2): 183-198

[12] Xiong Li, Liu Ling. PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities. IEEE Transactions on Knowledge and Data Engineering, 2004, 16(7): 843-857

SHAN Ming-Hui, born in 1981, Ph. D. candidate. His research interests include distributed network and digital rights management.

GONG Jia-Wei, born in 1983, Ph. D. candidate. His research interests focus on broadband communication.

NIU Er-Li, born in 1981, Ph. D. candidate. His research interests include network and information security.

CHEN Jun, born in 1977, associate professor. Her research interests include broadband communication and information security.

NI Hong, born in 1964, professor, Ph. D. supervisor. His research interests include broadband multimedia communication.

Background

In recent years, reputation is becoming a hotspot to address the trust problem in open and dynamic environments. It has been widely used in file-sharing applications, e-market and grid computing. However, the problem of unfair ratings is probably the hardest to solve in any reputation system that is based on subjective ratings form participants. Many researches are working on this in the academic community and have proposed many methods which can broadly be grouped into two categories: endogenous method and exogenous method.

The research group presents a new exogenous method called RulerRep. It is based on departure degree and has advantages in filtering out unfair ratings in open environments. It can effectively weaken the influence of unfair ratings and strengthen the accuracy of the reputation's calculation. In many cases, it is very close to the optimal results. Specifically, it even shows great performance in extreme bad environment which is much better than that of using other unfair-rating-filtering techniques.

This work is supported by the National High Technology Research and Development Program (863 program) of China (No. 2008AA01A317) and the Knowledge Innovation Program of the Chinese Academy of Sciences.