

群组协同决策中基于决策者可信的信任模型研究

彭 涛^{1,2}, 窦万峰^{1,2}

(1 南京师范大学 计算机科学与技术学院, 江苏 南京 210097
2 江苏省信息安全与保密技术工程研究中心, 江苏 南京 210097)

[摘要] 针对群组协同决策支持系统的特点, 提出了基于决策者可信的信任模型. 该模型通过决策者实体的历史行为证据来建立实体之间的信任关系, 评估分布式环境下动态的决策者的可信度. 给出了基于历史交互行为的直接信任度、间接信任度和通过信息熵理论来计算决策者的总体信任度的计算方法, 为系统的安全决策提供了有效的解决方案. 通过模拟实验验证了该信任模型的可靠性.

[关键词] 信任模型, 群组协同决策支持系统, 信任关系, 决策者可信

[中图分类号] TP311 [文献标识码] A [文章编号] 1672-1292(2010)02-0079-05

Research on Trust Model Based on Trusted Decision Makers in Group Collaborative Decision Making

Peng Tao^{1,2}, Dou Wan feng^{1,2}

(1 School of Computer Science and Technology, Nanjing Normal University, Nanjing 210097, China
2 Jiangsu Research Center of Information Security & Privacy Technology, Nanjing 210097, China)

Abstract This paper presents a trust model based on trusted decision makers with the characteristics of Group Collaborative Decision Supported Systems (GCDSS). The trust model establishes the trust relationship among entities and evaluates the trust value of dynamic decision makers in distributed environment by historical actions of decision makers. The paper proposes a method of direct trust value computation, indirect trust value computation based on historical actions and integrated trust value computation by using entropy theory, which provides an effective resolvent for secure decision making. Lastly, the paper validates the reliability of the trust model by simulation experiment.

Key words trust model, GCDSS, trust relationship, trusted decision makers

随着计算机网络技术的发展, 大规模分布式系统的应用越来越广泛, 安全日益成为影响系统效率的重要问题. 系统的形态正从面向封闭、熟识用户群体的静态形式, 向开放、公共可访问的动态协作的服务模式转换^[1]. 传统的安全技术和手段, 尤其是安全授权机制, 如访问控制列表 (ACL)、公钥证书体系 (如 X.509、PGP) 等依靠可靠的第三方授权认证的方法, 已不能够有效解决动态的 Web 应用中的安全问题.

信任是社会情形中的基本特征, 在工业环境中具有重要的作用, 在群组协同工作环境中尤为重要. 群组协同决策支持系统是决策支持系统和计算机支持协同工作 (CSCW) 理论共同发展的产物, 需依靠网络环境下多个动态决策者协同工作来完成复杂的任务. 但在网络环境下由于决策者实体的动态性和不确定性, 使得群组决策专家难以区分和选择可信的决策者. 例如在电子商务和电子政务等需要群众广泛参与决策的应用中, 更难以控制决策者的可信, 致使决策结果的可信度不高, 甚至一些决策者为恶意实体. 不可信的决策者往往会给整个决策环境带来很大风险, 特别是在应急决策系统中的损失更是不可估量. 在协同决策过程中, 由于动态协同的需要, 各个决策者之间的关系并不是固定不变的, 决策者集合和决策任务的分配也是动态变化的, 这就需要一种安全可靠的方法来评估决策者实体的可信度, 保障决策过程中的可信决策问题.

收稿日期: 2010-01-16
基金项目: 江苏省高校自然科学基金 (07KJD520112).
通讯联系人: 窦万峰, 博士后, 副教授, 研究方向: 协同软件开发、计算机支持的协同工作等. E-mail: douwanfeng@njnu.edu.cn

1 相关工作

1996 年, Blaze M 等人为解决 Internet 网络服务的安全问题, 首次使用了“信任管理 (trust management)”的概念^[2], 并将其定义为“一个统一的方法定制和诠释安全策略, 安全凭证, 以及允许直接授权关键性安全操作的信任关系”。随后出现了大量的由静态的安全控制策略向动态的信任机制发展的研究成果。本文将信任机制的研究进展按时间先后和可信决策的解决方案分为如下 3 个方面:

(1) 基于策略的信任机制研究.

计算机领域的信任研究最早是从基于策略的研究开始, 主要使用基于访问控制策略和信任证相结合的方式来进行信任管理. 其基本内容包括: 制定安全策略、获取安全凭证、判断安全凭证是否满足相关安全策略, 最终综合本地安全策略和获取第三方的信任证来进行安全决策. Blaze M 提出的信任管理系统 PolicyMaker 和 KeyNote 都是基于策略的方法.

(2) 基于属性的信任机制研究.

基于策略的信任研究本质上是以一种精确的、理性的方式来描述和处理复杂的信任关系. Winsborough 等人^[3]称这类信任管理系统为基于能力的授权系统, 它们仍需要服务方预先为请求方颁发指定操作权限的信任证, 无法与陌生方建立动态信任关系. 于是提出了依赖主体属性授权的方法, 该方法通过实体属性请求和展示的方法来协商建立实体之间的信任关系, 并且将实体与访问许可权之间引入角色的概念, 把实体与特定的一个或多个角色相联系.

(3) 基于信任度的信任机制研究.

基于策略和基于属性的信任机制是建立在一种理性的证据和自身属性基础上的. 其信任关系的刻画是二值的, 即信任和不信任, 没有刻画实体之间的信任程度. Rahman 等人^[4]则认为信任是非理性的、是一种经验的体现, 不仅要有具体内容, 还要有程度的划分, 并提出了一些基于此观点的信任度评估模型. 该模型建立在数学模型基础上, 用数学建模的方法表示、评估和计算信任度的大小, 从而进行可信决策.

Beth 等人^[5]提出了一种基于经验和概率统计的信任模型, 引入经验的概率来表达和度量信任关系, 并给出了信任的传递和综合计算公式. Wang 等人^[6]利用贝叶斯方法对 P2P 节点的可信度进行评估, 建立动态节点间的信任关系.

目前, 国内外学者在群组协同决策支持系统中信任机制的研究才刚刚开始, 几乎没有相关的研究成果. 本文结合群组协同决策的信任需求, 提出了通过决策者实体的历史行为证据来评估、计算决策者实体的可信度, 以可信度作为动态决策者选择的依据, 实施可信的决策.

2 信任模型

2.1 信任的定义和表示

目前尚未对信任的定义达成共识, 信任的定义都是根据具体的研究背景提出的, 在不同的领域里的定义、计算和表示不同. 本文将信任定义为“在一定的上下文环境中, 群组决策专家对分布式环境下决策者提供资源、服务和决策能力的期望, 以及决策者参与决策的安全性和决策结果的可靠性”.

信任的概念是模糊的, 这种相信的程度是一种信念, 是主观的, 但又是根据经验、各方面的知识以及对客观情况的了解, 利用收集到的信息进行分析推理、综合判断而得到的. 信任的大小用信任度来度量, 本文将信任度设置为一个 $[0, 1]$ 之间的值.

将网络环境下的各个实体的信任关系用关系网来表示, 如图 1 所示. 在信任关系网中, 用节点代表实体, 实体集为某一区域实体的集合, 表示为 $V = \{A, B, C, D, E, F, G, H, I, J\}$. 用边来表示实体之间的交互关系和信任关系, 如 $VR = \{\langle A, B \rangle, \langle A, J \rangle, \langle B, I \rangle, \dots, \langle D, E \rangle\}$, 即存在直接或间接的信任关系. 由于信任具有非对称性, 每一条边上都存在着两个权值. 例如实体 A 和 B 之间的边 $\langle A, B \rangle$ 有 DT_{AB} 和 DT_{BA} 两个值, 分别表示实体 A 对实体 B 的直接信任度 DT_{AB} 和实体 B 对实

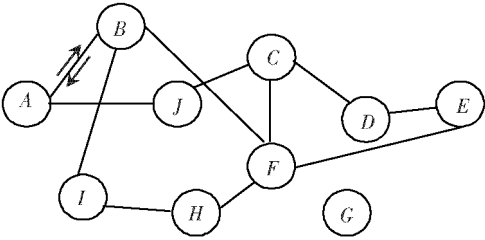


图 1 信任关系网

Fig.1 Trust relationship network

体 A 的直接信任度 DT_{BA} . 这里的 DT_{AB} 和 DT_{BA} 不一定相等.

2.2 信任度评估

2.2.1 直接信任度计算

直接信任度的计算是建立在群组决策专家与决策者实体之间的直接交互历史记录上的, 通过分析交互记录, 并结合时间衰减性、内容相关性等因素计算决策者实体的信任值.

定义 1 直接信任度: 实体 E_i 对实体 E_j 之间发生了 n 次直接交互, 其中每次交互完成后都有服务请求方评价的交互满意度 $E_{ij} = \{e_{ij}^1, e_{ij}^2, \dots, e_{ij}^n\}$, 其中 $0 \leq e_{ij}^n \leq 1$ 有满意的服务和不满意的服务. 设交互满意度的阈值为 Q , 则所有大于 Q 的值组成交互成功的集合 $A_{ij} = \{\alpha_{ij}^1, \alpha_{ij}^2, \dots, \alpha_{ij}^p\}$, 所有小于 Q 的值组成交互失败的集合 $B_{ij} = \{\beta_{ij}^1, \beta_{ij}^2, \dots, \beta_{ij}^q\}$, 则实体 E_i 对实体 E_j 第 $n+1$ 次交互成功的可能性定义为此次信任评估的直接信任度, 表示为 DT_{ij} . 直接信任度的计算方法如式 (1) 所示:

$$DT_{ij} = \begin{cases} Q & \text{if } \sum_{m=1}^p \alpha_{ij}^m < \sum_{s=1}^q (1 - \beta_{ij}^s), \\ \frac{\sum_{m=1}^p (\alpha_{ij}^m \cdot \phi_c) \cdot \theta_t + 1}{\sum_{m=1}^p (\alpha_{ij}^m \cdot \phi_c) \cdot \theta_t + \sum_{s=1}^q ((1 - \beta_{ij}^s) \cdot \phi_c) \cdot \theta_t + 2}, & \text{else.} \end{cases} \quad (1)$$

式中, θ_t 为时间衰减因子, ϕ_c 为内容相似因子. 对于近期发生的交互, θ_t 取值为 1 随着交互记录距今时间的增加而逐渐减小. 由于群组协同决策的动态性、决策任务的实时性等特点, 使得参与者对于一个不了解、内容不相关领域的决策能力会有所下降. 所以, 这里给出内容相似因子 ϕ_c , 将本次决策任务的内容和历史记录中提供的服务进行比较, 若提供的服务类似则取值为 1 否则取一个小于 1 的值, 表示没有相关服务决策经验的决策者的可信度会下降.

2.2.2 间接信任度计算

在开放网络环境中, 两个实体之间常常存在多条信任链. 如图 1 所示, 实体 A 对实体 C 的间接信任度可以通过信任链 $A-B-F-C$ 和 $A-J-C$ 来获得. 间接推荐的信任存在如下几个原则:

原则 1 某条推荐路径中, 最终得到的间接信任度不大于任一推荐者的信任值, 也不大于被推荐实体的直接信任值.

原则 2 从多条推荐路径中得到的间接信任度不小于所有的推荐路径得到的信任度.

原则 3 推荐路径中, 某一推荐实体不能同时作为两条路径中的推荐者.

原则 4 推荐路径中不能存在环, 即不能存在二次推荐.

定义 2 间接信任度: 设实体 E_i 对实体 E_j 之间存在着 N 条信任链, 其中每条信任链中通过 $M(N)$ 个实体相连, 并向 E_i 提供 E_j 的相关信任信息, 则 E_i 通过 N 条信任链中的实体获得的关于实体 E_j 的信任度为 E_i 对 E_j 的间接信任度, 表示为 IDT_{ij} . 计算方法如式 (2) 所示:

$$IDT_{ij} = \begin{cases} Q & N = 0 \\ \sum_{m=1}^N W_m \cdot TL_m, & N > 0 \end{cases} \quad (2)$$

式中, TL_m 为第 m ($1 \leq m \leq N$) 条推荐路径上获得的信任度, $0 \leq TL_m \leq 1$; W_m 为第 m 条推荐路径的权值, 表示请求实体对该条路径上推荐者的信任程度, 其大小根据推荐者自身的信任度以及推荐传递层次计算得到. 对于第 m 条推荐路径中有 $M(m)$ 层推荐的推荐信任度, TL_m 计算如式 (3) 所示:

$$TL_m = \prod_{d=1}^{M(m)} RT_{id}^m \times DT_{M(m)_{last}j} \quad (3)$$

式中, $DT_{M(m)_{last}j}$ 为最后一层中与实体 E_j 有直接交互的实体对其的直接信任度; RT_{id}^m 为实体 E_i 关于第 m 条路径上推荐者的信任度. 由于推荐层次的增加会导致推荐的信息偏差增加, 所以在本文中选择 $M(m) \leq 3$ 控制推荐的层次以保证推荐信息的准确性.

2.2.3 总体信任度计算

定义 3 总体信任度: 实体 E_i 对实体 E_j 的信任程度, 也即总体信任度, 表示为 T_{ij} . 总体信任度是判断

实体行为可信的最终依据,计算方法如式(4)所示:

$$T_{ij} = \begin{cases} DT_{ij} & n \geq \delta \\ W_d \cdot DT_{ij} + W_{id} \cdot IDT_{ij} & n < \delta \end{cases} \tag{4}$$

式中, W_d 和 W_{id} 分别为直接信任度和间接信任度的权值. 当直接交互次数 n 大于一个给定的阈值 δ 时, 则不必考虑间接的推荐信任, 因为实体自身足够的交互经验足以判断另一实体的信任度. 权值的大小根据直接信任度和间接信任度自身的不确定性来设定. 这里采用的信息熵理论, 直接信任度的熵函数如式(5)所示, 权值计算方法如式(6)所示:

$$H(DT_{ij}) = -DT_{ij} \log_2(DT_{ij}) - (1 - DT_{ij}) \log_2(1 - DT_{ij}), \tag{5}$$

$$W'_d = \begin{cases} 1 - \frac{1}{\log^P} H(DT_{ij}), & DT_{ij} > 0.5 \\ H(DT_{ij}) - 0.5 & DT_{ij} \leq 0.5 \end{cases} \tag{6}$$

式中, P 为本次交互过程中定义的评估等级数. 在群组协同决策系统中可将信任分为 5 个级别: 完全信任、比较信任、一般信任、不信任以及完全不信任. 间接信任度权值的计算方法同间接信任度计算方法一样. 最终得到直接信任度和间接信任度的权值分别为: $W_d = \frac{W'_d}{W'_d + W'_{id}}$ 和 $W_{id} = \frac{W'_{id}}{W'_d + W'_{id}}$.

3 模拟实验

本文采用 NetLogo^[7] 平台模拟实现一个分布式网络环境下多个决策者实体交互的环境, 验证文中提出的信任模型的可靠性. NetLogo 平台是美国西北大学网络学习和计算机建模中心推出的可编程的建模环境, 使用 turtles patches links 和 observer 四类主体来模拟现实世界中的各种实体和交互情况.

设系统中有 500 个 turtles 代表分布式环境中的实体. 这些实体能够提供 1 000 种服务, 每个实体能提供 30 种不同的服务, 所以当群组专家请求某个服务时, 可以有 15 个不同的参与者能够提供. 提供的能力根据信任等级平均分成 5 类. 设系统中存在 20% 的实体是恶意推荐者, 其中一半是具有诋毁和它有过交互的决策者实体的特点, 一半是具有夸大和它有过交互的决策者实体的特点, 其他的推荐者均为诚实的实体. 信任模型中其他的参数设置如下:

为方便实验操作, 设置时间因子 0, 对于最近 30 次交互记录设置为 1, 以后以 30 次交互为时间窗进行 90% 的交互满意度的衰减. 对于决策者实体历史交互记录中有与群组决策专家请求的服务相同的服务时, 内容相似度因子 φ_c 为 1, 否则均设置为 0.9 直接交互次数阈值 δ 设为 50 次. 推荐者最小信任度和决策者选择的阈值均设置为 0.5

信任模型可靠性的衡量标准是成功决策率 SD (SD = 可信决策的次数 / 系统中总的决策请求次数). 其中, 可信决策定义为群组决策专家最后选择的决策者实际的服务能力大于决策者选择的阈值. 将本文信任模型与 Wang 等人信任模型相比较, 实验结果如图 2 所示.

从图 2 可以看出, 在交互较少时本文信任模型的 SD 同 Wang 等人的信任模型差不多, 但随着交互次数的增加, 本文信任模型的 SD 也逐渐增大, 可信决策的成功率明显高于后者.

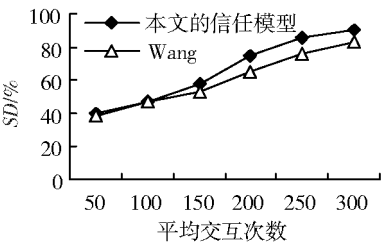


图 2 成功决策率

Fig.2 Success decision ratio

4 结语

在群组协同决策支持系统的研究背景下, 本文分析了协同决策系统中的信任需求, 并给出了信任的定义、属性以及信任关系的网状图表示. 从直接信任度和间接信任度两个方面来分析和计算动态决策者的信任度, 并通过熵理论将二者相结合, 计算出决定实体是否可信的总体信任度. 直接信任度的评估以实体之间的历史交互记录为依据, 并结合交互满意度、时间衰减因子、内容相识度等因素. 间接信任度的评估是通过收集多条信任链上的多层推荐信息得到. 该信任模型解决了群组协同决策环境中动态决策者的安全选择问题, 为可信决策提供依据. 最后, 本文通过模拟实验验证了该信任模型具有良好的可靠性.

本文还存在一些问题,也是下一步工作的重点:网络环境下的动态决策者实体信任信息的发现和收集还缺少有效技术手段,在今后的工作中还要致力于信任管理系统中的各个组件的设计和整个系统原型的实现方面.

[参考文献] (References)

- [1] 徐锋, 吕建. Web安全中的信任管理研究与进展 [J]. 软件学报, 2002, 13(11): 2057-2064
Xu Feng Lü Jian. Research and development of trust management in web security [J]. Journal of Software, 2002, 13(11): 2057-2064 (in Chinese)
- [2] Blaze M, Feigenbaum J, Lacy J. Decentralized trust management [C] // Dale J, Dinitz G. Proceedings of the 17th Symposium on Security and Privacy. Oakland, CA: IEEE Computer Society Press, 1996: 164-173.
- [3] Winsborough W H, Seamons K E, Jones V E. Automated trust negotiation [C] // DARPA Information Survivability Conference and Exposition, 2000. New York: IEEE Computer Society, 2000: 88-102.
- [4] Abdul-Rahman A, Hailes S. A distributed trust model [C] // Proc of the 97 New Security Paradigms Workshop. Cumbria ACM, 1997: 48-60.
- [5] Beth T, Borcherding M, Klein B. Valuation of trust in open network [C] // Gollmann D. Proceedings of the European Symposium on Research in Security (ESORICS). Brighton UK: Springer-Verlag, 1994: 3-18.
- [6] Wang Yaq, Vassileva J. Trust and reputation model in peer-to-peer networks [C] // The Third International Conference on Peer-to-Peer Computing. Singapore: IEEE, 2003: 761-763.
- [7] Wilensky U. NetLogo [CP/OL]. [2010-01-16]. <http://ccl.northwestern.edu/netlogo/>. Center for Connected Learning and Computer Based Modeling. Northwestern University, Evanston, IL, 1999.

[责任编辑: 严海琳]