doi:10.3969/j.issn.1000-436X.2012.10.008

基于交互感知的动态自适应的信任评估模型

李峰[1,2]，申利民[1,3]，司亚利[1]，牛景春[1]

(1. 燕山大学 信息科学与工程学院，河北 秦皇岛 066004；2. 东北大学 秦皇岛分校 计算机与通信工程学院，河北 秦皇岛 066004；
3. 河北省计算机虚拟技术与系统集成重点实验室，河北 秦皇岛 066004)

摘 要：构建了一种基于交互感知的动态自适应信任评估模型，将历史交互窗口和可信推荐数引入到了总体信任评估中，克服了传统模型对交互证据感知能力不足的问题。提出了基于满意度迭代的直接信任积累方法，并采用实体稳定度实现了激励和惩罚 2 种迭代策略，有效抑制了恶意伪装实体的作弊行为。给出了一种基于直接和间接相结合的综合推荐信任聚合方法，通过引入实体熟悉度和评分相似度解决了传统模型推荐准确度低和不可靠的问题。实验结果表明，与已有模型相比，该模型有效地提高了信任评估的准确性，并具有更强的抵御串谋实体协同作弊的能力。

关键词：网络计算；信任；信任评估；交互感知；交互满意度

中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2012)10-0060-11

Dynamic adaptive trust evaluation model based on interaction-aware

LI Feng[1,2], SHEN Li-min[1,3], SI Ya-li[1], NIU Jing-chun[1]

(1. Information Science and Engineering College, Yanshan University, Qinhuangdao 066004, China;
2. Computer and Communication Engineering College, Northeastern University at Qinhuangdao, Qinhuangdao 066004, China;
3. The Key Laboratory for Computer Virtual Technology and System Integration of Hebei Province, Qinhuangdao 066004, China)

Abstract: A dynamic adaptive trust evaluation model was established based on interaction-aware. The historical interaction window and trustworthy recommendation number was introduced in overall trust evaluation method, which overcomes the shortage of traditional models that lack the capacity to interaction-aware. The direct trust accumulation method based on interaction satisfaction degree iterative calculation was proposed, which achieved the incentive and penalty iterative strategy based on entity stability factor, and effectively inhibits malicious entities with camouflage. A synthetical recommendation trust aggregating method based on combination of direct and indirect recommendation trust was given, which solved the accuracy low and unreliable problems of traditional recommendation methods by introducing entity familiarity factor and scoring similarity factor. Simulation results show that, compared to the existing trust model, the model can effectively improve the accuracy of trust evaluation, and can provide a better capacity of resisting collusive entities.

Key words: internet computing; trust; trust evaluation; interaction-aware; interaction satisfaction degree

收稿日期：2011-09-22；**修回日期**：2012-08-29

基金项目：国家自然科学基金资助项目（61272125）；河北省自然科学基金资助项目（F2011203234）；河北高等学校科学技术研究重点基金资助项目（ZH2011115）

Foundation Items: The National Natural Science Foundation of China (61272125)； The Natural Science Foundation of Hebei Province (F2011203234); Key Project of Hebei Higher Education of China (ZH2011115)

1　引言

新型互联网计算模式使得软件系统凸显出服务化、协同化和泛在化的趋势，表现为由多个自治域构成的大规模动态分布的协作模式，实体具有强自治性可以跨域访问多个自治域中的实体[1]。在这种开放、动态和不确定的大规模环境下，首先需要突破的问题就是如何在来源于不同自治域、可能陌生的实体之间促成协作活动，并且保证协作的安全性和高效性，以及如何解决实体行为不可信导致的系统可用性降低和安全风险增长问题[2]。而系统无安全控制中心的特性，导致难以采用传统的基于PKI(public key infrastructure) 和 CA(certificate authority)的静态信任机制对多个自治域进行集中授权和直接信任关系定义，为此，动态信任管理成为了新一代互联网技术研究的热点问题。动态信任管理是一种增加了行为可信的网络安全新技术，强化对网络实体行为状态的动态收集、评估和推理，为实施跨域协作和可信互联网计算系统的设计提供策略基础[3]。研究适用于新型网络计算环境的信任关系建模和评估方法，则是动态信任管理理论必须解决的核心问题。

目前，大多数信任建模和评估方法都借鉴人际社会中的信任关系形成和传播方法建立的，其建模方法主要基于主观逻辑、模糊数学理论、概率统计和证据理论[4]。实践表明，这些模型极大增强了互联网应用系统的安全性和可协作性，尤其对于网络中恶意实体和行为不可信实体的活动具有明显的抑制作用，但模型在交互感知、动态适应性和顽健性方面仍有待深入研究，主要呈现的问题如下：

1) 在信任关系建模和评估时对交互过程中证据变化因素考虑不全，致使模型动态感知证据变化的能力不足，评估策略无法根据信任证据的变化动态自适应地调整，从而影响了评估结果的合理性和科学性。

2) 大部模型分采用简单的评估策略，只针对实体提供服务的成功与否进行评价，缺乏对服务质量的多维度评估机制，致使 n 次收敛后所有成功提供服务的实体信任度一致，导致实体信任度计算的准确性降低。

3) 现有模型只能对简单的攻击和欺骗行为进行识别和防护，而对间谍攻击、共谋团体攻击和策略性攻击等复杂隐蔽的作弊行为缺乏有效的识别和防护机制，导致模型的安全性和顽健性较差。

针对上述不足，本文提出了一种适用于新型网络计算环境的动态自适应的信任评估模型，旨在提高模型的交互感知能力和对恶意实体的抑制能力。模型将实体的历史交互窗口、可信推荐数、实体稳定度和推荐实体熟悉度等反映信任可靠的因素，应用到了总体信任度、直接信任度和综合推荐信任度的评估中，增强交互感知和随着证据变化动态自适应的调整评估策略的能力，提高实体信任度评估的准确性和合理性。

2　相关工作

以信任关系的评估方式为依据，现有模型可以划分为全局信任模型和局部信任模型。全局信任模型采用信誉的方式来评估网络实体的信任度，典型代表是文献[5]提出的 EigenRep 信誉模型、文献[6]提出的基于相似度加权推荐的 SWRTrust 全局信任模型、文献[7]提出的 PETrust 惩罚激励机制以及文献[8]提出的具有激励效果的分布式 P2P 信任管理模型 IMTM，其特征表现为网络中的每个实体都具有唯一的全局信任值，即实体在网络中的信誉值，通过指定的信任管理节点收集其邻居节点的反馈信息迭代计算得出。优点是综合了整个网络对实体的信任评价，评价信息比较全面可靠，对一些通过互相吹捧来骗取信任值的恶意实体具有明显的抑制作用。缺点是信任的主观性和动态性体现不足，不能区分直接信任和推荐信任，没有考虑时间因素和环境因素对信任变化的影响，此外模型的安全性和顽健性较差，不能识别和抵御间谍和策略性攻击行为。

局部信任模型采用共享局部评价信息的方式来评估网络实体的信任度，特征表现为网络中的每个实体对其邻居节点的历史评价信息作为直接信任度保存在本地，对其邻居实体的总体信任度计算，通过在网络中查询其他实体的推荐信任度，然后与自己的直接信任度融合得出。代表模型为文献[9]提出的面向普适计算的 FTM 模型，它采用多级推荐协议和路径衰减方法来计算推荐信任，但在评估实体总体信任度时，采用加权平均法使得评估策略缺少灵活性，而且没有考虑信任随时间动态衰减的影响以及协同作弊的问题。文献[10]提出了上下文感知的 CAT 模型，该模型将信任规则和上下文概念引入到了直接信任评估中，提高了直接信任计算

的准确度，在推荐信任方面通过推荐精确度过滤不可靠和恶意推荐，保证了推荐的可靠性和准确性，但仍存在信任关系不能随时间因素和环境因素动态变化的问题。文献[11]提出了一种基于声誉的多维度信任算法，给出了具体的直接信任和推荐信任计算方法，但在模型的安全性和顽健性方面考虑较少。文献[12]提出了一种基于多影响因素的信任传播算法，通过将节点的交互能力和诚实能力引入到推荐信任的评估中，有效增强了推荐信任计算的合理性。文献[13]将认知行为应用到了信任关系的建模过程中，构建了自适应的基于历史证据窗口的总体信任决策方法，通过 DTT 信任树实现全局反馈信息的搜索与聚合，降低了网络带宽开销，提高了模型的可扩展性。

在安全性和顽健性研究方面，文献[14]依据恶意节点采用的攻击策略和攻击的目的，总结出已存在的恶意攻击行为的类别，对每类攻击行为所表现出的特征进行了分析，并给出了简单的应对方法。文献[15]提出了一种防止欺骗行为的信任度计算方法，通过引入时间衰减因子明显抑制了智能伪装的作弊行为，通过反馈管理机制有效阻止了间谍行为和恶意反馈行为。文献[16]针对共谋节点具有相似和一致的行为，提出了基于行为相似度的共谋团体识别模型，通过分析节点之间的行为相似度来识别共谋团体。

3 信任评估模型及其存储机制

3.1 模型的总体框架

定义 1 设 e_1,e_2,L,e_n 表示组成新型网络应用系统的 N 个自治实体或进程，称集合 $E=\{e_1,e_2,\mathrm{L},e_n\}$ 为系统实体域。设服务请求域为 $SR\subseteq E$，服务提供域为 $SP\subseteq E$，使得 $\forall e_i\in SR$，$\exists e_j\in SP$，满足操作 $\tau:e_i\xrightarrow{c_w}e_j$，操作 τ 为实体在 c_w 条件下的协作活动，$c_w\in(c_1,c_w,\mathrm{L},c_m)$ 表示实体协作的上下文条件。

定义 2 设实体信任度评价有 8 个等级 Ma、d_{H}、d_{M}、d_{L}、n、b_{L}、b_{M}、b_{H}，分别表示为恶意、非常不信任、不信任、稍微不信任、不确定、稍微信任、信任和非常信任，称 $L=\{Ma,d_{\mathrm{H}},d_{\mathrm{M}},d_{\mathrm{L}},n,b_{\mathrm{L}},b_M,b_H\}$ 为信任等级空间。为了量化计算，用−1 表示恶意等级，其他等级区间定义为[0,1]，如图 1 所示。

实体 e_i 对 e_j 的总体信任度由直接信任度和推荐信任度综合得出，如何合理分配两者的权重是关系总体信任度计算准确性的关键。权重分配应该与 2 种因素有关：1) 实体之间的交互次数，交互次数越多说明直接信任证据越充分，直接信任度的权重应该越大；2) 网络中可信推荐实体的个数，推荐实体越多说明网络中的其他实体对 e_j 越熟悉，推荐信任度的权重应越大。因此，总体信任度定义如下。

定义 3 设 $T(e_i,e_j,c_w,t)$ 表示实体 e_i 对实体 e_j 在时间戳 t 时刻和上下文 c_w 条件下的总体信任度，令

$$T(e_i,e_j,c_w,t)=\begin{cases}T_D(e_i,e_j,t),|R|=0\mathrm{I}\ h_{ij}(c_w)=0\\ R(e_i,e_j,c_w,t),h_{ij}(c_w)=0\\ T_D(e_i,e_j,c_w,t),|R|=0\\ \dfrac{h_{ij}(c_w)}{h_{ij}(c_w)+|R|}T_D(e_i,e_j,c_w,t)+\dfrac{|R|}{h_{ij}(c_w)+|R|}R(e_i,e_j,c_w,t),\text{其他}\end{cases}\tag{1}$$

式(1)中 $h_{ij}(c_w)$ 为实体 e_i 与实体 e_j 在上下文 c_w 条件下的历史交互次数，称 $h_{ij}(c_w)$ 为实体 e_i 与 e_j 的历史交互窗口。$|R|$ 为推荐实体的个数。在上下文 c_w 条件下既没有交互记录又不存在推荐实体时，即 $|R|=0\mathrm{I}\ h_{ij}(c_w)=0$，应考虑在其他上下文条件下对实体 e_j 的直接信任度 $T_D(e_i,e_j,t)$。在综合计算总体信任度时，若 $h_{ij}(c_w)<|R|$，说明直接证据不如推荐证据充分，推荐信任度权重较大；若 $h_{ij}(c_w)>|R|$，说明直接证据比较充分，直接信任度权重较大些。该方法充分考虑了权重分配的影响因素，使得权重分配更加合理和科学，并且权重随着交互过程中证据的不断积累能够动态自适应的调整。

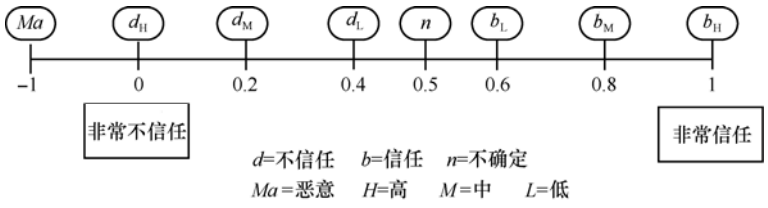


图 1 信任等级

3.2　基于满意度迭代的直接信任度计算方法

定义 4　设 $\forall e_i \in E$ 有 p 项度量指标综合评估其协作实体的交互满意度，其集合表示为 $I=\{I_1, I_2, \mathrm{L}\ , I_p\}$，则称 $f: I \to L$ 为满意度等级度测函数。

定义 5　设 $\eta(e_i, e_j, c_w, t)$ 表示实体 e_i 对实体 e_j 在时间戳 t 时刻和上下文 c_w 条件下的交互满意度，令

$$\eta(e_i,e_j,c_w,t)=\begin{cases}-1, & \exists I_u \in I, f(I_u)=Ma\\ \sum_{u=1}^{p} w(I_u)\times f(I_u), & \text{其他}\end{cases} \tag{2}$$

式(2)中如果任意一项指标 $I_u \in I$，其评估结果是恶意等级，则该次交互满意度为–1。否则，依据多指标决策理论对各项指标评价结果与该指标的权重因子乘积求和，综合计算在时间戳 t 时刻实体交互的满意度值。$w(I_u)$ 是度量指标 $I_u \in I$ 的权重因子，表示度量指标的重要程度，且满足：$\forall w(I_u) \in (0,1)$, $\sum_{u=1}^{p} w(I_u)=1$。

定义 6　设 $T_D(e_i, e_j, c_w, t)$ 表示实体 e_i 对实体 e_j 在上下文 c_w 条件下时间戳 t 时刻的直接信任度，即对实体 e_j 历史交互满意度的迭代计算，令

$$T_D(e_i,e_j,c_w,t)=\begin{cases}0, \eta(e_i,e_j,c_w,t)=-1\\ \eta(e_i,e_j,c_w,t), h_{ij}(c_w)=0\\ T_D(e_i,e_j,c_w,t_o)\zeta(t,t_o,c_w), t-t_o \geqslant T\ \mathrm{I}\ T_D(e_i,e_j,c_w,t_o)\geqslant 0.5\\ \beta(h_{ij}(c_w))T_D(e_i,e_j,c_w,t_o)+(1-\beta(h_{ij}(c_w)))\eta(e_i,e_j,c_w,t), \eta(e_i,e_j,c_w,t)\geqslant 0.5\\ (1-\beta(h_{ij}(c_w)))T_D(e_i,e_j,c_w,t_o)+\beta(h_{ij}(c_w))\eta(e_i,e_j,c_w,t), \eta(e_i,e_j,c_w,t<0.5\end{cases} \tag{3}$$

式(3)中 t, t_o 分别表示为当前时间戳和最后一次信任建立或更新的时间戳，其单位可以根据实体交互的频繁度定义。函数 $\beta(h_{ij}(c_w)) \in [0,1]$，称为实体 e_j 对于实体 e_i 在网络环境中的稳定度，稳定度反映了实体持续提供服务的能力和稳定运行的程度，与该实体交互的次数越多说明实体的稳定度越高，因此函数 $\beta(x)$ 应具有如下 2 个性质。

性质 1　$\beta(x_1)<\beta(x_x)$，当 $1 \leqslant x_1 < x_2$。

性质 2　$\beta(1)=1/2$，且 $\lim_{x\to\infty}\beta(x)=1$。

依据上述 2 个性质，函数 $\beta(x)$ 构造如下：

$$\beta(x)=1-\frac{1}{\sqrt[\delta]{\mathrm{e}^{x-1}}+1},\quad x\geqslant 1 \tag{4}$$

其中，调节因子 $\delta \geqslant 2$ 的任意常数，用于控制稳定度 $\beta(h_{ij}(c_w))$ 趋于 1 的速度，δ 的取值越大，$\beta(h_{ij}(c_w))$ 趋于 1 的速度越慢。通过性质 1 和性质 2 可知，$\beta(x)$ 是单调递增函数，当 $x=1$ 时，其值最小为 $1/2$，当 $x\to\infty$ 时，其值最大趋于 1，所以取值范围为 $1/2 \leqslant \beta(x)<1$，则 $0<1-\beta(x)\leqslant 1/2$，得出 $\beta(h_{ij}(c_w)) \geqslant 1-(h_{ij}(c_w))$。

式(3)采用了 2 种不同的直接信任迭代更新策略，当交互满意度 $\eta(e_i,e_j,c_w,t)\geqslant 0.5$ 时，历史交互满意度在迭代过程中占较大比重，历史交互窗口 $h_{ij}(c_w)$ 越大，直接信任积累的难度越高，说明了实体只有长期稳定地提供真实服务才能获得高信任值，从而激励实体长期提供真实服务；当交互满意度 $\eta(e_i,e_j,c_w,t)<0.5$ 时，交互满意度在迭代过程中的权重较大，增加了信任值下降的速度，说明了实体如果提供不真实服务将导致信任值的急剧下降，对该实体进行严厉的惩罚。因此，该方法能够有效遏制伪装恶意实体或策略性恶意实体的攻击。

随着时间的推移历史信任度对于当前信任评估的参考价值越来越弱，函数 $\zeta(t,t_o,c_w)\in(0,1)$ 作为时间衰减因子，如式(5)所示，其中实体的稳定度决定衰减的速度，实体的稳定度越高信任值衰减速度慢，反之衰减速度越快，时间衰减因子充分体现了信任随时间变化而衰减的特性，而且与实体的稳定度具有相关性。

$$\zeta(t,t_o,c_w)=2^{-(1-\beta(h_{ij}(c_w)))(t-t_o)} \tag{5}$$

3.3　综合推荐信任度的聚合方法

定义 7　设实体 e_j 的推荐实体集合为 $R=\{r_1, r_2, \mathrm{L}\ , r_z\}$，其中，直接推荐实体集合为 $R_d=\{r_{d1}, r_{d2}, \mathrm{L}\ , r_{dx}\}$，间接推荐实体集合为 $R_{id}=\{r_{id1}, r_{id2}, \mathrm{L}\ , r_{idy}\}$，满足关系式 $x+y=z$ 并且 $R_d \subseteq R, R_{id} \subseteq R$，则实体 e_i 从集合 R 中获取的有关实体 e_j 的综合推荐信任度定义为 $R(e_i,e_j,c_w,t)$，令

$$R(e_i,e_j,c_w,t)=\begin{cases}\phi, |R|=0\\ R_d(e_i,e_j,c_w,t), |R_{id}|=0\\ \beta(H_d(c_w))R_d(e_i,e_j,c_w,t)+(1-\beta(H_d(c_w)))\\ R_{id}(e_i,e_j,c_w,t), |R_{id}|>0\end{cases} \tag{6}$$

式中，$R_d(e_i,e_j,c_w,t)$ 表示实体 e_i 从直接推荐实体中获取的有关实体 e_j 的信任度，$R_{id}(e_i,e_j,c_w,t)$ 表示实体 e_i 从间接推荐实体中获取的有关实体 e_j 的信任度。在综合计算推荐信任度时，重点考虑直接推荐实体推荐的信任度，为此采用式(4)提供的函数 $\beta(H_d(c_w))$ 作为直接推荐和间接推荐合成的权重因子，称 $\beta(H_d(c_w))$ 为实体 e_i 对直接推荐实体的熟悉度。$H_d(c_w)$ 为实体 e_i 与直接推荐集合 R_d 中的实体在上下文 c_w 条件下的历史交互总数目，称 $H_d(c_w)$ 为实体 e_i 与集合 R_d 总的历史交互窗口，显然，$H_d(c_w)$ 值越大实体 e_i 与集合 R_d 中的实体交互经验就越多，也就越熟悉，则熟悉度 $\beta(H_d(c_w))$ 的值也越大，而且 $\beta(H_d(c_w))\geqslant 1-\beta(H_d(c_w))$，说明在获取推荐信任时总是优先考虑直接推荐实体的推荐信息。$H_d(c_w)$ 的计算公式为

$$H_d(c_w)=\sum_{x=1}^{|R_d|}h_{ix}(c_w) \tag{7}$$

其中，$h_{ix}(c_w)$ 表示实体 e_i 与实体 $r_{dx}\in R_d$ 的历史交互窗口。

$R_d\left(e_i,e_j,c_w,t\right)$ 采用每个实体的历史交互窗口占总的历史交互窗口的比重为权重影响因子，说明越熟悉的实体推荐可信度越高，计算公式为

$$R_d(e_i,e_j,c_w,t)=\sum_{x=1}^{|R_d|}h_{ix}(c_w)\times T_D(r_{dx},e_j,c_w,t)/H_d(c_w) \tag{8}$$

$R_{id}(e_i,e_j,c_w,t)$ 采用路径衰减因子作为权重，因为不同的间接推荐实体被搜索所经过的路径长度不同，不能采用简单的加权求和，而路径衰减因子较好地解决了实体的路径问题，在网络中搜集到实体的路径越长，则实体的路径衰减因子越小，说明该实体的推荐可信度越低，计算公式为

$$R_{id}(e_i,e_j,c_w,t)=\sum_{y=1}^{|R_{id}|}L(l_{r_{idy}})\times T_D\left(r_{idy},e_j,c_w,t\right)\Big/\sum_{y=1}^{|R_{id}|}L(l_{r_{idy}}) \tag{9}$$

式(9)中 $L(l_{r_{idy}})$ 为实体 $r_{idl}\in R_{id}$ 的路径衰减因子，$l_{r_{idy}}$ 为实体 r_{idl} 的路径长度，其计算采用式(10)的衰减函数，参数 λ 是模型自适应设定的最长路径搜索长度，参数 $\psi\in[0,1]$ 是推荐信任路径衰减快慢的调节因子，用于控制 $L(x)$ 趋于 0 的速度，参数 ψ 的值越大 $L(x)$ 趋于 0 的速度越快。

$$L(x)=1-\frac{(x-1)\psi}{\lambda},\quad x\geqslant 2 \tag{10}$$

在实际网络中进行推荐实体搜索时，路径长度 λ 越大搜索到的推荐实体数量越多，但搜索速度越慢、网络带宽占用率也越高，导致模型运算效率下降。所以，λ 的取值应该与直接信任证据的多少成反比，即在直接信任证据较少时，无法依靠直接信任证据确定实体的可信程度，此时推荐路径的长度稍大些；而在直接信任证据比较充分时，采用直接信任证据基本可以确定实体的可信程度，此时推荐路径的长度应较小，从而可以提高模型的运算效率。基于这一原则，利用式(11)自适应地设定 λ 的大小。

$$\lambda=\begin{cases}\lfloor\log_p n\rfloor+1, & h_{ij}(c_w)=0\\ \left\lceil\left(\lfloor\log_p n\rfloor+1\right)\left(1-\dfrac{h_{ij}(c_w)}{H}\right)\right\rceil, & 0<h_{ij}(c_w)<H\\ 1, & h_{ij}(c_w)\geqslant H\end{cases} \tag{11}$$

式中，p 为实体 e_i 的邻居实体的数量，n 为网络的规模数，H 为系统设定的参与路径选择最大历史交互窗口。当 $h_{ij}(c_w)=0$ 时，说明实体 e_i 对实体 e_j 在上下文 c_w 条件下没有直接信任证据，此时需要最大的查询深度，以尽可能地查找到所有推荐实体，因为在推荐实体搜索时以树型结构递归地向其邻居实体发送查询请求，所以查找的最大深度为 $\lfloor\log_p n\rfloor+1$。当 $h_{ij}(c_w)\geqslant H$ 时，说明实体之间的直接信任证据比较充分，此时设定查找深度为 1，即只查找直接推荐实体。当 $0<h_{ij}(c_w)<H$ 时，λ 的取值随着历史交互窗口 $h_{ij}(c_w)$ 的增大逐渐减小，满足了推荐搜索路径随直接交互经验多少动态自适应调整的特性。

3.4 信任数据的分布存储机制

为了提高模型的存储和查询效率，确保信任信息不会因为个别实体的失效或退出而受到损失，本文在充分考虑了网络消息代价和负载平衡的基础上，设计了具有信息冗余能力的分布式树型存储机制（DST, distributed storage tree），在该方案中，网络中的每个实体采用 4 层的树型结构存储和维护其邻居实体的信任信息，包括每一个上下文条件下的直接信任度以及发生的时间戳和交互记录等数据，其结构如图 2 所示。其中，根节点 e_i 是存储信任信息的实体，子节点 $e_{i1},e_{i2},e_{i3},\mathrm{L}\ ,e_{ip}$ 是与实体 e_i 有过直接交互的实体，称为 e_i 的邻居实体。任意节点 $e_{ij},1\leqslant j\leqslant p$ 最多有 m 个子节点 $c_1,c_2,\mathrm{L}\ ,c_m$，为实

体交互的上下文条件，每个上下文节点有 3 个叶子节点：T_D 为直接信任度、t_o 为最近交互的时间戳、h 为交互记录数。

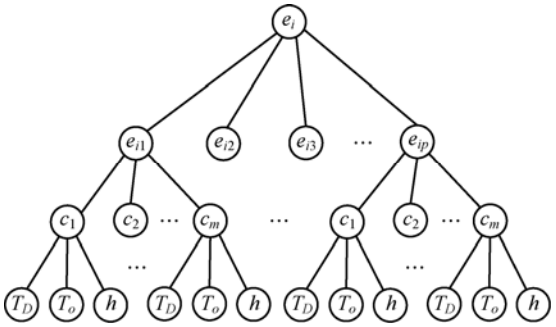


图 2　信任信息的树型存储结构

DST 机制采用网络实体存储其邻居实体信任信息的方法，当需要计算某实体信任度时，首先在本地数据库中查找该实体的直接信任度，然后在信任网络中搜索其他实体对该实体的推荐信任度。该存储机制由于对某实体信任度的评估都分散存储在网络中的不同实体中，所以即使有实体退出网络仍然可以查找该实体的推荐信任度，所以该机制具有较强的信息冗余能力，增强了模型的稳定性和顽健性。在网络带宽开销方面，由于在计算某个实体总体信任度时，从本地获取该实体的直接信任度，相对于已有模型从网络中其他实体获取直接信任度的方法，DST 机制大大减小了网络的带宽开销。在安全性方面，对于虚假和恶意推荐信息可以通过实体评分相似度来剔除，而本地存储的信任信息很难被恶意篡改，从而保证了信任信息的安全性。

3.5　信任评估的相关算法及分析

在操作 τ 执行前首先度测 e_j 在上下文 c_w 条件下的总体信任度，依据信任度决定是否与其协作，下面给出模型求解实体总体信任度的算法。

算法 1　总体信任度求解算法

OverallTrustDegree( ) //实体 e_i 计算实体 e_j 在上下文 c_w 条件下的总体信任度

begin

//首先计算实体 e_j 在上下文 c_w 条件下的直接信任度

实体 e_i 从其维护的信任树中查找 e_j 是否存在;

if(没有查找到实体 e_j)　　//实体 e_i 与 e_j 以前没有过交互记录

$T_D(e_i,e_j,t)=\phi$; }　　//实体 e_i 对 e_j 的信任记录为空

else

从子树 e_j 中查找 c_w 是否存在;

If (存在 c_w)

则获取 T_D、t_o 和 h 的值利用式(3)和式(5)计算 $T_D(e_i,e_j,c_w,t)$ 的值;

else

$h_{ij}(c_w)=0$;　//实体 e_i 与 e_j 在上下文 c_w 下的历史交互窗口为 0

查找其他子节点 c_x，获取 T_D、t_o 和 h 的值利用式(3)和式(5)计算 $T_D(e_i,e_j,c_x,t)$;

end if

end if

//查找实体 e_j 的推荐实体

for(所有 $e_{ix}\in NeighborSet(e_i)$ 并且 $e_{ix}\neq e_j$)　//集合 $NeighborSet(e_i)$ 表示实体 e_i 的所有邻居实体，即树中 e_i 的所有孩子节点的集合

if(节点 e_{ix} 存在孩子节点 c_w)　　//说明实体 e_{ix} 在上下文 c_w 下与实体 e_j 有过交互记录

$R_d=R_d+e_{ix}$;　　//形成直接推荐实体集

QueryIREntity(e_{ix} , e_j , c_w);　//根据算法 2 查找间接推荐实体集 R_{id}

end if

end for

//计算推荐信任度

基于 R_d 利用式(8)计算 e_j 的直接推荐信任度 $R_d(e_i,e_j,c_w,t)$;

基于 R_{id} 利用式(9)和式(10)计算 e_j 的间接推荐信任度 $R_{id}(e_i,e_j,c_w,t)$;

利用式(6)计算 e_j 的综合推荐信任度 $R(e_i,e_j,c_w,t)$;

//计算总体信任度

利用式(1)计算实体 e_i 对实体 e_j 的在上下文 c_w 条件下的总体信任度 $T(e_i,e_j,c_i,t)$;

return $T(e_i,e_j,c_i,t)$ 的值;

end

算法 2　间接推荐实体递归搜索算法

QueryIREntity(e_y , e_j , c_w)　//搜索与实体 e_j 交互过的实体

begin

input: e_y 查询实体; e_j 目标实体;

c_w 查询的上下文条件;

$\lambda \Leftarrow$ 利用式(11)计算

if(path(e_y)> $\lambda - 1$)

return 结束; // path (e_y)表示搜索到实体 e_y 的路径长度

end if

for(所有 $e_k \in NeighborSet(e_y)$ 并且 $e_k \neq e_j$) // 依次搜索 e_y 的所有邻居实体

if(实体 e_k 未搜索) // 对没有遍历过的实体进行搜索

对实体 e_k 进行搜索标记;

实体 e_k 在其信任树中对孩子节点进行遍历，查找节点 e_j 是否存在;

if(存在 e_j 节点)

$R_{id} = R_{id} + e_k$;

path(e_k); // 记录搜索到实体 e_k 的路径长度

end if

QueryIREntity(e_k , e_j , c_w);

end if

end for

return R_{id} ; //返回查找到的实体 e_j 的间接推荐实体集

end

4 仿真实验及性能分析

采用芝加哥大学的 Repast(recursive porous agent simulation toolkit)软件包搭建实现了一个服务共享的网络模拟环境，对本文模型及相关算法进行分析，为了体现本文模型的优势，在搭建的环境中又对文献[9]提出的 FTM 模型和文献[10]提出的 CAT 模型进行了模拟。

4.1 实体类型的定义

在网络中有 2 类实体：正常实体和恶意实体。正常实体总能提供真实服务，并为对方提供公正的服务评价。恶意实体总提供不真实服务，并为正常实体提供虚假服务评价，依据恶意实体行为将其分为以下 4 种类型。

1) IM(individual malicious)类，是最简单的一类恶意实体，只提供不真实服务和虚假评价。

2) CM(camouflage malicious)类，此类恶意实体按某种策略提供真实服务，而当信任度高于可信门限值时就会提供不真实服务。

3) MC(malicious collectives)类，是一类共谋的协同作弊实体，对正常实体提供不公正服务评价，对同伙却极力夸大使其具有很高的信任度。

4) MS(malicious spy)类，是一类间谍实体向外提供真实服务，但作为推荐者时专门提供不诚实推荐，夸大恶意实体诋毁正常实体。

为了充分体现本文模型在抵御“狡猾”恶意实体方面的优势，在模拟实验中只对 CM 类、MC 类和 MS 类 3 种典型的恶意实体进行仿真来评估模型的性能。

4.2 实验环境设置及性能指标

实验环境设置为：实体规模为 2 000，总服务种类为 10 000，其中，真实服务种类为 8 000，每个实体提供 10 种服务，同时请求 10 种服务(即请求上下文)。正常实体提供和请求的服务在创建时从真实服务集合中随机分配，其中提供和请求的服务种类不同；不真实服务种类为 2 000，包括虚假服务和恶意服务，每个恶意实体在创建时从 2 000 种不真实服务中随机分配提供的服务，而其谎称提供的服务从 8 000 个可信服务种类中随机分配；模拟交互次数为 1 200，即仿真模型每次运行的最大时间片值，模拟环境的参数设置见表 1。

表 1 仿真实验参数说明

参数	缺省值	描述
N	2 000	实体规模
TS	8 000	真实服务种类数
FS	2 000	不真实服务种类数
S	10	实体提供的服务数
C	10	实体请求的服务数
t	1 200	实体间的交互次数

信任模型的主要目的是为跨域协作的实体建立信任关系，检测和抵御各种恶意网络实体的攻击，为动态演化的实体提供可靠、安全的协作环境。因此，从顽健性和准确性方面来评估模型的性能。

顽健性是指模型抵御各类恶意实体的能力，一个健壮的模型应该具有准确识别恶意实体以及遏制恶意欺骗行为的能力。评估一个模型顽健性的性能指标是恶意实体的服务成功率（MSR），恶意实体的服务成功率越高说明模型的顽健性越差，反之

恶意实体的服务成功率越低模型的顽健性越强。

定义 8　恶意实体的服务成功率定义为某时刻被选择作为服务提供者的恶意实体个数占响应服务请求者的恶意实体个数的比率，假设在时间片 t 有 $R(t)$ 个响应服务请求的恶意实体，其中有 $S(t)$ 个恶意实体被选择为提供服务，则 MSR 为

$$MSR(t)=S(t)/R(t) \tag{12}$$

其中，如果有多个恶意实体响应了同一个服务请求，则把所有恶意实体看作一个恶意响应实体。因为这是多个恶意实体攻击同一实体，如果有一个恶意实体成功，则本次恶意实体攻击成功。

准确性是指网络中实体信任值度量的准确程度，本文采用实体的服务请求成功率（SR）作为衡量信任模型准确性的重要性能指标，实体的服务请求成功率越高说明实体信任度越准确，反之准确度越低。

定义 9　实体的服务请求成功率定义为网络中所有实体成功使用服务的次数占所有实体服务请求总数的比率，设任意实体 $e_i \in E$ 请求的服务数为 N_i，成功使用的服务数为 S_i，仿真结束后统计每个实体的 N_i 和 S_i，则整个网络的实体服务请求成功率为

$$SR=\sum_{e_i\in E} S_i \Big/ \sum_{e_i\in E} N_i \tag{13}$$

4.3　仿真结果及其讨论

实验 1　遏制 CM 类恶意实体仿真及其讨论

图 3(a)~图 3(c)是不同规模 CM 类恶意实体环境下的 MSR 比较，实验设定 CM 类实体提供真实服务和虚假服务的比例以 4:6，CM 类恶意实体分别为 10%、30%和 50%。从图 3(a)~图 3(c)的实验结果中可以看出，在网络运行初期，3 种模型的恶意服务攻击成功率呈现较大的变化，这是因为网络运行初期 CM 类实体需要提供好的服务来积累信任值，当积累到一定程度后开始提供恶意服务，所以在网络运行初期恶意服务攻击的成功率呈上趋势。随着 CM 类实体提供恶意服务的增多逐渐进入了模型的惩罚期，恶意服务攻击的成功率逐步下降，随着网络的不断运行恶意服务攻击的成功率逐渐趋于稳定。图 3(a)~图 3(c)表明，本文模型在抑制 CM 类恶意实体方面，明显优于其他 2 种模型，恶意服务攻击的成功率下降速度远远大于另外 2 种模型，说明本文模型对直接信任度积累的激励和惩罚机制以及对恶意实体的严厉惩罚措施在抑制 CM 类实体方面效果更加明显。

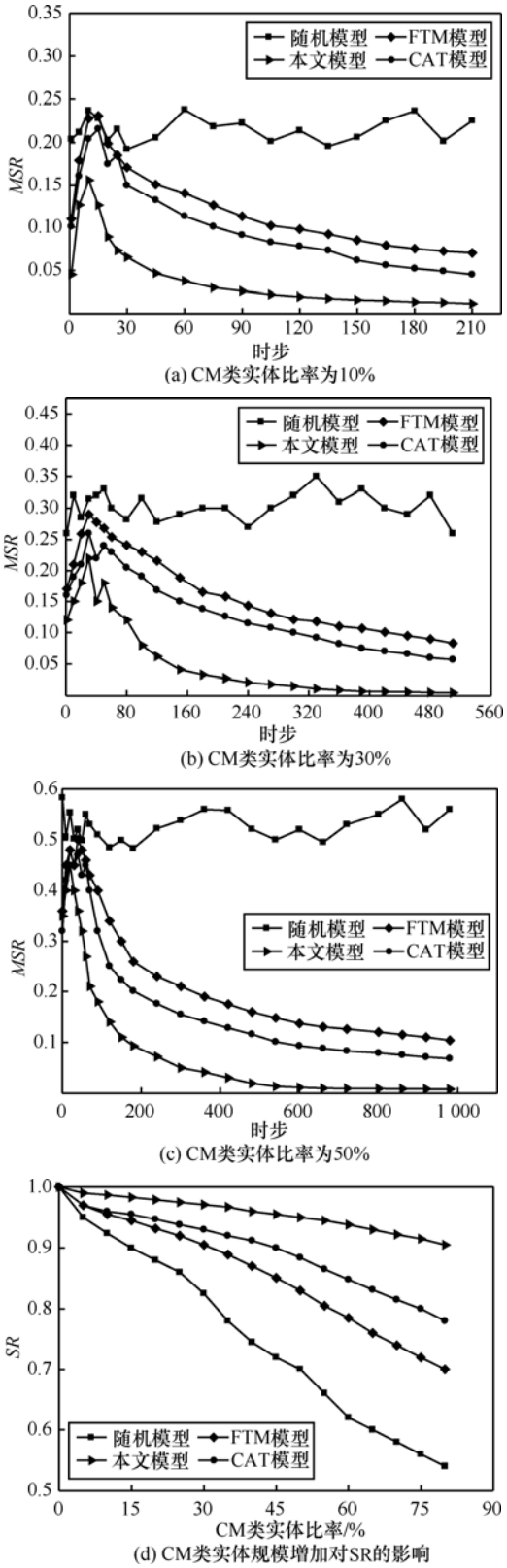


图 3　在不同规模的 CM 类实体恶意环境下 MSR 和 SR 的变化规律

图 3(d)是考察在不同规模的 CM 类恶意实体环境下的 SR 变化情况，从图给出的比较结果可以看出，当 CM 类恶意实体的比例较低时，3 种模型都具有很

高的服务请求成功率，这是因为CM类实体以不同比例提供正常服务的缘故。而随着CM类恶意实体比例的逐步增加，其他2种模型的服务请求成功率下降趋势较快，而本文模型仍能保持很高的服务请求成功率，特别当CM类实体达到80%时，服务请求成功率仍能保持在90%左右，说明本文模型的上下文机制和直接信任度的评估策略起到了主要作用。

实验2 抵御MC类恶意实体仿真及其讨论

图4(a)~图4(c)给出了MSR随不同规模MC类实体的变化规律，从实验结果中可以看出，在网络运行初期，3种模型的恶意服务请求成功率都比较高，这是由于在网络初期实体还没有信任度而采用随机选择的缘故。而随着网络的运行，恶意服务请求的成功率逐步下降，这是由于恶意实体进入了模型的惩罚和过滤阶段。图4(a)~图4(c)表明，本文模型在遏制串谋团体方面较其他2种模型具有明显的效果，恶意服务请求成功率下降趋势非常明显，这说明本文模型利用评分相似度过滤了大量的恶意推荐实体，而且在推荐信任度计算方面具有较好的效果。

图4(d)是考察*SR*随不同规模MC类实体的变化情况，由对比结果可以看出，当MC类实体比率较少时，3种模型的服务执行成功率都较高，在90%以上。而随着MC类实体比率的增加，本文模型较其他2种模型具有较高的服务成功率，这说明本文模型的总体信任度和综合推荐信任度的计算方法在抵御协同作弊和虚假推荐方面具有较好的效果。

实验3 抵御MS类恶意实体仿真及其讨论

图4(a)和图4(b)给出了恶意实体为50%，间谍实体占恶意实体的比例分别为10%和20%时的实验结果。从实验结果中可以看出，在运行初始阶段，间谍实体为10%时3种模型的恶意服务攻击成功率要高于间谍实体为20%时恶意服务攻击成功率，这是因为间谍实体在网络运行初期需要大量的交易来积累信任度以及对其他实体进行虚假评分。而随着网络的运行，间谍实体为20%时恶意服务攻击成功率开始高于间谍实体为10%时恶意服务攻击成功率，这是因为间谍实体虚假推荐的缘故。但在总体上随着网络的运行，恶意服务攻击的成功率逐步下降，这是由于模型对间谍实体的抑制起到了作用。图4(a)和图4(b)说明，本文模型在抑制间谍实体方面较其他2种模型有较大优势，恶意服务执行成功率下降趋势较快，而且能在400个时间片时将恶意服务成功率控制在2%左右，而其他2种模型在该环境下对恶意服务的抑制不是很理想，这说明了本文模型的综合推荐信任计算方法能够有效抑制间谍实体的虚假推荐，并且充分利用了间谍实体提供的正常服务。

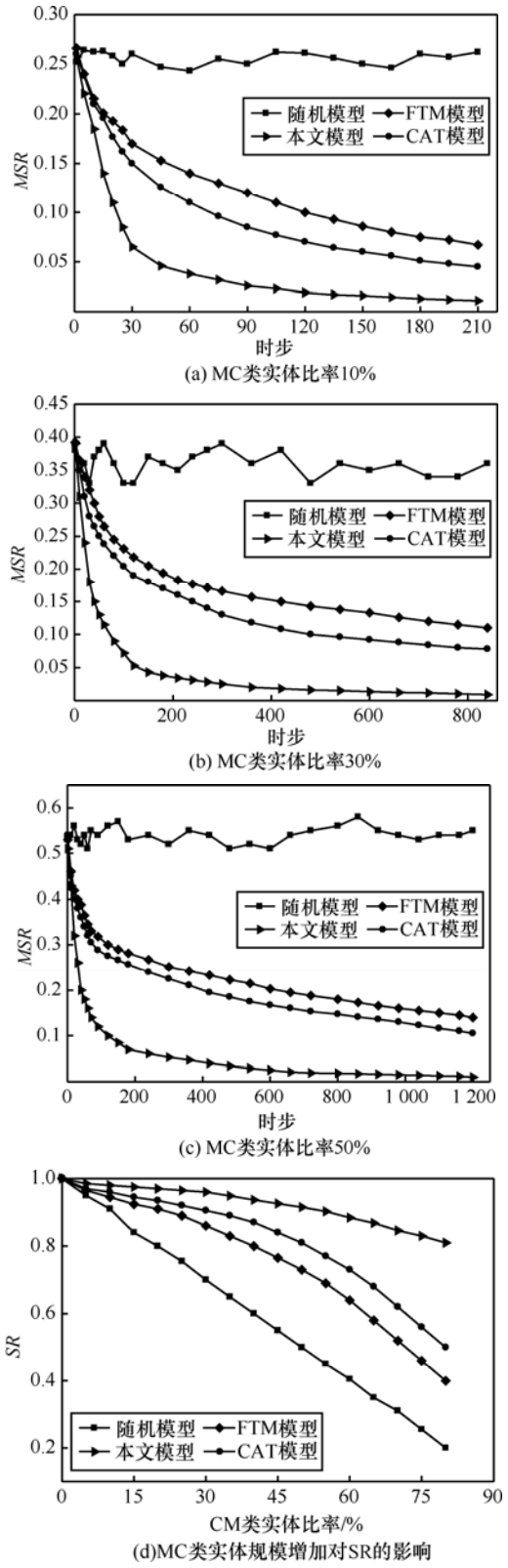
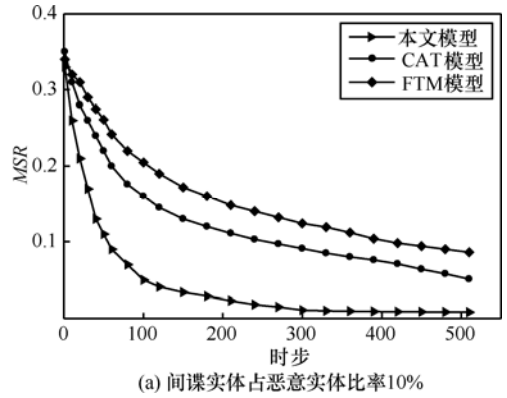
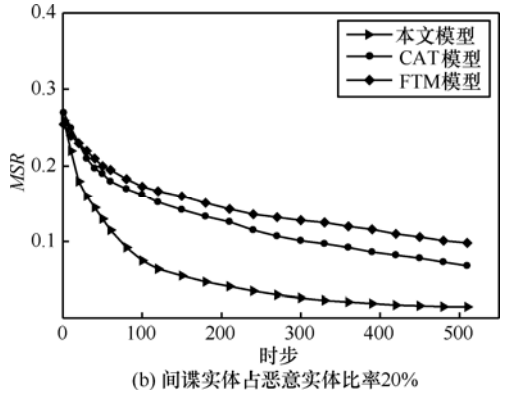


图4 在不同规模的MC类实体恶意环境下*MSR*和*SR*的变化规律



(a) 间谍实体占恶意实体比率10%



(b) 间谍实体占恶意实体比率20%

图 5　*MSR* 随不同规模恶意实体和间谍实体的变化规律

5　结束语

本文将实体历史交互窗口和可信推荐数等证据因素引入到了总体信任评估方法中，使得评估策略能够随着证据变化动态自适应地调整，有效地增强了交互证据的感知能力和评估的科学合理性。给出了一种基于满意度迭代计算的直接信任积累方法，在该方法中通过引入实体稳定度实现了激励和惩罚 2 种不同的迭代策略，有效地促进了实体长期稳定地提供真实服务，并且采用惩罚机制抑制了策略性伪装实体的作弊行为，大大提高了信任评估的准确性。在基于直接和间接相结合的综合推荐信任聚合方法中，通过采用实体熟悉度、路径衰减因子和评分相似度，提高了推荐信任的准确性和可靠性，过滤了恶意和虚假推荐实体。

参考文献：

[1] WANG J, SUN H J. A new evidential trust model for open communities[J]. Computer Standards and Interfaces, 2009, 31(5): 994-1001.

[2] BONNAIRE X, ROSAS E. WTR: A reputation metric for distributed hash tables based on a risk and credibility factor[J]. Journal of Computer Science and Technology, 2009, 24(5): 844-854.

[3] 李小勇, 桂小林. 大规模分布式环境下动态信任模型研究[J]. 软件学报,2007, 18(6):1510-1521.
LI X Y, GUI X L. Research on dynamic trust model for large scale distributed environment[J]. Journal of Software, 2007, 18(6): 1510-1521.

[4] JSANG A, ISMAI R, BOYD C. A survey of trust and reputation systems for online service provision[J]. Decision Support Systems, 2007, 43(2): 618-644.

[5] KAMVAR S, SCHLOSSER M. EigenRep: reputation management in P2P networks[A]. Proceedings of the 12th International World Wide Web Conference[C]. 2003, 123-134.

[6] 李景涛,荆一楠,肖晓春.基于相似度加权推荐的 P2P 环境下的信任模型[J].软件学报,2007, 18(1):157-167.
LI J T, JING Y N, XIAO X C. A trust model based on similarity-weighted recommendation for P2P environments[J]. Journal of Software, 2007, 18(1):157-167.

[7] 桂春梅,蹇强,王怀民.虚拟计算环境中基于重复博弈的惩罚激励机制[J].软件学报,2010, 21(12):3042−3055.
GUI C M, JIAN Q, WANG H M. Repeated game theory based penalty-incentive mechanism in internet-based virtual computing environment[J]. Journal of Software, 2010, 21(12):3042-3055.

[8] 胡建理,周斌,吴泉源.P2P 网络中具有激励机制的信任管理研究[J]. 通信学报, 2011, 32(5):22-32.
HU J L, ZHOU B, WU Q Y. Research on incentive mechanism integrated trust management for P2P networks[J]. Journal on Communications, 2011, 32(5):22-32.

[9] HAQUE M, AHAMED S. Design, analysis, and deployment of omnipresent formal trust model (FTM) with trust bootstrapping for pervasive environments[J]. Journal of Systems and Software. 2009, 83(2): 253-270.

[10] Mohammad G U, Mohammad Z, Sheikh I A. CAT: a context aware trust model for open and dynamic systems[A]. Proceedings of the 23rd Annual ACM Symposium on Applied Computing, SAC'08[C]. Fortaleza, Ceara, Brazil, 2008, 2024-2029.

[11] 甘早斌,丁倩,李开.基于声誉的多维度信任计算算法[J].软件学报, 2011,22(10): 2401-2411.
GAN Z B, DING Q, LI K, Reputation-based multi-dimensional trust algorithm[J]. Journal of Software, 2011, 22(10):2401-2411

[12] 张琳,王汝传,王海艳.基于多影响因素的网格信任传播算法[J].通信学报, 2011, 32(7):161-168
ZHANG L, WANG R C, WANG H Y. Trust transitivity algorithm based on multiple influencing factors for grid environment[J]. Journal on Communications, 2011, 32(7):161-168.

[13] 李小勇,桂小林.动态信任预测的认知模型[J].软件学报,2010, 21(1): 163-176.

LI X Y, GUI X L. Cognitive model of dynamic trust forecasting[J]. Journal of Software, 2010, 21(1):163-176.

[14] FÉLIX G M, GREGORIO M P. Security threats scenarios in trust and reputation models for distributed systems[J]. Computers and Security, 2009, 28(7): 545-556.

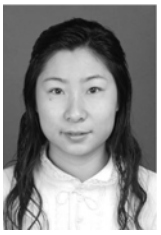
[15] 鲍宇,曾国荪,曾连荪.P2P 网络中防止欺骗行为的一种信任度计算方法[J]. 通信学报,2008, 29(10):215-222.
BAO Y, ZENG G S, ZENG L S. Reputation computation based on new metric in P2P network[J]. Journal on Communications, 2008, 29(10): 215-222.

[16] 苗光胜,冯登国,苏璞睿.P2P 信任模型中基于行为相似度的共谋团体识别模型[J].通信学报,2009, 30(8):9-20.
MIAO G S, FENG D G, SU P R. Colluding clique detector based on activity similarity in P2P trust model[J]. Journal on Communications, 2009, 30(8):9-20.

作者简介：

李峰（1978-），男，山东德州人，东北大学讲师，主要研究方向为信任管理和信任建模技术。

申利民（1962-），男，黑龙江佳木斯人，博士，燕山大学教授、博士生导师，主要研究方向为软件工程和可信计算。



司亚利（1981-），女，黑龙江齐齐哈尔人，燕山大学讲师，主要研究方向为物联网与信息安全。

牛景春（1977-），男，河北秦皇岛人，燕山大学博士生，主要研究方向为信任管理和信任建模技术。

（上接第 59 页）

[5] ACHARYA M, GIRAO J. Secure comparison of encrypted data in wireless sensor networks[A]. 3rd International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks[C]. Trentino, Italy, 2005.47-53.

[6] HUANG S I, SHIUHPYNG S, TYGAR J D. Secure encrypted-data aggregation for wireless sensor network[J]. Springer Wireless Networks, 2010, 5(16):915-927.

[7] CHAN H, PERRIG A. ACE: an emergent algorithm for highly uniform cluster formation[J]. LNCS, 2004,2(2920):154-171.

[8] SCHNEIER B. Fast software encryption[A]. Cambridge Security Workshop Proceedings[C]. Springer-Verlag, 1994.191-204.

[9] WANDER A, GURA N, EBERLE H, *et al*. Energy analysis of public-key cryptography on small wireless devices[A]. Proc of PerCom'05[C]. Kauai Island, Hawaii, USA, 2005.324-328.

[10] MICA. datasheet[EB/OL]. http://www.xbow.com/Pro-ducts/ Product_pdf_files/Wireless_pdf/MICA2_Datasheet.pdf/, 2006.

作者简介：

郭江鸿（1975-），男，山西长治人，西安电子科技大学博士生，主要研究方向为无线移动安全、网络安全。

马建峰（1963-），男，陕西西安人，博士，西安电子科技大学教授、博士生导师，主要研究方向为计算机安全、密码学、移动与无线网络安全。