

开放分布式环境中信任管理综述

官尚元 伍卫国 董小社 梅一多

(西安交通大学计算机科学与技术系 西安 710049)

摘 要 信任是以网络为媒介的交互主体之间重要决策的依据,为主体处理交互过程中的不确定因素、不可控因素、模糊性和不完备信息等提供新思路。信任管理是描述、建立、验证和维护主体之间信任关系的方法,正日益成为研究热点。首先在分析信任及信任管理相关概念的基础上,给出了信任管理的描述性定义和形式化定义,并讨论了二者的关系;其次,分类对典型的信任管理系统进行分析、点评和对比;最后,总结了当前研究中存在的不足并讨论了信任管理未来的发展趋势。

关键词 分布式系统,信任管理,信任协商,决策

中图法分类号 TP393 **文献标识码** A

Survey of Trust Management in Open Distributed Environments

GUAN Shang-yuan WU Wei-guo DONG Xiao-she MEI Yi-duo

(Department of Computer Science and Technology, Xi'an Jiaotong University, Xi'an 710049, China)

Abstract Trust is an important aspect of decision making for network-mediated principals, which can handle uncertainty, uncontrollability, fuzziness and incomplete information during interactions. Since trust management specifies, establishes, verifies and maintains trust relationships among principals, it receives increasing attention. On the basis of analyzing the existing concepts of trust and trust relationship, this paper presented the descriptive definition and the formal one of trust management, and discussed the relationship between them. Next, some typical trust management systems were introduced and compared. Based on the analysis of the shortcomings and problems of the existing trust management systems, we ended this paper with discussions on the trend of research and application.

Keywords Distributed systems, Trust management, Automated trust negotiation, Decision making

随着计算机网络飞速发展和应用范围不断扩大,基于开放网络的新兴分布式计算模式,例如网格计算、普适计算、对等计算、服务计算、协同计算和移动计算等,正在蓬勃地发展。新兴计算模式与传统的封闭、集中式的计算模式存在本质差别。在新兴计算模式中,参与主体和资源具有高度自治、无序成长和复杂多样等特性,应用从集中、封闭、相对静止、面向熟知用户群体的服务模式向分布、开放、动态、面向陌生用户群体的服务模式转变,跨组织域或安全域的事务处理、交互行为和动态协作需求更加突出^[1,2]。然而,新兴计算模式中的决策主体难以获取目标主体的全部信息,甚至可能对目标主体一无所知,进而导致系统难以严格地预测和控制参与主体的行为及其产生的影响,由此为交互过程带来了不确定因素、不可控因素、模糊性和不完备信息等问题,增加了交互主体的风险。为此,需要在交互双方之间建立信任关系,为主体决策提供依据,减小交互主体的风险,提高系统的安全性、健壮性和可信性等。信任管理^[3-7]研究描述、建立、验证和维护主体之间的信任关系,相关研究已经在信任和安全的概念、方法和机理等方面产生了一系列的突破,正受到越来越多学者的关注。

信任是基于开放网络的新兴分布式计算模式中交互主体之间的重要决策因素。然而,对于信任和信任管理的研究涉及到计算机科学、经济学、心理学和社会学等多个学科,其复杂性为信任和信任管理的研究带来了巨大的挑战。虽然经过多年的发展,但是目前并没有就信任及信任管理达成统一的系统性认识。因此,本文首先在分析信任及信任管理相关概念的基础上,给出信任管理描述性定义和形式化定义,并讨论二者之间的关系,以便把握信任管理的本质;其次,分类对典型的信任管理系统进行分析和点评;最后,总结当前研究中存在的不足并讨论信任管理未来的发展趋势。本文试图通过对研究进展的总结,使更多研究人员和机构关注信任管理,同时帮助感兴趣的研究人员更加迅速地把握信任管理问题的本质,提出创新性见解,实现理论突破。

1 信任与信任管理

1.1 信任定义及性质

信任是与被信任者诚实(honesty)、真实(truthfulness)、能力(competence)和可靠性(reliability)等信仰(belief)有关的

到稿日期:2009-04-10 返修日期:2009-06-24 本文受国家自然科学基金项目(60773118),863项目(2006AA01A109)资助。

官尚元(1979—),男,博士生,主要研究方向为信任管理及信任协商等,E-mail:guansy@gmail.com;伍卫国(1963—),男,教授,博士生导师,主要研究方向为高性能计算机系统及分布式处理等;董小社(1963—),男,教授,博士生导师,主要研究方向为高性能计算机系统及分布式处理等;梅一多(1981—),男,博士生,主要研究方向为高性能计算机系统及分布式处理等。

复杂主题^[3-5]。很多学者虽然已经意识到信任的重要性,但由于信任的多面性和复杂性,并未对其概念形成统一认识。本文在综合文献[3-7]的基础上给出了信任的描述性定义。

定义 1 信任是指信任者在给定上下文中基于自身经验和相关知识相信被信任者的某些属性或行为。

在定义 1 中,信任者和被信任者均为主体,例如个人、组织、Web 服务等;信任与上下文相关,例如 Alice 虽然相信其金融顾问关于投资方面的建议,但是不会相信关于卫生保健方面的建议;信任者相信被信任者,则可能相信由被信任者所产生的信息或引导的动作;信任是许多属性的综合,考虑哪些属性由所在上下文决定。

信任本质上是动态、模糊、复杂的关系^[7,8],具有如下性质:

性质 1(自反性, reflexivity) 任何主体完全相信自己,即

$$\forall A | G(T(A, A) = 1) \quad (1)$$

其中, A 为主体; $T(A, B) \in [0, 1]$ 表示 A 对 B 的信任程度, 0 表示完全不信任, 1 表示完全信任; $G()$ 表示括号中陈述命题为永真式。

性质 2(非对称性, asymmetry) 由“主体 A 信任主体 B ”不能推出“ B 也信任 A ”,即

$$\exists A, B | \exists T(A, B) \rightarrow \exists T(B, A) \quad (2)$$

性质 3(有条件传递性, conditional transitivity) 只有满足一定条件的信任才具有传递性。例如, 如果“主体 A 信任主体 B 的推荐”且“ B 信任主体 C ”, 那么“ A 信任 C ”, 即

$$\exists T(A, B), T(B, C) \wedge \exists T(A, C) \cup \exists P(A, B, C) \quad (3)$$

其中, $x \cup y$ 表示如果命题 y 为真, 则命题 x 为真; $P(A, B, C)$ 表示 A 通过 B 信任 C 。

性质 4(不确定性, implicitness) 信任是动态的, 会随着上下文和时间而改变。信任者不能清楚地判断被信任者的属性变化, 只能根据交互历史或相关知识进行评估, 即

$$\exists T(A, B) = \alpha | G(\alpha^+ \rightarrow R(A, B) \geq \alpha) \wedge G(\alpha^- \rightarrow T(A, B) < \alpha) \quad (4)$$

其中, α^+ 表示正面行为, α^- 表示负面行为。

1.2 信任管理定义及分类

1.2.1 信任管理定义

定义 2 信任管理是描述、建立、验证和维护主体之间信任关系的方法, 以支持系统决策, 减小交互主体的风险, 提高系统性能, 如安全性、健壮性和效率等。

信任描述研究如何描述主体之间的信任关系; 信任建立研究如何在主体之间建立初始信任关系, 并将所建立的关系以信任数据的形式保存, 为信任验证提供证据; 信任验证研究主体之间信任关系的存在性及其属性, 为系统决策提供依据; 信任维护研究各主体之间信任关系的衍化, 包括撤销信任关系和修改信任关系等。针对信任管理缺乏统一定义的问题, 本文提出了信任管理的形式化定义, 见定义 3。

定义 3 信任管理系统 $TM = \langle Principals, Type, Attribute, Context, Facts, Rules \rangle$, 其中 $Principals$ 为可数主体集, $Type$ 为可数信任类型集, $Attribute$ 为可数信任属性集, $Context$ 为可数上下文集。在此基础上定义如下关系:

(1) $Trust \subseteq Principals \times Principals$ 表示主体之间存在信任关系;

(2) $Facts \subseteq Trust \times Type \times Attribute \times Context$ 描述主体之间的信任关系;

(3) $Rules: Facts^m \rightarrow 2^{Facts}$ 定义在 $Facts$ 上的函数且对 $Facts$ 封闭, 用于建立、验证和维护信任关系。

在定义 3 中, 信任类型可参考文献[4], 上下文和信任属性通常与具体应用相关。

公理 1 给定信任管理系统 $TM = \langle Principals, Type, Attribute, Context, Facts, Rules \rangle$, $Facts$ 满足: $(\forall f_1) (\exists f_2) ((f_1 \in Facts) \wedge (f_2 \in Facts) \wedge ((f_1)_{Trust} = (f_2)_{Trust}) \wedge ((f_1)_{Type} = (f_2)_{Type}) \wedge ((f_1)_{Context} = (f_2)_{Context}) \Rightarrow ((f_1)_{Attribute} = (f_2)_{Attribute}))$ 。

公理 1 说明, 在给定环境中, 如果主体之间存在某类信任关系, 则此信任关系唯一。设 $f_1 \in Facts$ 和 $f_2 \in Facts$, 如果 f_1 和 f_2 满足 $((f_1)_{Trust} = (f_2)_{Trust}) \wedge ((f_1)_{Type} = (f_2)_{Type}) \wedge ((f_1)_{Context} = (f_2)_{Context})$, 则 f_1 与 f_2 相同, 记为 $f_1 = f_2$ 。根据公理 1, 可以对 $Rules$ 进行分类。

设 $r \in Rules$, 则 $dom(r) = \{f_1, f_2, \dots, f_m | (\exists facts) ((facts(2^{Facts}) \Rightarrow (r(f_1, f_2, \dots, f_m) = facts)))\}$, 而 $cod(r) = \{f_1, f_2, \dots, f_k | \exists (f_{21}, f_{22}, \dots, f_{2m}) ((\forall i) ((f_i \in Facts) \wedge (i \in [1 \dots m]) \Rightarrow (r(f_{21}, f_{22}, \dots, f_{2m}) = \{f_1, f_2, \dots, f_k\})))\}$ 。

定义 4 给定 $TM = \langle Principals, Type, Attribute, Context, Facts, Rules \rangle$, 设 $r \in Rules$, 则 $Rules$ 分类如下:

(1) 如果 $dom(r) \cap \emptyset$ 且 $cod(r) = \emptyset$, 则 r 为撤销规则, 所有撤销规则组成集合为 $Rules_w$; 如果 $dom(r) = \emptyset$ 而 $cod(r) \cap \emptyset$, 则 r 为原生规则, 所有原生规则组成集合为 $Rules_p$ 。

(2) 如果 $\emptyset \subset dom(r) \subset (dom(r) \cup cod(r))$, 则 r 为衍生规则, 所有衍生规则组成集合为 $Rules_D$ 。特别地, 如果 $1 \leq |cod(r)| < |dom(r)|$, 则 r 为聚合规则。

(3) 如果 $\emptyset \subset dom(r) = cod(r)$, 则 r 为衍化规则, 所有衍化规则所组成集合为 $Rules_E$ 。

$Rules_w, Rules_p, Rules_D$ 和 $Rules_E$ 满足如下性质:

(1) $Rules = Rules_w \cup Rules_p \cup Rules_D \cup Rules_E$;

(2) $(\forall i) (\forall j) ((i \in \{W, P, D, E\}) \wedge (j \in \{W, P, D, E\}) \wedge (i \neq j) \wedge (Rules_i \cap Rules_j = \emptyset))$ 。

在定义 3 与定义 4 中, $Facts$ 用于描述信任关系, 原生规则用于建立信任关系, 撤销规则和衍化规则用于维护信任关系, 衍生规则用于验证信任关系。因此, 虽然描述性定义和形式化定义从不同角度对信任管理进行描述, 但是二者本质上是相同的, 如图 1 所示。本文将结合信任管系统实例对各规则具体含义做进一步解释。

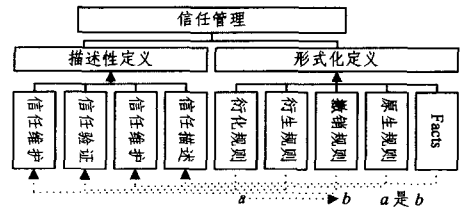


图 1 描述性定义和形式化定义之间的关系

信任管理本质上研究如何描述主体之间信任关系、初始信任关系、基于信任关系的推理规则、利用推理规则确定新信任关系、维护已有信任关系、保存信任关系和推理规则的信任数据存储和收集方法以及信任管理中安全问题等。

1.2.2 信任管理分类

根据主体之间信任关系描述和获取方法,将信任管理分为基于策略和证书的信任管理(policy & credential-based TM)、基于声誉的信任管理(reputation-based TM)以及基于模糊逻辑的信任管理(fuzzy logic-based TM)。图2总结了信任管理分类以及各类信任管理的典型系统。

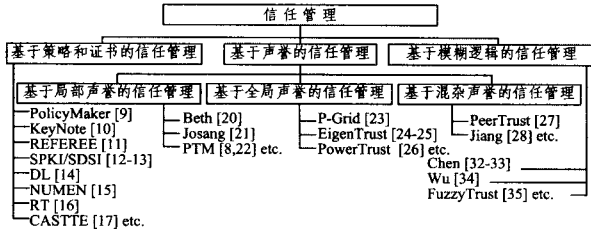


图2 信任管理分类

基于策略和证书的信任管理利用证书验证的方法建立和验证信任关系,如 PolicyMaker^[9], KeyNote^[10], REFEREE^[11], SPKI/SDSI^[12-13], DL^[14], DTMAN^[15], RT^[16], CASTTE^[17], TrustBuilder^[18], Trust- χ ^[19]等,旨在解决大规模分布式计算系统中的权限管理问题,以保护敏感资源或服务。因此,相关概念局限于根据应用制定的策略验证证书以及限定对资源或服务的访问。此类信任管理仅适合资源或服务提供者可信的应用场景,而不能为请求者提供安全保护,故难以为分布式应用提供完整的信任管理解决方案。

基于声誉的信任管理利用已有的历史经验和推荐经验建立信任关系,主要用于隔离恶意服务或服务提供者,确保请求者的安全。根据信任值计算方法可将此类信任管理分为3类:基于局部声誉的信任管理,如 Beth^[20], Josang^[21], PTM^[8,22]等;基于全局声誉的信任管理,如 P-Grid^[23], EigenTrust^[24,25], PowerTrust^[26]等;基于混杂声誉的信任管理,如 PeerTrust^[27], Jiang^[28]等。此类信任管理适合服务选择^[29]、路由选择^[30]和调度^[31]等应用,但不适合保护敏感服务或资源。

基于模糊逻辑的信任管理利用模糊逻辑描述或获取主体之间的信任关系,可以有效地处理不确定性、模糊性以及信息不完备性等问题,常见的如 Chen^[32,33], Wu^[34], FuzzyTrust^[35]等。然而,作为完备的信任管理系统仍存在诸多问题,例如缺乏信任数据存储和收集机制以及信任路径发现方法等,从而阻碍了其应用和推广。

2 典型信任管理系统及其评述

许多学者面向各种应用研究开放分布式环境中的信任关系,并采用不同的数学方法和工具建立了信任管理模型。本节选取了典型的信任管理系统进行分类介绍、评述和对比。

2.1 基于策略和证书的信任管理系统

2.1.1 RT

RT(Role-based Trust-management framework)旨在解决分布式系统中的授权问题,定义了两类实体:主体(principal)与角色(role)。主体是指能够颁发证书或发出服务请求的进程、程序、个人或组织等,由公私钥对唯一标识。角色由主体和角色名组成。主体确定角色成员,而角色名为标识符,二者之间用点分隔,如 $K_A.r$ 。角色 $K_A.r$ 的值 $members(K_A.r)$ 是角色所有成员所组成的集合。RT 是系列语言集合,包括 RT_0 , RT_1 , RT^T 和 RT^D ,其中, RT_0 是 RT 的基础。RT 角色

定义由两部分组成:头(head)与体(body),用谓词连接起来。根据角色定义体,可分为如下4种基本类型:

Type-1: $K_A.r \leftarrow K_B$, 定义主体 K_B 是角色 $K_A.r$ 的成员,即 $K_B \in members(K_A.r)$;

Type-2: $K_A.r \leftarrow K_B.r_1$, 定义角色 $K_B.r_1$ 的成员是角色 $K_A.r$ 的成员,即 $members(K_B.r_1) \subseteq members(K_A.r)$;

Type-3: $K_A.r \leftarrow K_A.r_1.r_2$, 定义角色 $K_A.r$ 的成员包含所有角色 $K_B.r_2$ 的成员且 $K_B \in members(K_A.r_1)$, 即 $members(K_A.r) \supseteq members(K_A.r_1.r_2) = \bigcup_{K_B \in members(K_A.r_1)} members(K_B.r_2)$;

Type-4: $K_A.r \leftarrow K_{B_1}.r_1 \cap \dots \cap K_{B_k}.r_k$, 定义角色 $K_A.r$ 的成员包含角色 $\{K_{B_i}.r_i\} (i \in [1 \dots k])$ 成员的交集,即 $(members(K_{B_1}.r_1) \cap \dots \cap members(K_{B_k}.r_k)) \subseteq members(K_A.r)$ 。

此外, RT_0 还支持简单委托和链接委托等,例如简单委托 $K_A.r \leftarrow K_B:K_C.r_2$, 表示 K_A 将确定角色 $K_A.r$ 成员权限委托给 K_B , K_B 又将该权限委托给角色 $K_C.r_2$, 即等价于 $K_A.r \leftarrow K_B.r \cap K_C.r_2$; 链接委托 $K_A.r \leftarrow K_A.r_1:K_C.r_2$, 表示 K_A 将确定角色 $K_A.r$ 成员的权限委托给 $K_B.r_1$ 成员并且委托局限于 $K_C.r_2$ 成员, 即等价于 $K_A.r \leftarrow K_B.r_1.r \cap K_C.r_2$ 。 RT_1 在 RT_0 的基础上增加了携带参数的功能,即允许增加参数来约束角色; RT^T 语言通过提供两种角色操作(角色集成 $\odot$ 与角色互斥 $\oplus$)满足职责分离(Separation of Duty, SoD)原则; RT^D 语言主要用于处理角色激活的委托,以处理角色之间的关系。

为了抵抗非授权推测(unauthorized inferences)攻击, RT 引入了属性确认策略(attributed acknowledge policies, ACK)的概念,其基本思想是:对证书中的敏感属性设置一层新的访问控制策略,在建立更高级别的信任关系之后,再释放一些重要的信息,从而避免了非授权推测。基于 ACK 策略和 RT_0 , W. H. Winsborough 等人提出了 TTG (Trust Target Graph) 协议,信任协商双方构建共享 TTG 以建立信任关系。在构建 TTG 时,信任协商双方可以采用前向搜索算法、后向搜索算法或双向搜索算法,以发现并收集证书。

RT 具有如下优点: (1) 具有丰富的策略概念,例如角色相交、角色笛卡尔操作、角色参数化等,不仅能够简洁地表示安全策略,而且能够表示已有 TM 系统所不能表示的安全策略; (2) 具有角色推理功能,即基于某主体是某角色的成员推断该主体是否是其它角色的成员; (3) 不管采用集中或者分布方式存储证书, RT 都能自动发现并收集证书,且具有前向、后向及双向证书搜索算法。但是, RT 存在如下不足: (1) 可以实现布尔委托深度控制,但是不支持整数委托深度约束,故在委托深度控制方面表达能力较弱; (2) 虽然利用 ACK 策略可保护敏感属性或证书,但是不能够有效地保护协商者未持有或可以自由披露的证书,而且可能会引发协商的意外失败,从而降低了协商成功率; (3) 缺乏研究如何维护主体之间的信任关系,即如何撤销表示信任关系的证书。

2.1.2 各信任管理系统的比较

文献[36]和文献[37]总结了基于策略和证书的描述方法需要满足良好的语义、单调性、证书合并、属性值约束、内部证书约束、证书链传递、闭包、认证、敏感策略、统一的形式化以及互操作语言等需求。目前,基于策略和证书的信任描述方法有很多,如 KeyNote^[10], SPKI/SDSI^[12], TPL^[35], DL^[14], $RT^{[16]}$, TrustBuilder^[17] 和 Trust- χ ^[18]等。表1对上述信任描

述方法满足需求情况进行了比较(Y 表示支持或满足, N 表示不支持或不满足, P 表示部分支持或满足)。

表1 基于策略和证书的信任管理系统的比较

需求	典型的基于策略和证书的信任管理系统						
	KeyNote	SPKI/SDSI	TPIL	DL	RT	Trust-Builder	Trust-X
良好语义	Y	Y	Y	Y	Y	Y	Y
单调性	Y	P	N	P	Y	Y	Y
证书合并	Y	Y	Y	Y	Y	Y	Y
属性约束	N	N	Y	N	Y	Y	Y
内部证书约束	N	N	Y	N	Y	Y	Y
证书链	Y	Y	Y	Y	Y	N	N
传递闭包	P	Y	Y	Y	Y	N	N
认证	P	Y	N	Y	Y	N	Y
敏感策略	N	N	N	N	Y	Y	Y
统一形式化	Y	Y	Y	Y	Y	N	Y
互操作语言	Y	Y	Y	Y	N	Y	Y

2.2 基于声誉的信任管理系统

2.2.1 PTM

马德里卡洛斯三世大学 F. Almenarez 等人^[8,22]提出面向普适计算环境的信任管理模型 PTM,其利用 $[0,1]$ 上的值描述主体之间信任关系,即主体 A 对主体 B 的信任表示为

$$R(A,B)=\alpha, \alpha \in [0,1] \quad (5)$$

PTM 中主体可以通过推荐建立对其他主体的初始信任关系,并利用加权平均综合多个推荐值。

$$R(A,C)=\frac{1}{n} \sum_{i=1}^n R_{B_i} \cdot R(A,B_i) \quad (6)$$

其中,权重因子 R_{B_i} 表示主体 A 对主体 B 关于其推荐的信任度。式(6)中 $R(A,B_i)$ 应为 $R(B_i,C)$,但为了尊重原文,并未修改式(6)。

PTM 中信任关系随着双方交互行为以及行为上下文的改变而改变,其演化关系如下。

$$T_i = \begin{cases} T_{i-1} + \omega \cdot V_{a_i} \cdot (1 - T_{i-1}), & V_{a_i} > 0 \\ T_{i-1} \cdot (1 - \omega + \omega \cdot V_{a_i}), & \text{Else} \end{cases} \quad (7)$$

其中, ω 是由用户设定的限制因子,用于调整过去行为和当前行为的影响比率,其取值范围为 $[0.25, 0.75]$,默认值为0.5,且 V_{a_i} 定义为

$$V_{a_i} = W_{a_i}^{(m)} \cdot \frac{(a^+ - a^-)((a^+ - a^-) \cdot \delta)^{2m}}{(a^+ - a^-)((a^+ - a^-) \cdot \delta)^{2m} + 1} \quad (8)$$

其中, W_{a_i} 为 a_i 的行为类型权值,正确行为为取1,错误行为为取0.5,恶意行为为取0; a^+ 和 a^- 分别是正面行为和负面(包括错误和恶意)行为的历史计数; $m \in N$ 为安全等级; $\sigma \in (0, 0.05]$ 可根据 m 计算且反比于 m 。

PTM 具有如下优点:(1)根据交互双方的行为、行为上下文以及时间动态改变信任值,并给出数学模型以描述上述演化关系,因而很好地表现了信任的不确定性;(2)信任演化规则体现了严格的惩罚性,即信任容易失去但难以获取,与现实情况比较接近;(3)与 EigenTrust 等信任管理模型相比,信任演化规则没有复杂的迭代运算,更适合能源受限的应用;(4)非集中式的 PTM 具有良好的可扩展性。然而,PTM 存在如下不足:(1)适合固定的信任域,难以满足不同应用背景下的需求;(2)利用加权平均建立初始信任的方法难以有效地消除恶意推荐所带来的影响;(3)没有考虑到信任的主观性、不确定性等问题。

2.2.2 EigenTrust

基于信任的传递性,斯坦福大学 S. D. Kamvar 等人^[24,25]提出了 P2P 环境下基于全局声誉的信任管理模型 EigenTrust,其中每个主体 i 保存另外主体 j 的满意事务次数 $sat(i,j)$ 和非满意事务次数 $unsat(i,j)$,则 i 对 j 局部声誉值定义为

$$s_{ij} = sat(i,j) - unsat(i,j) \quad (9)$$

局部声誉值通过式(10)转换为标准的局部声誉值,并能够保证 $c_{ij} \in [0,1]$ 。

$$c_{ij} = \frac{\max(s_{ij}, 0)}{\sum_j \max(s_{ij}, 0)} \quad (10)$$

主体 i 通过咨询朋友而建立对主体 k 的信任 t_k 为

$$t_k = \sum_j c_{ij} c_{jk} \quad (11)$$

利用矩阵的概念表示式(11):设 C 为局部信任值矩阵 $[c_{ij}]$,向量 t_i 包含 t_k ,则 $t_i = C^T \cdot c_i$ 且 $\sum_j t_{ij} = 1$ 。类似地,主体 i 通过咨询朋友的朋友而建立的信任向量为 $t = (C^T)^2 c_i$ 。在经过 n 次迭代以后, t_i 收敛于矩阵 C 的左主特征向量,即全局声誉值。

为了处理非激活主体、防止恶意推荐以及保证迭代收敛等问题,EigenTrust 假定网络中预先存在固定可信主体集 P 。如果 $i \in P$,则 $p_i = 1/|P|$;否则, $p_i = 0$ 。利用 p_i 改进式(10):当 $\sum_j \max(s_{ij}, 0) \neq 0$,则与式(10)相同;否则, $c_{ij} = p_i$ 。如果主体与其他主体无交互记录,则只相信 P 中主体对其的评价。EigenTrust 将迭代公式重新定义为

$$t^{(k+1)} = (1-\alpha)C^T t^{(k)} + \alpha p \quad (12)$$

其中, $\alpha \in [0,1]$ 为权重因子,调整对 P 中主体与非 P 中主体的推荐声誉比重,从而消除恶意推荐所带来的影响。同时,式(12)保证了迭代收敛性。

EigenTrust 通过邻居节点间相互满意度的迭代来获取节点全局可信度,所得声誉值可以较好地反映节点的真实行为。因此,EigenTrust 利用全局声誉值选择交互节点的方法可以有效地鉴别并隔离恶意节点。然而,存在如下问题:(1)为了保证收敛性,EigenTrust 假定网络中始终存在固定可信节点集合 P ;(2)未考虑获取推荐信任的消息开销以及迭代计算的开销;(3)虽然作者在文献[25]中探讨了模型安全性问题,但其安全保证需要依赖于 P ,这在 P2P 环境下很难实现。

2.2.3 各信任管理系统的比较

在基于声誉的信任管理中,主体可以建立对其他主体的信任关系并为关系指派一个信任值。指派给信任关系的信任值是主体局部声誉、全局声誉或信任者对被信任者感知(perception)的组合函数。目前,此类信任管理系统主要包括 Beth^[20], Jøsang^[21], PTM^[8,22], P-Grid^[23], EigenTrust^[24,25], PowerTrust^[26] 和 PeerTrust^[27] 等,表2参考文献[6,36]对上述信任管理系统进行了对比。

表2 基于声誉的信任管理系统的比较

	典型的基于声誉的信任管理系统						
	局部声誉				全局声誉		混杂声誉
	Beth	Jøsang	PTM	P-Grid	Eigen-Trust	Power-Trust	Peer-Trust
身份	Y	Y	Y	Y	Y	Y	Y
动态评估	Y	Y	Y	Y	Y	Y	Y
商业价值	N	Y	N	Y	Y	Y	Y
声誉	Y	Y	Y	Y	Y	Y	Y
动作	Y	Y	Y	Y	Y	Y	Y
能力	N	N	N	N	N	Y	Y

信心	N	N	N	N	Y	Y	Y
上下文	N	N	Y	N	Y	Y	Y
历史	Y	Y	Y	Y	Y	Y	Y
第三方	N	N	Y	N	Y	N	N
合谋攻击	低	低	中	低	中	好	中
收敛性	无	无	无	低	好	更好	好
精确性	低	中	好	中	好	更好	好

2.3 基于模糊逻辑的信任管理系统

针对基于声誉的信任管理系统将信任的主观性和不确定性等同于随机性的问题,北京大学陈钟教授^[32]提出了基于模糊集合理论的主观信任管理模型。设集合 X 为论域且非空,其元素为主体。利用多个模糊子集合 $T_j \in \mathcal{F}(X) (j \in [1 \cdots M])$ 定义具有不同信任度的集合, x_0 对 x_i 的信任可以用信任向量 $V = \{v_0, v_1, \dots, v_M\}$ 来表示,其中 v_j 表示 x_i 对 T_j 的隶属度,主体 P 对主体 Q 的直接信任为

$$P \text{ trusts}_c^{\omega} Q \text{ value } V \quad (13)$$

式(13)表示主体 P 认为,就 c 类信任而言,主体 Q 的信任值为 V , c 为特定信任类型, ω 为直接信任向量 V 的合成权重。

$$P \text{ trusts}_c^{\omega} \text{ rec}_{rc}^n Q \text{ when path } S_p \text{ when target } S_i \text{ value } V \quad (14)$$

式(14)表示主体 P 将以推荐信任度 V 接受主体 Q 提供的关于其他主体 c 类直接信任或推荐信任。与直接信任类似, ω 为推荐信任向量 V 的合成权重, c 为特定信任类型。 n 为推荐层数限制,当进行推荐迭代时, n 限定推荐的最大迭代次数。 $S_i \subset X$ 限定 P 只接受 Q 提供的关于 S_i 中主体的信任关系; S_p 中元素是主体的有序序列 $(x_i, x_j, x_k, \dots)$, 每个列表描述一条合法推荐路径。此外, rc 描述推荐内容类型或简称推荐类型:直接推荐(rd)和推荐的推荐(rr)。前者推荐内容为直接信任,后者推荐内容为推荐信任。

为了对信任关系进行推理,先介绍信任向量的连接(join)和合并运算(union)。设信任向量 $V_1 = \{v_{11}, v_{12}, \dots, v_{1M}\}$ 和 $V_2 = \{v_{21}, v_{22}, \dots, v_{2M}\}$, 则 $V = V_1 \oplus V_2 = \{v_1, v_2, \dots, v_M\} = \{v_{11} \epsilon^- v_{21}, v_{12} \epsilon^- v_{22}, \dots, v_{1M} \epsilon^- v_{2M}\}$ 和 $V = V_1 \oplus V_2 = \{v_1, v_2, \dots, v_M\} = \{v_{11} \epsilon^+ v_{21}, v_{12} \epsilon^+ v_{22}, \dots, v_{1M} \epsilon^+ v_{2M}\}$, 其中 ϵ^- 和 ϵ^+ 是 Einstein 算子。在此基础上,定义了推演规则和合意规则:前者是信任通过推荐沿信任链传递的机制。对于相同类型的信任关系来说,当有推荐发生时,推演规则可以将推荐信任及其推荐内容(其它信任关系)连接起来,构成新的信任关系;后者是对主体间的多重信任关系进行综合的方法,当两个主体之间存在多重信任关系时,运用合意规则可以将各信任关系综合起来,构成新的信任关系。在信任验证时,利用推演规则和合意规则作用于现有的信任关系,进而确定给定主体之间的信任关系以及属性,从而为系统的决策提供支持。

与 RT, PTM 和 EigenTrust 等模型相比, Chen 模型使用模糊逻辑处理主观信任中对主体特征和行为认知的主观性及不确定性,作为一种直观而有效的评价、分析和推导工具,为开放式网络环境中的主体信任决策提供有效的支持。Chen 在信任关系的形式化推理中,简单地采用 Einstein 算子来实现信任向量间的运算,没有考虑人类信任推理的一般知识,缺乏直观的实际意义。陈钟教授在文献^[33]中进一步将语言变量和模糊逻辑引入到信任推理研究中,运用模糊 IF-THEN 规则对人类信任推理的一般知识和经验进行建模,定义信任向量间的连接(join)与合并(union)运算,构造信任管理模型。

然而,上述模型仍然存在如下问题:(1)在信任关系推导规则中指定信任路径的方法使得信任管理模型缺乏灵活性,难以适应信任路径频繁变化的环境,而且不利于模型的实现;(2)诸如是否能够有效消除恶意推荐带来的影响、是否能够保证各主体的身份鉴别、信任信息的完整性和机密性等问题,还有待进一步研究;(3)缺乏研究信任数据的存储和收集机制。

2.4 典型信任管理系统与形式化定义的关系

虽然上述各信任管理系统中的 (Facts) 及推理规则 (Rules) 在形式上与定义 3 不一致,但是本质上是相同的。下面以 RT_0 语言为例进行探讨。首先,对 RT_0 进行等价转换。

RT_0 信任描述方法为 Type-1: $K_B \in \text{members}(K_A, r)$, 表示主体 K_B 为角色 K_A, r 的成员,推理规则包括:

(1) Type-2: $(\exists K_c) (K_c \in \text{members}(K_B, r_1)) \Rightarrow (K_c \in \text{members}(K_A, r))$;

(2) Type-3: $(\exists K_c) (\exists K_B) (((K_B \in \text{members}(K_A, r_1)) \wedge (K_c \in \text{members}(K_B, r_2))) \Rightarrow (K_c \in \text{members}(K_A, r)))$;

(3) Type-4: $(\exists K_c) (((K_c \in \text{members}(K_{B1}, r_1)) \wedge \dots \wedge (K_c \in \text{members}(K_{Bk}, r_k))) \Rightarrow (K_c \in \text{members}(K_A, r)))$ 。

在不撤销原有信任关系的前提下,上述推理规则均作用于已有信任关系并推出新的信任关系,故均为衍生规则。然而, RT_0 并没有就初始化信任关系、撤销已有信任关系以及信任关系变化等问题进行深入讨论。

其它信任管理系统与 RT_0 类似,故不再进一步讨论。表 3 对上述典型的信任管理系统与信任管理的形式化定义进行了对比,并指出上述典型系统存在的不足 (N 表示缺乏对该领域进行深入研究)。

表 3 典型信任管理系统与形式化定义的映射关系

TM 系统	信任管理(TM)的形式化定义				
	Facts	原生规则	撤销规则	衍生规则	衍化规则
RT_0	Type-1	N	N	Type-2, Type-3, Type-4	N
PTM	式(5)	式(6)	N	N	式(7)
EigenTrust	$c_{ij} \in [0, 1]$	式(10)	N	式(12)	式(9)
Chen	式(13), 式(14)	N	N	推演规则 与合意规则	N

3 现有工作的不足及发展趋势

3.1 现有工作的不足

研究描述、建立、验证和维护主体之间信任关系的信任管理已经吸引了许多学者和机构的关注,并取得了丰硕成果,但是仍然存在如下问题:

(1) 各类信任管理技术本身并未成熟

在基于策略和证书的信任管理中,主要存在如下问题:1) 信任描述方法应该具有哪些表达安全策略和证书的能力以及满足哪些应用需求,有待进一步确定;2) 系统主要集中于信任的描述和验证,而忽视证书的颁发、撤销、存储和收集等问题;3) 虽然多数系统对委托深度进行控制,但对深度的表达、语义和实现机制各异,且对委托深度的表现力有限,难以满足应用需求;4) PoC (Proof of Compliance) 是影响系统性能的关键因素,而现有 PoC 算法比较复杂;5) 不可忽视由于主体间信任数据交互而引入的安全漏洞;6) 多种信任管理系统共存使得互操作问题亟待解决,互操作不仅可以使不同信任管理系统中的主体之间可以进行无缝交互,而且为应用提供了更大的

灵活性。

在基于声誉的信任管理中,主要存在如下问题:1)系统倾向于采用事件概率的方式来表述和度量信任关系,即将信任的主观性和不确定性等同于随机性,难以有效地描述信任关系;2)简单地采用加权平均方法聚合多个信任值,不能有效地消除恶意推荐对信任评估的影响,特别是当恶意推荐者所占比例较大时;3)在自动获取观察信息以及将所观察信息转换成对信任或声誉的更新等方面缺乏研究;4)在跨主体信任数据存储方案中,未进一步考虑如何确保存储方按规定策略保存信任数据且不能够对数据进行篡改;5)保护主体匿名性是信任管理系统的基本能力,特别是在开放、动态的分布式计算系统中,虽然一些学者对此进行了初步研究,但仍需要进一步努力。

在基于模糊逻辑的信任管理中,主要存在如下问题:1)利用模糊逻辑描述和推导信任关系,其合理性有待进一步分析;2)此类系统倾向于在信任关系推导规则中指定信任路径,从而使得系统缺乏灵活性,难以适应信任路径频繁变化的环境;3)系统强调如何用模糊逻辑描述和推导信任关系,而忽视信任数据的获取、存储、收集以及信任关系维护等问题。

(2) 难以为分布式系统提供完整的信任管理解决方案

基于策略和证书的信任管理利用策略和证书确定服务提供者对请求者的信任,以此进行访问控制决策,对敏感服务提供者提供安全保护,但其仅适合服务或服务提供者可信的应用场景;基于声誉信任的信任管理通过历史经验和推荐经验确定服务请求者对服务提供者的信任,以此进行服务选择,隔离恶意服务或服务提供者,为请求者提供安全保护,但不适合保护服务;基于模糊逻辑的信任管理可以有效地表达信任的模糊性,但合理性有待进一步研究,且在信任关系推导规则中指定信任路径的方法使得系统缺乏灵活性。因此,现有信任管理系统难以为分布式系统提供完整的信任管理解决方案。

(3) 信任管理中的安全问题

在跨主体信任数据存储方案中,主体可以通过篡改或伪造信任数据对系统实施攻击,故信任管理系统需要抵制主体操控信任数据,而现有存储方案无法确保存储者不能篡改信任数据、鉴别消息真伪以及有效地过滤恶意消息等机制。在信任验证过程中,可能在多主体之间交互信任数据,而信任验证策略将控制交互过程。因此,攻击者发起主动攻击时,通过分析信任验证中的交互信息可获取主体的敏感信息。因此,信任验证策略不仅要保证互操作,而且不可忽视由于信任数据交互而引入的安全漏洞^[40-42]。虽然许多学者对交互过程中的隐私保护进行了研究,如 ACK、策略过滤、策略迁移以及 UniPro 方案等^[43],但是仍存在诸多问题,如难以抵抗合谋攻击等,值得进一步研究。因为新的和无法预知的攻击不断涌现,所以信任管理中的安全问题难以得到彻底解决。

(4) 信任管理的研究多停留在理论上,缺乏实用系统

目前,对信任管理的研究如火如荼,研发项目和参与机构不断增加,各种理论与技术相继提出。然而,对信任管理的研究多停留在理论上,缺乏实用系统。在前面介绍的信任管理系统中,仅 SPKI/SDSI, PTM 和 TrustBuilder 等少数实现了原型系统,而其他的未讨论实现问题。研究信任管理的目的是为交互主体提供系统决策,如果缺乏实用系统,则会极大地阻碍信任管理系统的普及。此外,应考虑如何方便地将信任

管理系统集成到已有应用中。

(5) 缺乏通用的评价体系

评价信任管理系统的功能和性能是非常困难的工作。在现有的信任管理系统中,多采用模拟实验、启发式评估与认知性遍历(heuristic evaluation and cognitive walkthrough)等方法进行功能评价,而缺乏对性能的测评。文献[44]通过试验场景比较 KeyNote, PolicyMaker 和 SPKI/SDSI 的可用性,文献[45]设计了试验场景来对信任更新算法进行比较,而文献[46]介绍了信任管理测试的相关概念。然而,仍然缺乏通用的评价体系,故合理地测评各信任管理系统有待进一步研究。

3.2 信任管理发展趋势

从信任管理目的、应用需求以及研究历程和现状来看,信任管理未来发展趋势体现在:

(1) 完善现有的信任管理技术

结合应用背景和需求,利用现有的知识,如密码学、机器学习和人工智能等,完善信任管理技术,主要包括:1)研究信任与信任管理的相关概念和性质等,给出其 ontology 模型,并且分析信任表述和度量的合理性等;2)基于现有的信任描述方法,研究完备、有效、相对简单且具有自适应能力的信任描述方法,使其兼具各描述方法的优点并满足应用需求;3)研究合理的信任关系初始化方法;4)基于应用结构化知识以及信任验证方法,利用机器学习和人工智能等知识,研究灵活、高效、安全的信任数据获取、撤销、存储和收集等方案;5)改进信任验证方法,缓解信任验证效率和成功率之间的矛盾,提高其验证能力、效率以及安全性等;6)研究如何对众多的信任管理系统进行客观的性能评测,提出通用的评价体系。此外,结合三类信任管理系统研究信任管理是新的研究方向,从而可以扬长避短,扩大信任管理的应用范围,为分布式系统提供完整的信任管理解决方案。

(2) 解决信任管理中的安全问题

在跨主体信任数据存储方案中,不仅要确保存储者不会篡改或伪造信任数据,而且要防止存储者拒绝提供对其不利的信任数据;此外,应提供鉴别消息真伪以及有效地过滤恶意消息等机制,从而确保信任数据安全,提高信任管理系统安全性。在信任验证中,利用现有密码技术或借鉴其他领域的隐私保护技术防止隐私泄漏,例如利用并发零知识和可重置零知识等来保护参与方的隐私,这不仅可以防止披露敏感信息,而且可以有效地抵抗合谋攻击等。现有信任验证方法属于抽象工作模型,难以对系统进行形式化描述,其安全级别受到限制,故应研究信任验证的形式化描述方法,并分析其安全性等。

(3) 新应用的产生为研究信任管理带来新的机遇和挑战

随着无线通信、电子与传感技术的发展,无线传感器网络引起了人们的广泛关注。无线传感器网络中的信任管理技术可以用于访问控制决策和路由选择等^[47]。无线传感器网络具有无线自组织、资源受限等特点,而现有信任管理技术主要针对有线、对等的分布式系统,故难以满足无线传感器网络的需求。因此,无线传感器网络中的信任管理技术是值得深入研究的。信任管理技术也可以向普适计算方面发展,特别是用于服务选择等。此外,可以考虑将信任用于其他系统决策,以提高系统的某些性能,例如 P2P 中拓扑构造和资源发现等。

综上所述,信任管理发展趋势主要体现在3个方面:1)完善现有信任管理技术,包括其中的安全问题;2)以新应用为背景研究信任管理技术,如无线传感器网络、对等网络和普适计算等;3)除了前面所提到的访问控制、服务选择、路由选择和调度算法等典型应用外,还可以研究将信任用于其他系统决策。

结束语 基于开放网络的新兴分布式计算模式中,由于参与主体具有自治性,因此主体在交互过程中存在不确定因素、不可控因素、模糊性和不完备信息等问题,而信任是主体进行决策的重要因素,可以用于处理上述问题,从而减小主体交互风险,提高系统性能。虽然信任管理在理论和技术方面发展迅速,但尚未建立起完整的理论体系和方法体系。鉴于此,本文给出信任管理描述性定义和形式化定义,并讨论二者关系,以便把握信任管理的本质;其次,根据信任描述方法对信任管理进行分类,并分类对典型的信任管理系统进行分析和点评;最后,总结现有工作的不足并展望未来的发展趋势。通过本文综述来看,信任管理技术是一个活跃的研究方向,仍处在初始阶段,需要学者们继续努力。

参 考 文 献

- [1] Foster I. Service-Oriented Science [J]. Science, 2005, 308(5723): 814-817
- [2] 卢锡城,王怀民,王戟. 虚拟计算环境 iVCE: 概念与体系结构 [J]. 中国科学(E辑), 2006, 36(10): 1081-1099
- [3] Blaze M, Kannan S, Lee I, et al. Dynamic Trust Management [J]. Computer, 2009, 42(2): 44-52
- [4] Ma J, Orgun M A. Trust Management and Trust Theory Revision [J]. IEEE Transactions on Systems, Man and Cybernetics-Part A: systems and humans, 2006, 36(3): 451-460
- [5] Jøsang A, Ismail R, Boyd C. A Survey of Trust and Reputation Systems for Online Service Provision [J]. Decision Support Systems, 2007, 43(2): 618-644
- [6] 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
- [7] 李小勇,桂小林. 大规模分布式环境下动态信任模型研究 [J]. 软件学报, 2007, 18(6): 1510-1521
- [8] Almenarez F, Marin A, Campo C, et al. PTM: A Pervasive Trust Management Model for Dynamic Open Environments [C] // Proc. of the 1st Workshop on Pervasive Security, Privacy and Trust. Boston, 2004
- [9] Blaze M, Feigenbaum J, Lacy J. Decentralized Trust Management [C] // Proc. of the 17th Symposium on Security and Privacy (SP'96). IEEE Computer Society Press, 1996: 164-173
- [10] Blaze M, Feigenbaum J, Ioannidis J, et al. The KeyNote Trust Management System Version 2 [S]. Internet RFC 2704. 1999
- [11] Chu Y H, Feigenbaum J, LaMacchia B, et al. REFEREE: Trust Management for Web Applications [J]. World Wide Web Journal, 1997, 2(2): 127-139
- [12] Clarke D, Elien J E, Ellison C, et al. Certificate Chain Discovery in SPKI/SDSI [J]. Journal of Computer Security, 2001, 9(4): 285-322
- [13] Li N, Mitchell J C. Understanding SPKI/SDSI Using First-order Logic [J]. International Journal of Information Security, 2006, 5(1): 48-64
- [14] Li N, Grosz B N, Feigenbaum J. Delegation Logic: A Logic-based Approach to Distributed Authorization [J]. ACM Transactions on Information and System Security, 2003, 6(1): 128-171
- [15] 官尚元,伍卫国,董小社,等. 分布式环境中高效信任管理的研究 [J]. 西安交通大学学报, 2009, 43(6): 15-19
- [16] Li N, Mitchell J C, Winsborough W H. Design of a Role-based Trust-management Framework [C] // Proc. of the 23th IEEE Symposium on Security and Privacy (SP'02). 2002: 114-130
- [17] Guan S, Dong X, Mei Y, et al. CASTTE: a Trust Management for Securing the Grid [C] // Proc. of the 10th IEEE International Conference on High Performance Computing and Communications (HPCC'08). 2008: 728-735
- [18] Yu T, Winslett M, Seamons K E. Supporting Structured Credentials and Sensitive Policies Through Interoperable Strategies for Automated Trust Negotiation [J]. ACM Transactions on Information and System Security, 2003, 6(1): 1-42
- [19] Bertino E, Ferrari E, Squicciarini A C. Trust- γ : A Peer to Peer Framework for Trust Negotiations [J]. IEEE Transactions on Knowledge and Data Engineering, 2004, 16(7): 827-841
- [20] Beth T, Borcherding M, Klein B. Valuation of Trust in Open Network [C] // Proc. of the European Symposium on Research in Security (ESORICS). 1994: 3-18
- [21] Jøsang A, Knapskog S J. A Metric for Trusted Systems [J]. Global IT Security, 1998: 541-549
- [22] Almenarez F, Marin A, Diaz D, et al. Developing a Model for Trust Management in Pervasive Devices [C] // Proc. of the 3rd IEEE Int'l Workshop on Pervasive Computing and Communication Security (PerSec 2006). 2006: 267-272
- [23] Aberer K. P-Grid: A Self-organizing Access Structure for P2P Information Systems [C] // Proc. of the 9th International Conference on Cooperative Information Systems. 2001: 179-194
- [24] Kamvar S D, Schlosser M T. EigenRep: Reputation Management in P2P Networks [C] // Proc. of the 12th Int'l World Wide Web Conf. (WWW 2003). 2003: 123-134
- [25] Kamvar S D, Schlosser M T, Molina H G. The EigenTrust Algorithm for Reputation Management in P2P Networks [C] // Proc. of the 12th Int'l World Wide Web Conf. (WWW 2003). 2003: 640-651
- [26] Zhou R, Hwang K. PowerTrust: A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing [J]. IEEE Transactions on Parallel and Distributed Systems, 2007, 18(4): 460-473
- [27] Xiong L, Liu L. PeerTrust: Supporting Reputation-based Trust for Peer-to-Peer Electronic Communities [J]. IEEE Transactions on Knowledge and Data Engineering, 2004, 16(7): 843-857
- [28] 姜守旭,李建中. 一种 P2P 电子商务系统中基于声誉的信任机制 [J]. 软件学报, 2007, 18(10): 2551-2563
- [29] Zhang Y, Fang Y. A Fine-grained Reputation System for Reliable Service Selection in Peer-to-Peer Networks [J]. IEEE Transactions on Parallel and Distributed Systems, 2007, 18(8): 1134-1145
- [30] Pirzada A A, McDonald C, Datta A. Performance Comparison of Trust-Based Reactive Routing Protocols [J]. IEEE Transactions on Mobile Computing, 2006, 5(6): 695-710
- [31] 王伟,曾国荪. 一种基于 Bayes 信任模型的可信动态级调度算法 [J]. 中国科学(E辑), 2007, 37(2): 285-296
- [32] 唐文,陈钟. 基于模糊集合理论的主观信任管理模型研究 [J]. 软件学报, 2003, 14(8): 1401-1408
- [33] 唐文,胡建斌,陈钟. 基于模糊逻辑的主观信任管理模型研究 [J]. 计算机研究与发展, 2005, 42(10): 1654-1659
- [34] Wu Z, Weaver A C. Application of Fuzzy Logic in Federated Trust Management for Pervasive Computing [C] // Proc. of the 30th Annual International Computer Software and Applications Conference (COMPSAC'06). 2006: 215-222
- [35] Song S, Hwang K, Zhou R. Trusted P2P Transactions with Fuzzy Reputation Aggregation [J]. IEEE Internet Computing, 2005, 9(6): 24-34

根据命题 1 可知: $M \models \text{roles} \subseteq (\sim(\text{user} \circ \sim \text{UA})) \circ \text{RH}^-$ iff $S \models \text{roles}(s) \subseteq \{r: \exists r' \geq r ((\text{user}(s), r') \in \text{UA})\}$;

对断言 $\text{permissions}(s) = \{p: \forall r \in \text{roles}(s) \exists r' \leq r ((p, r') \in \text{PA})\}$, 则根据命题 1 可知: $M \models \text{permissions} \subseteq \sim(\text{roles} \circ \sim(\text{RH}^- \circ \text{PA}^-))$ iff $S \models \text{permissions}(s) = \{p: \forall r \in \text{roles}(s) \exists r' \leq r ((p, r') \in \text{PA})\}$ 。

同理可证(2)。这里省略证明过程。证毕。

定理 1 说明了 DL_{RBAC} 可以忠实地表示 RBAC 中的各种关系。

4 相关研究比较

目前已有的用描述逻辑来研究 RBAC 建模的有 Zhao 等提出的表示^[10], 还有用描述逻辑对 RBAC 的扩充模型进行的形式化描述^[11,12], 这些表示在基本 RBAC 建模方面都有类似的表达。

本文与它们的主要区别如下:

(1) DL_{RBAC} 和 Zhao 的 DL 方法都包含了 RBAC96 模型的组件中的 $U, R, P, S, \text{UA}, \text{PA}$ 等。由于 Zhao 的方法中没有对角色层次 RH 的表示, 直接利用子概念 RR_1 和 RR_2 之间的包含关系来表示它们实例之间的优势关系。这样做显然存在缺陷。首先找不到语义模型来解释这种关系, 其次对 RBAC 模型中隐含的角色继承无法表示; (2) 对于用户和权限的关系, 在 RBAC96 模型中, 用户是通过角色的激活来获得权限的, 如果表示了 roles 和 permissions , 就不需要再用 authorized 来表示用户和权限之间的联系, 这样 Zhao 的表示违背了 RBAC96 的本意。而在 DL_{RBAC} 表示中没有对用户的直接授权, 而是用权限激活约束公理(公理 13)来表示角色间接授权, 这样更忠实于 RBAC96 模型的本意。

从以上分析可以看出, 本文对基本 RBAC 模型的形式化表示体现了 RBAC 模型的特点, 即用户不是直接被授予权限, 而是通过激活他所在的角色, 间接获得该角色所分配的权限, 并且补充了 RBAC 模型中的继承性定义。

结束语 根据 RBAC 的特点, 结合基本描述逻辑语言 ALC 及其扩展语言, 对基本的 RBAC 模型进行了形式化描述。这种描述不但表示出了基本 RBAC 模型中的各种关系,

还将 RBAC 中与角色继承有关的 RH 继承性、 UA 继承性和 PA 继承性等都定义出来, 从而弥补了 RBAC 模型对这些关系只有隐含说明, 没有明确表示的缺陷。在表示了 RBAC 中的关系和约束基础上, 还通过定义 RBAC 状态和 DL_{RBAC} 模型之间的转换关系, 得出 DL_{RBAC} 模型是忠实对应一个 RBAC 状态的表示方法, 从而为进一步研究 RBAC 的性质打下基础。

参考文献

- [1] Sandhu R, Coyne E, Feinstein H, et al. Role-based access control models[J]. IEEE computer, 1996, 29(2): 38-47
- [2] Ferraiolo D, Sandhu R, Gavrila S, et al. Proposed NIST standard for role-based access control[J]. ACM Transactions on Information and System Security, 2001, 4(3): 224-274
- [3] ANSI INCITS 359-2004. Role Based Access Control[S]. American National Standards Institute, 2004
- [4] Osborn S, Sandhu R, Munawer Q. Configuring role-based access control to enforce mandatory and discretionary access control policies[J]. ACM Transactions on Information and System Security (TISSEC), 2000, 3(2): 85-106
- [5] Li N, Byun J W, Bertino E. A critique of the ANSI standard on role-based access control[J]. IEEE Security and Privacy, 2007, 5(6): 41-49
- [6] Ferraiolo D, Kuhn R, Sandhu R. RBAC standard rationale: Comments on "A critique of the ANSI standard on role-based access control"[J]. IEEE Security and Privacy, 2007, 5(6): 51-53
- [7] Koch M, Mancini L V, Parisi-Presicce F. A graph-based formalism for RBAC[J]. ACM Transactions on Information and System Security, 2002, 5(3): 332-365
- [8] Baader F, Calvanese D, McGuinness D L, et al. Description Logic Handbook[M]. Cambridge University Press, 2002
- [9] Baader F, Küsters R, Wolter F. Extensions to Description Logics [M]. Cambridge University Press, 2002: 226-268
- [10] Zhao C, Heilili N, Liu S, et al. Representation and reasoning on RBAC: a description logic approach[C]// Hung D V, Wirsing M, eds. ICTAC 2005, LNCS 3722. Berlin: Springer, 2005: 381-393
- [11] Ji G, Tang Y, Jiang Y, et al. A description logic approach to represent and extend RBAC model[C]// 1st International Symposium on Pervasive Computing and Applications. 2006: 151-156
- [12] Yu H, Xie Q, Che H. Description Logic Based Conflict Detection Methods for RB-RBAC Model[J]. International Journal of Computer Science and Network Security, 2006, 6(1A): 120-125

(上接第 28 页)

- [36] Seamons K E, Winslett M, Yu T, et al. Requirements for Policy Languages for Trust Negotiation [C]// Proc. of the 3rd IEEE Int'l Workshop on Policies for Distributed Systems and Networks. 2002: 68-79
- [37] Bertino E, Ferrari E, Squicciarini A C. Trust Negotiations: Concepts, Systems and Languages [J]. Computing in Science & Engineering, 2004, 6(4): 27-34
- [38] Herzberg A, Mass Y, Mihaeli J, et al. Access Control Meets Public Key Infrastructure, or: Assigning Roles to Strangers [C]// Proc. of the 21th IEEE Symposium on Security and Privacy (SP'00). 2000: 2-14
- [39] Viljanen L. Towards an Ontology of Trust [C]// LNCS 3592. 2005: 175-184
- [40] Li N, Mitchell J C. Beyond Proof-of-Compliance; Security Analysis in Trust Management [J]. Journal of the ACM, 2005, 52(3): 474-514
- [41] Li N, Tripunitara M V. Security Analysis in Role-based Access Control [J]. ACM Transactions on Information and System Security, 2006, 9(4): 391-420
- [42] Sun Y, Han Z, Liu K J R. Defense of Trust Management Vulnerabilities in Distributed Networks [J]. IEEE Communications Magazine, 2008, 46(2): 112-119
- [43] 廖振松, 金海, 李赤松, 等. 自动信任协商及其发展趋势[J]. 软件学报, 2006, 17(9): 1933-1948
- [44] Liimatainen S. Usability of Decentralized Authorization Systems-A Comparative Study [C]// Proc. of the 38th Hawaii International Conference on System Sciences (HICSS'05). 2005: 186b-186b
- [45] Kinader M, Baschny E, Rothermel K. Towards a Generic Trust Model-Comparison of Various Trust Update Algorithms [C]// Proc. of the iTrust 2005. LNCS 3477. 2005: 177-192
- [46] Fullam K K, Sabater-Mir J, Barber K S. A Design Foundation for a Trust-Modeling Experimental Test Bed [C]// LNAI 3577. 2005: 95-109
- [47] Hassan J, Sirisena H, Landfeldt B. Trust-based Fast Authentication for Multiowner Wireless Networks [J]. IEEE Transactions on Mobile Computing, 2008, 7(2): 247-261