SOA 环境中的跨域认证方案研究

郭晶晶[1]，马建峰[1,2]，郭鑫鑫[3]，张涛[4]

（1. 西安电子科技大学网络与信息安全学院，陕西 西安 710071；
2. 通信信息控制和安全技术重点实验室，浙江 嘉兴 314033；
3. 西安邮电大学计算机学院，陕西 西安 710121；
4. 西安电子科技大学计算机学院，陕西 西安 710071 ）

摘 要：鉴于现在的网络越来越复杂，其中，用户数量大、服务类型多、安全机制不统一的特点决定了 SOA 环境中异构多域的情况，给出了一种基于模糊理论的信任管理方法，并将该方法与证书转换服务结合起来提出了一种 SOA 环境中的跨域认证方案，在该方案中，用户域使用信任管理方法来保证安全性，服务域结合信任管理与证书认证来保证安全性，并且用户可以透明地访问采用不同底层安全机制的域中服务，实现安全跨域认证。分析表明，该方案具有安全与普适的优势，可以满足 SOA 环境下身份认证的需求。

关键词：SOA；跨域；身份认证；信任管理；模糊理论；证书转换

中图分类号：TP309

文献标识码：A

doi: 10.11959/j.issn.2096-109x.2016.00111

Study of cross-domain identity authentication in SOA environment

GUO Jing-jing[1], MA Jian-feng[1,2], GUO Xin-xin[3], ZHANG Tao[4]

(1. School of Cyber Engineering, Xidian University, Xi’an 710071, China;
2. Science and Technology on Communication Information Security Control Laboratory, Jiaxing 314033, China;
3. School of Computer, Xian University of Posts and Telecommunications, Xi’an 710121, China;
4. School of Computer, Xidian University, Xi’an 710071, China)

Abstract: For the network nowadays becoming more and more complex, the SOA environment has the properties of heterogeneous and multiple domain. A trust management scheme was proposed based on the fuzzy theory, and a cross-domain identity authentication in SOA was constructed by the combining of the trust management scheme with the credential transform service. During the authentication, a user’domain used the trust management scheme to guarantee its security, and the service provider’s domain used both the trust management and credential to ensure its security. Furthermore, the credential transform made users can access services in the domains whose security mechanism was different from the users’. It is shown that the proposed authentication scheme has superiority in both security and pervasive, and is suitable for the SOA environment.

Key words: SOA, cross-domain, identity authentication, trust management, fuzzy theory, credential transform

---

收稿日期：2016-09-16；**修回日期**：2016-10-20。**通信作者**：郭晶晶，jjguo@xidian.edu.cn

基金项目：国家自然科学基金资助项目（No.61602360, No.61602365）；国家高技术研究发展计划（“ 863 ”计划）基金资助项目（No.2015AA017203, No.2015AA016007）；促进海峡两岸科技合作联合基金资助项目（No.U1405255）

Foundation Items: The National Natural Science Foundation of China (No. 61602360, No.61602365), The National High Technology Research and Development Program (863 Program) (No. 2015AA017203, No.2015AA016007),The Key Program of NSFC (No. U1405255)

1 引言

面向服务的体系结构（SOA, service-oriented architecture）是一种用于根据需要对资源进行关联的企业级 IT 体系结构。这些资源被表示为与业务一致的服务，这些服务可以参与并包含到价值网、企业或业务线中，以满足业务需求[1]。SOA 以服务作为基本要素，实现分布应用的快速、低成本、易于组合的开发，为了满足分布应用的要求，SOA 必须具有技术的通用性、松耦合及服务可以组合和重用的特性[2]。在 SOA 环境下，由于服务通常分布在不同的安全域中，因此，为了防止未授权客户访问和使用这些服务，不仅要对请求者的身份进行认证，而且还涉及跨域身份认证（cross domain authentication）的问题。当用户跨域访问资源时，由于和访问域的认证服务器之间不存在事先的信任关系，因此访问域的认证服务器需要联合用户家乡域的认证服务器对用户进行认证[3~6]。SOA 环境中服务的分散性以及用户请求的动态性和频发性, 决定了 SOA 中的跨域认证应该安全、透明、高效。目前，关于跨域认证的技术有很多种，其中有利用联盟身份来实现单点登录，为了建立跨安全域的身份认证系统，参与的安全域之间需要建立信任关系，构成一个联盟（federation），由此建立联盟身份（federated identity），如 WS-Federation[7]和 Liberty Alliance[8]；SAML[9]在基于标准的单点登录基础设施方面也有举足轻重的地位，业内主要厂商使用它来支持单点登录和安全基础设施之间的互操作性；传统的身份认证协议 Kerberos[10]等也具有跨域身份认证的能力。

然而，上文提到的这些技术或协议完成跨域身份认证的前提都是它们只为具有相同的底层安全机制的安全域提供服务。为了在尽可能大的范围内使用户可以无障碍地访问服务，采用不同底层安全机制的安全域间的互操作性就变得非常重要。

Mello 等在文献[11]中提出了一种 SOA 环境下的基于证书翻译（credential translation service）的身份认证模型，该模型允许身份认证在不同的安全机制之间进行，可以为一个包含了不同类型的证书的联合环境提供认证。其中指出一个服务域的安全令牌服务（STS，security token service）接收到一个 SAML 认证断言后，它会请求客户域的 STS 为这个认证提供附加消息，使它可以评估该断言的信任级别，然而由于文中只考虑了用户域所提交的附加消息作为直接信任，而没有考虑到推荐信任等因素，因此并不能全面地评估认证的信任级别；同时，在客户域的 STS 向服务域的 STS 发送附加消息时也没有考虑到服务域的可信性。

为此，本文在文献[11]的基础上结合了信任管理机制，即在每一个安全域中都有一个信任代理，其作用就是通过对安全域之间直接的交互行为历史和间接的经验推荐等信息来建立各个域之间的信任关系，并提供信任监测、评估、存储、查询和更新等服务。新模型将用户身份信息与行为信息结合起来，使认证结果具有更高的可信性；同时，它比完全基于信任理论的模型计算量更少、更简洁。因此更能满足 SOA 环境的实际需要。

2 基于证书翻译的身份认证模型

文献[11]中介绍了一种证书翻译的思想，提出了一个主体的身份认证证书可以在采取不同安全技术（如 X.509、SPKI/SDSI）的多个域之间透明地进行翻译。该模型还支持用户属性的传递。该模型的整体框架如图 1 所示。由于本文的讨论范围只是身份认证，因此，授权服务模块的细节并未给出。

在图 1 中，安全令牌服务、身份提供者（IDP, identity provider）、属性/假名服务（APS, attribute/pseudonym service）以及证书翻译服务（CTS, credential translation service）是完成跨信任域身份认证的主要实体，这些实体的主要功能如下。

1) 安全令牌服务及身份提供者。STS/IDP 用于建立信任关系，进而形成一个联合环境。STS 之间存在的信任关系，使一个域发布的断言可以在其他域中得到有效使用。为了达到该目的，STS 接收到一个 SAML 认证断言，它会请求客户域的认证权威为这个认证提供附加消息，使它可以评

估该断言的信任级别。

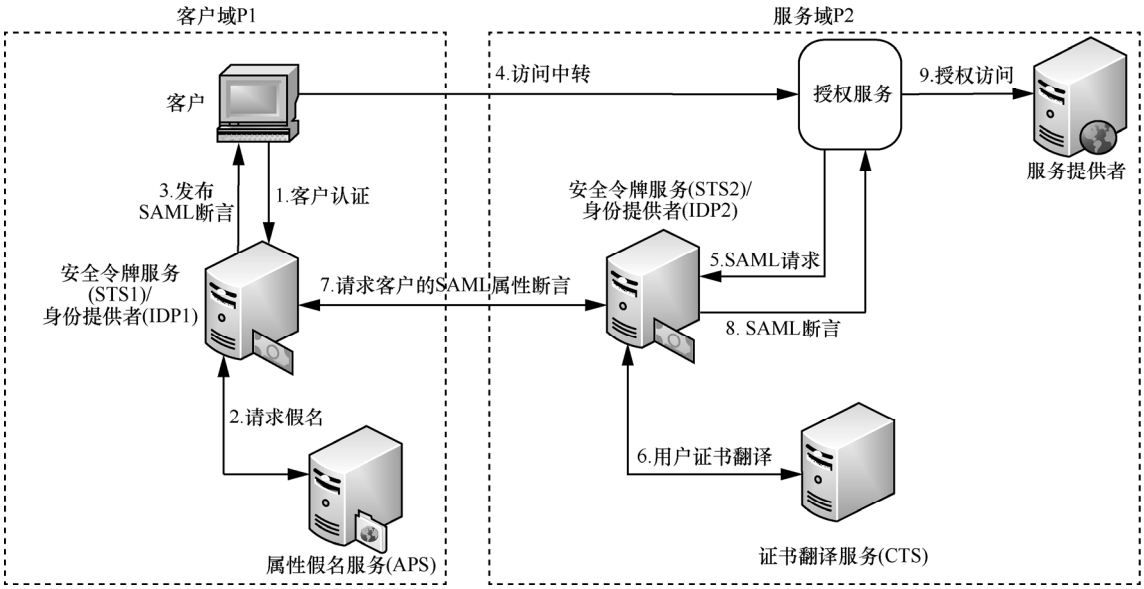

图 1　基于证书翻译的跨域认证框架

2) 证书翻译服务。CTS 的目的在于从一个 SAML 认证断言中抽取信息，来组成一个新的认证证书使其可以被 CTS 所在域内的实体理解。该功能确保用户和服务提供者保持自己的安全特性，CTS 将一种机制的属性翻译为另一种机制的属性。

3) 属性/假名服务。APS 用于为用户提供属性与假名，每一个信任域中的 APS 都应该提供一个属性标准，在一个联合环境中使用。目前许多研究工作已经着眼于为一个联合环境定义一个标准的属性集。目前，大约有 40 个属性已经被定义了并且作为普通身份属性（commonidentity attributes）。假名服务是为用户提供假名，实现匿名认证，保证用户的隐私。

该模型通过以下的工作流程来完成跨域身份认证。在图 1 中，假设有客户域 P1 和服务域 P2，当 P1 中的客户 U 需要访问 P2 中的某服务 S 时：①客户 U 首先向 P1 中的 STS 服务发送认证请求；②如果有需要，STS 向假名服务索取用户假名；③STS 为客户 U 生成证书并将证书发给客户 U；④客户 U 发出访问外域服务提供商 SP2 的请求并将自己的证书转发至 P2；⑤请求被授权服务截获，授权服务将用户的证书传递给 P2 的安全令牌服务 STS2，STS2 对用户的证书进行认证；⑥如果该登录凭证与域 P2 采用的是不同的认证机制，则需要进行证书翻译；⑦由于在证书翻译过程中，证书翻译服务还需要一些关于客户的其他属性以便生成完整的证书，此时 STS2 需要向 STS1 索取用户的其他属性信息；⑧STS2 对其可以理解的用户证书进行认证并将结果用 SAML 断言的形式发送给授权服务模块进行后续的处理。

3　信任管理方案

信任是一个常见但相当复杂的现象，其内涵十分丰富。它最初为心理学概念，但近年来信任逐步被用于安全技术中，目前，信任管理已经成为国内外研究的热点。例如由欧盟赞助的 SECURE（secure environment for collaboration among ubiquitous roaming entities）[12]项目、斯坦福大学 Kamvar 等[13]提出的 P2P 全局信誉系统 Eigentrust 等。基于信任度的信任管理模型从信任的主观性入手，使用数学的方法评估信任意向。实体根据收集到的所有相关信息，包括对被评估实体的行为观察、与被评估实体的交互记录以及其他个体的意见等，利用适当的计算模型推导出信任度。

众多研究者已经开展了关于信任建模、推理等问题的研究，并取得了一定成果。Beth 模型[14]将信任问题分为了直接信任与推荐信任两类，使用了概率论描述和评估信任度，并给出了信任度

的计算方法，但他没有考虑到恶意推荐的情况。Song 等[15]提出了用模糊逻辑表示信任度，建立了信任的模糊推理规则。相对精确的数学模型，模糊逻辑可以更好地体现出信任的模糊性与不确定性。但该模型仅考虑了任务成功率和入侵防御能力这 2 个因素，忽略了第三方的推荐等因素，因此也具有一定局限性。本文在分析上述方案的基础上，建立了一种基于模糊理论的信任管理方案。

3.1 信任的定量描述

Zadeh[16]首先提出了模糊理论。模糊理论将数学研究的对象扩大到质与量统一的对象和具有模糊性的概念。

定义 1 设论域为非空集合 X，x 为 X 中的元素，对任意的 $x\in X$ 给定了如下映射

$$x\to[0,1], x\mapsto \mu_A(x)\in[0,1]$$

则称由序偶组成的集合 $A=\{(x\mid \mu_A(x))\}, \forall x\in X$ 为 X 上的模糊子集合（简称模糊集合）。称 $\mu_A(x)$ 为 x 对 A 的隶属函数（也可表示为 $A(x)$）。对某个具体的 x 而言，称 $\mu_A(x)$ 为 x 对 A 的隶属度。

X 上的一切模糊集的集合记为 $A(X)$。

用多个模糊子集合 $T_j\in F(X)(j=1,2,\cdots,M)$ 定义具有不同信任度的主体集合（简称信任集合）。即用离散的标度{1,2,⋯,*m*}来描述主体信任的高低。同时，采用自然语言对 T_j 命名，可以赋予其直观、实际的意义。例如假设 M=4，那么 T_1 表示不信任、T_2 表示有点信任、T_3 表示比较信任、T_4 表示非常信任。

用主体对各 T_j 的隶属度所构成的向量来描述主体的信任度更符合主体信任的实际情况。所以，本文中 x_0 对 x_i 的信任度可以用信任向量 $\boldsymbol{V}$={v_0, v_1,⋯,v_m}来表示，其中 v_j 表示 x_i 对 T_j 的隶属度。

本文在论域 U=[0,1]上定义 4 个模糊子集，分别是模糊集 T_1 表示“ 不信任 ”、模糊集 T_2 表示“ 有点信任 ”、模糊集 T_3 表示 “ 比较信任 ” 和模糊集 T_4 表示“ 非常信任 ”。下面设计了这 4 个模糊子集的隶属函数。其中，T_1 与 T_4 采用 Z 型隶属函数，T_2 与 T_3 采用梯形隶属函数。

$$T_1(x)=\begin{cases}0, & 0.5\le x\le 1\\ \dfrac{0.5-x}{0.3}, & 0.2\le x<0.5\\ 1, & 0\le x<0.2\end{cases}$$

$$T_2(x)=\begin{cases}0, & 0.85\le x\le 1\\ \dfrac{0.85-x}{0.45}, & 0.4\le x<0.85\\ 1, & 0.3\le x<0.4\\ \dfrac{x-0.3}{0.1} & 0.2\le x<0.3\\ 0, & 0\le x<0.2\end{cases}$$

$$T_3(x)=\begin{cases}0, & 0.9\le x\le 1\\ \dfrac{0.9-x}{0.2}, & 0.7\le x<0.9\\ 1, & 0.5\le x<0.7\\ \dfrac{x-0.2}{0.3} & 0.2\le x<0.5\\ 0, & 0\le x<0.2\end{cases}$$

$$T_4(x)=\begin{cases}1, & 0.9\le x\le 1\\ \dfrac{x-0.2}{0.65}, & 0.2\le x<0.9\\ 0, & 0\le x<0.2\end{cases}$$

00111-4

3.2 信任关系的表示及传递

本文同时考虑了 2 种信任方式：直接信任和推荐信任。文献[17]提出了一种比较直观的信任关系的表示及传递方法。本文以此为基础，定义了直接信任和推荐信任的表示及传递方法。如果 Alice 信任 Bob，那么 Alice 与 Bob 之间存在一个直接信任关系；如果 Alice 信任 Bob 给她的关于其他对象的信任值（trustworthiness），那么 Alice 与 Bob 之间存在一个间接信任关系。本文提出的信任度模型中假设信任关系是有向的，即在 2 个实体间互相存在信任关系，但这 2 个信任关系被看作 2 个独立的信任关系。

图 2 所示的是信任代理中的存储信息。每个信任域中的信任代理都存储着 3 个表，分别是交易信息表、待考察列表与黑名单。交易信息表中存储着该信任域最近 t 次交易的对象域的标识以及对其的信任度；待考察列表中存储着该信任代理怀疑其有恶意行为的对象的标识；黑名单中存储着信任代理认为是完全不可信的域的标识。

每个信任代理都可以发出信任请求消息，也可以生成信任响应消息，还可以生成恶意实体通

知消息。这些消息的结构如下所示。

信任请求消息结构为：[*RequesterID, TargetID, RequestID, Expiry*]，其中，*RequesterID* 为该消息发出者的标识；*TargetID* 为将要对其进行信任评估的信任域的标识；*RequestID* 为该消息生成的唯一的标号；*Expiry* 为该消息的有效期，每一个信任请求消息都有一个有效期，当时间超过该有效期后，该信任请求消息将失效。

信任响应消息结构如下。

1) 直接推荐（即 A 向 B 请求其对 C 的信任评估，B 将其对 C 的信任评估告诉 A）

该信任方式下的消息结构为：[*RecommenderID, requested, TrustValue, Time*]，其中，*RecommenderID* 为该消息的产生者的标识；*requestID* 为该响应消息对应的请求中的 *requestID*；*TrustValue* 表示 *RecommenderID* 对与该响应对应的信任请求消息中 *TargetID* 的信任度，在 3.1 节中已经说明信任度用信任向量来表示，因此 *TrustValue* 为一个信任向量；*Time* 表示 *TrustValue* 的生成时间，如果 *TrustValue* 生成的时间太久，那么该 *TrustValue* 将被视为无效。

2) 间接推荐（即推荐的推荐，B 把其他实体对 C 的信任评估告诉 A）

该结构是一个嵌套结构，下面的消息为一层嵌套的格式

[*RecommenderID*, *requestID*, [*RecommenderID'*,*requestID'*, *TrustValue'*,*Time'*], *TrustValue*, *Time*]

其中，[*RecommenderID'*, *requestID'*, *TrustValue'*, *Time'*]为 *RecommenderID'*对消息标号为 *requestID'* 的信任请求消息中的 *TargetID* 发送的信任响应。

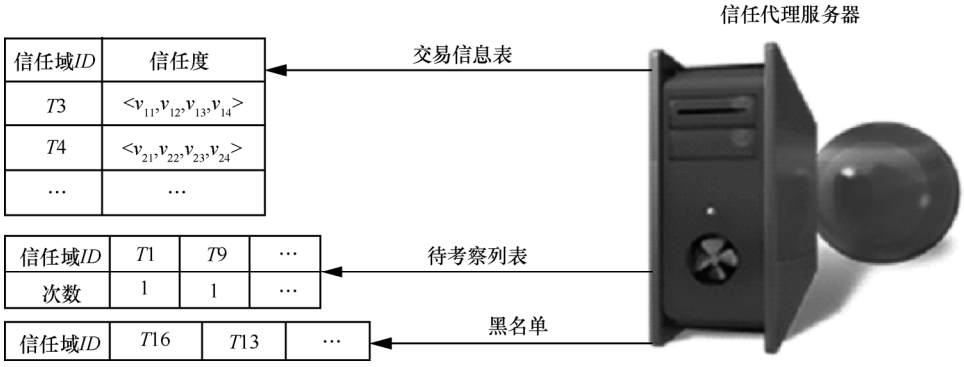

图 2　信任代理中的存储信息

恶意实体通知消息结构为：[*RecommenderID, TargetID,Time*]，其中，*RecommenderID* 为该消息生成者的标识；*TargetID* 为恶意实体的标识；*Time* 为该通知生成的时间。

下面给出信任传递算法与一个简单的例子，如图 3 所示，该算法考虑了实际情况下的各种信任类型，包括直接信任与推荐信任，并给出一个防止恶意推荐行为与减少某些安全域提供恶意服务的机制。

算法　信任传递算法

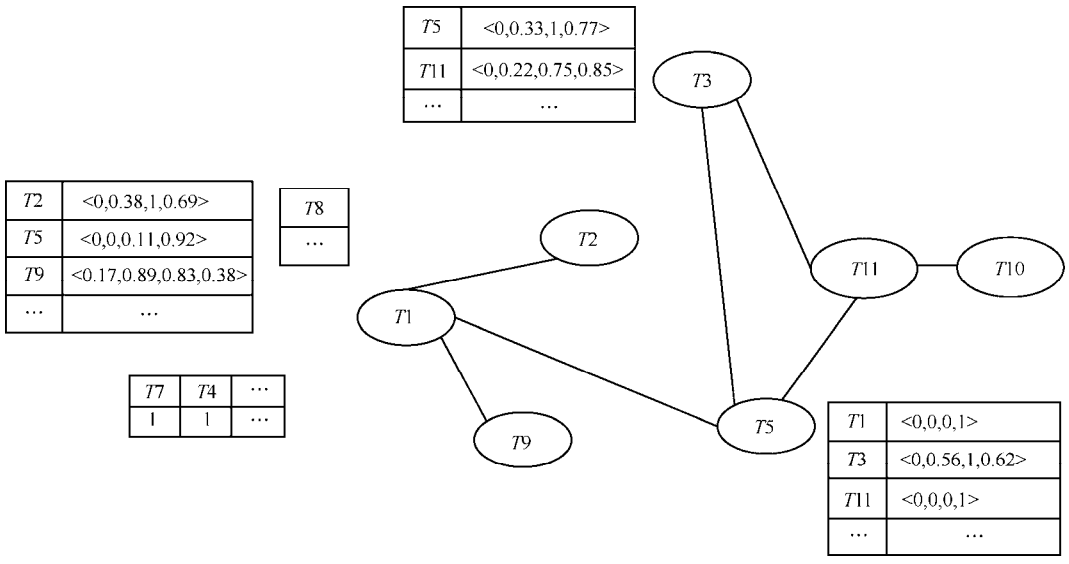

图 3　推荐信任网络结构

初始条件：信任域 *T*1 的信任代理 Agent.*T*1 需要对信任域 *T*2 进行信任评估。

输出：Agent.*T*1 得到关于 *T*2 的直接信任与间接信任消息。

1) Agent.*T*1 查找自己的交易信息表，如果 Agent.*T*1 的交易信息表中有 *T*2 的信息，那么取出其对 *T*2 的直接信任值。

2) Agent.*T*1 向在其交易信息表中除了 *T*2 以外的（如果该表中存在 *T*2）其他信任域的信任代理发送请求消息[Agent.*T*1, *T*2, *requestid*, *expiry*]。

3) 当某一信任域 *Tk* 收到信任请求消息后，查看该信息的有效期，若该消息未过期：

①如果 Agent.*Tk* 的交易信息表中存在 *T*2（即 *Tk* 对 *T*2 有直接信任关系），那么向其前驱信任域返回响应消息[Agent.*Tk*, *requestid*, *TrustValue*, *Time*]；

②Agent.*Tk* 向其交易信息表中除 *T*2 以外的信任域发送信任请求消息[Agent.*Tk*, *T*2, *requestid'*,*expiry*]，请求其返回对 *T*2 的信任度。

4) 当某一信任域 *Ts*（*s* 不等于 1）收到其他域对其发出的信任请求的响应[Agent.*Tx*, *requestid'*,*TrustValue'*]后，Agent.*Ts* 将响应[Agent.*Ts*, *requestid*, [Agent.*Tx*, *requestid'*, *TrustValue'*, *Time*'], *TrustVa*lue,*Time*]发送给其前驱信任域。

5) 当时间过了 *expiry*，Agent.*T*1 将不再等待信任响应消息，它将根据已经得到的对 *T*2 的信任消息对其进行信任评估，若它没有得到任何 *T*2 的信任消息，那么它就暂且认为 *T*2 是可信的，同时将其对 *T*2 的信任度设为最具模糊性的 0.5，即它对 *T*2 的信任向量为<0,0.78,1,0.46>。

6) 每次 2 个信任域 *Tx* 与 *Ty* 交易完成后，参与方的信任代理都对对方做出一个主观信任评价，如果 *Tx* 对 *Ty* 评估的信任向量低于 *Tx* 设定的某一信任下界，那么就将 *Ty* 与对其做出高级信任推荐的域都列入待考察列表中，当一个信任代理收到了其他信任代理发来的恶意实体通知消息后，也会将该消息中的恶意实体加入该表中，如果一个域已经在该列表中，那么将其在列表中对应的参数加 1，当某个域对应的参数达到 *p* 时，就将其视为完全不信任对象列入黑名单中，此外，*Tx* 还向其交易信息表中的信任域代理发送消息通知它们 *Ty* 不可信，甚至在一些情况下还可以对 *Ty* 的行为诉诸法律作为惩罚。这一机制主要的作用是防止恶意推荐行为，并且当发现恶意服务后做出惩罚来减少某些服务做出恶意行为的可能。

下面针对本文中的信任管理方法给出一个简单的例子，在本文后面进行信任值计算时也以此为例。在实际环境中，不同信任代理间的推荐关系构成了一个推荐网络，如图 3 所示。

在图 3 所示的无向图中，顶点表示信任域 *Ti* 的信任代理，2 个顶点间有连线表示它们之间存在某种信任关系，即与某一顶点相连的顶点都在该顶点的交易信息表中。图 3 左边 3 个表格分别是 *T*1 的信任代理的交易信息表、待考察列表和黑名单，上方与右边的表格分别是 *T*3 和 *T*5 的信任代理的交易信息表。现在假设信任域 *T*1 需要对信任域 *T*11 进行信任评估，那么根据信任传递算法，整个信任传递的过程如下。

1) *T*1->*T*2、*T*5、*T*9

[Agent.*T*1,*T*11, rrq*T*101, 20120428164213]

2) *T*5->*T*1

[Agent.*T*5,rrq*T*101,<0,0,0,1>,20120412231343]

3) *T*5->*T*3

[Agent.*T*5,*T*11,rrq*T*501,20120428164208]

4) *T*3->*T*5

[Agent.*T*3,rrq*T*501,<0,0.22,0.75,0.85>,20120407102309]

5) *T*5->*T*1

[Agent.*T*5,rrq*T*101,[Agent.*T*3,rrq*T*501,<0,0.22,0.75,0.85>,20120407102309],<0,0.56,1,0.62>,20120428164210]

3.3 信任值的计算及信任关系决策

目前，在有关的模糊数学文献中，多数都采用 Zadeh 算子∧和∨作为模糊算子来进行分析和讨论。但这对算子的缺点是比较粗糙，丢失的信息太多。对此，人们相继提出了多种新的广义模糊算子[18]。本文选择 Einstein 算子作为模糊算子。

定义 2 设模糊集合 $A,B\in F(x)$，则 Einstein 算子 $\dot{\varepsilon}$ 和 $\overset{+}{\varepsilon}$ 的定义如下。

$$(A\dot{\varepsilon}B)(x)=\frac{A(x)B(x)}{1+[1-A(x)][1-B(x)]}$$

00111-6

$$(A \overset{+}{\varepsilon} B)(x) = \frac{A(x)+B(x)}{1+A(x)B(x)}$$

其中，$A(x)$和 $B(x)$分别表示 $x \in X$ 对模糊集合 A、B 的隶属度。

在信任的形式化推导过程中，需要对信任向量进行运算。本文定义了 2 种信任向量的运算: 连接运算 (⊗) 和合并运算 (⊕)。

定义 3　设有信任向量

$$\boldsymbol{V} =< v_1, v_2, v_3, \cdots, v_m > \text{和} \boldsymbol{V}' =< v_1', v_2', v_3', \cdots, v_m' >,$$

则

$$\boldsymbol{V} \otimes \boldsymbol{V}' =< v_1'', v_2'', v_3'', \cdots, v_m'' >$$
$$=< v_1 \dot{\varepsilon} v_1', v_2 \dot{\varepsilon} v_2', v_3 \dot{\varepsilon} v_3', \cdots, v_m \dot{\varepsilon} v_m' >$$

$$\boldsymbol{V} \oplus \boldsymbol{V}' =< v_1'', v_2'', v_3'', \cdots, v_m'' >$$
$$=< v_1 \overset{+}{\varepsilon} v_1', v_2 \overset{+}{\varepsilon} v_2', v_3 \overset{+}{\varepsilon} v_3', \cdots, v_m \overset{+}{\varepsilon} v_m' >$$

属于连接关系的 2 个信任向量通过连接运算得到合成信任向量；属于并联关系的 2 个信任向量通过合并运算得到合成信任向量。若某信任代理得到了对其他信任域的综合信任向量，那么最后利用最大隶属原则决定该信任域的信任度隶属于论域中的哪个模糊集。

现在以图 3 中的例子来说明信任度的计算方法, 信任域 $T1$ 的信任代理 Agent.$T1$ 收到 3.2 节最后列出的消息 2)和 5)。

[Agent.$T5$,rrq$T101$,<0,0,0,1>,20120412231343]；

[Agent.$T5$,rrq$T101$,[Agent.$T3$,rrq$T501$,<0,0.22,0.75,0.85>,20120407102309],<0,0.56,1,0.62>,20120428164210]。

那么，Agent.$T1$ 就可以利用前面提到的 2 种运算得到其对 $T11$ 的综合信任值，$T1$ 与 $T11$ 之间的信任网络如图 4 所示，信任度向量 $\boldsymbol{V}_1$、$\boldsymbol{V}_2$、$\boldsymbol{V}_3$ 以及 $\boldsymbol{V}_4$ 分别表示其对应信任关系（图 4 中对应的有向边）中信任评估者对被评估者的信任度。例如，$\boldsymbol{V}_1$ 表示 Agent.$T1$ 对 $T5$ 的信任度，可以看出，$\boldsymbol{V}_3$ 与 $\boldsymbol{V}_4$ 属于连接关系，$\boldsymbol{V}_2$ 与 $\boldsymbol{V}_3$、$\boldsymbol{V}_4$ 属于并联关系，以此类推。下文中出现的 $\boldsymbol{V}_5$ 与 $\boldsymbol{V}_6$ 都是计算信任度过程中的中间量，$\boldsymbol{V}_7$ 表示 Agent.$T1$ 对 $T11$ 的信任向量。

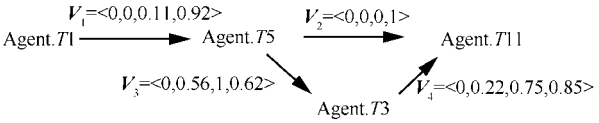

图 4　$T1$ 与 $T11$ 之间的信任网络

Agent.$T1$ 计算其对 $T11$ 的综合信任向量的步骤如下。

①$\boldsymbol{V}_5 = \boldsymbol{V}_3 \otimes \boldsymbol{V}_4$

$=< 0 \dot{\varepsilon} 0, 0.56 \dot{\varepsilon} 0.22, 1 \dot{\varepsilon} 0.75, 0.62 \dot{\varepsilon} 0.85 >$

$=< 0, 0.09, 0.75, 0.5 >$

②$\boldsymbol{V}_6 = \boldsymbol{V}_2 \oplus \boldsymbol{V}_5$

$=< 0 \overset{+}{\varepsilon} 0, 0 \overset{+}{\varepsilon} 0.09, 0 \overset{+}{\varepsilon} 0.75, 1 \overset{+}{\varepsilon} 0.5 >$

$=< 0, 0.09, 0.75, 1 >$

③$\boldsymbol{V}_7 = \boldsymbol{V}_1 \otimes \boldsymbol{V}_6$

$=< 0 \dot{\varepsilon} 0, 0 \dot{\varepsilon} 0.09, 0.11 \dot{\varepsilon} 0.75, 0.92 \dot{\varepsilon} 1 >$

$=< 0, 0, 0.07, 0.92 >$

最后得到的 V_7 就是 Agent.$T1$ 对 $T11$ 的信任向量, 根据最大隶属原则得出 Agent.$T1$ 对 $T11$ 的信任度隶属于模糊集 T_4，即非常信任。Agent.$T1$ 就可以根据其设置可信界限来判断其对 $T11$ 的信任决策是否属于可信范围, 若是, 则双方可以继续进行交互。

4　基于证书翻译与信任管理的跨域身份认证方案

4.1　系统结构

如图 5 所示, 系统包括 2 个安全域 P1 和 P2, 相较于第 2 节中 Mello 等提出的身份认证模型, 该模型中的每个域中多了一个信任代理服务，通过对实体之间直接的交互行为历史和间接的经验推荐等信息来建立各个域之间的信任关系，同时 STS 服务只需要完成认证权威的功能即可，不需要再根据客户域发来的附加消息来主观判断客户域的信任级别。

基于已建立的信任关系，域之间的认证权威基于标准的认证断言协议实现访问者身份的传递, 将源信任域内的身份信息映射到本地信任域, 同时获取必要的主体属性信息供授权服务使用, 最终实现跨域安全互操作。

4.2　方案设计

每个安全域中的用户 U 都事先在 STS/IDP 处进行注册，STS/IDP 中为用户建立身份信息。当用户需要访问某域内的资源时，用户所在域的

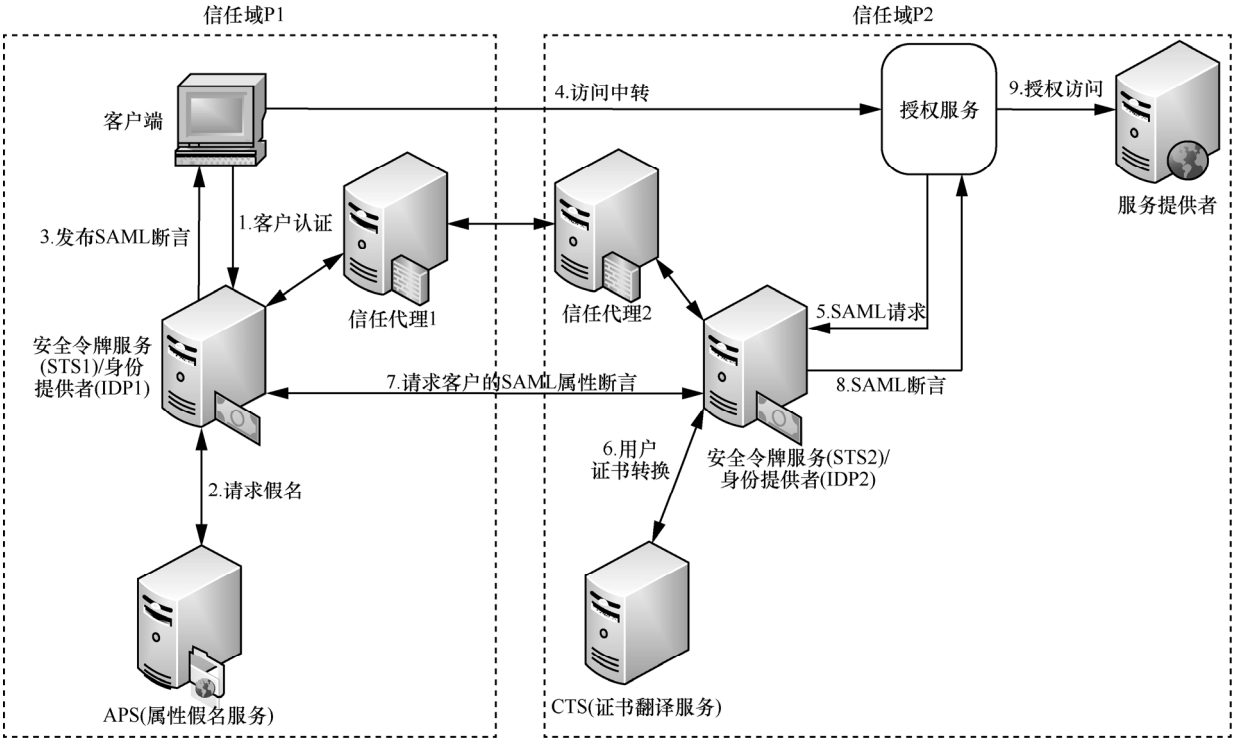

图 5 跨域认证模型

STS/IDP 服务直接验证用户的身份。当用户需要访问的资源与用户不在同一个域时，就需要进行跨域身份认证。加入了信任管理的基于证书转换服务的跨域身份认证流程主要包括：用户域对服务域的信任评估、用户域内身份认证、服务域对用户域的信任评估、服务域对用户身份进行认证。

当 P1 中的用户 U 需要访问 P2 中的服务时，P1 的信任代理首先需要对 P2 进行信任评估，Agent.P1 采用第 3 节中的信任计算方法计算其对 P2 的综合信任向量，并判断对 P2 的信任度隶属于哪个模糊集，如果 Agent.P1 认为该模糊集中的对象是可信的，可以与其进行交易，那么就开始进行域内身份认证，否则，Agent.P1 会阻止用户访问该服务。

用户向其所在域的 STS1/IDP1 提出身份认证请求（图 5 中第 1 步），如果有需要的话 STS1 向假名服务索取用户假名（图 5 中第 2 步），STS1 为客户 U 生成证书并将证书发给客户 U，完成域内身份认证后，用户将证书发送至服务所在域 P2 请求访问 P2 中的服务（图 5 中第 4 步）。

P2 收到 U 的请求后，Agent.P2 需要对 P1 进行信任评估，步骤与 Agent.P1 对 P2 的评估步骤相同，如果 P2 最终认为 P1 可信，那么 P2 中的授权服务截获该用户的证书将其转发给 P2 的 STS2/IDP2，如果该登录凭证与域 P2 采用的是不同的认证机制，则进行证书翻译，之后的认证流程与第 2 节中描述的流程相同。

5 方案分析

5.1 安全性分析

1) 双向安全

文献[11]中服务域只依赖证书来认证客户，没有考虑到用户的安全性，如果用户在不知情的情况下访问了恶意实体，那么用户的安全就得不到保证。该方案在每个域中都设计了信任代理，客户所在域与服务所在域的信任代理都会在与对方交互前对对方进行信任评估，如果信任代理认为信任评估结果是不可信的，那么信任代理会终止认证过程，因此，用户域与服务域会在信任对方的前提下进行交易，从而保证了双方的安全性。

2) 信任管理与证书认证双重安全

从服务域的角度来看，首先服务域的信任代理会对客户域做信任评估，在评估结果允许双方继续交互的情况下才继续交互，接下来才根据用户证书对用户进行身份认证，而信任评估是根据用户域的历史行为等因素进行的，因此该方案中同时考虑了用户的身份信息（证书）与行为信息

（信任评估），使服务域的安全得到了双重保障。

3) 减少恶意实体提高安全性

文中提出的信任管理方案中恶意实体通知消息使信任代理可以将其发现的恶意实体告知其他实体，当某实体被发现的恶意行为达到某一上限时，该实体就会被列为黑名单，甚至诉诸法律来惩罚恶意实体，这一惩罚机制可以在一定程度上减少实体进行恶意行为的意愿，从而提高了整个环境的安全性。

5.2 通用性分析

由于第 4 节提出的方案结合了信任管理与证书转换机制，而每个信任代理采取的是相同的信任管理方案，因此信任管理机制可以在各个信任代理之间通用，证书转换机制使采用不同安全机制的域之间可以完成身份认证，因此最大程度地扩大了用户访问服务的范围，因此该方案不会降低文献[11]中方案的通用性。

6 结束语

在多安全域的 SOA 环境下，跨域认证面临更多的安全问题。本文设计了一种信任管理方法，并将该方法与证书转换机制结合起来形成了一种新的 SOA 环境下的跨域认证模型。该模型结合了信任管理与证书转换的优势，使跨域身份认证在保证了最大范围内成功的基础上，具有了现实世界中人与人交互的模糊性与动态性，并且同时考虑了用户的身份信息与行为信息，提高了认证安全性与可信性。

参考文献：

[1] [EB/OL].http://www.ibm.com/developerworks/cn/webservices/ws-soa-enterprise1/.

[2] 蔡希尧.信息系统的发展与创新[M]. 西安：西安电子科技大学出版社, 2011.
CAI X Y. Development and innovations of information systems[M].Xi'an: Xidian University Press, 2011.

[3] YAO L, WANG L, KONG X W, et al. An inter-domain authentication scheme for pervasive computing environment[J]. Computers and Mathematics with Applications, 2010, 59(2):811-821.

[4] SINGH N, CHHABRA G, SINGH K P, et al. A secure authentication scheme in multi-operator domain (SAMD) for wireless mesh network[C]//The International Conference on Data Engineering and Communication Technology. 2016: 343-357.

[5] KHEDR W I, ABDALLA M I, ELSHEIKH A A. Enhanced inter-access service network handover authentication scheme for IEEE 802.16m network[J]. IET Information Security, 2015, 9(6): 334-343.

[6] YAN J, LU Y, LIU Y, et al. Research on beidou-based inter-domain identity authentication for mobile object[C]// 2014 IEEE Workshop on Advanced Research and Technology in Industry Applications (WARTIA). 2014: 923-926.

[7] Web service federation language (WS-Federation) version1.0 [EB/OL].http://www.pdfdrive.net/web-services-federation-language-ws-federation-version-1-e3427173.html.

[8] Liberty alliance project. Liberty architecture overview v1.1[EB/OL]. http://www.projectliberty.org/specs/liberty-architecture-overview-v1.0.pdf.

[9] OASIS. Security assertion markup language v2.0[S]. 2005.

[10] RFC 1510. The kerberos network authentication service(V5)[S].

[11] MELLO D E R, WANGHAM M S, SILVA DF J. Model for authentication credentials translation in service oriented architecture[J]. Transactions on Computational Sciences Journal, 2009, 5430: 68-86.

[12] CAHILL V, GRAY E, SEIGNEUR J M, et al. Using trust for secure collaboration in uncertain environment[J]. Pervasive Computing, IEEE 2003, 2:52-61.

[13] KAMVAR S, SCHLOSSER M, GARCIA-MOLINA H. The eigentrust algorithm for reputation management in P2P networks[C]//The 12th International Conference on World Wide Web. 2003:640-651.

[14] BETH T, BORCHERDING M, KLEIN B. Valuation of trust in open networks[C]//The European Symposium on Research in Security (ESORICS). 1994: 3-18.

[15] SONG S, HWANG K, MACWAN M. Fuzzy trust integration for security enforcement in grid computing[J]. Network and Parallel Computing, 2004, 3222:9-21.

[16] ZADEH L A. 模糊集合、语言变量及模糊逻辑[M]. 北京:科学出版社, 1982:23-33.
ZADEH L A. Linguistic variable and fuzzy logic[M]. Beijing: Science Press, 1982:23-33.

[17] ALFAREZ A R, HALLES S. A distributed trust model[C]//New Security Paradigms Workshop Langdale. 1997.

[18] 汪培庄，李洪兴. 模糊系统理论与模糊计算机[M].北京:科学出版社,1996:219-243.
WANG P Z, LI H X, Fuzzy system theory and fuzzy computer[M]. Beijing: Science Press, 1996:219-243.

作者简介：

郭晶晶（1988-），女，陕西榆林人，博士，西安电子科技大学讲师，主要研究方向为网络安全、身份认证、信任管理。

马建峰（1963-），男，陕西西安人，博士，西安电子科技大学教授、博士生导师，主要研究方向为信息安全、编码理论以及密码学。

郭鑫鑫（1995-），女，陕西榆林人，西安邮电大学本科生，主要研究方向为信息安全。

张涛（1986-），男，陕西西安人，博士，西安电子科技大学讲师，主要研究方向为信任管理、社交网络、Web 服务以及信息安全。