基于动态线性相关的访问控制模型研究

吴春琼[1] 黄榕宁[2]
(福州大学阳光学院 福州 350015)[1] (福建师范大学数学与计算机科学学院 福州 350117)[2]

摘 要 访问控制是网络资源共享领域的重要研究内容。为了提高访问控制中对未知节点的预测能力,提出了一种基于动态线性相关的访问控制模型。首先,提出了一种包含服务请求者、服务推荐节点和服务提供者的访问控制结构。其次,提出了一种动态的信任值线性计算方法,该方法将节点的全局信任值表示为直接信任值和推荐信任值的线性组合,并根据节点间的历史记录动态地调整直接信任值和推荐信任值的权重。最后通过仿真实验表明,提出的访问控制模型与其他相关的访问控制模型相比,不仅具有更高的预测成功率,而且能更好地抵御节点的恶意攻击。

关键词 访问控制,信任推荐,信任模型,线性组合
中图法分类号 TP319 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.9.019

Dynamic Linear Relevance Based Access Control Model

WU Chun-qiong[1] HUANG Rong-ning[2]
(Yango College, Fuzhou University, Fuzhou 350015, China)[1]
(College of Mathematics and Computer Science, Fujian Normal University, Fuzhou 350117, China)[2]

Abstract The research of access control is an important issue in resource sharing based on networks. In order to improve the prediction ability of access control for unknown nodes, this paper proposed a dynamic linear relevance based access control model. Firstly, we proposed an architecture of access control containing service requestor, service recommendation node and service provider. Then, we proposed a dynamic trust score linear computing approach. The proposed approach represents the global trust score of node with the linear combination of direct trust score and recommendation trust score, and adjusts the weights of direct trust score and recommendation trust score with history records between nodes. Finally, the simulation experiments show that, compared with related access control models, the proposed model has higher prediction success rate, and can resist malicious attacks more efficiently.

Keywords Access control, Trust recommendation, Trust model, Linear combination

随着网络技术的快速发展,资源共享成为了网络的主要应用之一,并普及到人们的日常生活中。在网络资源共享中,通过对不同的资源设置不同的访问权限,信息发布者可以灵活地控制资源的访问控制过程[1]。目前,研究人员对访问控制安全的研究已经取得了很大的进展,现有的信任模型可以分为基于政策的[2]和基于声望的[3]信任模型两类。从系统结构的角度来看,信任模型又可以分为集中式的[4]和分布式的[5]信任管理模型。

EigenRep模型[6]是一种全局信任模型,该模型可以有效地克服恶意节点的欺骗和诽谤攻击。Li等人提出了一种基于相似性的加权信任模型,该模型提出了推荐信任相似性的概念,并且因此提高了信任的可靠性[7]。然而,该模型假设节点的服务兴趣是相同的,忽略了每个服务节点的兴趣具有差异性,并且计算是粗粒度的。基于贝叶斯的信任模型[8,9]通过每个节点的贡献因子计算节点的信任值,该模型忽略了节点的反馈可靠性之间的差异性(不同的兴趣相似性导致不同的反馈可靠性)。随着时间和节点兴趣的动态改变,Li等人[10]基于节点的服务质量对信任的粒度进行了分类,然而该方法并没有考虑节点的服务内容之间的相似性。Fernandez-Gago等人[11]提出了一种P2P环境下的电子商务推荐信任模型,该模型认为信任度与交易值、交易评估和交易时间相关,解决了计算局部声望的问题。该模型虽然考虑了服务概念的相似性,但是忽略了信任是随着时间和交易数量而动态变化的。Bahtiyar等人[12]通过分析发现,全局声望可以提高信任机制应对攻击的能力。

在上述研究中,现有的信任模型没有充分考虑影响信任值的影响力因子,因此这些访问模型在信任值计算时缺乏通用性。本文提出一种包含服务请求者、服务推荐节点和服务提供者的动态访问控制模型。当服务请求者进行服务请求时,目标节点的信任值由直接信任值和推荐信任值线性组合而成。在这种线性组合中,直接信任值的权重随着二者交互次数的增加而增大。

1 访问控制结构

从社会心理学的角度分析,熟悉节点推荐的可信性要比

到稿日期:2014-09-29 返修日期:2014-11-14 本文受福建省省教育厅资助项目(GH-13147)资助。
吴春琼(1972—)女,硕士,讲师,主要研究方向为数据挖掘与网络安全;黄榕宁(1958—),男,硕士,副教授,主要研究方向为计算智能、计算机网络组建。

陌生节点推荐的可信性高。此外，直接向量的熟悉节点的可信性要比间接熟悉节点的可信性高。因此，本文定义节点的全局可信度与如下两个因素相关：

i)节点 i 的全局可信度依赖于与 i 相连接的其它节点的可信度；

ii)可信度评估的客观性和准确性与交易内容的相似性相关。

本文定义的信任模型结构包括服务请求者、服务推荐节点和服务提供者，三者的定义如下。

定义 1(服务请求者) 服务请求者相当于信息共享中信息的访问者，或者网络中的服务评估节点，用符号 E 表示。

定义 2(服务推荐节点) 服务推荐节点向服务请求者推荐服务，其目的是获取相应的信息或者信任度，用符号 SR 表示。

定义 3(服务提供者) 服务提供者相当于信息共享中信息的提供者，或者网络中的服务被评估的节点，用符号 SP 表示。

图 1 是一个简单的网络节点交易图。其中，$C_{a,d}$ 是节点 a 和 d 的交易内容，$C_{b,d}$ 是节点 b 和 d 的交易内容，$C_{c,d}$ 是节点 c 和 d 的交易内容。以 $C_{a,d}$ 为例，a 对 d 的信任值依赖于 $C_{a,d}$ 与 $C_{b,d}$ 以及 $C_{a,d}$ 与 $C_{c,d}$ 之间的相似性，其中 a 为服务请求者，d 为服务提供者，b 和 c 为服务推荐节点。

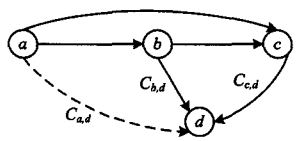

图 1 网络节点交易内容图

给定节点 i，其推荐信任值依赖于 i 的服务推荐节点与服务请求者之间的熟悉度，这种关系在网络中产生一个链式的推荐路径，并且不同的推荐路径具有不同的推荐信任值。节点 i 的推荐信任值是这些推荐路径中最大的推荐信任值。

在节点 a 向节点 d 请求服务时，d 的信任值取决于 a 到 d 的路径的信任值，如图 2 所示。节点 d 的推荐路径为 $a\rightarrow b\rightarrow d$，$a\rightarrow e\rightarrow d$，$a\rightarrow b\rightarrow c\rightarrow d$，$a\rightarrow e\rightarrow b\rightarrow d$ 以及 $a\rightarrow e\rightarrow c\rightarrow d$ 等，节点 d 相对于 a 的信任度取决于这些推荐路径的最大推荐信任值。

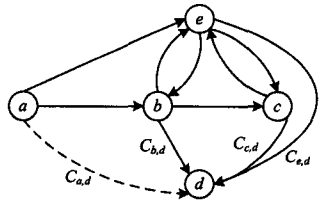

图 2 网络节点信任值推荐路径示意图

2 信任值计算

本文提出一种动态的访问控制模型。在该模型中，全局信任值的计算依赖于服务请求者和目标节点之间的直接信任值以及其它推荐节点的推荐信任值，并且是这二者的线性组合。

2.1 直接信任值计算

直接信任取决于服务请求者和目标节点，直接信任值的计算可通过服务请求者的历史交易记录获得。当 i 作为服务请求者发起交易请求时，其与目标节点 j 之间的直接信任值计算公式如式(1)所示。

$$DT_{i,j}=\frac{S_{i,j}}{G_{i,j}}=\frac{S_{i,j}}{S_{i,j}+F_{i,j}} \tag{1}$$

其中，$DT_{i,j}$ 表示节点 i 与 j 之间的直接信任值；$S_{i,j}$ 表示 i 与 j 之间进行愉快合作的交易数，或者交易的成功率；$F_{i,j}$ 表示 i 与 j 之间进行不愉快合作的交易数，或者交易失败的概率；$G_{i,j}$ 表示 i 与 j 之间进行交易的总数，并且 $G_{i,j}=S_{i,j}+F_{i,j}$。当 i 与 j 之间还没有交易记录即 $G_{i,j}=0$ 时，令 $DT_{i,j}=0.5$。于是，可得：

$$DT_{i,j}=\begin{cases}\dfrac{S_{i,j}}{S_{i,j}+F_{i,j}}, & G_{i,j}\neq 0\\ 0.5, & G_{i,j}=0\end{cases} \tag{2}$$

由于服务请求者和服务提供者之间的关系是单向的，因此 $DT_{i,j}\neq DT_{j,i}$。

2.2 推荐信任值计算

对于推荐节点 k，其推荐信任值的计算如式(3)所示。

$$RT_k=\frac{\sum\limits_{\substack{i,j=1\\ i\neq j}}^{n} Sim(C_{ik},C_{jk})*(\sqrt[3]{\alpha*w_{ik}*DT_{i,k}}+\sqrt[3]{\beta*w_{jk}*DT_{j,k}})}{n} \tag{3}$$

式中，RT_k 表示推荐节点 k 的推荐信任值；C_{ik} 和 C_{jk} 分别为节点 i 和 j 与 k 的交互内容，$Sim(C_{ik},C_{jk})$ 为 C_{ik} 和 C_{jk} 之间的内容相似度；$w_{ik}=DT_{i,k}$ 为熟人推荐权重；陌生人推荐权重 w_{jk} 的初始值为 0.5，表明陌生人的推荐有 50% 的概率是可信的。α 为直接或者间接熟人节点的推荐权重，表示推荐节点对于被推荐节点的信任度，α 的定义为：

$$\alpha=\begin{cases}DT_{i,j}, & i\text{ 和 }j\text{ 直接交互}\\ \dfrac{\sum\limits_{k=1}^{n}\prod\limits_{i\neq j\neq k} DT_{i,k}*DT_{k,j}}{n}, & \text{否则}\end{cases} \tag{4}$$

令 ε 为设定的信任链(路径)的门限值，当 $\alpha<\varepsilon$ 时，放弃该节点。β 为陌生人推荐权重，并且 $\beta=\dfrac{\sum\limits_{i=1}^{n}DT_{i,j}}{n}$。如果 $\sum\limits_{i=1}^{n}DT_{i,j}=0$，那么 $\beta=0$，此时该节点为新加入到系统的节点或者隐匿的节点。

2.3 全局信任值计算

目标节点的全局信任值是一种合成的信任值，表示为直接信任值和推荐信任值的加权和，其计算公式如式(5)所示。

$$GT=\begin{cases}RT, & s=0,\tau\neq 0\\ DT, & s\neq 0,\tau=0\\ \rho*DT+(1-\rho)*RT, & s\neq 0,\tau\neq 0\end{cases} \tag{5}$$

其中，s 为推荐节点个数；τ 为服务请求者和目标节点之间的直接交易个数；ρ 为服务请求者和目标节点之间进行直接交易的权重；$1-\rho$ 为推荐信任值的权重。$\rho(x)$ 为交互个数 x 的动态函数，其计算公式如下：

$$\rho(x)=1-\left(\frac{1}{2}\right)^{\frac{x}{n-x}} \tag{6}$$

其中，$n\in\{1,2,3,\cdots\}$，x 为一段时间内服务请求者和目标节点之间的第 x 个交互，并且 $n-x\neq 0$。

当 x 的取值越大时，ρ 的值越大。当服务请求者和目标节点进行第一次交互时，服务请求者将更依赖于其它节点的推荐信任值。随着服务请求者和目标节点之间交互次数的增多，服务请求者将更多地依赖其自身的交互经验来进行目标

节点的信任值计算。因此，其它推荐节点的推荐权重将逐渐减小，ρ 的值随着交互次数 x 的增加逐渐变大。

3 实验分析

本节通过仿真实验对提出的模型进行评估。该实验在一个包含 15 个节点和 81 个项的小规模网络中进行。其中 81 个项被随机分配到 15 个节点中，并且保证每个节点最少包含一个项，最多包含 15 个项。实验采用的平台为普通 PC，操作系统为 Ubuntu 11.04，算法通过 Java 编程语言实现。在实验中，令信任值的门限值 $\varepsilon=0.3$。

3.1 节点类型定义

在仿真实验中，参与交易的节点属于两种类型，即正常节点和恶意节点。恶意节点又进一步分为完全恶意节点和协作恶意节点。

完全恶意节点有两个主要目的：一是提供虚假信息或者服务；二是诋毁正常节点提供的信息或者服务。协作恶意节点也包含两个目的：一是这些节点间相互进行恶意好评从而夸大信息或者服务的质量；二是与其它协作恶意节点共同诋毁正常节点提供的信息或者服务。

3.2 性能评价指标

本实验采用的性能评价指标为预测的成功率。在每组仿真实验结束后，预测的成功率为服务请求者与正常节点进行成功交易的个数与全部交易个数的比值。成功的交易为服务请求者向正常节点(服务提供者)进行的服务请求，失败的交易为服务请求者向恶意节点(服务提供者)进行的服务请求。

3.3 实验结果

为了验证本文提出的访问控制模型的性能，实验将本文提出的模型与 EigenRep 模型和 Hassan 模型[13]进行了对比。

首先，实验对比了本文提出的模型与 EigenRep 模型的成功率随着恶意节点比例的变化，实验结果如图 3 所示。在本组实验中，恶意节点既包含完全恶意节点，又包含协作恶意节点。图 3 中的横坐标表示恶意节点占所有节点的比例，纵坐标表示交易的成功率。从中可以看出，随着恶意节点比例的不断增大，两种算法的成功率都逐渐减小。在两种算法的对比中，本文提出的信任模型的成功率始终大于 EigenRep 算法的成功率。当恶意节点的比例为 0.5 时，EigenRep 算法的成功率已经低于 40%，而本文提出的信任模型的成功率却仍然高于 60%。

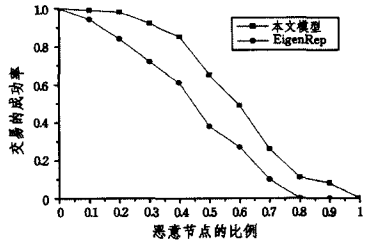

图 3 交易的成功率随着恶意节点比例的变化

然后，实验分析了本文提出的模型与 EigenRep 模型的成功率随着交易个数的变化，实验结果如图 4 所示。横坐标表示实验模拟的交易个数，纵坐标表示算法的成功率。仿真实验中，在原有交易记录的基础上每次增加一定数量的交易记录(10 个)，并对比两种算法的成功率。从图 4 中可以看出，随着交易个数的增加，两种算法的成功率都有所增加；EigenRep 算法的成功率增长缓慢，而本文提出的信任模型的成功率增长迅速，并且明显高于 EigenRep 算法。其原因在于：在式(5)定义的全局信任值计算中，服务请求者和目标节点之间进行直接交易的权重 ρ 随着直接交易个数的增加而增加；此外，在仿真过程中，随着交易个数的增加，直接交易的个数也增加，因此本文提出的信任模型的成功率随着交易数量的增加迅速增长。

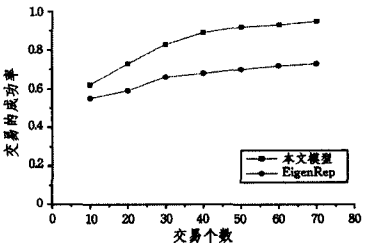

图 4 交易的成功率随着交易个数的变化

最后，实验对比了本文提出的模型与 Hassan 模型对恶意节点的攻击的抵御能力。本组实验中，在原有交易记录的基础上每次增加 10 个攻击，并观察两种模型对攻击的识别能力，实验结果如图 5 所示。横坐标为攻击的个数，纵坐标为攻击的识别率。从图 5 可以看出，随着攻击个数的增加，Hassan 模型对攻击的识别能力逐渐降低；而本文提出的信任模型对攻击的识别能力虽然有所降低，但是基本上保持在 80%以上。Hassan 模型虽然对信任值的推荐攻击有一定的识别能力，但是存在以下缺点：1) Hassan 模型假设推荐节点有着较高的信任值；2) Hassan 模型缺少惩罚机制，不能有效地弱化恶意推荐节点的影响力。由于 Hassan 模型具有上述两个缺点，因此其交易的成功率(即对攻击的识别能力)快速下降。

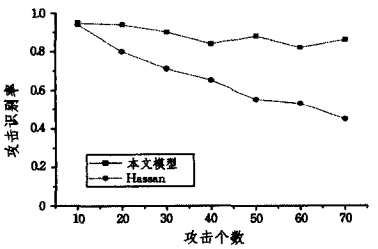

图 5 攻击的识别率随着攻击个数的变化

结束语 访问控制是网络资源共享领域的重要研究内容。本文提出一种包含服务请求者、服务推荐节点和服务提供者的动态访问控制模型。当服务请求者进行服务请求时，目标节点的信任值由直接信任值和推荐信任值线性组合而成。在这种线性组合中，直接信任值的权重随着二者交互次数的增加而增大。仿真实验表明，本文提出的访问控制模型与相关的访问控制模型相比，不仅具有更高的预测成功率，而且能更好地抵御节点的恶意攻击。

参 考 文 献

[1] Al-Slamy D N M A. E-Commerce security[J]. IJCSNS International Journal of Computer Science and Network Security, 2008, 8(5): 340-344

[2] 李凤华，苏铓，史国振，等. 访问控制模型研究进展及发展趋势[J]. 电子学报，2012，40(4)：805-813
Li Feng-hua, Su Mang, Shi Guo-zhen, et al. Reasearch Status and Development Trend of Access Control Model[J]. Acta Electronica Sinica, 2012, 40(4): 805-813

(下转第 106 页)

的情形。用干扰对齐和干扰中和相结合的方法，分析了该共存网络最大可达自由度，并给出了自由度上界，得出3种感知情况的自由度的上下界是紧的。通过比较发现：在接收端进行感知获得的最大可达自由度与没有感知的三用户IC的自由度值相同；而在发射端进行感知可以获得更大的自由度。

参考文献

[1] Cadambe V R, Jafar S A. Interference Alignment and Spatial Degrees of Freedom for the K User Interference Channel[C]// ICC. 2008:971-975

[2] Cadambe V R, Jafar S A. Interference alignment and degrees of freedom of the k-user interference channel[J]. IEEE Transactions on Information Theory, 2008, 54(8):3425-3441

[3] Tresch R, Guillaud M, Riegler E. On the achievability of interference alignment in the K-user constant MIMO interference channel[C]// IEEE/SP 15th Workshop on Statistical Signal Processing, 2009(SSP'09). IEEE, 2009:277-280

[4] Yetis C M, Gou T, Jafar S A, et al. Feasibility conditions for interference alignment[C]// Global Telecommunications Conference, 2009(GLOBECOM 2009). IEEE, 2009:1-6

[5] Suh C, Tse D. Interference alignment for cellular networks[C]// 46th Annual Allerton Conference on Communication, Control, and Computing. IEEE, 2008:1037-1044

[6] Bolcskei H, Thukral I J. Interference alignment with limited feedback[C]// IEEE International Symposium on Information Theory, 2009(ISIT 2009). IEEE, 2009:1759-1763

[7] Lee N, Lim J B, Chun J. Degrees of freedom of the MIMO Y channel: Signal space alignment for network coding[J]. IEEE Transactions on Information Theory, 2010, 56(7):3332-3342

[8] Ning H, Ling C, Leung K K. Feasibility condition for interference alignment with diversity[J]. IEEE Transactions on Information Theory, 2011, 57(5):2902-2912

[9] Gou T, Jafar S A, Wang C, et al. Aligned interference neutralization and the degrees of freedom of the 2×2×2 interference channel [J]. IEEE Transactions on Information Theory, 2012, 58(7):4381-4395

[10] 周璐娜，刘锋，曾连荪. CSIT对无线MIMO网络自由度的影响[J]. 计算机应用研究，2014，31(12)：3813-3817
Zhou Lu-na, Liu Feng, Zeng Lian-sun. Influence of CSIT on degrees of freedom of wireless MIMO networks[J]. Application Research of Computer, 2014, 31(12):3813-3817

[11] Kim J, Park S H, Sung H, et al. Sum rate analysis of two-cell MIMO broadcast channels: spatial multiplexing gain[C]// IEEE International Conference on Communications (ICC), 2010. IEEE, 2010:1-5

[12] Shin W, Lee N, Lim J B, et al. On the design of interference alignment scheme for two-cell MIMO interfering broadcast channels[J]. IEEE Transactions on Wireless Communications, 2011, 10(2):437-442

[13] Lee N, Shin W, Heath R W, et al. Interference alignment with limited feedback for two-cell interfering MIMO-MAC[C]// International Symposium on Wireless Communication Systems (ISWCS). 2012 IEEE, 2012:566-570

[14] 周璐娜，刘锋，曾连荪. 两个点对点(PTP)网络并存时的自由度研究[J]. 计算机科学，2015，42(1)：110-112
Zhou Lu-na, Liu Feng, Zeng Lian-sun. Research on degrees of freedom of two PTP networks coexistence [J]. Computer Science, 2015, 42(1):110-112

[15] Chaaban A, Sezgin A. Interference alignment and neutralization in a cognitive 3-user MAC-interference channel: degrees of freedom[C]// 12th Canadian Workshop on Information Theory (CWIT 2011). IEEE, 2011:26-29

[16] Jafar S A, Shamai S. Degrees of freedom region of the MIMO X channel[J]. IEEE Transactions on Information Theory, 2008, 54(1):151-170

[17] Huang C, Jafar S A. Degrees of freedom of the MIMO interference channel with cooperation and cognition[J]. IEEE Transactions on Information Theory, 2009, 55(9):4211-4220

(上接第96页)

[3] Xiang Y, Ling Y. The Research on Chinese Taxation Policies Based on E-commerce Model Classification [C]// ISECS'09. Washington DC, USA, 2009:431-434

[4] Li Q. Analysis on Channel Information and Control Structure Performance in Food Supply Chain Under E-commerce Environment [C]// ISISE'09. Washington DC, USA, 2009:119-121

[5] Xia Y, Li Q, Wang L. Research on Decentralized E-commerce Architecture in P2P Environment [C]// ICECE'10. Washington DC, USA, 2010:2929-2932

[6] Fan X, Li M, Ren Y. Dual-EigenRep: A Reputation-Based Trust Model for P2P File-Sharing Networks [C]// UIC-ATC'10. Washington DC, USA, 2010:358-363

[7] Li J, Wang X, Chen Y, et al. A Reputation Management Framework Based on Global Trust Model for P2P Systems [C]// ICCS'06. Berlin, Heidelberg, 2006:896-899

[8] 刘武，段海新，张洪，等. TRBAC：基于信任的访问控制模型[J]. 计算机研究与发展，2011，48(8)：1414-1420
Liu Wu, Duan Hai-xin, Zhang hong, et al. TRBAC: Trust Based Access Control Model[J]. Journal of Computer Research and Development, 2011, 48(8):1414-1420

[9] Mehdi M, Bouguila N, Bentahar J. A QoS-Based Trust Approach for Service Selection and Composition via Bayesian Networks [C]// ICWS'13. Washington DC, USA, 2013:211-218

[10] 李唯冠，赵逢禹. 带属性策略的RBAC权限访问控制模型[J]. 小型微型计算机系统，2013，34(2)：328-331
Li Wei-guan, Zhao Feng-yu. RABC Permission Access Control Model with Attribute Policy[J]. Mini-micro Systems, 2013, 34(2):328-331

[11] Fernandez-Gago C, Agudo I, Lopez J. Building Trust from Context Similarity Measures[J]. Comput. Stand. Interfaces, 2014, 36(4):792-800

[12] Bahtiyar S, Caglayan M U. Security Similarity Based Trust in Cyber Space[J]. Know-Based Syst. 2013, 52(2):290-301

[13] Rahmani M. Software modeling & design: UML, use cases, patterns, & software architectures by Hassan Gomaa [J]. ACM SIGSOFT Software Engineering Notes, 2011, 36(4):35-45

[14] 林庆国，刘宴兵. 一种基于信任的动态访问控制策略[J]. 重庆邮电大学学报(自然科学版)，2010，22(4)：478-482
Lin Qing-guo, Liu Yan-bing. A trust-based dynamic access control scheme[J]. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition), 2010, 22(4):478-482