# 分布式多信任域信任管理技术研究综述

朱 重 吴国新
(东南大学计算机网络和信息集成教育部重点实验室 南京 210096)

**摘 要** 随着Internet技术的迅速发展和广泛应用,出现了基于Internet虚拟社会,如P2P、网格、无线网络、多代理网络、无线传感器网络等,从而引起了信任概念从人类交互世界向虚拟交互世界的迁移。近年来研究者针对虚拟交互世界提出了各种信任管理模型,这些模型的多样性使得在实际应用中会产生多种信任域。一些文献提出了如何实现多信任域中代理间的可信交互。分析了多信任域的相关概念及其产生的原因,对选取新的典型的多信任域信任管理模型及其使用的各种方法进行了评述;分析了目前研究中存在的问题,并展望了未来的发展方向。研究表明,多信任域中代理间的可信交互是目前信任管理中的难点问题。

**关键词** 多信任域,信任管理,上下文,本体
**中图法分类号** TP393 **文献标识码** A

## Survey of Trust Management in Distributed Multi Trust Domain

ZHU Zhong WU Guo-xin
(Key Laboratory of Computer Network and Information Integration, Ministry of Education, Southeast University, Nanjing 210096, China)

**Abstract** With the rapid development and extensive application of Internet technology, emergence of Internet-based virtual community, such as P2P, Grid, wireless networks, multi-agent networks, wireless sensor networks, has caused the migration of reputation related concepts from the world of human interactions to the world of virtual interactions. In recent years, researchers have proposed various trust management models for virtual interactive world, such diversity of trust management model will bring multi trust domains in the different application environments. Some papers have proposed how to achieve trusted interactions between multi domain agents. The interrelated concepts and reasons of multi trust domain were summarized and presented. Several typical trust management systems of multi trust domain including their various methods were described in detail. The current problems and the challenges of this field for future research were presented. The research work indicates that the trusted interactions between multi domain agents create the biggest challenge in the trust management.

**Keywords** Multi trust domain, Trust management, Context, Ontology

随着Internet技术的迅速发展和广泛应用,出现了基于Internet虚拟社会,如P2P、网格、无线网络、多代理网络、无线传感器网络等,从而引起了信任概念从人类交互世界向虚拟交互世界的迁移。目前,国内外科研机构的工作主要集中在信任模型、信任管理和信任决策方案的研究。在不同的应用领域利用基于多种理论研究实体间的信任关系,涌现了大量丰富的研究成果。电子商务网站已经使用了其中的几个信任模型(如eBay, Amazon),这些模型认为信任是系统每个参与者的集中式全局属性,而信任是系统接收用户反馈的等级评价计算得出的。当潜在的买主选择卖主时考虑这些信任值。更多的信任模型(文献[10,11])认为信任是主观和上下文相关的属性。因此,每个代理有其自己的信任系统,该系统通过外部通信和直接经历对其他代理提供评估,产生该代理对整个代理系统的印象。此外,其他系统[12]认为当提供这些评估时还考虑社会信息。这种多样性的美景就会与不使用同样模型的虚拟社会产生冲突。上述作者由于使用自己的术语、评估表示方法甚至交互方法,因此无法建立使用不同信任模型进行有关社会评估所需信息交互的代理间的通信。如图1所示,源代理C要与目标代理F进行交互,它需要获得目标代理F的信任值,但是它不知道目标代理F所在的信任域正在使用哪种信任模型。即使它知道F所在的域使用什么信任管理模型,那它如何把自己的表示转换成目标代理的信任模型?近几年,一些学者开展了多信任域动态信任管理方面的研究。他们主要使用本体论或桥接技术建立跨信任域交互的信任管理模型,并取得了一些新的进展。本文综述这方面的研究进展。

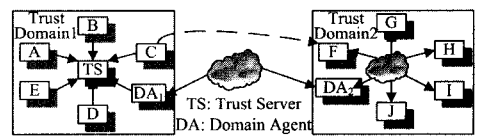


图1 支持多信任域的联合信任管理模型

到稿日期:2010-04-13 返修日期:2010-11-13 本文受国家863计划项目(2007AA01Z422)资助。
朱 重(1967—),男,博士生,主要研究方向为网络与信息系统安全等,E-mail:zhuzhong67@sohu.com;吴国新(1956—),男,教授,博士生导师,主要研究方向为分布式计算、网络安全、信息化关键支撑技术等。

## 1 多信任域的相关定义及其产生背景

### 1.1 信任域的相关定义

下面综合各种不同的文献，给出一些与信任域相关的描述性定义。

**定义 1**(上下文，Context) 一个上下文是属性集及其在一个环境中的实例值[8]。所有属性集可能是可数无穷的。即上下文就是一个代理所处的环境，上下文服务就是代理在特定环境下所能得到的服务和它所能提供的服务。

**定义 2**(信任域，Trust Domain) 一个信任域是被单一管理和单一安全策略支配的主体和客体的集合。它是由一个或多个代理组成的具有统一上下文环境的自治系统。该自治系统使用统一的信任管理模型。

**定义 3**(本体，Ontology) 本体是对共享概念形式化的明确表示，从而使计算机能够解释处理信息的语义。共享和明确是本体的两个基本特征，共享是指本体表达了公认的知识，被一组人所接受；明确意味着这些概念以及概念使用中的限制具有明确的定义。本体提供一种泛化的知识，而上下文提供一种特例化的知识。

**定义 4**(域内信任关系，Inter-domain trust relationships) 它是基于同一信任域内节点间的交互而形成的信任关系。

**定义 5**(域间信任关系，Cross-domain trust relationships) 它是基于多信任域间不同节点的交互而形成的信任关系。域间信任值的计算涉及的内容非常复杂，如两个域的上下文环境是否一致、信任语义和信任计算方法是否相同等。本文将综述一个信任域的某个节点需要计算另一信任域的节点的信任值时所使用的各种管理技术。

### 1.2 多信任域的产生和分类

1)上下文环境的不同产生多个信任域

根据信任域的定义可知，信任域是与其上下文环境紧密联系的。例如，作为一个计算机科学家的信任应该对他作为厨师没有影响。因此不同的上下文环境会产生不同的信任域。

2)管理域的不同产生多个信任域

管理域是被管对象的集合。一般地，管理域满足下列要求：1)按若干个功能用途划分管理环境，或者按每一个管理用途诸如按地理、技术或组织结构划分环境。2)在被管对象的每个集合内，按每个用途，临时指定并且合理修改管理者和代理角色。3)以一致的手段施加控制形式(例如安全方针)。不同的管理域会产生不同的信任域。

3)信任管理方法的不同产生多个信任域

目前，存在两种不同的管理信任的方法：基于策略的信任管理和基于信誉的信任管理。基于策略的信任依赖客观的“强安全(或说硬安全)”机制，如签名证书和可信证书权威机构(CA)来控制用户对服务的存取。存取决策通常基于定义好的语义机制(如逻辑程序设计)提供强的认证和分析支持。而基于信誉的信任依赖一种“软计算(或说软安全)”机制来解决信任问题。在这种情形下，主要是根据网络中其他实体反馈和本身交互经历来计算信任。例如，在 eBAY 系统中，买卖双方在每次交易结束后互相进行等级评价。基于信誉的方法是受到环境制约的，如 P2P、语义 Web，其中常常不会有认证权威机构存在，但是会存在大量可用的个体用户的等级评价。两种不同的信任管理方法就会形成不同的信任域。

4)信任管理模型的不同产生多个信任域

一个信任管理模型涉及实体的标识、信任的定义和测度、信任计算算法、信任存储以及信任网络结构和信任信息交换协议等。在开放多代理系统中，目前没有一个完全清晰的社会控制思想和机制，过去几十年对这些机制的研究兴趣在该领域产生了极大影响。结果在文献中出现了大量的信任模型，其中的信任语义、计算方法及信任网络结构多不相同，从而形成不同的信任域。

5)本体的不同产生多个信任域

近年来，信任本体已引起了一些研究者的关注，他们提出了一些通过本体研究信任管理模型的方法。然而这些方法都集中在各自的研究领域，相应的本体彼此独立或不一致，很难实现相互映射，因此出现了本体不一致而产生的不同信任域。

## 2 典型模型及评述

### 2.1 基于本体论

1)基于功能本体(Functional Ontology)

文献[3]提出了代理信任的功能本体。该本体的目标是两方面的。首先，用清晰一致的方法把分散在各个文献里的有关信任的广泛知识集中到一起。其次，用一般和结构化的形式表示这些知识。该信任功能本体实施 Valente[13]所建议的在法律功能本体工作中的知识分类。作者通过把法律规则的概念扩展到社会规范以及社会控制机制在代理意识中的内部化，使得法律世界中的概念可用于建模社会世界。在法律世界里，规则的违反产生对破坏代理的法律惩罚；在社会世界里，对违反社会规范代理的惩罚是坏的信任。该文献描述了一些概念，用来表示信任维：信任本质、涉及信任形成和传播的角色、用于信任的信息源、信任评估、信任范围和信任维持。这些概念构成了用来开发信任功能本体内核的本体术语集。这个本体包括 4 个主要的、功能上有明显区别的分类：信任知识、责任知识、规范化知识和世界知识。

信任知识是信任功能本体中最典型的分类。它是受法律功能本体中的反应知识所启发，其主要功能是根据代理行为处理代理奖励(好的信任)或代理惩罚(坏的信任)。作者用类图来描述信任知识本体分类，如图 2 所示。

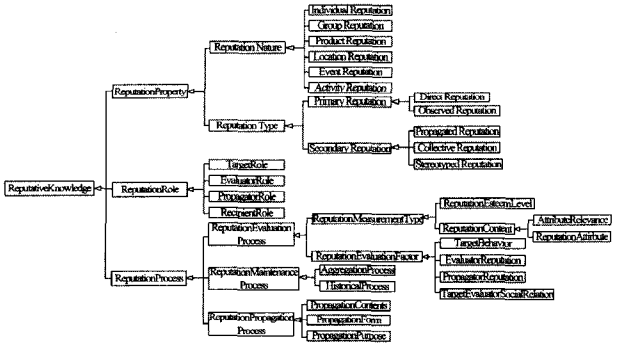


图 2 信任知识分类

责任知识分类也是借用法律功能本体中的概念。它的主要功能是把一个原因与一个具体的代理行为相关联，以便定义代理是否必须考虑对它的行为负责，或者相反，是否存在削弱它的责任的环境。责任知识表示 4 个主要概念，即归因概念、行动者-观测者影响、责任分配和责任限制。其本体结构如图 3 所示。

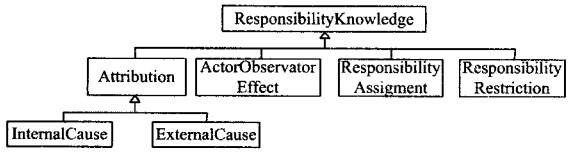


图 3　责任知识分类

规范化知识分类和世界知识分类，文献中没有进一步讨论。

该文献主要是从非常概念化的水平上把所有有关信任的知识放到一起。它基于法律功能本体(Functional Ontology of Law)所定义的概念。从理论观点来看，该方法是非常有趣的，因为它提供了信任及其相关概念的结构化定义。这种结构化定义被用作信任概念的元模型，这个元模型能映射到现有的模型。但从实际应用来看，该方法没有给出具体的语义映射等方面的实现，因此很难嵌入到分布式应用环境。

2)基于公共本体(Common Ontology)

文献[4]对信任管理模型的多样性给出一个可行的解决方案。对信任给出了一个公共本体，这样允许使用不同信任模型的代理间的社会评估可以进行通信。这个实现是基于公共 API，该 API 作为中间件工作于公共本体和每个特殊模型之间。该文献特别强调如何处理社会评估值表示的差异。

文献[4]作者认为信任模型最重要的方面之一是用于信任评估的值表示和语义。在现有的文献中，大量的模型彼此使用不同的方法表示评估值，从简单的布尔值表示好或坏到概率分布和模糊集。例如，eBay 模型使用着色星来显示卖主信任，该系统可以看成 0～100 间的简单实数，而 Repage 模型在离散集(很坏、坏、中立、好、很好)上使用概率分布。当设计有关信任的公共本体时，对评估一致的表示是至关重要的，因为它们是使用不同信任模型的代理间希望能理解的关键。因此，文献[4]作者在检查大多数广泛使用的信任模型后，决定允许不同类型的表示(布尔、实数、离散集和概率分布)提供类型间的自动转换功能，从而允许使用不同信任表示的不同模型的代理间实现连接。表示类型封装在本体 Value 类里。具体转换见表 1。

表 1　信任评估值各种表示间的转换

| | BO | RE | DS | PD |
|---|---|---|---|---|
| X:BO | X | $CM(B_T):X$<br>$CM(B_F):\neg X$ | $R(CM(B_T)):X$<br>$R(CM(B_F)):\neg X$ | $B_T:X$<br>$B_F:\neg X$ |
| X:RE | $X\geqslant 0$ | X | R(X) | $i_1=\min\{R'(X), R'(\max\{X-0.1,0\})\}$<br>$i_2=\min\{5,i_1+1\}$<br>$B'(i_1,1-\frac{X-C(i_1)}{C(i_2)-C(i_1)})$ |
| X:DS | $S(X)\geqslant 3$ | C(S(X)) | X | B(S(X)) |
| X:PD | $CM(X)\geqslant 0.5$ | CM(X) | R(CM(X)) | X |

BO:Boolean Representation(布尔表示)
RE:Bounded Real Representation(有界实数表示)
DS:Discrete Sets Representation(离散集合表示) 用{VB,B,N,G,VG}表示
PD:Probabilistic Distribution Representation(概率分布表示)

$$CM(X)=\frac{1}{10}\sum_{i=1}^{5}(2i-1)X_i$$

$$B'(i,p)=\{X\in PD:\forall_{r\neq i,i+1}X_r=0\&X_i=p\&X_{i+1}=1-p\}$$

$$R(X)=\begin{cases}VB & 0\leqslant X\leqslant 0.2\\ B & 0.2\leqslant X\leqslant 0.4\\ N & 0.4\leqslant X\leqslant 0.6\\ G & 0.6\leqslant X\leqslant 0.8\\ VG & 0.8\leqslant X\leqslant 1\end{cases}\quad S(X)=\begin{cases}1 & X=VB\\ 2 & X=B\\ 3 & X=N\\ 4 & X=G\\ 5 & X=VG\end{cases}\quad R'=\begin{cases}1 & 0\leqslant X\leqslant 0.2\\ 2 & 0.2<X\leqslant 0.4\\ 3 & 0.4<X\leqslant 0.6\\ 4 & 0.6<X\leqslant 0.8\\ 5 & 0.8<X\leqslant 1\end{cases}$$

由表 1 可知，类型的转换会出现精度的损失和不确定性的增加。例如，一些表示为布尔型的评估，经转换后对应 B。而被转换为实数时，也许是在 0 到 0.5 之间(不包含 0.5)。当被转换成离散集时，也许是{VB,B}中的一个，等等。作者把一个值转换成另一个值时所出现的不确定因素称作转换不确定性(CU:Conversion Uncertainly)，这也是接收者应该知道的信息。为了计算这种 CU，作者使用 Shannon 引入的信息论中的有关熵和条件熵理论。如果把每种表示看成是随机变量，那么源随机变量 $X$ 到目标随机变量 $Y$ 的转换不确定性如下：

$$CU(X,Y)=H(Y|X) \tag{1}$$

换句话说，CU 是当一个值被表示成 $X$ 且被转换成类型 $Y$ 的值时所产生的不确定性的增量。每种类型熵的值显示在表 2 中。

表 2　类型转换的熵

| 类型 | 熵 |
|---|---|
| BO | 1.00 |
| DS | 2.31 |
| RE | 6.64 |
| PD | 22.19 |

每个转换的 CU 值显示在表 3 中，每行是源，每列是目标。从表 2、表 3 中可以看出布尔型转换成概率型不确定性最大，而布尔型转换成离散型不确定性最小，与实际情况相符。此外，评估的不确定性是累加的，不允许循环。

表 3　CU 值

| CU 类型 \ 值类型 | BO | DS | RE | PD |
|---|---|---|---|---|
| BO | 0 | 1.29 | 5.64 | 21.19 |
| DS | 0 | 0 | 4.32 | 19.89 |
| RE | 0 | 0 | 0 | 15.55 |
| PD | 0 | 0 | 0 | 0 |

该文献给出了信任的公共本体，同时提出了不同信任表示的转换方法，并用信息论的熵和条件熵定量计算了不同信任表示转换的不确定性，指出了从理论分析到实际应用的明确方向。但是没有给出实际应用的完整模型以及进一步消除信任表示的不同转换方法中不确定性的处理方法。

### 2.2　基于通用安全框架

文献[5]引入了ˣTrust。ˣTrust 是一个标识终端实体的路径并通过这些路径实现信息安全交换的系统。它是一种通用的安全框架，支持大范围的应用和安全机制，通过这种方式使得信任高度可见。它提供了标识可信对等体之间用于具体目的路径的基本服务，而且将这些路径用于信息的可信交换。该系统设计基于 4 个通用的准则：1) 信任通常是依赖上下文的；2) 信任关系由人来定义，而不是应用，所以信任应该与应用分离开独立处理；3) 使用本地语义定义信任关系；4) 信任存在时，是绝对的，这在于来自可信对等体的信息是不加怀疑被接受的。

ˣTrust 同时定义了一个信任网络。ˣTrust 是通过信任连接的域之间的 P2P 信任网络。ˣTrust 系统中的通讯是ˣTrust 网络上的实体以类似 Internet 上 IP 包路由的方式进行路由。ˣTrust 的主体包括人、计算机、组织等等。他们希望使用的系统必须至少是一个域。ˣTrust 系统提供一个通用平台用

于可信通讯，而且上面概括的4个思想表示它的设计目标。它便于加密和相互认证的可信参与者间的通讯，同时组合了4个设计思想。与现有的模型和框架相比，该系统提供了大量的相对优点。该系统主要包括以下几个方面。

1)上下文

上下文是xTrust系统的基本方面。信任连接是上下文敏感的：从Domain A到Domain B的连接在一些情况下也许存在，而在另一些情况下不一定存在。若连接存在于几个上下文中，Domain A的预言(一个域在给定上下文环境信任，另一个域用于属性和观点的特别集合)在每个上下文中也不同。信任连接源：Domain A，决定连接存在的上下文以及什么信任预言用于每个上下文。由于可信对等体域的变化依赖上下文，因此上下文将影响整个可信网络。一个上下文可能是任何应用或情形，它们需要xTrust系统进行决策。当一个信任连接建立后，源域标识哪个上下文可以使用这个连接。每个上下文表示不同的可信对等体和信任预言集合。每个域在自身的上下文集合内运转，而且域的每个上下文都有其自身的本地命名。

2)xTrust标识

一个域的每个实体被分配一个称作xID的标识。每个xID由两部分组成。

a) 域标识(DI，Domain Identifier)，它是全局唯一的，而且允许实体识别属于一个特定域的实体xID。

b) 实体标识(PI，Principal Identifier)，它是针对一个域内实体的本地名字。

即xID可表示成PI@DI。xTrust系统对xID的表示格式和内容没有限制：任何字符串都可以用作域或主体标识。xID提供唯一的标识关联属性值和观点。

3)xTrust协议

xTrust协议是无状态请求-响应协议。请求是要获得一个目标主体的属性或观点。xTrust请求也详细说明需求所存在的上下文。xTrust协议发生在两个域之间，一个是请求者，另一个是响应者。请求者常常是信任连接的源，而响应者通常是需求者可信对等体之一。当信任连接建立后，对等体能够使用交换的证书进行互相认证。请求者通常认证响应者；响应者也可以有选择地认证请求者。

4)信任路由

xTrust实体基本操作是决定哪个可信对等体响应一个特别的需求，这种决定非常类似于数据网络中路由器需要决定什么时候转发数据包。在xTrust系统中，响应者被认为是在信任网络中转发查询的路由器。与ISO's OSI 7层网络模型粗略比较，信任连接取代了物理和数据链路层。正像三层数据路由器，信任路由器使用路由协议帮助它们决定哪个对等体更能提供查询回答。信任路由协议工作方式在许多方面类似数据路由协议，但它们之间也存在一些差别。正如数据网络中的路由器，xTrust响应者参与路由协议，执行分布式计算来决定响应查询的最优对等体。由于信任是上下文敏感的，一个域为它的每个上下文执行这些计算。

5)语义

xTrust系统允许每个域采用它自己的语义处理信任和安全问题。每个域的上下文和信任预言集合是彼此独立的，使得xTrust网络能够以无尺度方式增长，即允许新的域加入到信任网络中，无需重新配置现有的域。尽管xTrust协议的语法是固定的，但它的负载语义，即产生的查询、涉及的上下文和反映的内容是限制在每个域内本地解释。域间负载语义协商为域间信任连接建立处理的一部分。因此，每个域理解它的语义如何与它的对等体语义相关，使得一个域能够改变一个查询的语义。当一个查询转发到邻居域时，这个过程称作语义映射。

所以文献[5]提出了一个通用的安全框架，该框架规定了相关的实体标识、信息交换协议、信任路由及语义等。基于该框架通过信任路由和信任语义映射等实现不同信任域的实体间可信交互。可以把分布式信任管理系统研究的已有成果，如信任本体、信任语义映射技术和信任表示的转换技术等融合到该框架里。

### 2.3 复合型

目前，研究者已对基于策略的信任模型和基于信誉的信任模型开展了大量研究工作，每项工作都有其优点和限制。基于证书的信任适合标示一个可信参与者的前提条件。此外，基于策略的信任系统有严格定义的正式语义和相对严格的结构，来确保它们遵从正规的分析。可是，基于证书的信任是二进制的，即一个主体要么是可信的，要么是不可信的。另一方面，基于信誉的信任系统更加灵活，因为它们能够反映从一个主体过去行为演绎而得到的信任。不幸的是，由于分布式系统的开放特性，这些系统通常容易受到攻击者的操纵。随着计算机系统开始不断紧密地模仿物理世界，人们可以通过结合用于分布式系统的水平(基于信誉)和垂直(基于策略)信任建立机制来发挥其更大的益处。为了尽力实施一个全面的方法来集成分布式系统中的水平和垂直信任测度，文献[2]给出了一个统一信任管理(CTM，Composite Trust Management)策略语言。不像现有的方案，CTM允许策略编写者以任何方式组合水平和垂直信任。此外，CTM策略能够嵌套至任意深度，允许表示重要决策过程。这种信任管理方法允许用户在数字世界里通过使用物理世界里的推理方法来进行信任决策。该文献的主要工作如下：

1)通过检查来自社会网络、处理自动化和虚拟组织域的用户实例，系统地确定一个满足复合信任管理模型的所需属性。

2)开发了一个统一信任管理策略语言——CTM，该语言扩展了RT策略语言族，从而允许水平和垂直信任测度任意组合。

3)基于角色成员的概念提出了用于该语言的形式语义。

4)提出了详细而实际的例子，来说明所提出的方法的灵活性和表示。

5)注意到该项工作只是构建用于各种应用域的复合信任管理架构的第一步。最后，该文献也讨论几个感兴趣的研究问题，这些问题涉及分布式系统中CTM策略的有效评估。

### 2.4 桥接型

文献[1]提出了在移动通信中，通过"桥接"实现不同信任域的通信。可信桥是不止一个域信任的组件(component)或组件的集合。因此这样的组件能够担当桥，从而桥接这些域间的信任。作者认为在今天的移动通信领域，可以发现许多实例，它们实际上由大量的可信域组成，通信和交互发生在域内或跨域进行。这样会出现如下的问题：不同的域彼此合作

以提供完整的服务，尽管这些域的信任概念，甚至信任管理模型都不尽相同。特别地，缺乏域间信任会产生安全问题。这种缺乏可能是阻止移动通信和交互快速发展的障碍之一。信任缺乏显然成为由不同实体组成的可信域的“鸿沟”。现在有几种方法桥接这种信任“鸿沟”，如基于法律的、契约的和风险管理的方法。本文作者相信技术是重要方法之一，并提供了一种技术方法桥接信任“鸿沟”，即研究使用移动个人可信设备(PTD，Personal Trusted Device)作为移动通信和交互领域的可信桥接。具体可分为图 4 给出的 3 种情形。

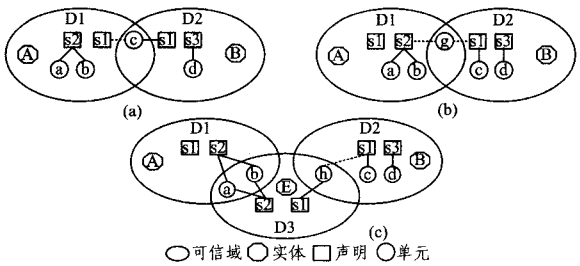


图 4　桥接不同信任域的方法

1)使用现有的组件

通过详细分析现有系统，可以发现现有的组件，可以被不只一个域所信任，那么该组件可以担当可信桥，如图 4(a)所示。

2)构造新的组件。

如果不存在桥接组件，可以创建这样的组件，一些组件仅符合一个信任声明，以致它们要求这样的声明在两个域间都是一致的；一些组件也许符合不只一个声明，以致它们被用作桥接不同声明的域，如图 4(b)所示。

3)构造新的域

如果没有潜在的组件满足这些域，解决方法是可以创建一个独立的域，以便该域的组件实现来自两个彼此不连接域的声明。这样的一个域共享它所桥接的所用域的现有或新组件，称创建的域为桥接域，如图 4(c)所示。

## 3　存在的问题和研究展望

### 3.1　当前研究存在的问题

多信任域信任管理模型的研究还处于初始阶段，存在一些明显的问题：

1)信任本体的不一致性。随着信任本体领域的迅速发展，各信任域间代理的交流日益广泛，各个信任域之间需要彼此使用对方的信息，这样本体和本体之间需要相互理解。但是彼此定义的不一致性，决定了本体映射存在的必要性。

2)信任表示转换的不确定性。信任模型研究最重要的方面之一是用于信任评估的值表示和语义。在现有的文献中，我们发现大量的模型彼此使用不同的方法表示评估值，从简单的布尔值表示好或坏到概率分布和模糊集。这就要求为不同类型的表示提供类型间的自动转换功能。然而，这种转换势必存在不确定性。如何削弱这种不确定性，还需进一步探索。

3)CTM 中策略核查和信息不完整问题。核查复合信任管理系统中的遵从证据需要超越现有的方法。对现有信任模型的遵从核查常形成分布式证据构造过程，该过程用自上而下的方式插入到策略发现和评估过程中。尽管这是严格垂直系统中的智能方法，但其破坏了策略是否调用信任评估函数的方法。如在执行潜在费用较高的水平信任评估算法时，如何有效插入分布式证书搜索，是非常复杂的问题，面临许多需要仔细考虑的挑战。此外，CTM 策略的任意组合可能导致不完整信息，从而负面影响策略的评估过程。

4)桥接的建立和管理问题。由于移动环境及其设备的易变性，导致其中的桥接也经常发生变化，从而给桥接的建立和管理带来很大的难度。

5)模型的实现问题。本文介绍的各种多信任域管理模型中，仅有桥接型多信任域信任管理模型实现了一个原型系统，即使用移动个人可信设备(PTD)作为移动通信和交互领域的可信桥接。其他模型目前都没有实现完整的原型系统。

### 3.2　理论模型

针对上述多信任域信任管理模型存在的问题，我们提出了通用信任管理模型(UTM，Universal Trust Management Model)，它负责在分布式系统中跨越多个信任域实现实体间的信任关联。UTM 既可作为一个独立的信任模型使用，也可以在异构信任域间提供实体信任的语义转换，因而可以实现跨域的信任协商和信任关系传递。UTM 模型的框架如图 5 所示。

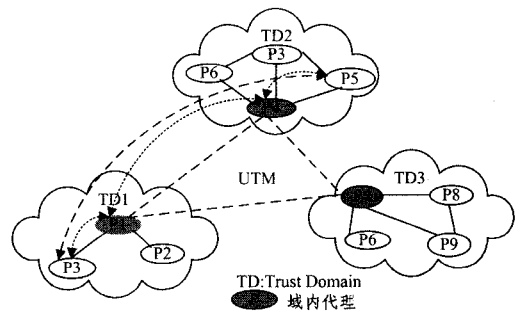


图 5　通用信任管理模型及代理间交互过程

UTM 是一个聚集前面介绍的多信任域管理典型模型的各自优势于一身的信任管理模型，包括节点的标示管理、域信任本体、本体映射、担当“桥接”的域代理节点建立和管理以及不同信任模型的数据换算(信任协商)、反馈控制(自学习优化)、实体加入某个信任域和新的信任域加入 UTM 等主要功能模块，提供消息处理、数据管理、安全、系统监控等基础模块。我们可以把 UTM 看成一个管理多个信任管理模型的信任管理模型，其自身的节点由各个域的代理节点组成。

针对集中式(如淘宝等)和分布式(如 P2P 环境)两种应用背景，UTM 部署均采取代理节点的服务结构，由代理节点实现本域本体的管理和跨域本体的映射以及信任参数设置和域间信任关系的协商和转换等，如图 5 所示。

下面以 TD1 域中的节点 P3 与 TD2 域中的节点 P5 交互过程为例，简要说明 UTM 的基本原理。

1)获取待交互节点与信任值计算的相关信息

节点 P3@TD1 将查询请求提交给本域的代理节点 P1@TD1，代理节点 P1@TD1 在 UTM 中向其它代理节点发送查询请求。接收到查询请求的域代理节点，首先检查被查询节点是否本域内的。如果是，如代理节点 P4@TD2，就以本域内的代理功能，获取被查询节点 P5@TD2 在域内的信任值，经过转换，再以 UTM 成员的身份，返回给查询的代理节点

(下转第 92 页)

Switching(MPLS)-based Recovery[S]. RFC3469. IETF, February 2003
[23] ITU-T Recommendation Y. 1720, Protection switching for MPLS networks [R]. ITU-T. 2006
[24] Haung C, Sharma V, Owens K, et al. Building Reliable MPLS Networks Using a Path Protection Mechanism[J]. IEEE Commun. Mag., 2002, 40(3): 156-162
[25] ITU-T Recommendation G. 8031/Y. 1342, Ethernet Protection Switching [R]. ITU-T. 2006
[26] 竺叶子, 窦军. SUPANET 中 OAM 仿真设计[J]. 计算机科学, 2010, 37(8 专刊): 244-248
[27] IEEE Std 802. 3as-2006, Amendment 3: Frame format extensions[S]. November 2006
[28] Reinemo S-A, Skeie T, Södring T, et al. An Overview of QoS Capabilities in InfiniBand, Advanced Switching Interconnect, and Ethernet[J]. IEEE Communications Magazine, 2006, 44(7): 32-38

(上接第 42 页)

P1@TD1。如果被查询节点不是本域内的成员，如代理节点 P7@ TD3，它将自己保存的与 P5@TD2 相关的信息，即本域内(域 TD3)节点与 P5@TD2 交易的评价记录返回给查询节点 P1@TD1。

2)计算信任值

P1@TD1 根据查询结果和 UTM 的信任值计算算法进行计算，得出 P5@TD2 信任值，并将值转换成 TD1 域的表示方法后，返回给向其发送查询请求的节点 TD1@P3。

3)保存交易结果

P3@TD1 与 P5@TD2 进行交互。交互结束后，P3@TD1 给出一个此次交易的评价值，并将此值返回给其代理节点 P1@TD1。节点 P1@TD1 把评价值转换成 UTM 表示方法，并在本地保存评价信息。

在上述交互过程中，还存在域代理的选取和维护以及基于域本体的域相似度的判别等内容，因篇幅关系，就不加以介绍。

### 3.3 展望

结合第 3.1 节中提出的问题和 3.2 节提出的理论模型，我们认为在分布式环境下多信任域信任管理模型的研究中，可以在以下几个方面做进一步的工作。

1)进一步研究信任本体，尤其是探讨分布式动态环境下信任本体映射的方法，这对研究基于本体的多信任域信任管理模型是至关重要的，是多信任域中代理间交互的基础。

2)通用多信任域信任管理模型的进一步研究及其实现。我们应该在本文提出的通用信任管理模型的基础上，根据不同的应用环境给出具体的实现原型。同时我们认为，基于本体的多信任域信任管理模型为我们提供了明确的研究方向，应该基于现有的本体研究成果，建立一个基于信任本体的通用多信任域信任管理模型。

**结束语** 近十几年来，信任、信任模型和信任管理系统的研究非常活跃，获得了大量的研究成果。然而，这些研究成果间相关概念和算法彼此独立或不一致，导致彼此间只能使用某一特殊应用环境。为此，一些研究者开展了多信任域的信任管理模型研究，取得了一定的进展，也为我们下一步研究信任管理系统指明了一个方向。通过本文的综述可以发现，多信任域的信任管理模型研究工作刚刚起步，还需要相关的研究者不断努力。

## 参 考 文 献

[1] Yan Z, Cofta P. Methodology to Bridge Different Domains of Trust in Mobile Communications[C]// The 1st International Conference on Trust Management(iTrust'03). LNCS vol. 2692/2003. Greece, May 2003: 211-224
[2] Lee A J, Yu Ting. Towards a Dynamic and Composite Model of Trust[C]// Proceedings of the 14th ACM Symposium on Access Control Models and Technologies(SACMAT 2009). June 2009
[3] Casare S, Sichman J. Towards a functional ontology of reputation[C]// Proceedings of the Fourth International Joint Conference on Autonomous Agents and Multiagent Systems. The Netherlands, July 2005
[4] Pinyol I, Sabater-Mir J, Cuni G. How to talk about reputation using a common ontology: From definition to implementation[C]// Ninth Workshop on Trust in Agent Societies. 2007: 90-102
[5] Branchaud M, Flinn S. xTrust: A scalable trust management infrastructure[C]// Proceedings of Privacy, Security and Trust. Fredericton, Canada, 2004: 207-218
[6] Bonatti P, Duma C, Olmedilla D, et al. An integration of reputation-based and policy-based trust management[C]// Sematic Web and Policy Workshop. Galway, Ireland, Nov. 2005
[7] Kailar R, Muralidhar V. A Security Architecture for Health Information Networks[C]// American Medical Informatics Association(AMIA) Symposium. Chicago, Nov. 2007: 12-14
[8] Mui L. Computational models of trust and reputation: Agents, evolutionary games, and social networks [D]. Cambridge, MA, USA: Massachusetts Institute of Technology, 2003
[9] 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(06): 1510-1521
[10] Carbo J, Molina J, Davila J. Trust management through fuzzy reputation[J]. Int. Journal in Cooperative Information Systems, 2003, 12(1): 135-155
[11] Sabater J, Paolucci M, Conte R. Repage: Reputation and image among limited autonomous partners[J]. Journal of Articial Societies and Social Simulation, 2006, 9(2)
[12] Carter J, Bitting E, Ghorbani A. Reputation formalization for an information-sharing multi-agent system[J]. Computational Intelligence, 2002, 18(2): 515-534
[13] Valente A. Legal Knowledge Engineering-A modeling Approach [M]. Amsterdam: IOS Press, 1995
[14] Viljanen L. Towards an ontology of trust[C]// Proceedings of the 2nd International Conference on Trust, Privacy and Security in Digital Business(TrustBus'05). Springer-Verlag, 2005
[15] Huang Jingwei, Mark S. Fox: An ontology of trust: formal semantics and transitivity[C]// ICEC. 2006: 259-270
[16] Nardin L G, Brandao A A F, Sichman J S, et al. An Ontology Mapping Service to Support Agent Reputation Models Interoperability[C]// 11th Workshop on Trust in Agent Societies. Estoril, Portugal, 2008
[17] 文珠穆, 李瑞轩, 卢正鼎, 等. 多域环境中基于蚁群算法的抗攻击时态信任模型[J]. 计算机科学, 2009, 36(7): 46-51