

基于角色信任的 P2P 访问控制模型

李致远¹, 毕俊蕾²

(1 江苏大学 计算机科学与通信工程学院, 江苏 镇江 212013; 2 江苏大学 信息化中心, 江苏 镇江 212013)

摘 要: 近年来, 随着对等技术(Peer-to-Peer, P2P)应用的日益广泛, 其安全问题也愈显突出. 由于 P2P 网络的去中心化、动态性且网络规模较大, 使得传统的互联网安全技术不再适用于 P2P 网络. 目前, 对等网络安全机制的研究主要集中在信任管理和认证问题上, 而作为另一个重要的安全保障机制——访问控制, 则一直没有得到应有的重视. 鉴于此, 将基于角色的访问控制模型与 P2P 信任机制相融合, 提出基于角色信任的 P2P 网络访问控制模型(Trust&Role-Based Access Control Model for P2P Networks, TRACM). 最后, 在 P2P 文件共享的应用场景下, 设计和实现了 P2P 网络访问控制模型的原型系统. 实验结果表明 TRACM 模型既能很好地适应去中心化及动态性强的 P2P 网络环境, 又能高效地保障资源和用户的安全.

关键词: 对等网络; 安全; 访问控制; 信任; 角色

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2012)11-0045-05

Role and Trust-Based Access Control Model for Peer-to-Peer Networks

LI Zhi-yuan¹, BI Jun-lei²

(1 Department of Computer Science, Jiangsu University, Zhenjiang 212013, China;

2 Information Center, Jiangsu University, Zhenjiang 212013, China)

Abstract: In recent years, with the increasing development of Peer-to-Peer technology, secure issues have become more and more prominent for Peer-to-Peer networks. Peer-to-Peer networks have some new characteristics, such as decentralized, dynamic characteristics, and large scales, which makes the traditional internet security technology unsuitable for Peer-to-Peer networks. At present, Peer-to-Peer networks security researches mainly focus on the trust management and authentication. However, there is little research on access control mechanisms for Peer-to-Peer networks. In this paper, a role-based access control model is combined with Peer-to-Peer trust mechanism, and then an access control model based on trust and role for Peer-to-Peer Networks is proposed. Finally, under the Peer-to-Peer file-sharing environments, the Peer-to-Peer access control prototype system is designed and implemented. The experimental results show that the proposed scheme not only can well adapt to the decentralized and dynamic Peer-to-Peer network environments, but also can efficiently protect the safety of the resources and users.

Key words: Peer-to-Peer networks; security; access control; trust; role

1 引言

对等网络(Peer-to-Peer, P2P)受到了学术界和产业界的双重关注, 与云计算同时成为网络计算领域的两大主要研究热点, 财富杂志更将 P2P 列为影响 Internet 未来的四项科技之一. 然而, 随着 P2P 技术应用的日益广泛, 其安全问题愈加明显, 非法用

户对数据的篡改、用户隐私窃取、DDoS 攻击及病毒泛滥严重阻碍着 P2P 技术的发展. 目前, P2P 网络安全机制的研究主要集中在信任管理、密钥管理以及认证方面, 而作为网络安全的重要组成部分, 访问控制的研究成果还比较少. 现将 P2P 网络访问控制模型的研究成果分为以下三类: 改进基于角色的访问控制模型^[1-2]、基于风险评估的访问控制模型^[3]和

收稿日期: 2012-05-15; 修回日期: 2012-06-20

基金项目: 国家自然科学基金项目(61202474, 61272074, 61201160, 61103195, 61170065, 61100199)

基于信任的访问控制模型^[4-8]. 其中, 基于角色的 P2P 访问控制模型的主要问题在于没有充分考虑 P2P 网络中节点的动态性及去中心化, 从而使得安全的对等资源共享效率下降. 基于风险评估的访问控制模型的主要问题在于该模型需要大量的历史风险统计信息, 信息量越大决策越准确, 提供安全资源共享的效率也就越高. 然而, 复杂的 P2P 网络环境常常使得风险统计信息量较低、误差较大, 因此, 该模型的误报率较高. 基于信任的访问控制模型是目前 P2P 访问控制模型研究的主流方向, 该模型的优点是能够较好地适应 P2P 网络的动态性及其去中心化特点, 该模型的缺点是容易受到共谋攻击, 共谋攻击会破坏 P2P 网络中节点的信誉系统, 从而使得该访问控制系统存在着极大的授权风险.

针对 P2P 访问控制模型当前存在的问题, 本文提出基于角色信任的 P2P 网络访问控制模型 (Trust&Role-Based Access Control Model for P2P Networks, TRACM). TRACM 模型利用信任管理模型综合节点的局部信誉对 Peer 节点的全局信誉进行量化, 然后, 资源节点利用基于角色信任的 P2P 访问控制模型对资源请求节点进行授权, 从而较好地解决了具有去中心化及动态性强的 P2P 网络访问控制问题. 最后, 在 P2P 文件共享应用场景下, 实现了 TRACM 模型的原型系统.

2 基于角色信任的 P2P 网络访问控制模型

2.1 P2P 信任模型的建立

2.1.1 交互信任度计算

节点的交互信任度是评价节点能力和信誉的标准, 它是基于节点间交互记录产生的. 交互信任度是动态变化的, 每一次交互将得到不同的信誉值. 对节点的信誉计算考虑以下三个因素: 交互过程中节点的上传速率, 交易成功率及下载文件是否为虚假资源或者病毒.

假设节点 i 向节点 j 提出下载请求, 下面给出交互信任度的算法.

(1) 在节点连接时, 节点 i 记录开始时刻 t_s , 交互结束时, 记录结束时刻 t_e , 并计算文件大小 $Size$, 这样可算出文件下载速率 $Speed = \frac{Size}{t_e - t_s}$.

(2) 交易成功后, 节点 i 更新与节点 j 的交互成功次数 S_{ij} 和失败次数 F_{ij} , 当 $S_{ij} = 0$ 时, 节点交互成功率 $RS_{ij} = -10$, 否则节点间的交互成功率 $RS_{ij} = \frac{S_{ij}}{S_{ij} + F_{ij}} * 100$.

(3) 交易完成后, 调用病毒检测系统, 判断下载文件是否含有病毒. 若发现病毒, 则令 $V_{ij} = -20$, 否则为零. 此外, 如果节点 i 发现节点 j 提供的是虚假文件, 则令 $V_{ij} = -10$, 否则为零.

(4) 节点 i 通过式(1)计算与节点 j 的交互信任度 R_{ij} .

$$R_{ij} = \alpha \times \log_2^{Speed} + \beta \times RS_{ij} + \gamma \times V_{ij} \quad (1)$$

其中 $\alpha + \beta + \gamma = 1$.

(5) 按照公式(2)更新节点 i 对节点 j 的交互信任度.

$$R_{ij}^{(k)} = (1 - w) \times R_{ij}^{(k-1)} + w \times R_{ij}^{(k)}, \quad w = 0.4 \quad (2)$$

$R_{ij}^{(k)}$ 表示当前的交互信任度, $R_{ij}^{(k-1)}$ 表示前一个时刻的历史交互信任度.

在 P2P 系统中, 每个节点拥有唯一的 ID 号, 节点 j 作为节点 i 的交易伙伴, 将节点 j 的 ID 号及交互信任度存储在节点 i 上. 因此, 每个节点都会存放一张与其交互过的节点信誉值列表.

2.1.2 全局信任度计算

全局信任度是在节点交易前, 彼此考察对方是否可信的标准. 全局信任度由直接交互信任度和间接交互信任度通过矩阵运算得到. 前面已经阐述了直接交互信任度算法, 下面给出间接交互信任度和全局信任度求解算法.

(1) 间接交互信任度算法

① 节点 i 查询本地存储的直接信誉值表, 检查是否与节点 j 进行过直接交互, 若与节点 j 有交互记录, 则在表中能找出直接信誉值 R_{ij} ; 若无记录, 则转入步骤②.

② 节点 i 向直接信誉值表中的邻居节点 k 发送信誉查询请求.

③ 网络中的邻居节点 k 接收到查询请求后, 检查自己是否与 j 直接交互过. 若有, 则将节点 j 与其交互的直接交互信任度值 R_{kj} 发送给节点 i . 节点 i 接收了邻居节点传送的直接信任度值后, 采用式(3)计算节点 i 到节点 j 的间接信任度值.

$$T_{ij} = \sum_k (R_{ik} \times R_{kj} \times \alpha_k) \quad (3)$$

其中, α_k 表示节点 k 的可信推荐度, 设全网节点的初始可信推荐度为 1, 即假设全网的节点初始时都是可信和合法的.

④ 若仍然没有与节点 j 的交互信息, 则节点 k 的邻居节点继续向它的邻居节点发送查询请求, 直

到查询到与节点 j 有直接交互的节点为止. 然后, 采用式(3)计算节点间的间接信誉值.

(2) 全局交互信任度算法

网络中节点的全局信任值等于全网节点对节点 i 的直接信任向量和间接信任向量的合向量, 为此采用平行四边形法则求解节点的全局信任度.

为了便于算法描述, 无论 k 时刻的直接信任值或间接信任值均采用 $T_{v_{ji}}^{(k)}$ 表示.

算法 1 全局交互信任度计算方法

Input $T_{v_{ji}}^{(k)} \quad j \in [1, n], i \neq j$

Output $T_{v_i}^{(k+1)}$

Procedure

Begin

$$T_{v_i}^{(k)} = \sqrt{(T_{v_{ji}}^{(k)})^2 + (T_{v_{(j+1)i}}^{(k)})^2 - 2T_{v_{ji}}^{(k)} T_{v_{(j+1)i}}^{(k)} \cos \delta}$$

$j=0, \cos \delta$ 是两个信任矢量夹角的余弦值

for ($j=2; j < n-1; j++$)

{

$$T_{v_i}^{(k+1)} = \sqrt{(T_{v_{ji}}^{(k)})^2 + (T_{v_i}^{(k)})^2 - 2T_{v_{ji}}^{(k)} T_{v_i}^{(k)} \cos \delta}$$

$$T_{v_i}^{(k)} = T_{v_i}^{(k+1)}$$

}

End

2.2 基于角色信任的访问控制模型

将上节给出的信任模型结合基于角色的访问控制模型建立基于角色信任的 P2P 访问控制模型, 各模块关系如图 1 所示. 节点收到访问请求后提取相应的参数, 然后综合请求节点的历史行为和当前请求资源的类别及请求操作的种类, 进行信任评估. 根据节点的全局信任度决定节点的角色, 然后基于角色和本地授权策略决定是否允许节点访问. 授权结束后, 节点根据此次交易后的结果, 重新更新历史信息.

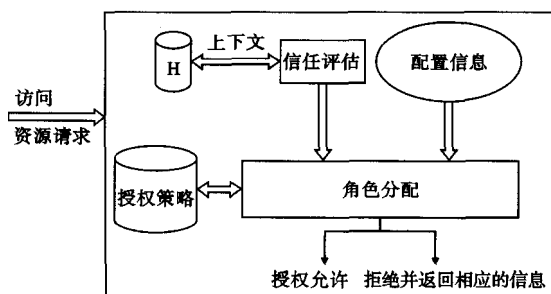


图 1 基于角色信任的访问控制框架

基于角色信任评估的授权模型如图 2 所示.

(1) 节点的全局信任度 T_k 与角色 R 间的关系

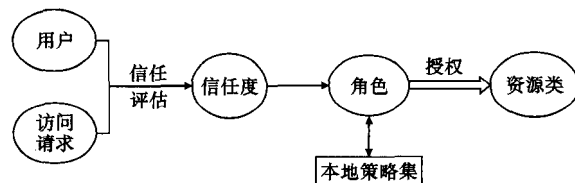


图 2 基于角色信任的授权模型

定义角色集合为 $\{A, B, C, D\}$, $0 \leq T_{v_i} \leq 100$.

$$R = \begin{cases} A, & 0 \leq T_{v_i} < 60 \\ B, & 60 \leq T_{v_i} < 85 \\ C, & 85 \leq T_{v_i} < 95 \\ D, & 95 \leq T_{v_i} < 100 \end{cases} \quad (4)$$

(2) 角色 R 和授权策略集间的关系

定义授权策略集集合为 $\{r(read), w(write), c(copy), d(delete), I(insert)\}$, 上述策略集集合表示节点对数据资源的操作权限.

表 1 角色 R 和策略集的关系

访问需求	需求较低	需求一般高	需求较高	需求非常高
角色	A	B	C	D
权限	r	$r \cup c$	$r \cup c \cup w$	$r \cup c \cup w \cup d \cup I$

3 基于角色信任的 P2P 访问控制模型设计与实现

3.1 模型设计和流程分析

TRACM 模型的基本流程是当资源请求者向资源节点发送服务请求时, 资源提供者首先查询请求节点是否已经通过了身份认证, 如果该节点通过了身份认证, 则启动信任评估模块对该请求节点进行评估, 根据评估结果, 匹配相应的授权规则, 最后根据规则授予相应的访问权限. 系统中的访问控制模块设计如图 3 所示.

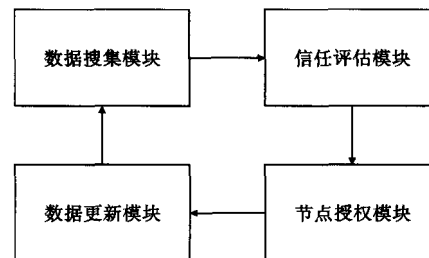


图 3 访问控制模块图

将共享资源分为两类: 一类是所有节点都能访问的资源, 另一类则是仅限好友可以访问的资源. 对于前者, 首先根据请求判断该节点是否在好友列表中, 若在好友列表中, 则仅根据本地评估结果进行授

权, 否则, 表明双方的信任关系尚未建立. 此时, 需根据节点当前的全局信任度对请求节点进行授权. 对于后者, 一旦请求节点不在好友列表内, 就拒绝授予权限. 若在好友列表内, 则根据本地交互历史和当前上下文进行评估, 然后根据规则匹配情况, 授予相应等级的访问权限, 具体流程如图 4 所示.

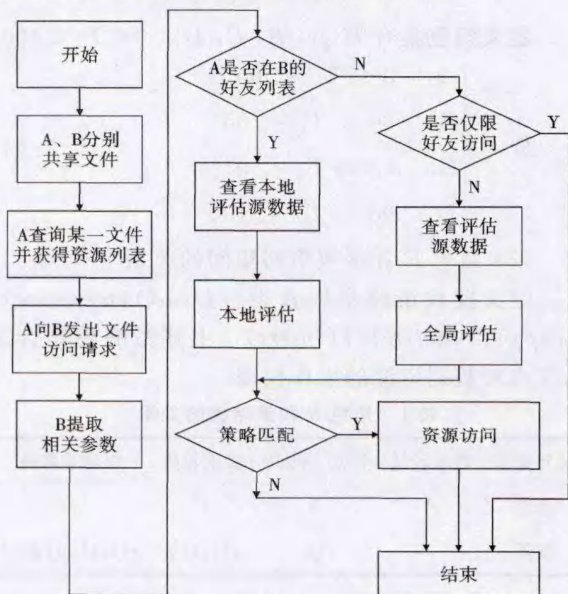


图 4 访问控制流程图

3.2 TRACM 系统实现

(1) 授权结果

当用户在界面上选择“下载”选项时, 文件下载模块通过发起资源访问请求建立请求节点和资源节点间的连接. 资源节点收到连接请求后, 首先查看请求的共享文件是否仅限于好友访问. 如果是, 但资源请求节点不在资源节点的好友列表时, 则需根据该资源的访问级别, 返回下载失败消息. 反之, 则需判断请求节点是否具有访问请求资源的权限. 图 5 表

示共享资源仅限于好友访问时, 资源请求者不在好友列表内的访问结果. 图 6 表示资源允许所有人访问, 但请求者评估值达不到授权要求时的访问结果.

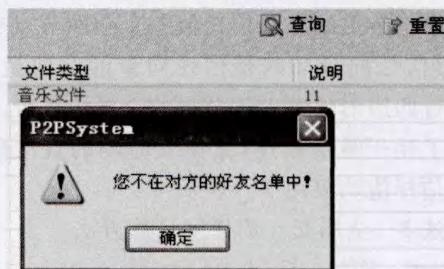


图 5 不是好友, 访问 0 级资源时被拒绝

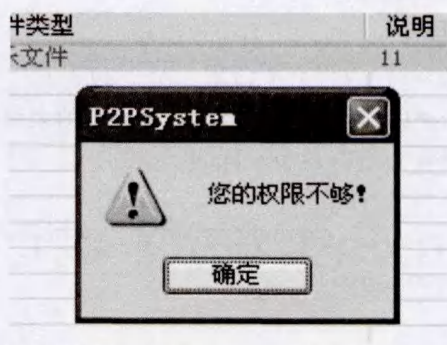


图 6 不是好友, 访问 1 级资源时权限不够

(2) 交易评估记录

节点注册时, 首先在本地生成 XML 文件用来保存用户的评价记录. 节点将对其他节点的评价值存储在该 XML 文件中. 图 7 表示了节点 2 在获得正确文件“Visual C++ 程序设计. zip”(文件 ID 为 785B28F6D26ED572124A2ADD5CFC3D540A2E8BEE)后对资源节点 1, 资源节点 3 和资源节点 4 的评价值, 该信息存储在节点 2 的 XML 中.

P2P安全原型系统									
评价记录									
共享文件ID	节点ID	重...	可...	平...	所...	病...	病...	交互	
785B28F6D26ED572124A2ADD5CFC3D540A2E8BEE	BFBD3AB77B63E7D76505893F	1	1	2	2	1	1	2008	
93E2B6542B4C02088EC16ED80FC2B1D627E42319		1	1	1	1	1	1	2008	
OCF1036513C4560CC0AA50B56569D3E8852B257F		1	1	3	3	1	1	2008	

图 7 节点 2 获得某一文件后的评价记录

4 结束语

本文提出基于角色信任的 P2P 网络访问控制模型 TRACM. TRACM 通过信任管理模型对节点

的局部信誉值进行高效地融合, 从而得到节点的全局信誉值. 然后, 通过建立节点的全局信任度与角色空间的映射关系, 完成基于角色信任的 P2P 网络访问控制模型设计, 之后, 根据该角色访问控制模型完

成对资源节点的授权. 该方案很好的解决了具有去中心化及动态性强的 P2P 网络环境下的访问控制问题. 最后, 在 P2P 文件共享应用场景下, 设计和实现了 TRACM 模型的原型系统, 经测试系统运行良好, 从而证明了方案的可行性、高效性和正确性.

参考文献:

- [1] Maruoka M, Nemati A G, Barolli V, et al. Role-based access control in peer-to-peer (P2P) societies[C]// Proceedings of the 22nd International Conference on Advanced Information Networking and Applications. Okinawa, Japan; IEEE, 2008: 495-500.
- [2] Lu J, Li R, Lu Z, et al, A role-based access control architecture for P2P file-sharing systems using primary/backup strategy[C]// Proceedings of the International Conference on Networks Security, Wireless Communications and Trusted Computing, Wuhan, China; IEEE, 2009: 700-703.
- [3] Diep N N, Hung L X, Zhung Y, et al, Enforcing access control using risk assessment[C]// Proceedings of the Fourth European Conference on Universal Multi-service Networks, Toulouse, France; IEEE, 2007: 419-424.
- [4] 李俊青, 谢圣献, 刘广亮, 等. P2P 网络基于蚁群优化的动态细粒度访问控制框架[J]. 微电子学与计算机, 2008, 25(10): 30-33.
- [5] 刘义春, 张焕国. 基于 Bayesian 信任网络的 P2P 访问控制[J]. 小型微型计算机系统, 2011, 32(6): 1059-1063.
- [6] Chen D H, Le J J, Wei J Y. A peer-to-peer access control management based on web of trust[C]// Proceedings of the International Conference on Future Computer and Communication, Kuala Lumpur, Malaysia; IEEE, 2009: 192-194.
- [7] Bo L. Trust degree based access control for social networks[C]// Proceedings of the International Conference on Security and Cryptography, Athens, Greece; IEEE, 2010: 43-48.
- [8] Wu Z P, Wu H. Access control and resource allocation for peer-to-peer video streaming based on fuzzy logic[J]. Advances in Intelligent and Soft Computing, 2010(75): 237-244.

作者简介:

李致远 男, (1981—), 博士, 讲师. 研究方向为 P2P 网络安全、物联网.

毕俊蕾 女, (1981—), 硕士, 讲师. 研究方向为无线传感器网络、网络安全.

(上接第 44 页)

5 结束语

本文提出了一种新的基于身份的在线/离线加密算法. 简化了节点内部的加密过程, 复杂运算由外部设备计算, 形成离线密文分发给需要发送消息的节点, 供其在在线加密阶段使用. 仿真实验结果与理论分析一致, 证实了本文算法的优势. 与当前几种在线/离线加密算法相比的结果是密文长度较短, 需要的存储量较小, 并在完全模型下可证明达到 CPA 安全. 因此该算法适用于无线传感器网络.

参考文献:

- [1] Boneh D, Franklin M. Identity-based encryption from the weil pairing[C]// Kilian, J. (ed.) CRYPTO 2001. LNCS, Springer, Heidelberg. 2011(2139): 213-229.
- [2] Sun D, Mu Y, Willy S. A generic construction of identity-based online/offline signcryption [C]// ISPA 2008. Australid, Sydney, 2008: 707-712.
- [3] Guo F, Mu Y, Chen Z. Identity-based online/offline

encryption[C]// FC 2008. LNCS, Springer, Heidelberg. 2008(5143): 247-261.

- [4] Liu J, Zhou J. An efficient identity-based online/offline encryption scheme[C]// ACNS, Springer, Heidelberg. 2009(5536): 156-167.
- [5] Chu C, Liu J, Zhou J, et al. Practical ID-based encryption for wireless sensor network[C]// ASIACCS' 10. China; Beijing, 2010.
- [6] Waters R. Efficient identity base encryption without random oracles[C]// Eurocrypt 2005. LNCS 3494. Berlin; Spriner-Verlag. 2005: 114-127.

作者简介:

王昱菲 女, (1988—), 硕士研究生. 研究方向为无线传感器网络、信息安全、计算机通信与网络.



杨庚 男, (1961—), 教授, 博士生导师. 研究方向为无线传感器网络、计算机通信与网络、信息安全.