基于 P2P的混合安全信任机制研究

汪 瑜

(南京邮电大学 计算机学院, 江苏 南京 210003)

[摘要] 提出了一种非集中管理认证的, 结合局部信任机制以及全局信任机制的 P2P安全信任机制. 该信任机制结合以往信任模型的优点, 既充分利用了 P2P中节点自身的交互历史, 又有效的考虑了整个网络的交互经历, 不仅使安全机制更具有针对性, 网络开销变小, 还推出了合理的惩罚机制, 有效预防冒名、诋毁等问题.

[关键词] P2P, 安全, 信任机制

[中图分类号] TP 311 [文献标识码] A [文章编号] 1672-1292(2008)04-0032-03

Research of Mixed Security Trust Mechanism Based on Peer-to-Peer

Wang Yu

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

Abstract In this paper, we describe a distributed security trust mechanism based Peer-to-Peer, in which local trust mechanism is combined with global trust model. Having considered all good qualities from traditional trust mechanism the mechanism not only takes full advantage of the history interactions between two peers, but also takes into accout interactions among all network. It is of pertinency, and occupies less network bandwidth. Besides, it is of reasonable punishment mechanism, which can avoid security problems effectively, such as pretending and slandering.

Key words P2P, security, trust mechanism

随着 P2P(peer-to-peer, 对等网络)应用的发展, P2P安全问题就一直被人们研究, 许多信任机制也相继出现. 目前除基于 PKI的信任模型外, 还存在以下几种模型:

(1)基于角色的信任模型. 在这个系统中, 依据节点对于不同社区的隶属程度, 决定其在不同方面的可信度. 如 Dynamic Coalitions种中所采用的信任模型.

(2)基于局部推荐. 在这类系统中, 节点通过询问有限的其他节点以获取某个节点的可信度. 其获取的节点可信度也往往是局部的和片面的. 如 Comelli对 Gnutella的改进建议中所采用的就是这种方法.

(3)基于 Bayesian的信任模型. 这类系统是依据一定的参数, 利用 Bayesian概率计算可信度, 其可信度的计算实质上是基于用户自身的主观判断, 往往具有片面性.

(4)数据签名. 这种方法不追求节点的可信度, 而是强调数据的可信度. 然而, 该方法仅针对数据共享应用, 同时无法防止集体欺诈行为. 如 Kazaa采用的就是该方法.

(5)全局可信度模型. 该模型通过邻居节点间相互满意度的迭代来获取节点的全局可信度. 如 Stanford的 EigenRep.

本文针对上述的安全信任模型存在的问题, 以及可信度模型在实际使用中存在的困难, 提出了一种基于 P2P的混合安全信任模型. 该模型结合了局部信任模型及全局信任模型, 除了使安全信任模型更具有针对性, 网络开销变小之外, 还推出了具有合理的惩罚机制, 有效预防冒名、诋毁等问题.

1 混合信任机制设计

1.1 总体设计

相对于以往的 P2P完全模型信任机制, 该信任机制主要是在 P2P应用层与网络模型中增加一个单独

收稿日期: 2008-06-18
基金项目: 华为基金资助项目.
通讯联系人: 汪瑜, 硕士研究生, 研究方向: 软件及其在通信中的应用. E-mail: wy19831226@163.com

的信任度安全机制模型, 该模块主要用于 P2P网络中两节点在交互之前的信任度的评估检测以及交互后的信任度的计算和修改.

该机制主要分为两部分: 一部分为交互前的信任度的检测; 一部分为交互后的对信任度的设置或修改.

交互信任度 T_{ba}是作为两个节点在进行交互之前确定是否可以进行交互的一个属性值, 它可以由几个方面的属性值结合而成; 推荐度 R_a 是全局的, 即相对于整个网络而言, 是两个节点第一次请求交互或者交互信任度刚好为一个临界值时作为交互前的参考值, 确定两节点是否交互的一个属性值.

1 2　算法详细设计

当节点 a请求与节点 b连接交互时, 节点 b首先查看本节点对节点 a的交互信任度 T_{ba}, 若没有或者交互信任度为 0, 则表示节点 b与节点 a没有过交互历史或交互信任度不确定. 此时节点 b通过网络查找节点 a的推荐度 R_a, 根据 R_a 的值最后判断节点 b是否与节点 a交互, 即若 R_a 小于 0, 则放弃连接; 否则, 进行连接交互.

每次交互结束后还需要进行的工作有:

(1) 利用 Bayesian网络模型对本次交互的评价得出一个评价值:

其方法是将交互的服务质量细化为几个不同的方面, 设为 $x = \{x_1, x_2, \ , x_n\}$, 然后对各方面 x_i进行评估得出 Ex_i. 考虑到评估的过程中, 对于每个方面到底给出一个什么样评估值可能拿不准, 我们可以将各个方面给出几个等级, 然后相应的有一个分数段. 对各个方面进行评估以后, 我们就可以计算出一个总的评估值如下:

$$E_x = \quad Wx_i \quad Ex_i, \tag{1}$$

其中 Ex表示总的评估值, 为 $[-1, 1]$区间的实数, Ex_i表示各个方面的评估值, 为 $[-1, 1]$区间的实数, Wx_i是根据各方面的评估在整个评估中作用的分量大小来定的, 其值在 $[0, 1]$之间, 这取决于用户的偏好, 且 $Wx_i = 1$. 并约定如果是一个恶意节点的话, 直接将其拉入黑名单, 不需要进行下面的工作了.

(2) 将本次评价结合以往的交互历史求出本节点对客户节点的交互信任度; 公式如下:

$$T_{rx}^{(k)} = W_x \quad T_{rx}^{(k-1)} + (1 - W_x) \quad E_x, \tag{2}$$

其中 $T_{rx}^{(k)}$表示新的交互信任度, $T_{rx}^{(k-1)}$表示以前的交互信任度, Ex 表示对当前交互行为的评估值, Wx 表示权值, 且 $0 < Wx < 0.5$.

(3) 如果利用了推荐度, 还需要根据本次的评价结果来判断推荐节点所给出的推荐度是否属实, 并根据判断结果修改推荐节点的推荐信任度.

将推荐信任度设定为全局的 (即相对于整个网络而言). 每个节点都有一个推荐信任度 TR_i, 其计算方法为: 第一, 网络中所有节点的推荐信任度初始值都定为 0, 即 $TR_i = 0$; 第二, 当某节点 i对网络中其它两节点在交互前给予过推荐时, 两节点交互后就要通过交互的评价值对节点 i的推荐信任度进行修改; 第三, 假设推荐节点 P_i 对节点 P_x 的交互信任度为 $T_{ix}^{(k-1)}$, 节点 P_i 与 P_x 当前交互的评估为 Ex, 则 P_i 对 P_x 的信任度与当前交互的评估之间的偏离度为:

$$D_ix = | E_x - T_{ix}^{(k-1)} |, \tag{3}$$

其推荐信任度:

$$TR_i^{(k)} = W \quad TR_i^{(k-1)} + (1 - W) \quad F \quad (2 - D_ix)/2, \tag{4}$$

其中 W 为权值, $TR_i^{(k)}$表示新的推荐信任度, $TR_i^{(k-1)}$表示已有的推荐信任度, F 表示一个符号值, 当 Ex与 $T_{mx}^{(k-1)}$同号或其中一个为 0时, $F = 1$, 否则, $F = -1$.

在这里假设要计算节点 x的推荐度, 首先, 我们在节点 x的资源中获得曾与节点 x 有过交互历史的所有节点; 其次, 我们对查找出这些节点按推荐信任度从大到小依次选出 k个节点, 若与之曾交互的所有节点个数都小于 k或者推荐信任度大于 0的节点个数小于 k, 则选出的节点个数可以小于 k; 最后, 计算出推荐度, 假设请求节点为 x节点, 曾与之有过交互历史的节点按推荐信任度 (大于 0)的高低排列为节点 1, 2, , n. 则其推荐度为:

$$Rx = (TR_1 * T_{1x} + TR_2 * T_{2x} \quad + TR_n * T_{nx})/k, \tag{5}$$

其中 $n <= k$, Rx为节点 x的推荐度, TR_1为节点 1的推荐信任度, 且 $TR_n >= 0$, T_{1x}为节点 1对节点 x的交互信任度.

2 仿真与结果分析

2.1 仿真实验设计

该仿真实验用来测评前面构造的信任模型. 在仿真实验中, 把交互服务简化为文件共享服务, 下载文件的真实性是判断一次交互是否成功的惟一标准. 假设节点有两类: 一类是诚实节点, 即它提供真实可信的文件下载服务; 另一类是恶意节点, 即它有可能提供一个假文件下载服务, 也有可能根本就不提供文件下载服务, 也可能在下载的文件中有恶意代码(例如病毒). 在实验中, 假定该网络是理想的, 即任意一个节点可以找到任意文件及其声称为该文件拥有者的所有节点. 用户的行为较为简单, 即从所有声称拥有其所需文件的节点中选择信誉度最高的节点, 从该节点上下载文件.

对于规模为 1 000个节点的仿真网络, 其中 100个恶意节点, 900个诚实节点. 我们将 10 000个文件随机分配给所有节点, 并保证每个文件至少被一个诚实节点拥有. 每个用户在整个仿真过程中必须完成 10次下载, 每次下载目标为从其不曾拥有的文件中随机选择一个并试图进行下载. 成功的下载使得该节点拥有该文件, 失败的下载不会增加该节点拥有的文件.

2.2 仿真实验结果及分析

(1)对整个系统中恶意节点, 判断准确率. 实验 4次, 其实验结果及分析如表 1:

从表 1可以看出对于恶意节点的简单发现率平均达到了 95%左右.

(2)对整个仿真系统中诚实节点的误判率. 实验 4次, 其实验结果及分析如表 2:

从表 2中可以看出恶意节点的误判率是 1.95%左右.

表 1 判断准确率结果及分析

Table 1 The results and analyses of veracity of justice

	第一次实验	第二次实验	第三次实验	第四次实验
恶意节点数	100	100	100	100
正确发现节点数	95	96	97	94
发现率	95%	96%	97%	94%
平均发现率	95.5%			

表 2 误判率结果及分析

Table 2 The results and analyses of miscarriage of justice

	第一次实验	第二次实验	第三次实验	第四次实验
诚实节点数	900	900	900	900
误判节点数	18	16	17	19
误判率	2%	1.78%	1.89%	2.11%
平均误判率	1.95%			

3 结语

本文在 P2P环境下构造了一个基于全局信任度和局部信任度的信任机制, 给出了信任度及推荐度推理的相关算法. 仿真实验与结果分析表明该机制克服了已有安全信任机制的若干局限性, 简单有效, 可以嵌入到各种 P2P软件开发中, 具有良好的工程可行性. 对于如何更好的存储文件的资源信息, 减少网络的开销等问题将是下一步的研究方向.

[参考文献] (References)

[1] Zhang Q, Zhang X, Wen X Z, et al. Construction of peer-to-peer multiple-grain trust model[J]. Journal of Software, 2006, 17(1): 96-107.

[2] Zhang Q, Sun Y, Liu Z, et al. Design of a distributed p2p-base grid content management architecture[C] // Proc of the 3rd Communication Networks and Services Research Conf. New York: IEEE Press, 2005: 339-334.

[3] Huu Tran, Michael Hitchens, Vijay Varadharajan, et al. A trust based access control framework for p2p file-sharing systems [C] // Proceedings of the 38th Hawaii International Conference on System Science-2005. New York: IEEE Press, 2005: 302-308.

[4] Dou W, Wang H M, Jia Y, et al. A recommendation-based peer-to-peer trust model[J]. Journal of Software, 2004, 15(4): 571-583.

[5] Khambatti M, Dasgupta P, Ryu K D. A role-base trust model for Peer-to-Peer communities and dynamic coalitions[C] // Cole JL, Wolthusen SD. Proc of the 2ed IEEE Int'l Information Assurance Workshop. New York: IEEE Press, 2004: 141-154.

[责任编辑: 孙德泉]