

文章编号:1001-9081(2006)12-2900-03

一种基于信任机制的混合式 P2P 模型

李玲娟,姬同亮,王汝传

(南京邮电大学 计算机学院,江苏 南京 210003)

(lilj@njupt.edu.cn)

摘 要:以改善 P2P 网络的安全性能为目标,介绍了基于关键节点的混合式 P2P 结构和基于信誉的信任机制,提出了一种基于该信任机制的混合式 P2P 模型,描述了该模型的工作机制。利用该模型可以在两个对等实体之间建立高效、可靠的信任关系,有效防止恶意攻击,提高 P2P 网络的效率和安全。

关键词:信任;混合式 P2P;信誉衰减

中图分类号: TP393.08 **文献标识码:** A

Trust-based hybrid P2P model

LI Ling-juan, JI Tong-liang, WANG Ru-chuan

(School of Computer, Nanjing University of Posts and Telecommunications, Nanjing Jiangsu 210003, China)

Abstract: To improve the security performance of P2P networks, the hybrid P2P structure based on sticking point and the reputation-based trust mechanism was introduced, and a hybrid P2P model based on the reputation-based trust mechanism was proposed. Meanwhile, the workflow of the model was described. The model can effectively build up a high efficient and reliable trust relationship between peers, prevent malicious attack and enhance security and efficiency of the P2P networks.

Key words: trust; hybrid P2P; reputation decrease

0 引言

P2P 网络(即对等网络)是一种点对点计算模式,因其强大的资源共享和平衡网络负载的能力,被誉为第三代网络。综合比较几种常见的 P2P 网络拓扑结构,集中式和分布式特点于一身的基于关键节点的混合式 P2P 结构,在资源搜索、查询效率以及通信安全等方面有着较为突出的优势。但是,混合式 P2P 网络仍因具有高度的动态、开放和匿名等特性而造成服务质量不可靠、欺诈行为大量存在的问题。因此,在混合式 P2P 环境中建立一个高效、安全的通信环境显得尤为重要。为此,本文提出了一种基于信誉的信任机制的混合式 P2P 模型,称之为 TBHPM(Trust-Based Hybrid P2P Model)。

所谓信任机制是指用户通过自己的过去经历或他人的推荐来选择符合自己要求的交互端的一种机制^[1],此机制能激励用户提供高质量的可靠服务,节省时间和通信开销,减少交互风险和损失,促进网络的良性发展。

本文提出的模型根据节点间的历史交互信息,首先计算出每个相关节点的信任度,节点依据计算结果与信任度高的节点或称可靠节点进行交易,以此在两个对等实体之间建立高效、可靠的信任关系,有效防止恶意攻击,明显提高系统的效率和安全性。

1 带关键节点的混合式 P2P 网络

在带关键节点的对等网络(拓扑结构见图 1)中,将系统中的资源按照不同的主题,分成多个簇。各个簇内连接较多

近邻节点、起着本区域中央服务器作用的节点称为关键节点(Sticking Point, SP);不同簇的关键节点之间相互连接,构成一个新的对等网络。每个关键节点上存放着两份列表:一份记录着所管区域内共享资源的地址信息;另一份记录着其他关键节点的地址信息。其工作机制可以以图 1 为例简单描述为:负责接收用户请求的节点(例如:P2)将用户查询条件和相关信息发送到本区域内的 SP(例如:SP1)上进行查询,SP1 在本地无符合条件的资源时,根据资源列表将查询进一步发至近邻域的 SP(例如:SP3),SP3 查到含有所需资源的节点 P7,此后 P2 和 P7 可以直接建立资源访问路由。

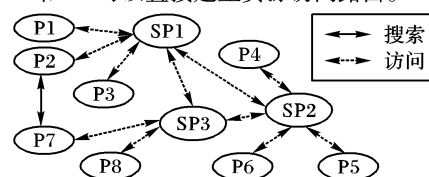


图 1 关键点搜索模型

与其他 P2P 网络相比,带关键节点的 P2P 网络有如下优点^[2]:

- 1) 减少搜索时的网络延时和所需网络带宽。
- 2) 良好的管理性。每个簇中的关键节点都是该组中可靠和值得信赖的节点,这保证了一些恶意攻击行为能在网络间得到很好的控制,而不致流传开来。
- 3) 负载均衡。在带关键节点的对等网络中关键节点处理能力强,网络带宽大,这可以在一定程度上提高整个网络的负载均衡。

收稿日期:2006-06-14;**修订日期:**2006-08-12 **基金项目:**国家自然科学基金资助项目(60573141;70271050);江苏省自然科学基金资助项目(BK2005146);江苏省自然科学基金预研资助项目(BK2004218);江苏省高技术研究计划资助项目(BG2004004);江苏省计算机信息处理技术重点实验室基金资助项目(kjs050001);江苏省高校自然科学研究计划资助项目(05KJB520092)

作者简介:李玲娟(1963-),女,辽宁辽阳人,副教授,博士,主要研究方向:数据挖掘、信息安全以及移动代理;姬同亮(1981-),男,山东临沂人,硕士研究生,主要研究方向:P2P 网络、信息安全;王汝传(1943-),男,安徽合肥人,教授,博士生导师,主要研究方向:计算机软件理论、计算机网络及信息安全、移动代理技术。

2 基于信誉的信任机制简介

2.1 信任和信誉

信任是指节点依据历史交往记录形成的对另一节点未来行为的能力、诚实、可靠等方面的主观期望^[3],是两个节点之间一对一的主观关系。

信誉是指依据节点的历史行为或意图形成的对节点在节点集中的总体形象与综合评价。信誉具有实时性、完整性等特征。

信誉评价是建立信任关系和实施信任管理的基础,而信任管理比信誉评价要更加复杂。在信任管理的信誉计算过程中,往往存在否认、报复、合谋等节点欺骗行为。

2.2 信任度的计算^[4,5]

在基于信誉的信任模型中,用 P 表示该 P2P 网络内节点的集合。 $A, B \in P$ 表示 A, B 是该网络内的两个节点。计算信任度的三个指标:

1) 交互总数:设 $I(A, B, t)$ 表示至 t 时刻节点 A 与节点 B 交互的总次数; $I(A, t)$ 表示至 t 时刻节点 A 与其他所有节点的交互总次数。则有:

$$I(A, t) = \sum_{B \in P, B \neq A} I(A, B, t) \quad (1)$$

2) 认可度:是其他节点对该节点服务满意的总量,可以用至 t 时刻节点 A 成功转发给 B 的报文数 $S(A, B, t)$ 来表示。令 $D(A, B, t)$ 表示至 t 时刻节点 A 放弃转发给节点 B 的报文数,则有:

$$S(A, B, t) = I(A, B, t) - D(A, B, t) \quad (2)$$

3) 可信度:由于网络内的恶意节点仍然可以对可信节点提供的服务做出错误断言,为了减少节点提供的错误信息带来的影响,引入可信度 C_{ij} 。 C_{ij} 是节点 j 对节点 i 而言的局部可信度,或节点 i 对节点 j 的局部信任度。有:

$$C_{ij} = \frac{Sat_{ij} - UnSat_{ij}}{\sum_j (Sat_{ij} - UnSat_{ij})} \quad (3)$$

Sat_{ij} 和 $UnSat_{ij}$ 分别为在历史交易中节点 i 对节点 j 累积的满意次数和不满次数。

当节点 A 需要了解任意节点 B 的全局可信度时,首先从节点 B 的交易伙伴(曾经与 B 发生过交易的节点)获知节点 B 的可信度信息,然后根据这些交易伙伴自身对节点 A 而言的局部可信度综合出节点 B 的全局可信度 $Cr(A, B, t)$:

$$Cr(A, B, t) = \sum_{j \in A \text{ 的交易伙伴}} C_{Aj} \times C_{jB} \quad (4)$$

综合考虑上述三方面的因素,为实现高效、准确地进行节点信誉评估,本文优先考虑相邻节点的样本观测状况。此时,节点 A 的信誉值可用公式(5)计算:

$$R(A, B, t) = \left[\frac{\sum_{B \in \text{neighbourhood}, B \neq A} S(A, B, t) \times Cr(A, B, t)}{\sum_{B \in \text{neighbourhood}, B \neq A} I(A, B, t)} \right] \quad (5)$$

由(5)式可知,节点的可信度越高,在信誉值计算时获得的权重也就越大。

另外,在 P2P 网络中一个常见的现象是节点在刚刚加入到网络中时行为良好,但是当获得一定信誉值时,开始表现出恶意性,影响网络性能。为避免这种现象,可以采取如下措施:对于节点的当前的、最近的反馈信息给予较大的权值,而对于以前的反馈信息给予较小的权值。因此,该模型倾向于看重节点当前的行为,而且能够反映节点近期行为随着时间的变化状况。为捕获节点近期行为的持续变化状况,引入信

息老化因素来最终确定节点信任度,将当前节点行为的权值用影响因子 a 表示, a 在 0 和 1 之间变化。

令 T_{old} 表示特定节点存储的以前的信任度,由此计算得到节点当前的信任度:

$$T_{current} = (1 - a) \times T_{old} + a \times R_{current} \quad (6)$$

其中, $R_{current}$ 表示运用公式(5)计算所得的节点的当前信誉值。 $a = 1$ 表示节点的信任度只取决于它的当前信誉状况; $a = 0.5$ 就是简单地将当前的信誉值和以前的信任度按相等权值加以考虑。

3 TBHPM 模型

3.1 TBHPM 模型的假设条件

TBHPM 是基于以下假设的:

- 1) 基本假设:信誉系统可以长期共存;
- 2) 该网络内节点与某一节点未来交互所采取的策略取决于该节点的历史行为,尤其是近期行为;
- 3) 网络中的个体在与其他个体的交互中会留下零星的“信誉”信息;
- 4) 网络内提供诚实服务的节点信誉值将会增加,而且将会得到好的服务;
- 5) 个体往往不看重绝对的可靠性或服务质量,即信誉信息可以具有一定的模糊性;
- 6) 对于节点间的一次交易,节点优先考虑本域内的诚实节点,其次考虑其他邻居域内的节点。

3.2 信誉衰减

在 TBHPM 中,存在三类节点:诚实节点、自私节点和恶意节点。恶意节点的存在严重影响了 TBHPM 网络性能,必须及时发现,尽早去除。自私节点是那些不积极对外提供服务而一味获取网络资源的具有贪婪性的节点。

自私节点和恶意节点的存在将导致节点间缺乏合作,进而严重影响 TBHPM 的效力。因此,为构建一个和谐的通信环境,引入信誉衰减激励机制和参与阈值的概念。所谓参与阈值是指节点以诚实节点身份参与网络活动的最小参与级别,可以量化为一定时间内节点与其他节点交互的最小次数。当一定时间段内节点与其他节点交互的总次数小于系统要求的最小交互次数时,节点的信任度开始降低;当节点的参与次数增加时,停止信任度衰减。但是要区别对待自私节点和恶意节点,自私节点的信任度降低的程度应当缓慢、平稳,不应像恶意节点那样剧烈。

设节点 M 至时刻 t 时,其交互总次数 $I(M, t)$ 小于网络要求的最小参与次数,则 M 的信任度按公式(7)中以指数方式衰减:

$$T(M, t) = T(M, t_0) \times e^{\frac{-(t-t_0)}{\lambda}} \quad (7)$$

其中 t_0 是节点的参与级别高于参与阈值的最近时刻;常数 λ 决定了节点信任度衰减的速度。若诚实节点、自私节点、恶意节点对应的信任衰减度分别为 $\lambda_1, \lambda_2, \lambda_3$,则依据上述分析,为保证节点行为良好,应有: $\lambda_1 > \lambda_2 > \lambda_3$ 。当自私节点信任度衰减至小于恶意节点的上限时,节点不再参与网络内的交互。因此,信誉衰减机制保证了自私节点将不能永远保持自私性。

3.3 TBHPM 模型的工作机制

TBHPM 的工作机制如图 2,图 3 所示。

1) 每个加入网络的节点既可以是评价节点又可以是评价节点,根据不同的交互背景而变化。每个节点将获得一个唯一的标识/证书,因此保证了网络内的节点不会呈现多重

身份,也不能进行地址哄骗。

2) 每个节点以客户证书的形式本地存储自己的客户信息以供其他节点方便地查询。为防止实体篡改自己的信誉值或者因为不满其他节点对自己信誉值评价而报复评价节点,它的信誉值以信誉证书的形式存储于评价节点^[6]。

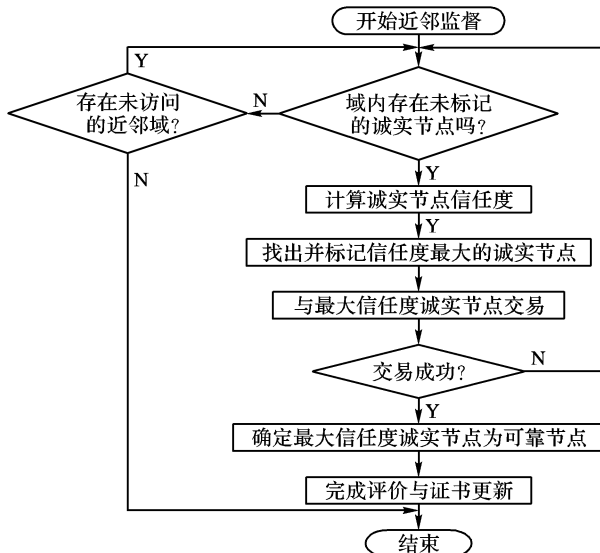


图2 可靠节点的搜索过程

3) 网络内的每个节点执行近邻监督,按2.2节所述,计算本域内节点信任度,识别诚实节点、恶意节点、自私节点,并赋予一定的信任等级。

4) 在本域的诚实节点中,利用冒泡排序等算法挑选信任度最大的节点,加以标记,同时与该节点进行交易。若节点交易成功,则将该节点作为本域内的可靠节点,退出冒泡排序循环,结束最大信任度节点的选择,转至5);否则,在未标记的节点中重复4),直到本域内的所有诚实节点都被访问过,此时转至6)。

5) 上述节点在与可靠节点双方交易完成后,就作为评价者根据交互过程对可靠节点进行评价,以信誉证书形式存储评价的信誉值,并生成新的证书单元附加到被评价节点的客户证书之后,作为以后自己和其他节点判断的依据。可靠节点作为被评价节点向先前已在与之交互的其他评价节点发布证书已经成功更新的通知。如果这些评价节点没有更新证书

或者更新的证书无效,则被评价节点向先前的客户端发出证书没有成功更新的通知,要求当前的客户端正确更新证书。转至7)。

6) 访问相邻的其他域,执行4)。

7) 结束节点间的访问过程。

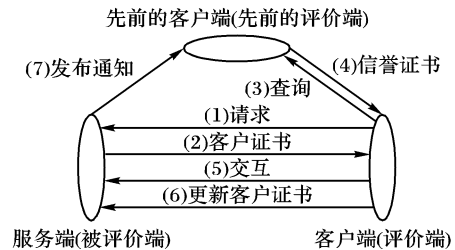


图3 节点间的认证、交互和证书修改过程

4 结语

基于信誉的信任机制的混合式 P2P 模型 TBHPM 可以加强节点间的合作,高效地实现节点间的交易,同时也在一定程度上很好地提高了系统的安全性。当然,随着与可靠节点通信量的增加,可靠节点可能成为网络内的瓶颈。在以后的研究中,需进一步完善这一方面的工作。但是总的说来, TBHPM 在无线通信领域特别是那些对能量、效率要求比较苛刻的对等 Ad hoc 领域都有很好的应用前景。

参考文献:

- [1] PAUL R, KUWABARA KO, ZECKHAUSER R, *et al.* Reputation systems[J]. Communications of the ACM, 2000, 43(12): 45-48.
- [2] 蔡晟, 王泽兵, 冯雁, 等. 基于 Super-peer 的对等网络研究[J]. 计算机应用研究, 2004, 21(6): 258-260.
- [3] WANG Y, VASSILEVA J. Trust and reputation model in peer-to-peer networks[A]. Proceedings of the 3rd IEEE Int'l Conference on Peer-to-Peer Computing[C]. Linköping: IEEE Computer Society, 2003. 150-158.
- [4] SANKHLA V. SMART: A Small World based Reputation System for MANETs[D]. California: University Of Southern California, 2004.
- [5] 窦文, 王怀民, 贾焰, 等. 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.
- [6] 赵恒, 权义宁, 胡子濮. 对等网环境下一种安全有效的信誉体制[J]. 计算机应用, 2005, 25(3): 551-553.

(上接第 2899 页)

和转发数据包,部分节点做简单的判断,因此计算量可忽略。根据三种方法的通信量和计算量可知本文方法节点的能量消耗最小。如图 3(a),本文所用的检测方法在网络中多于一个节点时通信量远低于文献[5]的通信量,如图 3(b)、(c),节点的计算量和能量消耗远小于文献[1,5]中的计算量和能量消耗。

4 结语

Sybil 攻击是一个节点向网络中的其他节点呈现出多个身份,会破坏无线传感器网络的数据融合、资源分配等机制。本文提出了一种检测 Sybil 攻击的方法,能够有效地降低通信量和计算量,节省节点的能量。我们将在以后的工作中对多个身份多个地理位置的 Sybil 攻击形式进行研究,以完善对 Sybil 攻击的检测。

参考文献:

- [1] ZHANG QH, PAN W, DOUGLAS S, *et al.* Defending against sybil attacks in sensor networks[A]. Proceedings of the 25th IEEE Inter-

national Conference on Distributed Computing Systems Workshops (ICDCSW'05)[C]. 2005. 1545-10678.

- [2] YU Y, GOVINDAN R, ESTRIN D. Geographical and energy aware routing: a recursive data dissemination protocol for wireless sensor networks[R]. Technical Report UCLA / CSD-TR-01-0023. UCLA Computer Science Department, 2001.
- [3] YU B, XIAO B. Detecting selective forwarding attacks in wireless sensor networks[EB/OL]. <http://www4.comp.polyu.edu.hk/~csbxiao/files/pub/SSN-06-Selective%20forwarding%20attacks.pdf>, 2006.
- [4] KARLOF C, WAGNER D. Secure routing in wireless sensor networks: attacks and counter-measures[A]. First IEEE Intl. Workshop on Sensor Network Protocols and Applications (SNPA 2003)[C]. Anchorage, AK, USA: IEEE computer Society, 2003. 113-127.
- [5] NEWSOME J, SHI E, SONG D, *et al.* The sybil attack in sensor networks analysis & defenses[A]. Proceedings of Third Intl. Symposium on Information Processing in Sensor Networks (IPSN'04)[C]. Berkeley, California, USA: ACM Press, 2004. 259-268.