一种基于风险和推荐的用户信任计算方法

刘绮虹,介利军
(桂林电子科技大学,广西 桂林 541004)

摘 要:结合客观的风险评估和主观的推荐信任共同计算用户可信度,并利用推荐可信度和域可信度来识别和惩罚提供虚假反馈的服务方,提出了基于风险和推荐的用户信任计算方法。仿真实验表明,该模型具有较好的动态适应性,能够准确反映用户行为,为信任决策提供安全、可靠的依据。

关键词:用户可信度;风险评估;推荐可信度;域可信度

中图分类号:TP393 **文献标识码**:A **文章编号**:1674-7720(2011)04-0055-04

A computing method of user trust based on risk and reputation

Liu Yihong, Jie Lijun
(Guilin University of Electronic Technology, Guilin 541004, China)

Abstract: We calculate the user reliability jointly with objective risk evaluation and subjective reputation trust. And the server which provides inveracious feedback can be identified and punished by reputation reliability and field reliability. This paper proposes a computing method of user trust based on risk and reputation. The experimental results show that the proposed model has good dynamic flexibility and reflects the activities of entities accurately. This method provides secure and reliable basis to trust decision.

Key words: user reliability; risk evaluation; reputation reliability; field reliability

随着网络传输速度的极大提高,人们已经不再满足于传统网络所带来的便利,而需要最大限度地共享资源并充分利用各类闲置资源。于是各种分布式系统应运而生,如云计算、可信计算、网格计算、对等计算等。但由于缺乏有效的信任机制来提高系统整体的可用性,分布式系统的应用受到了各种限制。因此,如何建立一种行之有效的信任机制,已成为当前信息安全领域研究的热点问题[1]。

信任是指在特定的情境下,对某一个体能够独立、安全且可靠地完成任务的坚定信念[2]。如何监控用户的行为,减少破坏系统安全行为的发生,是信任机制研究的一个方面。

在网格信任模型中,参考文献[3]提出的 Grid 环境下基于实体行为的信任评估模型,信任计算的过程过于简单,域信任值更新仅仅是域中个体信任值的简单叠加,惩罚机制与上下文的联系不大。参考文献[4]的综合信任计算综合硬件条件、服务能力、推荐可信度等因素采用 MADM(Multiple Attribute Decision Making)方法计算权值,但该模型仅考虑直接信任和间接信任,造成信任计算的主观性和片面性。DyTrust 模型[5]提出了累积滥用信任的概念,并通过对公共交互节点的评价差异来更新反馈可信度,可有效减少合伙欺骗节点提供的虚假反馈对信任计算的影响,再将反馈可信度与累积滥用信任相结合,可以对节点的摇摆行为进行惩罚。

针对以上问题,本文提出了一种基于风险和推荐的用户信任计算方法。该方法从主观和客观两方面着手,利用风险评估和推荐信任综合计算用户的信任值;同时使用时间帧和时间衰减来标示推荐的时间属性。上述方法引入了推荐可信度和域可信度衡量服务方推荐的可靠性,并对提供虚假推荐的服务方及其所在域进行相应的惩罚。

1 系统结构

本文的计算方法以网格为背景进行测试。网格环境分为两层结构:上层由域代理和服务器组成,域代理主要实现域间通信、与服务器通信、传递信任、更新数据、进行信任决策;服务器负责计算更新节点的风险评估值,同时存储部分数据。下层以域为单位,由域代理、用户和服务方构成,每个域可以采取适合本域的管理机制,充分体现域的高度自治性。系统的访问、计算、更新流程如图 1 所示。

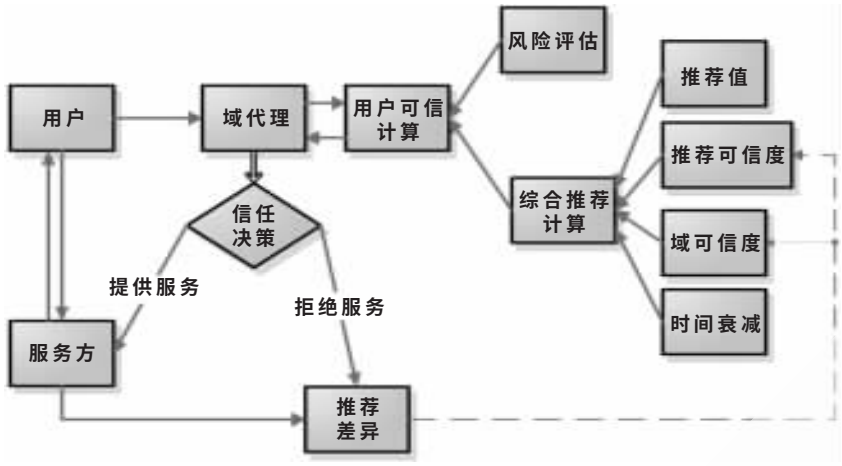

图 1 系统流程图

2 基于风险和推荐的用户信任计算方法

用户信任计算主要包括用户行为风险评估、综合推荐计算、用户可信度计算和反馈更新几个部分。

2.1 用户行为风险评估

用户行为风险评估采用了参考文献[6]的方法，即将日志中记录的用户行为通过资产识别、脆弱性识别和威胁识别评估其潜在的安全风险，并量化为风险值。

2.2 综合推荐计算

综合推荐计算就是把服务方对用户的推荐值乘以相应的权值进行综合计算的过程，每个权值由其推荐可信度、所属域的域可信度以及时间衰减共同决定。

2.2.1 推荐可信度

推荐可信度反映了域代理对域中服务方所提供的推荐的信任程度。针对联合欺骗和诋毁的行为，利用推荐可信度影响推荐值在综合推荐计算中的比重。当服务方的推荐可信度较低时，即使它提供虚假推荐，对综合推荐值的影响也很小。服务方 i 的推荐可信度计算如下：

$$C_i=\begin{cases} C_i^{t-1}+\alpha\times\dfrac{(1-C_i^{t-1})}{2}\times f_{in}, & f_{in}=-1 \\ C_i^{t-1}, & f_{in}=0 \\ C_i^{t-1}+\beta\times\dfrac{(1-C_i^{t-1})}{2}\times f_{in}, & f_{in}=1 \end{cases} \tag{1}$$

其中，α、$\beta(0<\alpha,\beta<1)$是可信调节因子，用于调节节点推荐可信度变化的快慢。C_i^{t-1} 为实体 i 近期推荐可信度，首次计算服务方 i 的推荐可信度时，令 $C_i^{t-1}=0.5$。f_{in} 是评价差异的映射函数。

2.2.2 域可信度

每个域代理维护一张域可信度表，用于记录该域对其他域的信任程度，由域中所有服务方的推荐情况决定其域可信度。域 j 的域可信度计算公式如下：

$$FT_j=\frac{u+1}{v+2} \tag{2}$$

$FT_j\in[0,1]$，u 为域中服务方提供真实推荐的总数，v 为域中服务方提供推荐的总数。

2.2.3 时间衰减函数

推荐值在信任评估中的重要性随时间衰减，即推荐值产生的时间越久远，它对综合推荐的影响就越小。采用式(3)描述时间的衰减特性：

$$S_{in}=\rho^{t-k} \tag{3}$$

其中，$0\leqslant\rho\leqslant1$，把一段时间分为若干个时间帧，使用正整数表示，数字越大表示时间越接近现在，式(3)中的 $k(1\leqslant k\leqslant t)$为产生推荐值的时间帧，$t$ 为当前时间帧。利用定义好的时间衰减函数 S_{in}，首次交易相对于当前的时间衰减为 $S_{in}=1$，可以认为没有衰减。

2.2.4 综合推荐

用户 n 的综合推荐是指将所有与用户 n 有过交互的服务方 i 对用户 n 的推荐值进行综合计算。每个服务方 i 提供推荐值所占的权重由其推荐可信度、域可信度和时间衰减函数共同决定。RT_n 为用户 n 的综合推荐：

$$RT_n=\sum\frac{e_{in}\times C_i\times FT_j\times S_{in}}{\sum C_i\times FT_j\times S_{in}} \tag{4}$$

2.3 用户可信度计算

用户可信度代表用户的可信程度，是进行信任决策的一个决定性的因素。用户可信度越高，用户越可靠安全。用户 n 的用户可信度 T_n 可表示为：

$$T_n=\begin{cases} T_n^{t-1}+a\times[RT_n+(\theta-R_n)] & \theta\geqslant R_n \\ T_n^{t-1}-b\times[RT_n+(R_n-\theta)] & \theta<R_n \end{cases} \tag{5}$$

T_n^{t-1} 是用户 n 的近期用户可信度，首次计算用户 n 的综合信任值时令 $T_n^{t-1}=6$，RT_n 是对用户 n 的综合推荐值，R_n 为用户 n 的风险值，θ 为风险阈值，即只有当用户行为的风险值小于阈值，并且用户的交互行为良好时，其综合信任值才能增加。a、b 为信任因子，a、$b\in[0,1]$，$a<b$，用于调节综合信任值变化的速度。用户可信度以快减慢增的规律变化，这样使得用户长期良好行为建立的信任值可能在几次不良交互行为中耗尽。

2.4 更新反馈

2.4.1 评价差异

交互结束或者拒绝服务后需要对相关数据进行更新操作。根据推荐值与综合推荐值的差异来对推荐可信度和域可信度进行更新。服务方 i 对用户 n 的推荐值与综合推荐值的推荐差异 $diff_{in}$ 定义为：

$$diff_{in}=|e_{in}-RT_n| \tag{6}$$

设服务方 i 对用户 n 可以容忍的最大推荐差异偏差为 ε，利用推荐差异 $diff_{in}$ 和服务方 i 所属域的域可信度 FT_j 构造一个映射函数 f_{in}：

$$f_{in}=\begin{cases}1, diff_{in}<\varepsilon \&\& FT_j \geqslant T_\theta \\ 0, diff_{in}<\varepsilon \&\& FT_j < T_\theta \\ -1, diff_{in}>\varepsilon\end{cases} \quad (7)$$

T_θ 是域可信度阈值，式(7)表明只有当推荐差异小于 ε，并且服务方所属域的域可信度大于阈值 T_θ 时才认为服务方 i 的推荐是真实的，令 $f_{in}=1$；当服务方所属域的域可信度大于阈值 T_θ 时，尽管推荐差异小于 ε，但是认为服务方 i 的推荐不确定是否真实，令 $f_{in}=0$；当推荐差异大于 ε，认定服务方 i 的推荐不真实，则令 $f_{in}=-1$。

2.4.2 推荐可信度更新

在上述推荐差异的基础上，各域服务器都采用式(1)对该域中服务方的推荐可信度进行更新。当 $f_{in}=-1$ 时通过降低推荐可信度的方式惩罚提供虚假推荐的服务方；$f_{in}=0$ 时由于不能确定服务方的推荐是否诚实，所以推荐可信度无法增加，保持原样。这样就要求域中的服务方都要进行诚实的推荐，使域可信度高于阈值，才能让域中提供诚实推荐的服务方的推荐可信度提高，从而在一定程度上遏制不诚实推荐的发生。

2.4.3 域可信度更新

域可信度的更新同样以推荐差异为基础，服务方所在域代理根据式(2)对其维护的域可信度表进行更新。$f_{in}=-1$ 时，v 加 1；$f_{in}=1$ 时，u 加 1，v 也加 1；$f_{in}=0$ 时，因为推荐差异在可以容忍的范围内，在此认为服务方 i 提供的推荐可信，所以 u 加 1，v 也加 1，域可信度就可以相应地提高。

3 仿真实验及结果分析

通过仿真实验考察本文的信任计算方法对交互成功的影响、对用户行为的动态适应能力和对服务方推荐的动态适应能力，分别使用成功交互率、用户可信度的变化情况，以及推荐可信度的变化情况来说明上述问题。本文采用 omnet++4.0 软件进行仿真，基于 C++实现。仿真参数如表 1 所示。

表 1 仿真参数

参数	数值	参数	数值
用户总数	24	信心因子 b	0.075
服务方总数	24	时间衰减参数 ρ	0.9
域代理总数	4	风险阈值 θ	6
服务器总数	1	可容忍最大差异偏差 ε	1
恶意行为节点比率	20.83%	域可信度阈值 T_θ	0.5
不诚实反馈节点比率	12.5%	可信调节因子 α	0.2
信心因子 a	0.025	可信调节因子 β	0.1

3.1 成功交互率

成功交互率是信任模型性能的一个重要体现。实验从两个方面评价用户的行为：是否滥用资源；操作是否符合要求。

从图 2 中可以看出，成功交互率随着时间的发展能够稳定在一个较大的数值上。这说明了基于风险和推荐的用户信任计算方法实现了预期目的，为信任决策提供了准确的依据，能够保障系统安全。

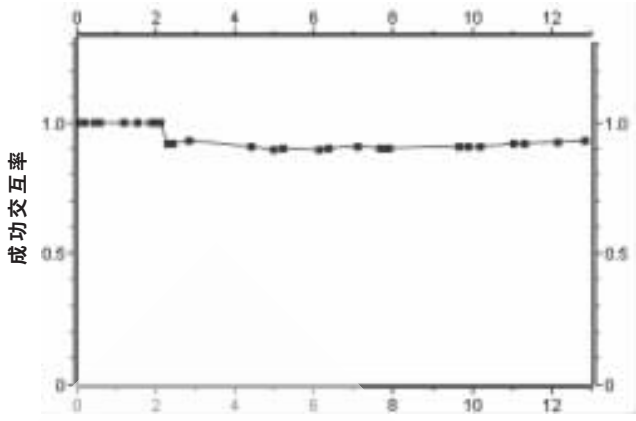

图 2 成功交互率随时间的变化

3.2 对用户行为的动态适应能力

恶意用户的行为分为静态和动态，动态的恶意行为又可以分为以下两种，用户首先与服务方建立良好信任关系，然后突然实施破坏行为；开始就实施破坏行为，然后改变策略想通过好的行为提高信任值。本实验对比好用户与提供第一种动态恶意行为用户的综合信任值的变化情况。

图 3 中上升曲线代表好用户的用户可信度变化，先上升后下降的曲线代表恶意用户的用户可信度变化曲线。图中曲线的变化趋势与用户的行为表现一致。同时由图可知，信任下降的速度远大于上升的速度，符合信任快减慢增的规律。

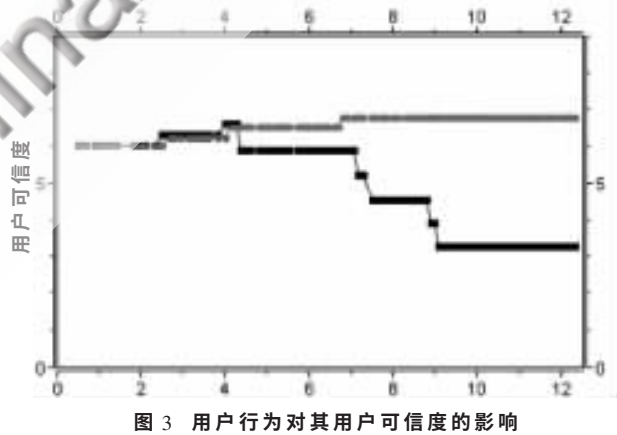

图 3 用户行为对其用户可信度的影响

3.3 对服务方推荐的动态适应能力

实验中服务方的不诚实推荐是动态变化的，即恶意服务方针对某些好用户给出较差的推荐值，对同伙用户则给出较好的推荐值，而对其他用户给出诚实的推荐值。

恶意服务方有时提供诚实推荐，有时提供不诚实推荐，故其推荐可信度上下波动，但由于推荐可信度的变化同样遵循慢增快减的原则，所以节点推荐可信度下降的速度明显快于上升的速度，经过多次恶意推荐后其推荐可信度降为 0。

本文提出了一种基于风险和推荐的用户信任计算方法，采用风险评估、时间衰减函数、推荐可信度和域可信度等共同计算用户的信任值，并通过推荐可信度和域可信度惩罚恶意推荐的服务方。仿真实验证明此计算方法具有较好的动态适应性，能够有效识别节点的虚假反馈和抵抗恶意用户的攻击。在后续的工作中，还需从反馈机制和调度算法方面进一步完善信任计算方法。

参考文献

[1] 张骞，张霞，刘积任，等. Peer-to-Peer 环境下多粒度 Trust 模型构造[J]. 软件学报，2006，17(1)：96-107.

[2] 田春岐. P2P 网络信任模型的研究[D]. 北京：北京邮电大学，2007.

[3] 刘莉平，葛志辉. Grid 环境下基于实体行为的信任评估模型[J]. 计算机应用研究，2008，25(7)：2020-2022.

[4] YU Yi Yu，TANG Jun Hua，HAO Li Ming，et al. A grid trust model based on MADM theory[J]. Journal of Computer Applications.2008，30(12):1-5.

[5] 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)：1302-1307.

[6] 张润莲，武小年，周胜源，等. 一种基于实体行为风险评估的信任模型[J]. 计算机学报，2009，32(4)：689-698.

(收稿日期：2010-10-20)

作者简介：

刘绮虹，女，1986 年生，硕士研究生，主要研究方向：网络信息安全。

介利军，男，1985 年生，硕士研究生，主要研究方向：信号与信息处理。