一种具有时间衰减和主观预期的 P2P 网络信任管理模型

李佳伦　谷利泽　杨义先
(北京邮电大学网络与交换技术国家重点实验室信息安全中心　北京　100876)

摘　要：该文提出了一种基于信誉的 P2P 网络信任管理模型。在 P2P 网络中，由于不存在中心节点，需要根据节点的行为来判断其是否可信。通过引入时间衰减算法，解决了对行为评估，本地信任值以及推荐的时间相关性问题。通过对近期表现和长期表现的对比，给出对该节点未来表现的主观预期，能够对节点异动做出反应。利用 DHT 资源发现算法，有效地降低了网络消耗，并使模型具有可扩展性。模型能够有效地提高 P2P 网络的交易成功率。

关键词：网络信任管理；P2P 网络；时间衰减；主观预期；分布式哈希表
中图分类号：TP393　　**文献标识码**：A　　**文章编号**：1009-5896(2009)11-2786-05

A New Trust Management Model for P2P Network with Time Self-Decay and Subjective Expect

Li Jia-lun　Gu Li-ze　Yang Yi-xian
(*Information Security Center*, *State Key Laboratory of Networking and Switching Technology*, *Beijing University of Posts and Telecommunications*, *Beijing* 100876, *China*)

Abstract: This paper presents a novel decentralized trust management model with reputation. In P2P (peer to peer) network, there is no trusted authority. Trust relations between peers should be established with peer's behaviors. There are three main contributions in this paper. Towards utilizing time self-decay function, the time-related problem is resolved. Also through comparing the nearly scores and general scores, the problem of servent's subjective expect can be resolved. After using the DHTs, bandwidth cost can be reduced and salability can be obtained. This model can promote the business succeed rate in P2P network efficiently.

Key words: Network trust management; P2P network; Time self-decay; Subjective expect; Distributed hash table

1　引言

P2P(Peer to Peer，对等)网络是分布式网络的主要类型。它打破了传统客户-服务器模式，每一个节点既提供服务又使用别人的服务，同时，具有匿名性，自治性，非中心性和不可靠连接等特点[1]。目前，P2P 网络已经在各个应用领域(例如文件共享，内容分发，语音与视频通信等[2])取得了巨大成功，与之相对应的是，P2P 网络的各种安全问题越来越引起人们的关注。由于不存在可信第 3 方和匿名特性，传统的以身份认证和角色控制为核心的安全机制已经不能满足 P2P 网络的需求。基于信誉的信任管理机制，采用模拟人类社会的社会信任方式来构建网络信任机制，能够有效地解决 P2P 网络的信任缺失问题，因而成为 P2P 网络安全研究的热点。

在 P2P 网络中，信任主要体现为一种关系，即信任关系，“A 信任 B”或者“A 不信任 B”都是信任关系。其中，A 称为信任者(trustor)，B 称为被信任者(trustee)。基于信誉的信任管理模型以信誉作为构建信任关系的依据，所谓信誉是指：trustor 以自己亲历与搜集的 trustee 过去行为的信息为依据，对 trustee 行为的期望[3]。其中，亲历的行为产生的信誉值(也就是 trustor 同 trustee 的直接交互)称为本地信任值，搜集的行为产生的信誉值称为推荐值。

根据推荐的范围，信任管理可以分为局部信任和全局信任。局部信任根据网络中局部节点的推荐来实现信誉评估，方法比较简单，但是准确性差，并且很容易被欺骗。文献[4]提出的 P2PRep 是一种典型的局部信任模型，采用投票的方式评估一个节点的信任值。全局信任则依靠所有节点的推荐来实现信誉评估。这种方式避免了推荐的片面性，能够反映节点在网络中的实际表现，然而需要解决推荐信息的存储和获取问题。目前已经存在许多全局信任模型[5−9]。全局信任模型的信誉值又称为全局信任值。

P2P 网络的信任关系具有时间相关性，即随着时间的推移，以前产生的信誉会衰减。文献[7, 8]没

2008-11-26 收到，2009-04-14 改回
国家 973 计划项目(2007CB310704)，国家自然科学基金(60821001, 90718001)和北京市自然科学基金(4073037)资助课题

有考虑时间相关性问题，文献[6]虽然在本地信任值生成的时候只考虑近期发生的事件，但是当本地信任值和推荐值生成后，就不再随时间变化。另一方面，许多模型[1,4−9]都没有考虑节点的主观预期，从而无法对节点异动(例如，某节点因恶意攻击而感染病毒)进行反应。

针对目前 P2P 网络信任管理模型存在的问题，本文提出了一种适合于 P2P 网络的信任管理模型 TimeTrust。该模型具有以下特点：(1)能够实时地反映网络中节点的信任情况。(2)良好的可扩展性，模型不会因网络规模的扩大而瘫痪。(3)良好的网络均衡型，优秀节点不会因为负载过重而成为瓶颈。(4)良好的主观预期特性，能够对节点异动进行反应。

2　符号说明

$A, B, \cdots$ 为网络中的节点；$\mathbf{Sc}_i^{AB}$ 为 A 对 B 的第 i 个服务评价；δ 为信任采信区间；NT 为当前时间；Ω_δ^{AB} 为 δ 采信的 A 对 B 的评价集；$\mathbf{DT}^{AB}$ 为 A 对 B 的本地信任值；$\mathbf{Re}^{AB}$ 为 A 对 B 的推荐值；Π^B 为针对 B 的推荐值集合；ID^B 为节点 B 的 ID 值；$\mathrm{old}T$ 为最早信任采信时间；$\mathbf{Rs}_A^{CB}$ 为 A 修正的 C 对 B 的推荐值；Φ_A^B 为 $\{Rs_A^{iB} \mid i \in \text{网络}\}$；$\mathbf{GT}^{AB}$ 为 A 对 B 的全局信任值；$\mathbf{Th}^A$ 为 A 的本地信任阈值。

3　TimeTrust 模型

3.1 本地信任值

本地信任值来源于 trustor 同 trustee 的直接交互情况。在 TimeTrust 中，交互情况由服务使用者的服务评价值 $\mathbf{Sc}$ 表示，定义如下：

定义 1　当 A 使用了 B 提供的服务后，将对 B 的这次服务进行评价，用 $\mathbf{Sc}^{AB}$ 表示。$\mathbf{Sc}$ 为 3 元向量，即 $\mathbf{Sc}=(\mathrm{ss},\mathrm{sf},\mathrm{st})$。其中，ss 为交易成功分量，成功置 1，失败置 0；sf 为交易失败分量，成功置 0，失败置 1；st 为评价发生时间。

用户生成的所有服务评价都存放在本地，按 trustee 分成不同的评价集。

定义 2　Ω^{AB} 表示 A 生成的针对 B 的评价集，$\Omega^{AB}=\{\mathbf{Sc}_i^{AB}\}$。$\Omega_\delta^{AB}$ 表示最近 δ 时间内生成的 A 对 B 的评价构成的评价集，即 $\Omega_\delta^{AB}=\{\mathbf{Sc}_i^{AB} \mid \mathrm{NT}-\mathrm{st}_i<\delta\}$。$\delta$ 称为信任采信区间。NT 为当前时间。

A 对 B 的本地信任值由 A 根据 Ω^{AB} 生成，考虑时间向关性，只考虑 Ω_δ^{AB} 中的评价值。本地信任值定义如下：

定义 3　A 对 B 的本地信任值由 $\mathbf{DT}^{AB}$ 表示。$\mathbf{DT}$ 为 5 元向量，即 $\mathbf{DT}=(\mathrm{dn},\mathrm{dt},\mathrm{te},\mathrm{td},\mathrm{al})$。各分量计算方法为

$$\mathrm{dn}=\left|\Omega_\delta\right| \ ; \quad \mathrm{dt}=\frac{\sum_1^{\mathrm{dn}}(\mathrm{ss}_i-\mathrm{sf}_i)}{\mathrm{dn}} \ ; \quad \mathrm{te}=\frac{\sum_1^{\mathrm{dn}}\mathrm{st}_i}{\mathrm{dn}} \ ;$$

$$\mathrm{td}=\sqrt{\frac{3\sum_1^{\mathrm{dn}}(\mathrm{st}_i-\mathrm{te})^2}{\mathrm{dn}}} \ ; \quad \mathrm{al}=\begin{cases}\dfrac{2\varepsilon-5}{5}, & \mathrm{dn}\geq 5\\ \mathrm{dt}, & \mathrm{dn}<5\end{cases}$$

其中 $\left|\Omega_\delta\right|$ 为 Ω_δ 中元素个数。$\mathbf{Sc}_i=(\mathrm{ss}_i,\mathrm{sf}_i,\mathrm{st}_i)\in\Omega_\delta$，$\varepsilon$ 为 Ω_δ 中最近 5 次评价中 ss 的和。

dn 表示 trustor 对 trustee 在最近 δ 时间内的评价次数，反映了 A 与 B 交互的频繁度。dt 为交易成功总次数和交易失败总次数的差并进行归一化，反映了 A 对 B 的本地信任度。$\mathrm{dt}\in[-1,1]$。te 表示 Ω_δ 中所有评价发生时间的均值，td 为 Ω_δ 中所有评价发生时间的均方差的 $\sqrt{3}$ 倍。$[\mathrm{te}-\mathrm{td},\mathrm{te}+\mathrm{td}]$ 构成了同 Ω_δ 中的所有评价时间相同均值和方差的均匀分布，为 $\mathbf{DT}$ 的时间戳，用于在全局信任值中对时间衰减的处理。al 反映了 trustee 最近的表现，用于 trustor 的主观预期中。

A 同 B 发生了新的交互后更新 $\mathbf{DT}^{AB}$，即当有 $\mathbf{Sc}_{\mathrm{new}}^{AB}$ 生成时更新 $\mathbf{DT}^{AB}$。

3.2 推荐值的管理与获取

A 在决定是否信任 B 时，不仅要考虑 $\mathbf{DT}^{AB}$，还需要考虑其他节点对 B 的信任情况，即其他节点提供的推荐情况。对推荐值定义如下。

定义 4　A 对 B 的推荐值由 $\mathbf{Re}^{AB}$ 表示，$\mathbf{Re}^{AB}=\mathbf{DT}^{AB}$。

定义 5　Π^B 表示网络中所有节点对 B 的推荐值构成的集合，即 $\Pi^B=\{\mathbf{Re}^{iB} \mid i\in\text{网络}\}$。

如何管理和获取 Π^B 是信任管理领域的一个重要课题。文献[4,9]将推荐值保存在本地，由 trustor 向各节点发送查询来搜集获得 Π^B。这种方式网络消耗较大，并且不具备良好的可扩展性。文献[8]将推荐值保存在邻居节点中。文献[7]借鉴 P2P 网络的资源发现算法，将 Π^B 集中到若干个节点管理，节点的选择采用 DHT(分布式哈希表)模式，具体为 CAN 协议。这种方法并不会占用过多的网络带宽，并具有良好的可扩展性。后来的模型大都沿用文献[7]的思路，如文献[5,6]。TimeTrust 也采用类似的方式。

DHT 模式是目前 P2P 网络的主流资源发现方法，其思想是：将网络中提供同一种资源的各用户的信息集中到网络中的一个或多个节点管理。网络中的每个节点都管理一定数量的资源，从而实现资源管理的分布式。在 DHT 模式中，每个节点将分配一个 ID 值(根据算法的不同可以是 IP 或者用户名

等)，每种资源有一个独特的关键字 key (例如文件内容的 md5 值或者文件名)。当用户要发布关键字为 key_1 的资源时，他首先将对该资源的描述信息发送到管理这种资源的节点上。节点的选择由 $h(\text{key}_1)$ 决定，$h(\bullet)$ 为哈希函数。ID 值等于 $h(\text{key}_1)$ 的节点负责管理资源 key_1。如果需要多个节点管理，可以定义多个哈希函数 $h_1(\bullet), h_2(\bullet), h_3(\bullet), \cdots$。当用户要获取资源 key_1 时，他首先计算 $h(\text{key}_1)$ 得到管理该资源信息的节点，并从该节点得到所有提供该资源的节点的信息，然后从中选择节点下载。目前已经有多种 DHT 算法，如 CAN，Chord，Pastry，ROAD[10] 等等。

TimeTrust 将 Π^B 视为一种特殊的资源，关键字为 ID^B。当节点 A 同 B 发生了新的交互并更新了 $\mathbf{DT}^{AB}$ 后，将其作为 Re^{AB} 发送给 $\text{ID} = h(\text{ID}^B)$ 的节点。而当 A 需要获取 Π^B 时，发送消息给 $\text{ID} = h(\text{ID}^B)$ 的节点，即可以获得 Π^B。由于不同的 DHT 资源发现算法适合于不同的网络情况，TimeTrust 不单独定义具体的 DHT 算法，而是沿用具体网络使用的 DHT 算法。

3.3 全局信任值

在获取 Π^B 后，为了获得对 B 的全局信任值，A 首先要对 Π^B 进行修正。这一方面是因为要考虑推荐值的时间衰减性，时间戳不在信任采信区间 δ 的推荐值将被忽略。另一方面是因为并非每个节点都会诚实地提供推荐值，需要根据 A 对各推荐节点的信任度对推荐值进行调整。

定义 6 $\mathbf{Rs}_A^{CB} = (\text{dn}_A^{CB}, \text{dt}_A^{CB}, \text{al}_A^{CB})$ 表示经过 A 修正的 C 对 B 的推荐值。令 $\mathbf{Re}^{CB} = (\text{dn}^{CB}, \text{dt}^{CB}, \text{te}^{CB}, \text{td}^{CB}, \text{al}^{CB})$，$\text{old}\,T = \text{NT} - \delta$ 为最早信任采信时间，$\mathbf{DT}^{AC} = (\text{dn}^{AC}, \text{dt}^{AC}, \text{te}^{AC}, \text{td}^{AC}, \text{al}^{AC})$。那么

$$\text{dn}_A^{BC} = \begin{cases} \text{dn}^{CB}\text{dt}^{AC} \cdot \eta(\text{te}^{CB}, \text{td}^{CB}), & \text{dt}^{AC} > 0 \\ 0, & \text{dt}^{AC} \le 0 \end{cases}$$

$$\text{dt}_A^{BC} = \text{dt}^{BC}, \quad \text{al}_A^{CB} = \text{al}^{CB}$$

其中 $\eta(\text{te}^{CB}, \text{td}^{CB})$ 为推荐时间衰减函数：

$$\eta(\text{te}^{CB}, \text{td}^{CB}) = \begin{cases} 1, & \text{te}^{CB} - \text{td}^{CB} > \text{old}\,T \\ \dfrac{\text{td}^{CB} + \text{te}^{CB} - \text{old}\,T}{2\text{td}^{CB}}, & \text{te}^{CB} - \text{td}^{CB} \le \text{old}\,T < \text{te}^{CB} + \text{td}^{CB} \\ 0, & \text{te}^{CB} + \text{td}^{CB} \le \text{old}\,T \end{cases}$$

$\mathbf{Rs}_A^{CB}$ 同 $\mathbf{Re}^{CB}$ 相比，去掉了 te 和 td 分量，并调整了 dn 分量。这是因为 te 和 td 分量的作用就是用于修正推荐值时提供 $\mathbf{Re}^{CB}$ 的时间衰减性。由于时间相关性，trustor 只考虑最近 δ 内发生的行为，因而，只有发生在 $\text{old}\,T$ 之后的行为才被计入。当 A 接到 $\mathbf{Re}^{CB}$ 后，认为 $\mathbf{Re}^{CB}$ 反映的是 $[\text{te}^{CB} - \text{td}^{CB}, \text{te}^{CB} + \text{td}^{CB}]$ 时间段中均匀分布的 dn^{CB} 个行为评价构成的推荐值。$\eta(\text{te}^{CB}, \text{td}^{CB})$ 输出的是 $\mathbf{Re}^{CB}$ 中发生在 $\text{old}\,T$ 之后的行为占总行为数的比例，为 [0,1] 区间内的一个值，如图 1 所示。

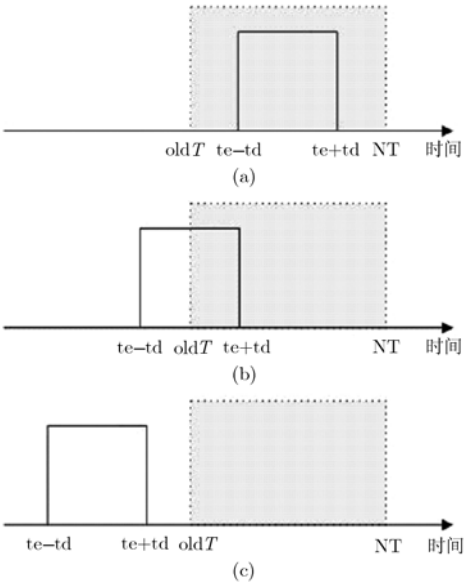

图 1 $\eta(t)$ 说明

经过时间衰减修正后的 Re^{CB} 还需要经过可信性修正。这是因为 C 可能会提供虚假的推荐值给 A。我们使用 $\mathbf{DT}^{AC}$ 的 dt^{AC} 分量来做修正，含义为：$\mathbf{Re}^{CB}$ 的可信度由 A 对 C 的直接信任度决定，A 越信任 C，$\mathbf{Re}^{CB}$ 的可信度越高，如果 A 不信任 $C(\text{dt}^{AC} \le 0)$，则 $\mathbf{Re}^{CB}$ 不具备参考价值。

之所以只修正 dn 分量是因为 dn 分量在全局信任值的计算中扮演了权重的角色。

此外，由于时间衰减性，在进行推荐值修正时，所有 $\mathbf{DT}^{Ai}$ 应是重新计算的，以保证新鲜性。

定义 7 Φ_A^B 表示所有经过 A 修正的对 B 的推荐值集合，即 $\Phi_A^B = \{\mathbf{Rs}_A^{iB} \mid i \in \text{网络}\}$。

全局信任值定义如下。

定义 8 $\mathbf{GT}^{AB} = (\text{gn}^{AB}, \text{gt}^{AB}, \text{gal}^{AB})$ 表示 A 对 B 的全局信任值，由 $\mathbf{DT}^{AB}$ 和 Φ_A^B 计算得到。令 $\mathbf{DT}^{AB} = (\text{dn}_0, \text{dt}_0, \text{te}_0, \text{td}_0, \text{al}_0)$，$\mathbf{Rs}_A^{iB} = (\text{dn}_i, \text{dt}_i, \text{al}_i)$，那么

$$\text{gn}^{AB} = \sum_0^n \text{dn}_i, \quad \text{gt}^{AB} = \frac{\sum_0^n \text{dn}_i \cdot \text{dt}_i}{\text{gn}^{AB}}$$

$$\text{gal}^{AB} = \frac{\sum_0^n \text{al}_i \cdot \text{dn}_i}{\text{gn}^{AB}}$$

其中 $n=|\Phi_A^B|$。gn^{AB} 表示 A 采信的 B 在网络中的活跃程度; gt^{AB} 表示 A 针对 B 的全局信任程度; gal^{AB} 表示 A 采信的 B 最近的表现。

在 TimeTrust 模型中各节点存在本地阈值 $\mathbf{Th}=(\mathrm{thn},\mathrm{tht},\mathrm{thl})$。Trustor 根据其本地策略将 trustee 划分为全局可信节点，全局陌生节点和全局不可信节点和异动节点。

定义 9　设 A 的本地阈值为 $\mathbf{Th}^A$，那么

如果 $\mathrm{gn}^{AB}\geq\mathrm{thn}^A$，$\mathrm{gt}^{AB}\geq\mathrm{tht}^A$ 且 $\mathrm{gal}^{AB}>\mathrm{thl}^A$，则 B 为 A 的全局可信节点。

如果 $\mathrm{gn}^{AB}<\mathrm{thn}^A$，则 B 为 A 的全局陌生节点。

如果 $\mathrm{gn}^{AB}\geq\mathrm{thn}^A$ 且 $\mathrm{gt}^{AB}<\mathrm{tht}^A$，则 B 为 A 的全局不可信节点。

如果 $\mathrm{gn}^{AB}\geq\mathrm{thn}^A$，$\mathrm{gt}^{AB}\geq\mathrm{tht}^A$ 且 $\mathrm{gal}^{AB}\leq\mathrm{thl}^A$，则 B 为 A 的全局异动节点。

3.4 服务选择

当P2P网络中的节点 A 想要获取关键字为 key_1 的资源时，首先通过资源搜索算法得到包含该资源的节点列表，然后采用 TimeTrust 模型计算各节点的全局信任值，并用 $\mathbf{Th}^A$ 将其归类。最后采用服务选择算法选择要使用的服务节点。如果存在全局可信节点，则从中选择服务能力最强(例如，下载带宽最宽)的节点提供服务。如果不存在全局可信节点，则从全局异动节点中选择服务能力最强的节点提供服务。如果也不存在全局异动节点，则从全局陌生节点中选择服务能力最强的节点提供服务。如果也不存在全局陌生节点，则不进行下载。

4　分析与仿真

4.1 交易成功率

在P2P网络中引入信任管理系统的主要目的之一就是提高系统交易成功率和抑制恶意节点。仿真实验表明，TimeTrust 能够有效地提高交易成功率和抑制恶意节点，结果如图 2 所示。

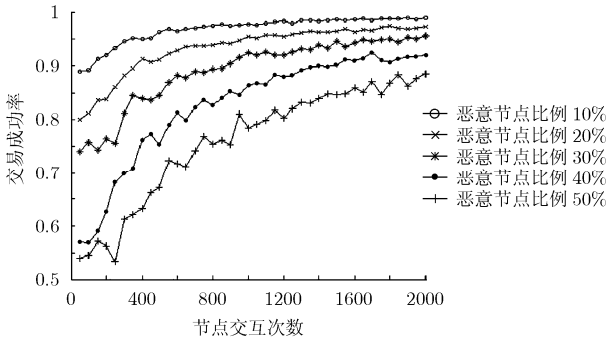

图 2 交易成功率

从图 2 中可以看出，随着网络的不断运行，交易成功率不断提高，即便在恶意节点比例高达 50% 的情况下 TimeTrust 仍然能够保证网络的正常运行。

4.2 时间相关性

时间相关性是 P2P 网络的重要特性。近期形成的信任信息应当比早期的有更高的说服力。在已有模型中，文献[1,6–8]没有考虑事件相关性。文献[5]只记录最新发生的 8 次交互，而没有考虑这 8 次发生的时间间隔。因而，可能其中 6 次发生的时间远早于另 2 次，从而无法真实反映节点的近期行为。文献[6]在计算一个节点对另一个节点的评价时，只考虑两个节点最近 τ 内的交互。然而，当评价 $E_{u,v}$(表示 u 对 v 的评价值)生成后，只有节点 u 可以对其进行更新。$E_{u,v}$ 不带有时间戳，并且不会定时更新，从而在计算全局信任值时，无法区分古旧的评价和新近的评价。

TimeTrust 中，只有当 A 同 B 发生了新的交互后，A 才会将更新后的 $\mathbf{DT}^{AB}$ 作为 $\mathbf{Re}^{AB}$ 发送到 B 对应的推荐信息存储节点。(在修正 B 提供的推荐值时也会更新 $\mathbf{DT}^{AB}$，但不会作为推荐值发送。)因而，当 C 需要计算 $\mathbf{GT}^{CB}$ 时，他获取的 $\mathbf{Re}^{iB}$ 的生成时间各不相同。而由于 TimeTrust 的 $\mathbf{Re}^{iB}$ 具有时间戳，能够近似地反映 $\mathbf{Re}^{iB}$ 统计的时间区间(同原时间区间具有相同的均值和方差特性的均匀分布时间区间)，因而，通过对 $\mathbf{Re}^{iB}$ 的修正，新生成的 $\mathbf{GT}^{CB}$ 能够近似地反映最近 δ 内 B 的活动情况。图 3 为网络中某节点对另一节点的 $\mathbf{GT}$ 随时间变化的情况，假设 δ 为 300 单位时间，并且在这段时间中 B 没有同其他节点交互。

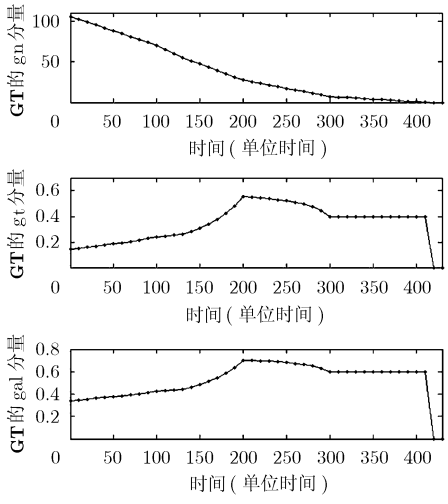

图 3 时间相关性

可以看出，随着时间的推移，**GT** 的 gn 分量不断降低，而 gt 和 gal 则非单向递减变化。这是因为不同的推荐值的时间戳不同的缘故。

4.3 可扩展性

可扩展性是指模型消耗的资源不因系统节点数目的增加而急速增大。对于信任管理模型而言，主要的消耗来源于推荐信息的获取和管理。由于 TimeTrust 采用 DHT 模式，搜索针对某一资源的推荐信息所需路由仅为 $O(\log N)$ (N 为网络节点数目)，因而具有良好的可扩展性。

4.4 网络均衡

TimeTrust 中，如果某资源存在多个可信节点可供选择，则服务申请者选择当前服务带宽最宽的节点进行下载，而不是选择可信度最高的节点，这使得网络的负债更加均衡，高可信度节点不会因扎堆而瘫痪。

4.5 主观预测性

主观预测性是指，trustor 对 trustee 异动的主观预测。举例来说，如果一个节点突然连续几次提供不正确的服务，我们会感觉该节点可能被攻击，并且最近一段时间都无法提供正常的服务。参考文献中列出的各种模型均未考虑主观预测性，因而当节点出现异动后，系统不能对此作出反应。只有通过不断地实践，直至该节点转化为不可信节点后，方能抑制该瘫痪节点。

TimeTrust 通过在 **GT** 中引入最近表现 gal 分量，通过其与长期表现 gt 分量的对比，可以对节点异动作出反应。TimeTrust 在可信节点和不可信节点之间引入了中间状态异动节点，以区分这三者。全局可信节点发生异动后将转化为全局异动节点。如果某节点发生异动，服务请求者将优先选择其他全局可信节点。

5 结束语

本文根据 P2P 网络中的信任管理需求，提出了一种基于信誉的全局信任管理模型。模型能够实时地反映节点的信誉情况，并能对节点异动作出反应。模型具有良好的可扩展性和网络均衡特性。下一步，我们将进一步对网络中的信任管理需求进行研究，改进协议的性能。

参 考 文 献

[1] Aberer K and Despotovic Z. Managing trust in a peer-2-peer information system[C]. International Conference on Information and Knowledge Management, New York: ACM, 2001: 310–317.

[2] Ciszkowski T, Eliasson C, and Fiedler M. SecMon: End-to-End Quality and Security Monitoring System[C]. 7th International Conference on Computer Science-Research and Applications (IBIZA 2008), Poland, Kazimierz Dolny 31.01-2.02 2008, Published in Annales UMCS, Informatica, AI 8 (2008): 186–201.

[3] Abdul-Rahman A and Hailes S. Supporting trust in virtual communities[C]. Proceedings of the Hawaii International Conference on System Sciences, Maui, Hawaii, 2000. Washington: HICSS, Vol. 6, 6007.

[4] Cornelli F, Damiani E, and Vimercati S, *et al*.. Choosing reputable servents in a P2P network[C]. International World Wide Web Conference, New York: ACM, 2002: 376–386.

[5] 张春瑞, 徐恪, 王开云. 基于信任向量的P2P网络信任管理模型[J]. 清华大学学报(自然科学版), 2007, 47(7): 1224–1228.
Zhang C, Xu K, and Wang K. Trust vector-based P2P trust management model[J]. *Journal of Tsinghua University* (*Science and Technology*), 2007, 47(7): 1224–1228.

[6] 窦文, 王怀民, 贾焰. 构造基于推荐的 Peer-to-Peer 环境下的 Trust 模型[J]. 软件学报, 2004, 15(4): 571–583.
Dou W, Wang H, and Jia Y. A recommendation-based peer-to-peer trust model[J]. *Journal of Sofware*, 2004, 15(4): 571–583.

[7] Repantis T and Kalogeraki V. Decentralized trust management for ad-hoc peer-to-peer networks[C]. Proceedings of the 4th international workshop on Middleware for Pervasive and Ad-Hoc Computing (MPAC), New York: ACM, 2006: 6.

[8] Kamvar S, Schlosser M, and Garcia-Molina H. The EigenTrust algorithm for reputation management in P2P networks[C]. International World Wide Web Conference, New York: ACM, 2003: 640–651.

[9] Lee S and Sherwood R. Cooperative peer groups in NICE[C]. IEEE Infocom, San Francisco, USA. 2003: 523–544.

[10] 杨峰, 李海霞, 余洪亮. 一种基于分布式哈希表的混合对等发现算法[J]. 软件学报, 2007, 18(3): 714–721.
Yang F, Li H, and Yu H. A hybird peer-to-peer lookup service algorithm on distributed hash table[J]. *Journal of Sofware*, 2007, 18(3): 714–721.

李佳伦： 男，1983 年生，博士，研究方向为网络安全和信任管理等.

谷利泽： 男，1965 年生，副教授，研究方向为现代密码学及电子商务等.

杨义先： 男，1961 年生，教授，博士生导师，从事现代密码学、编码理论、电子商务等方面的研究工作.