

DTM:一种面向网络计算的动态信任管理模型

李建欣 怀进鹏 李先贤 林 莉

(北京航空航天大学计算机学院 北京 100191)

摘 要 在开放的互联网中,信任关系的建立是实现跨自治域资源共享与协同的前提.然而,网络计算环境的分布自治特性,使得各类复杂系统中应用不同的信任管理机制,容易导致信任定义的不一致问题,特别是很多系统为支持多域协作,直接假设实体间信任具有传递特性,而在模型中缺乏该性质成立的条件;此外,网络计算环境中的动态演化特性,使得驱动实体间协作的信任关系随需而变,而现有信任管理模型仅仅关注于系统功能结构,缺乏对这种动态性的描述.文中提出了一种动态信任管理模型 DTM,基于信念公式形式化定义了主体间的信任公式,并将信任的传递特性(信任链)解释为模型的一条性质.在该模型中,针对信任关系的动态特征,以时间为参量刻画主体公式集,以事件为触发条件刻画主体间信任的变化,并基于正则事件序列描述信任管理的资源授权过程,可刻画主体间信任的建立过程.最终,设计、实现了一个信任管理系统 CROWN-TM,并进行了初步实验分析.

关键词 网络计算;信任模型;信任管理;信任协商;信任证;安全策略

中图法分类号 TP309

DOI号: 10.3724/SP.J.1016.2009.00493

DTM: A Dynamic Trust Management Model for Internet Computing Environments

LI Jian-Xin HUAI Jin-Peng LI Xian-Xian LIN Li

(School of Computer Science and Engineering, Beihang University, Beijing 100191)

Abstract Nowadays, many novel computing technologies such as Pervasive Computing and Grid Computing have emerged to empower resource sharing and collaboration over Internet. However, trust establishment across multiple autonomous domains has become an important issue because resources are dynamic and behaviours are uncontrollable over Internet. Firstly, existing trust management solutions and systems lack of a unified model, specially the definitions of trust in several security mechanisms are inconsistent, moreover there is no formal proof on trust transitive property referring to the trust management model. Additionally, dynamic short-lived collaboration among entities frequently happens, which may require the trust relationship among collaborating entities to be changed on demand. Therefore, this paper proposes a dynamic trust management model (DTM) to support flexible trust establishment between unfamiliar entities, in which the concept of trust is formally defined based on a belief formula, and the transitive property of trust (trust chain) is proved. In this model, an event is used to describe the cause of trust relationship evolution between principals. A regular event sequence is employed to describe the resource authorization process, and a dependent sequence on regular event sequences is designed for the resource authorization process of trust negotiation. Finally, a trust management system in

收稿日期:2008-09-19;最终修改稿收到日期:2009-01-06. 本课题得到国家“九七三”重点基础研究发展规划项目基金(2005CB321803)、国家“八六三”高技术研究发展计划项目基金(2007AA01Z426, 2007AA01Z120)、国家杰出青年基金(60525209)、NSFC-RGC 联合项目(60731160632)资助. 李建欣,男,1979年生,博士,讲师,主要研究方向为信息安全、信任管理、分布式计算. E-mail:lijx@act.buaa.edu.cn. 怀进鹏,男,1962年生,博士,教授,博士生导师,主要研究领域为计算机软件与理论、中间件技术、分布式计算、网络安全. 李先贤,男,1969年生,博士,教授,主要研究领域为信息安全、计算机科学理论. 林莉,女,1979年,博士研究生,主要研究方向为资源管理、信息安全.

CROWN middleware, and some preliminary experiments are conducted and the experimental results are given and analysed.

Keywords Internet computing; trust model; trust management; trust negotiation; credential; security policy

1 引 言

互联网的发展对软件系统的计算环境及应用模式转变产生了重大影响. 如今, 互联网已从传统的计算机通信平台演变为无处不在的分布式网络计算平台, 出现了多种新型网络计算模式(如普适计算、网格计算、对等计算等); 同时, 随着面向服务体系架构 SOA(Service Oriented Architecture)和软件即服务 SaaS(Software as a Service)理念等日益成熟, 软件系统应用模式凸显出网络化、服务化的趋势, 协作实体的自治性、应用边界的开放性、业务需求的动态增长性等成为典型分布式系统(如电子商务、政务、金融等)的主要特点. 然而, 这种计算环境和应用模式的转变, 为互联网中应用系统的信任管理带来诸多新的挑战: 首先, 系统的分布自治特性, 应用业务常涉及多自治域间的服务调用、组合等, 其中一个首先需要突破的问题就是如何在来源于不同自治域、可能陌生的实体间促成协作活动, 使得实体间信任成为跨域协作的瓶颈性难题; 其次, 系统的动态演化特性, 体现为主体的加入退出行为频繁, 导致协作环境及信任关系随需而变, 对有效的信任管理需求增强; 而系统的无安全控制中心特性, 导致难以形成集中资源授权和直接信任关系定义, 需要多域联盟、推荐及委托机制的支持, 这使得探讨信任传递性条件成为一个迫切需研究的问题; 因此, 如何建立互联网下信任管理模型, 以适应计算环境和应用模式发展的需要, 已经成为当前新一代互联网技术研究的热点问题.

信任作为主体间的一种重要关系, 各个领域的研究人员从不同角度试图对其进行规范化, 包括认证体系、安全协议等对其都有研究, 如 Maurer^[1]提出的 PKI 信任模型、Lampson 等^[2]提出的访问控制演算逻辑以及 BAN 逻辑^[3]针对安全认证协议给出的逻辑模型等. 在信任管理研究中, Blaze 等^[4]从系统功能角度给出一个静态概念模型 PolicyMaker, 研究人员还从策略表达能力角度给出多种信任管理系统和语言^[5-8]. 但是这些研究在信任定义、信任动态性刻画以及信任管理统一描述方面仍存在如下

3 个主要问题:

(1) 信任的形式化定义. 现有研究主要通过自然语言定义信任概念. 例如 ITU X. 509 标准中, 对“信任”的自然语言描述为: “当主体 A 假设主体 B 将严格按照其所期望的那样行动时, 则称 A 信任 B”. 该信任的定义是用来描述鉴别主体与认证权威(Certificate Authority, CA)之间关系的, 表示主体相信 CA 能够像其所期望的那样, 准确地建立并维持主体公钥与身份的绑定; 在 PKI 模型中, 常提到的信任模型(如层次式信任、网状信任等)实质则是对认证权威 CA 组织结构的描述. 依赖自然语言定义信任, 往往会导致应用系统中信任理解的不一致问题. 例如, 分属于不同安全域的主体 A 和 B, 如果仅简单陈述主体 A 信任主体 B, 就存在着不确定性, 很多应用场景中, A 信任 B 并不意味着主体 B 的所有行为和权限都可以被 A 信任, 比如 A 仅仅在计算机研究领域认为 B 的断言是可被信任的, 但在其他研究领域 B 的断言不一定是可被信任的. 这也恰恰说明了主体间的信任关系一般针对的是特定的环境和命题.

此外, 很多信任模型中通过假设信任具有传递性质, 并构造信任链来支持跨自治域实体间信任关系的建立, 但这种性质是否存在一直是有争议的. 例如 A 信任 B 是针对命题 p , B 信任 C 却是针对命题 q , 显然不能推导出 A 信任 B 的结论.

因此, 如何形式化定义实体间的信任, 并能够在模型中给出信任传递性成立的语义解释和约束条件是非常重要的, 这也是开放环境中实现可信协作的基础.

(2) 主体间信任关系的动态特征刻画. 由于计算环境的动态性, 主体安全策略的频繁变化, 使得在不同时间参照点主体间的信任关系往往不同. PolicyMaker 中首次所引入的信任管理模型, 其本质仍属于从系统功能角度给出的一个静态概念模型. 但是, 在信任管理系统的实际应用中, 由于信任证收集、策略更改等事件的发生, 主体间信任关系往往随需而变, 这就要求信任管理模型能够对主体间信任关系的动态性予以刻画.

(3)信任管理与协商资源授权过程的统一描述. 目前,针对不同应用系统,研究人员提出了不同的信任管理策略语言,在策略结构、表达能力等方面都存在着差别. 特别是,在信任管理策略语言设计之初,很少考虑到对信任证和策略中隐私信息的保护,近年来研究人员则通过定制信任协商协议扩展信任管理系统功能,例如基于 TPL(Trust Policy Language)的信任协商系统 TrustBuilder 是基于 RT 的 TTG(Trust Target Graph). 从而,针对不同信任管理语言研究不同的信任协商协议,由于缺乏对它们授权原理的统一描述,导致很多算法和协议难以被重用,反而又在不同信任协商系统间衍生出可互操作问题. 因此,在信任管理模型中综合考虑对信任证及策略隐私的保护,提出支持信任协商过程描述的信任管理模型是很有必要的.

针对上述问题,我们建立了一个动态信任管理模型(Dynamic Trust Management Model,DTM). 如图 1 所示,相比信任管理概念模型主要侧重于管理功能结构(如一致性验证器、信任证、策略等功能)和静态信任关系描述,DTM 模型主要工作包括信任的形式化定义、动态性刻画以及信任管理与协商过程的统一描述. DTM 模型基于信念公式定义了主体间的信任公式,并将信任的传递特性(信任链)解释为模型的一条性质. 在 DTM 模型中,以时间为参照点刻画主体公式集,以事件为触发条件研究主体间信任关系的动态变化,通过正则事件序列刻画信任管理资源授权过程,进而利用正则事件序列的依赖序列刻画包含协商的信任管理资源授权过程. 此外,通过在 DTM 模型中的信念和信任公式中引入信任度因子,DTM 模型同时可支持对主观信任模型的策略描述,从而可借助主体信任度和信誉度评估方法来提高信任管理模型中策略定义的灵活性和可适应性.

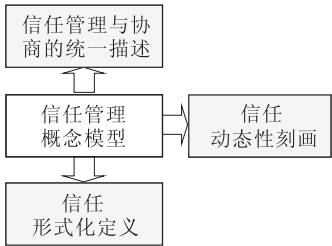


图 1 DTM 模型的主要工作

2 相关工作

在分布式网络环境中,一些典型安全系统中已

涉及到信念、信任及信任管理理论和技术研究,本节将主要介绍这三方面的研究工作.

2.1 知识与信念的研究

认知逻辑(Epistemic Logic)基于模态逻辑给出了知识及信念概念,特别是在知识管理和人工智能领域得到了较大发展. 20 世纪 60 年代,Hintikka^[9]首次将模型论运用到认知逻辑的研究之中,给出了认知逻辑的语义解释;进入 90 年代,Moore 等将关于知识的逻辑引入到人工智能的研究之中. 为形式化描述 Agent 理论中的主体特性^[10],Rao 和 Georgeff^[11]给出了一个形式化模型 BDI,采用信念(belief)、愿望(desire)和意图(intention)模态词描述主体的可能世界语义. Abadi 等^[12]为分析通信安全协议的可认证性,提出了 BAN 逻辑,定义了相应的操作语义用作主体信念的生成. 此外,Rangan 逻辑^[13]采用模态逻辑研究信任,YKB 逻辑则设定知识和信念的演化都是单调的,亦即知识和信念的演化只增不减,Moser 逻辑是唯一的例外,它的信念演化是非单调的,例如在推理过程中如果知道一个密钥已被泄露,则信念集会减少.

目前的研究认为:能够从主观上和客观上都判断为真的是知识,从主观上依据充分证据判断为真的是信念;而且知识具有传播性,即知识可以从一个认知主体传到另一个认知主体,但信念却不能在主体间传递,即一个主体的信念,并不一定能被另一个主体所接受. 在认知逻辑对信念的研究中,主要针对各个独立主体的信念及其与知识的关系,研究了主体对于信念的判断关系,而缺乏研究多个主体间信念的关系,即未涉及到主体间信任的研究. 此外,上述工作主要基于了知识与信念的逻辑方法,而且是针对特定领域内问题开展的研究,其中的信念概念亦作为本文信任管理模型的基础.

2.2 授权系统中信任的研究

围绕分布式系统的授权和访问控制技术,许多研究人员都试图对其中的信任概念给出形式化描述和定义. Maurer^[1]从用户角度建立了 PKI 形式化描述和推理模型,他的贡献之一就是引入了“推荐(Recommendation)”机制,使对一个主体的信任能够转化为对另一个主体的信任. Lampson, Abadi 等^[2,14]提出了分布式系统中认证和访问控制的逻辑模型,采用 speak for 表示委托,针对的仅仅是访问控制列表策略. 最近,Microsoft 研究院的 Becker 等^[15]提出了一种分布式授权语言 SecPAL,综合了信任、委托和授权概念,该语言能够基于约束、受限

委托和递归谓词以及查询表述多种策略规范,然而 SecPAL 主要关注于策略的语义和表达力研究,并不能够作为信任管理基础模型。

在认证体系中对信任的研究,主要是身份认证及委托概念的逻辑描述,缺乏对实体信任关系的形式化定义,特别是在现有的信任定义或模型中,为实现跨域认证,往往假设信任具有传递性质,而缺乏在模型中给出该性质成立的前提条件,所以具有本质的缺陷.因此,这些工作并非特定针对于信任管理研究领域,也缺乏对基于协商建立信任过程的描述。

2.3 信任管理与协商模型的研究

Blaze 最早提出的信任管理框架^[4,16],描述了基于本地策略 P 来判断资源请求 r 是否能够被授权的结构,PolicyMaker 和 KeyNote 是该框架的代表性系统.这些系统都给出了策略语法规则,但缺少严格的语义解释和推理规则. Li 等^[5,17-18]结合委托逻辑、RBAC 模型提出了信任管理语言 RT. 进而, Winsborough 等^[19]基于 RT,给出了一个信任协商协议 TTG. Bonatti^[20]针对信任协商提出了一个命题式框架 PROTUNE,该框架主要侧重协商过程控制元策略的形式化描述。

上述工作主要是针对信任管理中委托、约束等策略表达能力问题以及信任协商中敏感信息披露的控制元策略开展研究. 这些工作一方面缺乏对信任的形式化定义,缺乏对信任链成立条件的证明,另一方面缺乏对信任管理与协商中资源授权过程的统一描述。

3 动态信任管理模型 DTM

信任管理技术是随着互联网应用发展而提出,现有的研究工作较多地关注于其技术与系统,但信任管理技术的最终目标仍然是构建主体间的信任关系,这就需要对各类技术方法所依赖的信任、信任链等基本概念给出形式化定义. 因此,本文提出一个动态信任管理模型 DTM,能够基于信念公式描述主体间的信任关系。

3.1 模型的语法与语义

在 DTM 模型中,语法包括:

主体常量. 主体常量采用带或不带下标的大写字母 A, B 和 C 表示,在实例中,也采用以大写字母开头的主体简称来表示. 主体可以是一个用户,服务或进程,在信任管理中主要通过主体公钥来标识一个主体常量,例如主体 Alice 可由其公-私钥对

$K_{Alice}, K_{Alice}^{-1}$ 来标识。

时间变量. 在不同时间,主体的策略可能会不同,不同的时间采用 t_1, t_2, \dots 表示。

命题符号. 一个命题符号可以采用带或不带下标的小写字母 p, q, r 表示,每个命题通常是对主体身份、能力或属性的断言策略,例如命题 $p = \text{"Alice is a student"}$,即表示对主体 Alice 具有角色属性 student 的判断;命题 $q = \text{"Alice has Read permission on resource Service"}$,该命题实质为主体的一个授权项,即访问控制策略声明三元组 (subject, object, action)。

逻辑连接词. 包括命题逻辑中的逻辑连接词 $\neg, \wedge, \vee, \rightarrow$ 。

信念公式. 信念是一个主体在自身知识和经验基础之上的一种判断,是一种主体与命题间的关系,我们将信念关系符号记作 \models ,属于一个三元关系 (A, t, p) ,即表示主体 A 在时间 t 的策略可以推导出一个真命题 p ,即存在信念公式 $(A, t) \models p$ 。

一个公式 F (不同公式可以采用下标来区分)可如下递归定义:

(1) 如果 p 是一个命题符号,则 p 是一个原子公式;

(2) 如果 p 是一个命题符号,则 $(A, t) \models p$ 是一个公式 (亦称为信念公式);

(3) 如果 F_1, F_2 是公式,则通过逻辑连接词形成的 $F_1 \wedge F_2, F_1 \vee F_2, F_1 \rightarrow F_2, \neg F_1$ 也是一个公式;

在一个公式中,我们假定对于 $\neg, \models, \wedge, \vee, \rightarrow$,左边的连接符号要优于右边的连接符号. 由多个公式组成的集合用带或不带下标的字母 \mathcal{F} 表示。

DTM 的语义. 一个信任管理的模型是五元组结构 $\mathcal{TH} = (\mathcal{A}, \mathcal{T}, \mathcal{P}, \Sigma_{\mathcal{TH}}, \varphi)$,其中 \mathcal{A} 是一个主体集, \mathcal{T} 是一个时间集,而且时间集是一个全序集,即其中的时间元素存在全序关系 $<$, \mathcal{P} 是公式全集, \mathcal{TH} 为主体的一个公式集,称为主体的一个理论, $\Sigma_{\mathcal{TH}}$ 是主体理论的集合,满足 $\Sigma_{\mathcal{TH}} \subseteq 2^{\mathcal{P}}$, φ 是一个映射 $\mathcal{A} \times \mathcal{T} \rightarrow \Sigma_{\mathcal{TH}}$,表示主体 A 在时间 t 的公式集 (主体的一个理论). 对于主体 A 在时间 t 的一条信念 q ,即公式 $F: (A, t) \models q$,如果该信念包含在其理论内,则等价于该命题 q 包含在其理论内,即 $((A, t) \models q) \in \varphi(A, t)$ iff $q \in \varphi(A, t)$. 对公式的语义解释如下:

(1) 对于一个命题 p ,信念公式 $(A, t) \models p$ iff $\varphi(A, t) \models p$,即主体 A 在时间 t 存在信念 p ,当且仅当从相应的理论 $\varphi(A, t) = \mathcal{TH}$ 能够逻辑推导出命题 p 。

(2)对其他逻辑连接词形成公式的语义解释是自然的,不再赘述.

3.2 模型的性质及应用

在本节中,我们将讨论 DTM 的基本性质,对 \mathcal{TM} 模型中公式的有效性、可满足性,主体理论的协调性、等价性和单调性等概念给出形式化定义,并说明其在信任管理技术和系统中的应用.特别是,基于信念公式给出主体间的信任定义,并给出了主体间信任链成立的严谨证明.

定理 1. 在一个信任管理模型 \mathcal{TM} 中,对于每个理论 $\varphi(A,t)=\mathcal{TH}$,存在如下等价关系:

- (1) $(A,t) \models p$ iff $\varphi(A,t) \models p$;
- (2) $(A,t) \models (p \rightarrow q)$ iff $(A,t) \models p \rightarrow (A,t) \models q$;
- (3) $(A,t) \models \neg p$ iff $\neg((A,t) \models p)$;
- (4) $(A,t) \models p \wedge q$ iff $(A,t) \models p \wedge (A,t) \models q$.

证明. 对于关系(1),由模型的语义可知是显然成立的,该等价关系的直观含义为:命题 p 是主体 A 在时间 t 已存在的策略定义或经过逻辑推导得出的一个真命题.

对于关系(2),由关系(1)和命题逻辑的推理规则,证明过程如下:

$$\begin{aligned} (A,t) \models (p \rightarrow q) &\text{ iff } \varphi(A,t) \models (p \rightarrow q) \\ &\text{ iff } \varphi(A,t) \models p \rightarrow \varphi(A,t) \models q \\ &\text{ iff } (A,t) \models p \rightarrow (A,t) \models q \end{aligned}$$

所以关系(2)成立;

同理,对于关系(3)和(4)也可采用上述过程来证明. 证毕.

同时,在模型 \mathcal{TM} 中的理论相应也包括如下两条基本的逻辑推理规则:

- (R1) 分离规则: $\frac{(A,t) \models F_1, (A,t) \models (F_1 \rightarrow F_2)}{(A,t) \models F_2}$;
- (R2) 推广规则: $\frac{\models F}{(A,t_k) \models F}, \forall t_k \in Time$.

定义 1(公式的可满足性和有效性). 假设一个信任管理模型 \mathcal{TM} ,对其中的一个主体 A ,如果在时间 $t \in \mathcal{T}$ 的一个理论 $\varphi(A,t)=\mathcal{TH}$,存在 $(A,t) \models F$,则称公式 F 对于主体 A 是可满足的;如果在任意时间 $t_k \in \mathcal{T}$ 的理论 $\varphi(A,t_k)=\mathcal{TH}_k$,都存在 $(A,t_k) \models F$,称公式 F 对于主体 A 是有效的.

可以看出,信任管理模型中的时间集 \mathcal{T} 很关键,公式的有效性是针对 \mathcal{T} 内的所有元素而言. 在开放的网络计算环境中,该定义主要用于刻画已达成契约的协作策略,即在形成协作联盟的生命周期 \mathcal{T} 内,这些策略所表达的公式是一直成立的,即该公式是

有效的. 而且,基于该定义容易验证如下性质.

性质 1. 对于一个信任管理模型 \mathcal{TM} ,在主体 A 的一个理论集中,如果公式 F 是有效的,当且仅当 $\rightarrow F$ 是不可满足的.

DTM 模型所描述的主体理论为特定时间与主体相关的一个公式集,即信任管理系统应用中,对应于资源授权决策的策略集.下面将给出与主体理论相关的 3 个性质定义.

理论 \mathcal{TH} 间关系	性质定义
一个理论	协调性
两个理论间关系	等价性
多个理论间关系	单调性

定义 2(协调性). 假设一个信任管理模型 \mathcal{TM} ,其中主体 A 的一个理论为 \mathcal{TH} ,如果对于任何公式 F ,当满足 $(A,t) \models F$,不存在信念关系 $(A,t) \models \neg F$,则称理论 \mathcal{TH} 是协调的.

理论的协调性定义保证了从一个理论中推导出的公式不会出现矛盾的结论.

定义 3(等价性). 假设一个信任管理模型 \mathcal{TM} ,在两个时间 $t_1, t_2 \in \mathcal{T}$ 且 $t_1 < t_2$,相应的两个理论为 $\varphi:(A,t_1) \rightarrow \mathcal{TH}_1$ 和 $\varphi:(A,t_2) \rightarrow \mathcal{TH}_2$,如果存在一个公式 F ,使得两个信念公式 $(A,t_1) \models F$ 和 $(A,t_2) \models F$ 中仅有一个成立,则称两个理论 \mathcal{TH}_1 和 \mathcal{TH}_2 是不等价的,否则称两个理论是等价的.

在信任管理资源授权过程中,如果两个理论是等价的,则在两个时间对于同一主体的授权决策结果是相同的,该定义主要应用于服务器在执行多次授权决策操作时,如果两个时间的理论集是等价的,则不需要进行重复的推理计算.

定义 4(单调性). 假设一个信任管理模型 \mathcal{TM} ,如果对于主体 $A \in \mathcal{A}$,在一个时间集 $Time \subseteq \mathcal{T}$ 的任意两个时间 $t_1, t_2 \in Time$ 且 $t_1 < t_2$,满足 $(A,t_1) \models F \rightarrow (A,t_2) \models F$,则称主体 A 在时间集 $Time$ 上的理论是单调的.

由于信任管理研究所针对的是一种分散式网络环境,在一次授权决策过程中收集到 \mathcal{P} 中的所有策略公式是不容易的,因此需要假设在一次授权过程中(即一个时间集 $Time$ 的范围内),主体的理论要保持单调性^[21]. 也就是说,一个主体在授权决策过程中不会推导出与其之前相反的信念,而且信念集合中的公式也不会被删去. 该定义主要应用于指导运行系统中的信任管理策略配置.

定义 5(信任). 假设一个信任管理模型 \mathcal{TM} ,存在两个理论 $\varphi(A,t)=\mathcal{TH}_1$ 和 $\varphi(B,t)=\mathcal{TH}_2$,对于

一个公式 F , 若满足公式 $(B, t) \models F \rightarrow (A, t) \models F$, 则称在 t 时间对于公式 F , 主体 A 信任主体 B , 记作 $A \mapsto_{t, F} B$.

对于主体 A 的一个理论 \mathcal{TH}_1 中的公式集 \mathcal{F} , 存在信任公式 $A \mapsto_{t, \mathcal{F}} B$ 当且仅当对于每一个公式 $F \in \mathcal{F}$, 都满足 $(B, t) \models F \rightarrow (A, t) \models F$.

定理 2. 假设一个信任管理模型 \mathcal{TM} , 存在 3 个理论 $\varphi(A, t) = \mathcal{TH}_1$, $\varphi(B, t) = \mathcal{TH}_2$ 和 $\varphi(C, t) = \mathcal{TH}_3$, 对于其中的两个公式集 \mathcal{F}_1 和 \mathcal{F}_2 , 如果满足 $A \mapsto_{t, \mathcal{F}_1} B, B \mapsto_{t, \mathcal{F}_2} C$, 则存在 $A \mapsto_{t, (\mathcal{F}_1 \cap \mathcal{F}_2)} C$.

证明. 由条件 $A \mapsto_{t, \mathcal{F}_1} B$, 根据定义可得

$$\forall F_1, F_1 \in \mathcal{F}_1 \text{ s. t. } (B, t) \models F_1 \rightarrow (A, t) \models F_1, \quad (1)$$

即 $\forall F_1, F_1 \in (\mathcal{F}_1 \cap \mathcal{F}_2)$, 亦满足

$$(B, t) \models F_1 \rightarrow (A, t) \models F_1$$

同理, 由条件 $B \mapsto_{t, \mathcal{F}_2} C$, 根据定义可得

$$\forall F_2, F_2 \in (\mathcal{F}_1 \cap \mathcal{F}_2),$$

亦满足

$$(C, t) \models F_2 \rightarrow (B, t) \models F_2 \quad (2)$$

由式(1)、(2)可得

$$\forall F, F \in (\mathcal{F}_1 \cap \mathcal{F}_2),$$

满足

$$(C, t) \models F \rightarrow (A, t) \models F;$$

即存在信任公式 $A \mapsto_{t, (\mathcal{F}_1 \cap \mathcal{F}_2)} C$. 证毕.

当定理 2 中的公式集为两种特殊情形时, 可以得到如下两条推论.

推论 1. 假设一个信任管理模型 \mathcal{TM} , 存在 3 个理论 $\varphi(A, t) = \mathcal{TH}_1$, $\varphi(B, t) = \mathcal{TH}_2$ 和 $\varphi(C, t) = \mathcal{TH}_3$, 对于公式集 \mathcal{F} , 如果满足 $A \mapsto_{t, \mathcal{F}} B, B \mapsto_{t, \mathcal{F}} C$, 则存在 $A \mapsto_{t, \mathcal{F}} C$.

如果 \mathcal{F} 是一个公式全集, 则表示主体 A 对 B 的任何信念都信任, 即 B 作出的任何断言 A 都信任.

推论 2. 假设一个信任管理模型 \mathcal{TM} , 存在 3 个理论 $\varphi(A, t) = \mathcal{TH}_1$, $\varphi(B, t) = \mathcal{TH}_2$ 和 $\varphi(C, t) = \mathcal{TH}_3$, 对于命题 p , 如果满足 $A \mapsto_{t, p} B, B \mapsto_{t, p} C$, 则存在 $A \mapsto_{t, p} C$.

该信任定义可描述信任管理系统中关键概念委托授权, 类似委托逻辑 DL 中的 delegate 策略声明, 例如 $A \mapsto_{t, p} B$, 表示如果 $(B, t) \models p$, 则 $(A, t) \models p$.

对推论 2 进行推广, 当满足 $A \mapsto_{t, p} B_1, \dots, B_k \mapsto_{t, p} B_{k+1}, B_{k+1} \mapsto_{t, p} C$ 时, 可以推导出信任关系 $A \mapsto_{t, p} C$, 则称这些公式形成的一个序列:

$$A \mapsto_{t, p} B_1 \mapsto_{t, p} B_2 \mapsto_{t, p} \dots \mapsto_{t, p} B_k \mapsto_{t, p} B_{k+1} \mapsto_{t, p} C$$

为主体 A 和 C 在时间 t 形成关于命题 p 的一条信任链.

在信任管理模型中, 一个主体的理论公式集往往是动态变化的. 在策略管理阶段, 引起理论公式集发生变化的主要原因是策略更改, 而策略更改完全是为了适应主体间协作关系、安全环境等因素的变化. 在信任管理的资源授权过程中, 引起理论公式集发生变化的主要原因则是信任证的发现和收集, 这些信任证包括其他主体制定的策略或拥有的证书, 从而能够保证从主体的一个理论中推导出新的信念公式. 为了描述信任管理模型具有的这种动态性, 我们引入事件概念.

定义 6(事件). 假设一个信任管理模型 \mathcal{TM} , 对于主体 A , 在两个时间 $t_1, t_2 \in \mathcal{T}$ 且 $t_1 < t_2$, 对应的两个理论分别为 $\varphi: (A, t_1) \rightarrow \mathcal{TH}_1$ 和 $\varphi: (A, t_2) \rightarrow \mathcal{TH}_2$, 我们将引起理论发生变迁 $[\mathcal{TH}_1 \rightarrow \mathcal{TH}_2]$ 的过程称为一个事件 σ , 该事件所满足的理论迁移为 $(A, t_1) \xrightarrow{\sigma} (A, t_2)$.

基于事件及理论等价性的定义, 容易验证如下性质.

性质 2. 假设一个信任管理模型 \mathcal{TM} , 主体 A 的两个理论分别为 $\varphi(A, t_1) = \mathcal{TH}_1$ 和 $\varphi(A, t_2) = \mathcal{TH}_2$, 如果两个理论间不存在任意事件 σ , 则可判断这两个理论是等价的.

对于一个信任管理模型 \mathcal{TM} , 令

$$\Sigma_\sigma = \{ \sigma \mid (A, t_i) \xrightarrow{\sigma} (A, t_{i+1}), A \in A, t_i, t_{i+1} \in \mathcal{T}, t_i < t_{i+1} \},$$

称为模型 \mathcal{TM} 的事件空间. 由事件空间中的事件元素组成的一个序列 $\omega = \langle \sigma_1, \sigma_2, \dots, \sigma_n \rangle$, 相应称为事件序列.

定义 7(正则事件序列). 对于与主体 A 相关的一个事件序列 $\omega = \langle \sigma_1, \sigma_2, \dots, \sigma_n \rangle$, 如果该序列满足如下条件:

(C1) 事件序列 ω 中的每个事件 σ_i , 满足如下的理论迁移过程(其中主体不变):

$$(A, t_0) \xrightarrow{\sigma_1} (A, t_1) \xrightarrow{\sigma_2} \dots \xrightarrow{\sigma_n} (A, t_n),$$

也可以记作 $(A, t_0) \xrightarrow{\omega} (A, t_n)$;

(C2) 主体 A 在时间集 $Time = \{t_0, \dots, t_n\}$ 上的理论 $\varphi(A, t_i)$ 具有单调性,

则称事件序列 ω 为正则事件序列.

定义 8(信任管理资源授权). 假设一个信任管理模型 \mathcal{TM} , 资源提供主体为 A , 资源请求主体为 B , 对于资源访问请求形成的一个命题 r , 信任管理模型中对资源访问请求的可授权判定条件

是:存在与主体 A 相关的一个正则事件序列 ω , 使得 $(A, t_0) \xrightarrow{\omega} (A, t_n)$, 且满足 $(A, t_n) \models (A \mapsto_{t_n, r} B)$, 其中 (A, t_0) 是主体 A 在访问请求时间 t_0 的理论, (A, t_n) 是主体 A 在资源授权决策时间 t_n 的理论。

在这里,信念公式 $(A, t_n) \models (A \mapsto_{t_n, r} B)$ 的直观含义为:如果主体 B 向主体 A 发起资源访问请求,该请求可以表示为一个命题 r (例如命题为一个请求授权项,其内容由主体、客体和操作描述),则 A 可以推导出 B 具有资源访问权限的信念。同时,该定义实际上给出了在应用系统中实现信任管理资源授权决策的一个判定条件,即需要验证主体理论间的事件序列是一个正则事件序列。

对于一个典型的信任证或策略获取事件 σ_i , 当其中主体请求获取的信息(信任证或策略)是敏感的,对方则需要相应执行信任管理资源授权操作,这样双方建立信任关系就需借助协商方式经过多次的授权。

定义 9(基于协商的信任管理资源授权)。假设一个信任管理模型 TM , 资源提供主体为 A , 资源请求主体为 B , 对于资源访问请求形成的一个命题 r , 基于协商的信任管理资源授权判定条件是:存在一个由正则事件序列形成的依赖序列:

$\Gamma = \langle \omega_1^A, \omega_1^B, \dots, \omega_m^B, \omega_m^A \rangle$ 或 $\Gamma = \langle \omega_1^B, \omega_2^A, \dots, \omega_m^B, \omega_m^A \rangle$ 。

不失一般性,我们假设依赖序列为 $\Gamma = \langle \omega_1^A, \omega_1^B, \dots, \omega_m^B, \omega_m^A \rangle$, 即主体 A 首先无条件披露信任证(即 A 在时间 t_0 的理论可推出信任 B 的信任证请求命题 r_{B0} 成立), 该序列满足如下过程:

1. 在时间 t_0 。

在主体 A 的初始理论中可得

$$A \mapsto_{r_{B0}, t_0} B,$$

即存在 $(A, t_0) \models r_{B0}$, 请求 r_{B0} 包含的信任证可使事件序列 ω_1^B 执行完成;

在主体 B 的理论中可得

$$(B, t_0) \xrightarrow{\omega_1^B} (B, t_1),$$

即 $B \mapsto_{r_{A0}, t_1} A$, 请求 r_{A0} 包含的信任证可使事件序列 ω_1^A 执行完成;

在主体 A 的理论中可得

$$(A, t_0) \xrightarrow{\omega_1^A} (A, t_1),$$

即 $A \mapsto_{r_{B1}, t_1} B$, 请求 r_{B1} 包含的信任证可使事件序列 ω_2^B 执行完成;

2. 在时间 t_1 。

在主体 B 的理论中可得

$$(B, t_1) \xrightarrow{\omega_2^B} (B, t_2),$$

即 $B \mapsto_{r_{A1}, t_2} A$, 请求 r_{A1} 包含的信任证可使事件序列 ω_2^A 执

行完成;

在主体 A 的理论中可得

$$(A, t_1) \xrightarrow{\omega_2^A} (A, t_2),$$

即 $A \mapsto_{r_{B2}, t_2} B$, 请求 r_{B2} 包含的信任证可使事件序列 ω_3^B 执行完成;

...

m. 在时间 t_{m-1} 。

在主体 B 的理论中可得

$$(B, t_{m-1}) \xrightarrow{\omega_m^B} (B, t_m),$$

即 $B \mapsto_{r_{A, m-1}, t_m} A$, 请求 $r_{A, m-1}$ 包含的信任证可使事件序列 ω_m^A 执行完成;

在主体 A 的理论中可得

$$(A, t_{m-1}) \xrightarrow{\omega_m^A} (A, t_m),$$

即 $A \mapsto_{r_{B, t_m}} B$, 即主体 B 访问请求资源可以被信任。

上述事件变化过程还可以采用如下的一个正则事件序列依赖图来表示,如图 2,其中实线表示一个主体理论的迁移,虚线表示不同时间主体理论能够推导出满足对方请求的信念,从而使得主体可成功完成下一步的事件。

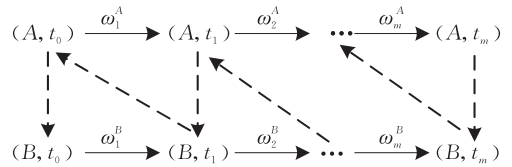


图 2 基于正则事件序列的依赖关系

基于正则事件序列的依赖关系可支持对敏感信任证的保护,实质上描述了支持分布式信任链构造的信任协商原理。因此,DTM 模型可以作为信任管理技术及系统的基础,一方面应用于信任管理语言设计的形式化基础,另一方面则主要应用于对信任管理资源授权(包括信任协商)的决策基础。

4 模型描述及扩展讨论

在信任管理语言中,所表达的命题策略一般具有特定的结构,可能包括多种属性及其约束。根据策略结构的不同,可以对主体信念进行分类,这将有助于管理员对策略实施更为有效的管理。此外,DTM 是一种依赖信任证的信任管理模型,在开放的网络计算环境中,很多研究也依赖主体历史交互行为记录和经验,形成对主体的主观信任度,提出了多种信誉度和信任度计算方法。因此,DTM 模型可以经过扩展增加表达能力,最终通过 XML 等元语言定义出适用于系统的信任管理语言(其关系如图 3 所示)。



图 3 模型与信任管理语言关系

4.1 对策略结构描述的扩展

在本文提出的动态信任管理模型 DTM 中,将策略的实例抽象成为一个命题公式,在实际的复杂应用中,可以进一步对其进行细粒度扩展描述,例如可以采用一个谓词 $pred(term_1, \dots, term_n)$ 表示与主体相关联的身份、能力或属性以及上下文环境等,其中 $term$ 是一个项,可以是常量或变量。例如对于谓词符号 $student$ 和一个主体变量 X ,公式 $student(X)$ 可描述主体 X 是否为具有 $student$ 属性,当存在变量替换 $student(X/Alice) = true$,表示公式 $student(Alice)$ 为真。

按照策略的含义和用途,主体信念存在两种分类方式(如图 4)。按照主体信念公式的生成方式,可以分为主体断言信念和主体推断信念。主体断言信念也就是主体定义的策略,例如存储在本地的一条策略规则所蕴含的信念关系,其作用等同于委托逻辑 DL 中的 $says$ 符号。主体推断信念是根据本地策略翻译过的信念公式以及收集到其他主体的信念公式,形成一个理论并根据规则进行推导而生成的新信念。按照主体信念公式的结构,可以分为主体事实信念和主体规则信念,其中主体事实信念就是对一个主体的身份、属性和权限事实的断言,例如一个证书权威定义了公钥 Key_{Alice} 拥有主体具有高校 BUAA 身份属性 $student$ (即为 BUAA 的学生),即 $(BUAA, t) \models student(Key_{Alice})$;主体规则信念表示公式包含一个蕴含表达式,例如 $(IEEE, t) \models (RegDiscount(X) \leftarrow IEEEMember(X))$,表示如果主体变量 X 属于一个 IEEE 的会员,则也能够享受会议注册费折扣。

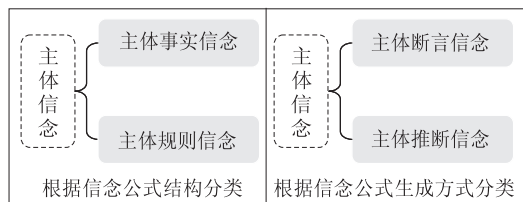


图 4 主体信念的分类

DTM 模型的一个核心特征是将信任传递性解释为模型的一条性质,可用于对信任管理系统中核

心概念委托的描述。基于该特征,DTM 模型中的信念和信任定义可作为信任管理语言的基础。例如通过 DTM 可以描述身份认证系统中信任,假设 Alice 访问北航 BUAA 提供的服务 S ,信念公式为 $(BUAA, t) \models Key'_{Alice} s \text{ name is } DN_{Alice}$,对应描述了对 Alice 身份 DN_{Alice} 的认证结果,而信念公式 $(BUAA, t) \models (Access(S) \leftarrow DN_{Alice})$ 则对应描述了对 Alice 请求的授权结果;而且,通过 DTM 模型也可以用于定义代表性信任管理语言 RT_0 中的 4 种信任证。对于 RT_0 中类型 1 信任证,形如 $A.r_0 \leftarrow B$ (表示主体 A 认为主体 B 具有角色 r_0 的权限),在 DTM 模型中则可表示为一条信念公式: $A \models p, p = "B \text{ has permissions of role } r_0"$;对于 RT_0 中类型 2 信任证,即基于身份的委托信任证 $B.r_0 \leftarrow A.r_0$ (表示主体 B 将一个主体是否具有角色 r_0 的权限定义委托给主体 A),在 DTM 模型中可表示为一条信任公式: $B \mapsto_p A, p = "C \text{ has permissions of role } r_0"$;对于 RT_0 中类型 3 和类型 4 信任证,即 RT_0 提出的主体结构(Principal Structure),在 DTM 模型中也可自然表示;同理,基于 DTM 模型也可以定义其他信任管理语言如 dRBAC、SD3 及 SDSI\SPKI 等的委托规则。

4.2 对主观信任模型策略描述的扩展

信任管理是一种依赖信任证作为信任建立基础的技术,具有易管理和可信程度高的优势,已得到了广泛的应用。然而,具有同一类信任证的主体往往在信誉及信任度等方面还存在着差别,例如加盟某组织的多个文件服务主体,由于各自的软硬件配置不同,就使得各主体提供文件服务的可信度完全不同,这种情形特别是在 P2P 计算中较为普遍。如今,研究人员提出了根据历史交互经验对主体行为进行主观预测的方法,这类信任模型相应的称为主观信任模型或计算型信任模型。在主观信任模型中,主体间的信任关系由直接信任(direct trust)和推荐信任(recommendation trust)合成,其中直接信任是主体直接根据其交互历史记录对另一个主体形成的信任度,推荐信任是主体根据其他主体对另一个主体的间接推荐形成的信任度,也称为间接信任(indirect trust)或信誉(reputation)。典型的研究工作包括 Beth^[22]、Rahman^[23]、Jøsang^[24] 以及 P2P 计算中的 P2PRep^[25]、EigenTrust^[26] 等。

通过对 DTM 模型中信念公式的扩展,引入信任度因子,可用于支持主观信任模型策略的描述,从而为网络计算环境提供了一种更为灵活的信任管理

方式. 当主体 A 访问 B 提供的某项文件服务时, 希望根据 B 提供服务的执行历史记录得出该服务的可信度. 对于 B 而言, 与其服务可信度相关的命题为 $p = "B \text{ provides a trustworthy file service}"$, 我们通过为信念公式引入 3 个信任度因子 v_D 、 v_R 和 v , 分别用于表示主体对命题 p 的直接信任度、推荐信任度和综合信任度, 而且信任度参数会存在一个值域, 例如常用的一个值域是 $[0, 1]$. 按照此思路, 通过对 DTM 模型中公式扩展, 可得

(1) 信念公式为 $A \models p: v$, 表示主体 A 对命题 p 成立的信任程度为 v (也可以是直接信任度);

(2) 信任公式为 $A \mapsto_p B: v_{D_1}$, 表示如果存在 $B \models p: v_{D_2}$, 主体 A 对命题 p 成立的信任程度, v_{D_1} 是主体 A 对推荐方 B 信念的直接信任度.

在主观信任模型中, 主体 A 的命题 p 的直接信任度记作: $A \models p: v_D$. 假设推荐主体集为 $\{B_1, B_2, \dots, B_n\}$, 而且这些推荐主体对命题 p 的信念公式形成的集合为: $F_1 = \{B_1 \models p: v_{D_1}, B_2 \models p: v_{D_2}, \dots, B_n \models p: v_{D_n}\}$, 主体 A 对所有推荐者的直接信任公式形成的集合为

$F_2 = \{A \mapsto_p B_1: v_{D_1}, A \mapsto_p B_2: v_{D_2}, \dots, A \mapsto_p B_n: v_{D_n}\}$, 所以主体 A 对命题 p 形成的信念公式记作: $A \models p: (v_R, v)$, 其中推荐信任度 (信誉) 为 $v_R = \lambda(F_1, F_2)$, 综合信任度为 $v = \delta(v_D, v_R)$.

按照 DTM 模型, 根据某个公式集 $\{B_1 \models p, A \mapsto_p B_1\}$, 即可以推导出信念关系 $A \models p$, 但在扩展的模型中, 则需要同时借助两个函数 λ 和 δ , 分别计算命题的推荐信任度和综合信任度. 至于函数 λ 和 δ 的计算方法, 在目前的信任度和信誉度研究中已经存在很多方法, 并不是本模型关注的主要问题.

在实际应用中, 基于信任证和信誉度的两种机制可互为补充, 例如在制定信任策略时, 当一个主体具有较高的信任度时, 则可以适当放松对其属性信任证的要求, 特别是在信任协商过程中, 这类优化策略能够有效减少正则事件序列的依赖序列的长度, 从而能够减少协商交互次数, 最终起到提高系统信任关系建立效率的目的.

5 信任管理系统 CROWN-TM

形成用户任务所需的资源集合, 动态有序实现面向广域网络的科研环境试验平台 CROWN 是为了建立基于网络的科学活动综合环境, 以满足跨地域的科学资源共享和协同需求, 提供对资源组织和

管理以及资源及其关联活动的安全可信的技术. 根据网络计算综合平台 CROWN 对信任管理理论与技术的需求, 基于 DTM 模型定义了相应的信任管理语言, 并研制了信任管理原型系统 CROWN-TM, 其中采用了 Web 服务、XML 安全策略等技术, 作为跨域信任建立的基础.

5.1 系统设计

CROWN-TM 系统的结构示意图如图 5 所示, 根据信任建立过程中主体的信任决策需求和交互控制需求, 分为两个核心功能单元.

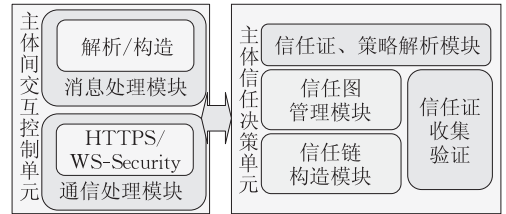


图 5 CROWN-TM 的系统结构

CROWN-TM 的第 1 个核心功能单元称为“主体信任决策单元”, 即针对信任建立过程中, 对信任链构造、信息披露控制, 其中信任证收集对应于 DTM 的“事件”处理, 授权过程对应于 DTM 模型中的“信任管理资源授权”处理. 该功能单元所包含的基础模块为

(1) 信任证、策略解析模块. 该模块实现对主体信任证和策略的解析, 并负责对对端披露的信任证进行有效性验证, 当前系统支持的信任证和策略格式为 SAML 扩展断言, 也可支持扩展的基于角色信任管理语言 ERTML^[27] 和 X. 509 属性证书;

(2) 信任证收集、验证模块. 该模块主要通过属性权威服务 (AASvc) 或者信任管理服务 (CredMan Service) 进行交互, 获取支持信任链构造的指定信任证或策略;

(3) 信任链构造模块. 该模块根据信任证和策略的收集和验证结果, 扩展主体信念公式集, 并根据推论 2 构造信任链, 并对信任链中实体属性约束项检查;

(4) 信任图管理模块. 该模块主要用于对交互过程中所形成的信任图进行维护, 并对交互方的会话状态实施管理, 可支持信任证 (策略) 的分布式存储, 以及多条信任链维护管理, 详细管理过程主要基于文献^[27]方法.

CROWN-TM 的第 2 核心功能单元称为“主体间交互控制单元”, 即针对信任建立过程中, 对传输协议和消息报文的处理, 以及多次协商的会话管理.

其中,依赖多次协商交互的信任建立过程,属于实现DTM模型中的“基于协商的信任管理资源授权”功能.该功能单元所包含的基础模块为

(1)消息处理模块.所有消息遵循了WS-Trust服务规范,封装为标准安全Token,以保障与其他安全服务的安全Token具有可互操作性;

(2)通信处理模块.可以基于传输安全HTTPS协议,或基于WS-Security规范实现消息级安全通信,安全通信策略采用WS-Policy规范描述.

5.2 实验结果及分析

实验目的:主要针对CROWN-TM系统的两个主要功能进行测试分析:第一是测试其信任链构造模块的运行性能,第二是测试信任管理系统服务的整体运行性能.

实验环境:信任管理服务部署在配置Intel Xeon 2.8GHz CPU,2GB内存,RedHat Linux EL 3.0操作系统和100 Mbps网络连接的集群节点上,客户端采用配置为AMD XP 2500+ CPU,1GB RAM,Windows XP操作系统和100Mbps以太网连接的PC.为确保评估的准确性,所用实验机器上不再运行其他程序.除非特别说明外,每项实验都执行5次

并取平均值.

实验采用的场景如下面用例,交互双方的信任证结构如图6所示.

实验用例:某个由ACM组织发起的国际会议Conference承办方为处理会议注册事务,制定并收集到相关的安全信任证(如图6).其中,信任证P1描述能够享受会议注册费折扣的注册成员条件;信任证P2是一条信任公式,描述了主体Conference信任IEEE对其成员member的判断;信任证P4则是ACM为会议承办方Conference签发,该信任证可用于向注册人证明该会议承办方的有效资格.此外,某个会议注册人Alice(其身份由 Key_{Alice} 标识)收集到信任证P3,该信任证是IEEE的一条信念规则,描述Alice是IEEE的有效会员.

如图6所示,Conference的信任证P1和P2可通过结构转换(根据本文第3节中定理1和定义5).显然,我们能够依据信任证 P_1 、 P_2 和 P_3 判断实体 K_{Alice} 享受主体Conference的会议注册优惠权限discount,此结论也可通过本文第3节中性质3简单证明.

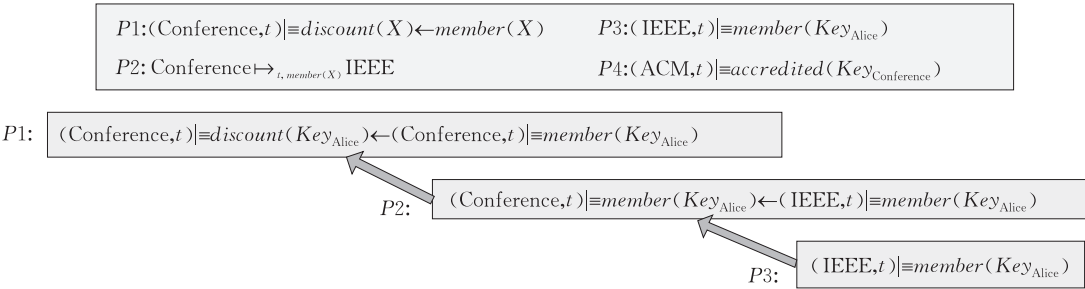


图6 信任证及其的信任链的构造

结合上述实验目的、环境及用例说明,下面给出两组实验方法、实验结果及其分析.

实验组 1. 在主体Conference的策略库中,存放所有信任证.控制实验中信任链的长度方法是:采用多个信任证替换信任证P2:

$$\begin{aligned} P_{2,0} &: \text{Conference} \mapsto_{t, \text{member}(X)} A_i \\ P_{2,i} &: A_i \mapsto_{t, \text{member}(X)} A_{i+1}, \quad 1 \leq i \leq N. \\ P_{2,(i+1)} &: A_{i+1} \mapsto_{t, \text{member}(X)} \text{IEEE} \end{aligned}$$

将信任证数目从5增加到100(即通过调节*i*值从1到96),分别测试策略加载时间(包括信任证和相关配置文件的读取和解析)以及信任链构造时间.

实验结果如图7~图9所示.

在图7中,其特征为:策略加载时间随着信任证数量的增加大致成线性关系增长,当信任证数量为

5、60和100时,策略加载时间分别为560ms、734ms和822ms;特征分析:由于在策略加载时不但需要读取和解析信任证,而且还包括相关配置文件,所以其

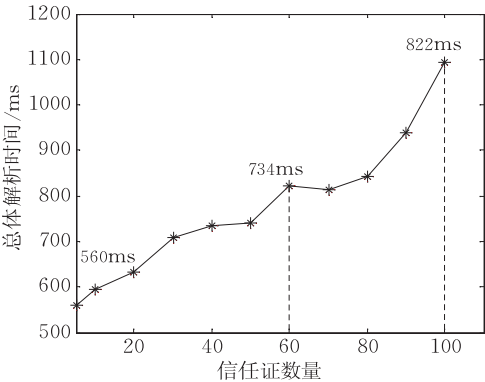


图7 信任证数量 vs 策略加载时间

他配置文件读取解析以及初始化耗用的总时间约为 500ms,而每增加 1 个信任证,其加载时间增加约在 10ms 以内。

在图 8 中,其特征为:信任链的构造时间同样随信任证数量的增加大致呈线性关系增长,当信任证数量为 5、60 和 100 时,信任链构造时间分别为 11ms、65ms 和 125ms;特征分析:在信任证链规模不大时(目前常见应用场景中信任链规模一般低于 100),信任链构造的时间消耗很小。

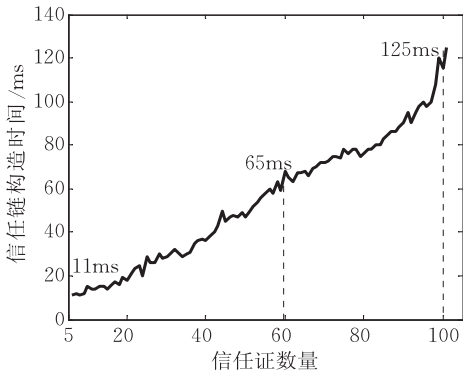


图 8 信任证数量 vs 信任链构造时间

在图 9 中,是从图 7 和图 8 中选取信任证数目为 5、20、40 和 60 时,对策略加载时间和信任链构造时间进行比较,可以看出信任链构造仅仅为策略加载时间的 10%~20%,所占比例很小。

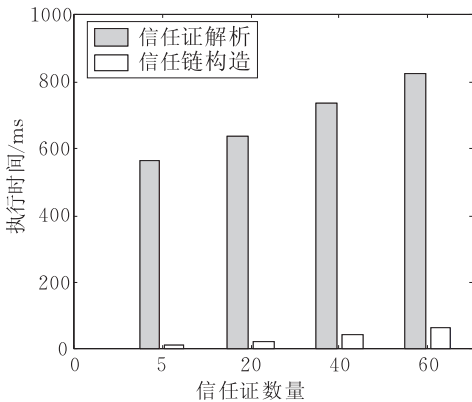


图 9 信任证解析与信任链构造执行时间对比

根据上述的实验结果和分析可以看出,在当前应用中信任链长度规模不大时,其构造时间很短,而策略加载时间占主要执行时间,这也为我们对系统的优化提供了指导;此外,在本实验中,所采用的信任链结构是比较简单的,其单条信任链构造算法很简单,当隐含有多条信任链且形成一个复杂的有向图时,其维护方法和链搜索算法效率将受到影响,当前 CROWN-TM 中采用的信任链构造算法支持信

任证(策略)的分布式存储,其细节及复杂度分析可以参见文献[27-28],在此不再赘述。

实验组 2. 在主体 Conference 的策略库中,存放实验用例的信任证 P1、P2 和 P4,在主体 Alice 存放信任证 P3. Alice 向 Conference 发起会议注册请求。

在该实验组中,主要测试信任管理系统服务的整体性能,设立了满足定义 8 和定义 9 的两种资源授权场景。

在场景 1 中,经过 2 轮消息交互:①主体 Alice 发起会议注册请求,主体 Conference 要求 Alice 出示 IEEE 签发信任证;②主体 Alice 提交信任证 P3, Conference 构造完毕信任证后返回结果给 Alice。

在场景 2 中,经过 3 轮消息交互:①主体 Alice 发起会议注册请求,主体 Conference 要求 Alice 出示 IEEE 签发信任证;②Alice 为保护信任证 P3,要求 Conference 披露其会议资质,当接收到信任证 P4 后方披露信任证 P3;③主体 Alice 提交信任证 P3, Conference 构造完毕信任证后返回结果给 Alice 在交互。

6 结束语

互联网下应用系统计算环境具有开放、自治、动态特性,使得资源共享与协同对实体间信任关系具有很强依赖性,一方面反映在如何给出有效的信任管理形式化模型,另一方面反映在刻画实体间静态信任关系同时,如何描述信任的动态变化特征.更重要的是,在社会学等研究中,主体间的信任是一种非常复杂的关系,因此,需要针对信任管理技术的特定研究范围,开展信任建模以及管理方法研究。

在本文中,针对当前互联网中计算环境 and 应用模式发展对信任模型的需求和挑战,提出了一种面向网络计算的动态信任管理模型 DTM. 在该模型中,首先,基于信念公式形式化定义了主体间的信任公式,并给出了信任链成立的条件;同时,以时间为参照点刻画主体公式集,以事件为触发条件研究主体间信任关系的动态变化,并通过正则事件序列描述信任管理资源授权过程;此外,讨论了如何引入信任度因子以使得 DTM 模型能够支持对主观信任模型中策略的描述;最后,结合当前网络计算综合试验平台 CROWN,介绍了信任管理系统 CROWN-TM 的结构,并给出了初步的实验分析。

在未来工作中,将依托 CROWN 试验床,并结合具体应用领域,收集系统运行过程的实际数据,以进一步对 DTM 模型的易用性进行分析,并制定优化方法;此外,基于 DTM 模型进一步探索可信网络计算的技术体系,为研究新一代互联网体系结构下的分布式资源共享和协同提供基础。

参 考 文 献

- [1] Maurer U. Modeling a public-key infrastructure//Proceedings of the European Symposium on Research in Computer Security (ESORICS). London, UK, 1996: 325-350
- [2] Lampson B, Abadi M, Burrows M, Wobber E. Authentication in distributed systems: Theory and practice. ACM Transactions on Computer Systems, 1992, 10(4): 265-310
- [3] Burrows M, Abadi M, Needham R M. A logic of authentication//Proceedings of the Royal Society of London A, 1989: 233-271
- [4] Blaze M, Feigenbaum J, Lacy J. Decentralized trust management//Proceedings of the IEEE Symposium on Security and Privacy. Oakland, CA, USA, 1996: 164-173
- [5] Li N, Mitchell J C, Winsborough W H. Design of a role-based trust management framework//Proceedings of the 2002 IEEE Symposium on Security and Privacy. Berkeley, California, 2002: 114-130
- [6] Jim T. SD3: A trust management system with certified evaluation//Proceedings of the 2001 IEEE Symposium on Security and Privacy. Oakland, California, USA, 2001: 106-115
- [7] Freudenthal E, Pesin T, Port L, Keenan E. dBAC: Distributed role-based access control for dynamic coalition environments//Proceedings of the 22nd International Conference on Distributed Computing Systems (ICDCS'02). Vienna, Austria, 2002: 411-420
- [8] Chu Y-H, Feigenbaum J, LaMacchia B, Resnick P, Strauss M. REFEREE: Trust management for Web applications. Computer Networks and ISDN Systems, 1997, 29(8/13): 953-964
- [9] Hintikka J. Knowledge and Belief. New York: Cornell University Press, 1962
- [10] Cohen P R, Levesque H J. Intention is choice with commitment. Artificial Intelligence, 1990, 42(2-3): 213-261
- [11] Rao A S, Georgeff M P. Modeling rational agents within a BDI architecture//Allen J, Fikes R, Sandewall E eds. Proceedings of the 2nd International Conference on Principles of Knowledge Representation and Reasoning (KR'91). Cambridge, Massachusetts, USA, 1991: 473-484
- [12] Burrows M, Abadi M, Needham R. A logic of authentication. ACM Transactions on Computer Systems, 1990, 8(1): 18-36
- [13] Rangan P V. An axiomatic basis of trust in distributed systems//Proceedings of the 1988 IEEE Symposium on Security and Privacy. Oakland, CA, USA, 1988: 204-211
- [14] Abadi M, Burrows M, Lampson B, Plotkin G. A calculus for access control in distributed systems. ACM Transactions on Programming Languages and Systems (TOPLAS), 1993, 15(4): 704-734
- [15] Becker M Y, Fournet C, Gordon A D. Design and semantics of a decentralized authorization language//Proceedings of the 20th IEEE Computer Security Foundations Symposium (CSF). Venice, Italy, 2007: 3-15
- [16] Xu Feng, Lu Jian. Research and development of trust management in Web security. Journal of Software, 2002, 13(11): 2057-2064(in Chinese)
(徐锋, 吕建. Web 安全中的信任管理研究与进展. 软件学报, 2002, 13(11): 2057-2064)
- [17] Li N, Mitchell J C. Datalog with constraints: A foundation for trust management languages//Proceedings of the 5th International Symposium on Practical Aspects of Declarative Languages. New Orleans, LA, USA, Springer, 2003: 58-73
- [18] Li N, Winsborough W H, Mitchell J C. Beyond proof-of-compliance: Safety and availability analysis in trust management//Proceedings of the 2003 IEEE Symposium on Security and Privacy. Oakland, CA, USA, 2003: 123-134
- [19] Winsborough W H, Li N. Safety in automated trust negotiation//Proceedings of the 2004 IEEE Symposium on Security and Privacy (S&P 2004). Oakland, CA, USA, 2004: 147-160
- [20] Bonatti P, Olmedilla D. Driving and monitoring provisional trust negotiation with metapolicies//Proceedings of the 6th IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'05). Stockholm, Sweden, 2005: 14-23
- [21] Seamons K, Winslett M, Yu T, Smith B, Child E, Jacobson J, Mills H, Yu L. Requirements for policy language for trust negotiation//Proceedings of the 3rd IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'02). Monterey, CA, USA, 2002: 68-79
- [22] Beth T, Malte B, Birgit K. Valuation of trust in open networks//Proceedings of the Conference on Computer Security. Brighton, UK, 1994: 3-18
- [23] Abdul-Rahman A, Hailes S. A distributed trust model//Proceedings of the 1997 Workshop on New Security Paradigms. Langdale, Cumbria, United Kingdom, 1997: 48-60
- [24] Jøsang A. A subjective metric of authentication//Proceedings of the ESORICS'98. Louvain-la-Neuve, Belgium, 1998: 329-344
- [25] Cornelli F, Damiani E, Vimercati S D C D, Paraboschi S, Samarati P. Choosing reputable servants in a P2P network//Proceedings of the 11th International Conference on World Wide Web Honolulu. Hawaii, USA, 2002: 376-386

[26] Kamvar S D, Schlosser M T, Garcia-Molina H. The eigen-trust algorithm for reputation management in P2P networks//Proceedings of the 12th International Conference on World Wide Web. Budapest, Hungary, 2003: 640-651

[27] Li Jian-Xin, Huai Jin-Peng. COTN: A contract-based trust negotiation system. Chinese Journal of Computers, 2006,

29(8): 1290-1300(in Chinese)

(李建欣, 怀进鹏. COTN: 基于契约的信任协商系统. 计算机学报, 2006, 29(8): 1290-1300)

[28] Li N, Winsborough W H, Mitchell J C. Distributed credential chain discovery in trust management. Journal of Computer Security, 2003, 11(1): 35-86



LI Jian-Xin, born in 1979, Ph.D., lecturer. His current research interests include information security, trust management and distributed computing.

HUAI Jin-Peng, born in 1962, Ph.D., professor, Ph.D. supervisor. His current research interests include computer

software and theory, network middleware and distributed computing, network security.

LI Xian-Xian, born in 1969, Ph. D., professor. His current research interests include information security, computer science theory.

LIN Li, born in 1979, Ph. D. candidate. Her current research interests include resource management, information security.

Background

This work is supported by the National Natural Science Funds for Distinguished Young Scholar under grant No. 60525209; National Basic Research Program of China (973 Program) of China under grant No. 2005CB321803 and the National High Technology Research and Development Program (863 Program) of China under grant No. 2007AA01Z426 and No. 2007AA01Z120. These projects aim to facilitate virtual computing and services computing across many organizations, and enable resources sharing and dynamic collaboration among a large scale of resources. However, the distributed systems have gradually evolved from closed and tight-coupled style to open and loosely coupled style, and resources are dynamic and behaviors are uncontrollable over Internet. Therefore, several security and trust challenges should be ad-

dressed in these projects and systems. The team has made important progress, amongst of which is the trust management framework for internet computing, which can be used to build trust relationship among resource consumers and providers across multiple organizations. Some trust negotiation protocols and algorithms are also investigated in this framework for information privacy protection. In this paper, authors propose a dynamic trust management model (DTM) to support flexible trust establishment between entities, in which the concept of trust is formally defined based on a belief formula, and the transitive property of trust (trust chain) is proved. A trust management system has been implemented and some preliminary experiments results show it is feasible.