一种支持隐私保护的角色访问控制模型

杨秋伟 刘 玲 李肯立 唐 卓
(湖南大学计算机与通信学院 长沙 410082)

摘 要 隐私保护是多域间资源共享、协同合作的关键性安全问题。在分析现有访问控制模型隐私泄漏问题的基础上,提出了一种支持隐私保护的角色访问控制模型。该模型以基于身份的密码体制为基础,避免了传统角色访问控制模型的诸多弊端,实现了多域环境下的隐私保护,并利用随机预言模型对该模型的安全性进行了详细的分析和证明。分析表明该模型满足IND-CCA2语义安全。通过实验仿真表明该模型具有较好的实用性。

关键词 访问控制,隐私保护,基于身份的加密,策略表达式,随机预言模型
中图法分类号 TP309 **文献标识码** A

Role-based Access Control Model for Privacy Protection

YANG Qiu-wei LIU Ling LI Ken-li TANG Zhuo
(Department of Computer and Communicate Science, Hunan University, Changsha 410082, China)

Abstract Privacy preservation is a vital problem to share resource and collaboration among multi-domains. We analyzed the privacy leakage problems of current access control models, and then proposed a role-based access control model supporting privacy preservation. The model is based on identify-based encryption, avoiding a number of drawbacks in traditional role-based access model and making privacy preservation among multi-domains come true. Finally, we analyzed and certificated the security of the model in details by random oracle, and the model meets the IND-CCA2 mantic security. According to the simulation, the method is a practical model.

Keywords Access control, Privacy protection, Identify-based encryption, Police expression, Random oracle

随着计算机网络技术及其应用技术的飞速发展,基于网络的商务、政务及科学实验活动逐渐成为一种主流应用模式。现今信息系统为了达到资源共享及高使用率的目标,地域分散的多个组织通过Internet动态结盟并实现互操作[1]。基于网络跨越多个组织的大规模应用系统具有分布性、动态性和开放性等特征,因而跨越多个管理域的访问控制必须呈现资源的分布性、主体的不可认知性、运行环境的异构性、活动目标的动态性和安全控制的自主性等特点[2,3]。

在传统的分布式访问控制模型中,往往采用"乐观"模式,服务请求者将能力(Ability)或主体属性(Attribute)等披露给资源提供者[5,6],访问控制决策完全取决于以请求、安全策略和资源请求者能力为输入的一致性证明[7]。但是,这些能力和主体属性等通常携带了大量隐私信息,无限制地披露势必给多域环境中的互操作带来许多安全隐患和风险[8,9]。随着信息共享技术和数据处理技术的发展,隐私保护已成为多域互操作的安全目标之一。通常,一个虚假的服务提供者通过发布虚假的访问控制策略来获取请求者的属性特征。例如,Alice宣称提供购房优惠服务,要求请求者Bob提供关于薪金收入以及家庭住址的属性证书,那么Alice将会了解到Bob的相关信息。而薪金收入和家庭住址这样的信息被认为是隐私属性,不允许随意泄露。针对这样的安全需求,基于PKI/PMI的解决方案,需要一个可信的第三方,并且需要在线地提供服务。而Li Ninghui等提出OSBE[10],需要预先知道对方属性证书的签名值,增加了通信量,却没有很好地解决此类问题。Winsboroug等人[6]以基于角色的信任管理模型为基础,引入属性确认策略(Attribute Ack Policy)的概念。它的基本思想是对于一个给定的敏感属性,任意主体无论是否拥有该敏感属性,都披露相同的属性确认策略,对手无法从披露的策略中判定主体是否拥有此属性。该机制的安全并不充分,依旧存在着隐私泄露[8,11]。Matthew等人[12]采用基于门限的加密技术对隐私信息进行保护,以访问控制策略作为信息加密变换的密钥,以对应的与该访问控制策略相关的属性值作为解密变换的密钥,使得该信息被披露是以满足访问控制策略为前提的。这样的系统将主体与策略进行绑定,但随着访问控制策略规模的增加,当面对复杂策略时,处理能力急剧下降。刘志远等人[13]采用基于标识的加密设计了一个隐私资源保护方案,该方案的表达能力和效率非常有限,不能满足多域安全互操作的需求。

针对以上问题,本文在传统基于角色的访问控制(Role-Based Access Control,简称RBAC)模型[4,14]的基础上,以角

到稿日期:2009-07-14 返修日期:2009-09-28 本文受国家自然科学基金(90715029),湖南省自然科学基金(09JJ5045)资助。
杨秋伟(1980-),男,博士,主要研究方向为分布式安全、访问控制模型,E-mail:yky_wenfeng@163.com;刘 玲(1984-),男,硕士生,主要研究方向为访问控制、网络安全;李肯立(1971-),男,教授,主要研究方向为并行处理、网格计算;唐 卓(1981-),男,博士,主要研究方向为访问控制模型。

色布尔变元来描述策略表达式，将策略表达式转化为析取范式，建立访问控制决策与策略布尔表达式取值之间的映射，以策略表达式的元素作为授权公钥分量，用户拥有的角色作为授权私钥分量，提出了一种基于身份加密的 RBAC 模型隐私保护方案。该方案在实施资源的访问控制的同时，避免了隐私资源的泄漏。通过随机预言模型证明本方案满足 IND-CCA2 语义安全。仿真实验表明该方案具有良好的执行效率和应用效果。

本文第 1 节简要介绍 RBAC 模型和基于身份的密码机制；第 2 节提出了一种支持隐私保护的角色访问控制模型；第 3 节分析了该方案的安全性和执行效率，并给出了分析结论及其证明；最后是全文的总结。

1 相关背景

1.1 RBAC 模型

作为本文研究的基本前提，本节首先简要介绍 RBAC 模型。RBAC 由许多组件组成，主要包含两大类。

1)实体类：用户集 U；角色集 R；管理角色集 AR；权限集 P；管理权限集 AP；会话集 S；

2)映射/函数类：$UA\subseteq U\times R$，建立 U 到 R 的关联；$AUA\subseteq U\times AR$，建立 U 到 AR 的关联；$PA\subseteq P\times R$，建立 P 到 R 的关联；$APA\subseteq AP\times AR$，建立 AP 到 AR 的关联；$RH\subseteq R\times R$，建立 R 的偏序层次关系；$ARH\subseteq AR\times AR$，建立 AR 的偏序层次关系(通常这种角色层次中偏序关系采用“$\geq$”，若 $r_1\geq r_2$，称 r_1 是 r_2 的父角色)；函数 $user: S\rightarrow U$ 将会话映射到一个用户；函数 $role: S\rightarrow 2^{RU AR}$ 将会话映射到一个角色集合，$role(s_i)\subseteq\{r|(\exists r'\geq r)[(user(s_i),r')\in UA\cup AUA]\}$。

此外，存在一个约束集合，规定了上面所列举的组件的哪些赋值被允许或拒绝。

1.2 基于身份的加密

基于身份的加密算法(Identity-Based Encryption，IBE)[15,16]的基本思想是直接使用标识用户身份的字符串作为加密用的公钥，如 e-mail 地址、ID 或其他标识。IBE 加密方案的安全性建立在 CDH(Computational Diffie-Hellman)困难问题的一个变形之上，称之为 BDH(Bilinear Diffie-Hellman)问题。但直到 2001 年 Boneh 和 Franklin 才给出了一个可实际应用的实现方法，具体算法见文献[16]。

IBE 的核心是使用了超奇异椭圆曲线上的一个双线性映射(Weil pairing)。我们将负责生成并传送用户私钥的可信第三方记为 PKG(Private Key Generator)，记 Z_q 为素数阶 q 的加法群，$Z_q=\{0,\cdots,q-1\}$，Z^+ 为正整数。

1)设 p 是一个大的素数，$p\equiv 2 \bmod 3$，并且存在大素数 q 使得 $p=6q-1$；

2)$E/GF(p)$是在 $GF(p)$上构造的椭圆曲线：$y^2=x^3+1$，P 是该曲线上阶为 q 的一个点，由 P 生成的循环群记为 G；

3)BDH 问题：对随机选取的 $a,b,c\in Z_p^*$，已知(P,aP,bP,cP)，目标是试图计算 $D=\hat{e}(P,P)^{abc}\in GF(p^2)$，其中 $\hat{e}$：$G\times G\rightarrow GF(p^2)$是一具有下列性质的映射：

①双线性性。如果对所有的 $x,y\in G,a,b\in Z$，都有 $\hat{e}(ax,by)=\hat{e}(x,y)^{ab}$，则映射 $\hat{e}$ 称为一个双线性映射。

②非退化性。存在 $P,Q\in G$，使得 $\hat{e}(P,Q)\neq 1$。

③可计算性。有一个多项式时间算法来计算 $\hat{e}(P,Q)$。

2 一种支持隐私保护的角色访问控制模型

通过前面的分析可以知道，大多数访问控制模型采用“乐观”模式的授权机制，使得访问者的隐私信息披露给了资源拥有者，从而导致隐私信息的泄露。我们的目标是尽可能让合法的用户在取得合法访问权限的同时，让资源拥有者尽可能少地获得关于访问者的信息。在该安全目标下，用户在请求资源访问的过程中，资源拥有者不能获得资源请求者除用户 ID 以外的其它信息，从而实现了对用户的隐私信息的保护。

2.1 模型框架

一个典型的支持隐私保护的角色访问控制模型框架如图 1 所示，具体流程如下。

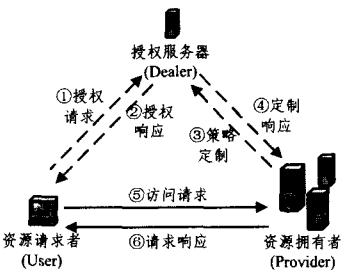


图 1 支持隐私保护的 RBAC 模型框架

①授权请求：用户为了获得在实施资源访问时的授权指派的凭据，向授权服务器(*Dealer*)申请授权票据；

②授权响应：*Dealer* 根据用户 *ID*、系统配置、相关业务逻辑实施对该用户的角色指派，分析该用户拥有的角色集，并分发用户的授权私钥分量；

③策略定制：资源拥有者从本地策略中提取与策略相关的所有角色的标识，向 *Dealer* 发送授权公钥分量，提取请求；

④定制响应：*Dealer* 根据资源拥有者提交的安全策略，向资源拥有者分发授权公钥分量；

⑤访问请求：用户向资源拥有者发起服务请求；

⑥请求响应：资源拥有者将包含安全策略加密了的资源的响应消息发送给用户。

最后，用户从响应消息中提取 *Policy* 的析取范式，对密文 C 成功解密，得到相应的明文 M。否则，拒绝此密文。

2.2 RBAC 模型中的访问控制策略

通常，访问控制决策是根据用户的访问请求、用户所拥有的权限以及访问控制策略的一致性证明得到的。访问控制策略是一类强制性约束条件，以权限作为逻辑变量组成的逻辑表达式，当且仅当访问者拥有的权限满足了该逻辑表达式的取值时才能访问资源。在 RBAC 模型中，策略通过约束“用户拥有某个角色”以及该角色拥有的权限来实施访问控制。为了进一步讨论，首先定义角色布尔变量和策略表达式。策略表达式本质是由角色布尔变元构成的布尔表达式。

定义 1(角色布尔变元) 设 $r_1,r_2,\cdots,r_n$ 是与 n 个角色一一对应的不同布尔变元，$r_1,r_2,\cdots,r_n\in\{\text{true},\text{false}\}$，当且仅当用户被指派了某个角色，该角色对应的布尔变量取真(true)，否则取值为假(false)，称 $r_1,r_2,\cdots,r_n$ 为角色布尔变元。

在 RBAC 模型中，一条策略往往涉及到用户对多个角色的拥有权的约束。本文中，用 $r_i\wedge r_j$ 表示用户必须同时拥有

r_i和r_j，$r_i \vee r_j$ 表示用户必须拥有 r_i和r_j 其一，$\neg r_i$ 表示用户不能拥有 r_i，$\neg r_i$ 大多用于互斥角色。

定义 2(策略表达式) 设与访问控制策略(access policy) p 关联的 n 个角色对应的角色布尔变元为 $r_1, r_2, \cdots, r_n$，由 $r_1, r_2, \cdots, r_n$ 通过$\neg, \wedge, \vee$ 连接的布尔表达式称为策略 p 的角色布尔变元表达式。

定理 1 访问控制模型的决策"允许"等价于策略表达式的"取真"；访问控制模型的决策"拒绝"等价于策略表达式的"取假"。

证明：由定义 1 可以看出，当且仅当用户被指派了某个角色，该角色对应的角色布尔变量在策略表达式的赋值为真，否则赋值为假。这在"用户是否拥有某个角色"和该角色对应的角色布尔变量的取值{true, false}之间建立了映射，变量取值为 true 等同于访问控制策略中对"用户拥有某个角色"的肯定，反之则是对该论题的否定。同理，在定义 2 中也建立了这样的映射。因此，访问控制模型的肯定决策"允许"等价于策略表达式的"取真"，访问控制模型的否定决策"拒绝"等价于策略表达式的"取假"。证毕。

假设存在策略表达式$(r_a \vee r_b) \wedge (r_c \vee r_d)$，当且仅当访问者必须同时拥有角色变元 r_a 和 r_b 对应的角色之一以及角色变元 r_c 和 r_d 对应的角色之一，策略表达式的取值为真，即访问者满足此条策略。从这个例子可以看出，一个策略的布尔表达式存在着多种取真的赋值方法。对于访问请求者来说，只需要具备其中一种条件就可以合法访问。这些条件之间是并列的关系，这种并列关系可用采用布尔表达式的析取范式来体现。为了方便处理，还需要将访问控制策略做进一步处理，将所有的策略表达式转化为析取范式。针对上例中的析取范式处理，求得$(r_a \wedge r_c) \vee (r_b \wedge r_c) \vee (r_a \wedge r_d) \vee (r_b \wedge r_d)$。对于策略表达式的析取范式转换本文不做赘述。

2.3 支持隐私保护的 RBAC 模型

2.3.1 模型初始化

模型初始化算法由 PKG 完成。给定一个安全参数 $k \in Z^+$，该算法按以下步骤工作：

Step 1 输入 k 产生一个素数 q 和两个阶为 q 的群 G_1，G_2。G_1 为乘法循环群，G_2 为加法循环群。一个可行双线形映射$\hat{e}: G_1 \times G_1 \to G_2$；随机选择一个 $P \in G_1$；

Step 2 选取一个随机数 $s \in Z_q^*$；

Step 3 选择一个散列函数 $H_1: \{0,1\}^* \to G_1^*$。选择一个密码学散列函数 $H_2: G_2 \to \{0,1\}^n$，$n \in Z^+$。选择散列函数 $H_3: \{0,1\}^n \times \{0,1\}^n \to Z_q^*$，选择散列函数 $H_4: \{0,1\}^n \to \{0,1\}^n$。密文空间为 $C = G_1^* \times \{0,1\}^n$。系统参数 $params = \langle q, G_1, G_2, \hat{e}, n, P, H_1, H_2, H_3, H_4 \rangle$，其中主密钥为 $s \in Z_q^*$。

2.3.2 授权指派

授权指派依旧由授权服务器完成，包括用户-角色的指派、权限-角色的指派以及它们的回收。用户为了获得在实施资源访问时的授权指派的凭据，必须向 Dealer 申请授权票据，具体步骤如下：

Step 1 用户向授权服务器发送自己的标识 $ID \in \{0,1\}^*$ 给 *Dealer*；

Step 2 *Dealer* 根据用户 ID、系统配置、相关业务逻辑实施对该用户的角色指派，分析该用户拥有的角色集$\{r_1, r_2, \cdots, r_m\}$；

Step 3 Dealer 计算 $Q_{ID} = H_1(ID) \in G_1^*$ 和 $r_i Q_{ID}$，$i = 1, \cdots, m$；

Step 4 将集合$\{r_1 Q_{ID}, \cdots, r_m Q_{ID}\}$发送给用户。

以上步骤的信息交换必须在安全信道中传输。至此，用户拥有了授权票据集合$\{r_1 Q_{ID}, \cdots, r_m Q_{ID}\}$，合法用户可以通过组合这些票据，在满足访问控制策略的前提下解密保密信息，亦称$\{r_1 Q_{ID}, \cdots, r_m Q_{ID}\}$是用户的授权私钥分量。

2.3.3 访问控制策略的定制

在 2.3.2 节中，我们成功地将授权票据跟私钥分量映射起来。下面，需要用策略表达式来构造用以加密的授权公钥分量，具体步骤如下：

Step 1 资源拥有者从本地策略中提取与策略相关的所有角色的标识 $r_1, \cdots, r_n$；

Step 2 资源拥有者向 *Dealer* 发送公钥分量提取请求 *Extract Request* $= \{r_1, \cdots, r_n\}$；

Step 3 *Dealer* 计算 $r_i P$，$i = 1, \cdots, n$；

Step 4 *Dealer* 向资源拥有者发送公钥提取响应 *Extract Response* $= \{r_1 P, \cdots, r_n P\}$。

类似于 2.2.3 小节，$\{r_1 P, \cdots, r_n P\}$被称为授权公钥分量。

2.4 资源/服务访问

资源/服务访问主要包含了加密处理和解密处理两个步骤，信息在公开信道上传输。

2.4.1 加密处理

Step 1 用户向资源拥有者发起服务请求 *Request Message* $= \langle ID, SID \rangle$，其中 SID 为资源/服务标识；

Step 2 资源拥有者计算 $Q_{ID} = H_1(ID) \in G_1^*$，并随机选取 $\sigma \in \{0,1\}^n$，让 $u = H_3(\sigma, m)$；

Step 3 资源拥有者根据 SID 提取对应的策略表达式的析取范式，每一个析取子项形如$(r_{i,1} \wedge \cdots \wedge r_{i,m})$，针对每个析取子项分别计算 $e_i = r_{i,1}^s P + \cdots + r_{i,m}^s P = (r_{i,1}^s + \cdots + r_{i,m}^s) P$；

Step 4 计算 $C = \langle uP, \sigma \oplus H_2(g_1^s), \cdots, \sigma \oplus H_2(g_k^s), m \oplus H_4(\sigma) \rangle$ where $g_i = \hat{e}(Q_{ID}, e_i) \in G_2^*$，$i = 1, \cdots, k$；

Step 5 资源拥有者给用户发送响应消息 *Response Message* $= \langle Policy, C \rangle$。

2.4.2 解密处理

Step 1 用户从响应消息中提取 *Policy* 的析取范式，确定 C 的元组项数 k，令 $C = \langle U, V_1, \cdots, V_k, W \rangle$表示用加密的密文。如果 $U \notin G_1^*$，则拒绝密文；

Step 2 用户根据 *Policy* 的析取范式构造私钥。构造方法是分析本地的角色私钥，选取符合析取子项的角色组合，$d_i = r_{i,1}^s Q_{ID} + r_{i,m}^s Q_{ID} = (r_{i,1}^s + r_{i,m}^s) Q_{ID}$；

Step 3 重复计算 $V_i \oplus H_2(\hat{e}(d_i, U)) = \sigma, W \oplus H_4(\sigma) = m$，让 $u = H_3(\sigma, m)$，测试 $U = uP$。如果不成立，则拒绝这个密文，直到测试成功或者测试结束；

Step 4 如果测试成功，则输出密文 C 对应的明文 M。否则，拒绝此密文。

由以上的加/解密的过程可知，当且仅当拥有加密公钥对应的私钥才能够正确解密。也就是说，在加密的过程中成功将策略隐含在公钥中，接受者的解密密钥包含了个体的授权指派，解密过程隐含着策略和用户所拥有的角色的一致性验

证，并且一次通信便完成了隐私资源的交换。此方案的安全性分析将在下一节展开。

3 安全性分析与性能分析

3.1 安全性分析

定义 3 如果没有任何多项式有界的敌手以一个不可忽略的优势赢得以下游戏，则称一个基于角色访问控制模型的隐私保护方案是 IND-CCA2 语义安全的。

Setup：挑战者 C 输入安全参数 k，运行 Setup 算法，并将系统参数 *params* 发送给敌手 A。

Phase 1：①敌手有目的性地选取 *ID* 发送给挑战者（为了支持复杂应用环境，一个主体可能拥有多个 *ID*，每个 *ID* 拥有的角色集可以不同），进行授权私钥抽取查询。挑战者首先要验证敌手 *ID* 的真实性，再将对应的授权私钥票据集发送给敌手；②敌手有目的性地选取策略集，将与该策略集相关联的角色标识集发送给挑战者，挑战者将对应的授权公钥票据集发送给敌手；③敌手有目的性地选取对应授权公钥票据子集加密的密文 $c_1,\cdots,c_k$，将密文 $c_j(j=1,\cdots,k)$ 发送给挑战者，挑战者使用对应的授权私钥票据集按解密算法对 $c_j(j=1,\cdots,k)$ 进行解密，并将明文 $m_j(j=1,\cdots,k)$ 发送给敌手。

Challenge：一旦敌手认为 Phase 1 结束，那么他将输出两个等长的明文 $m_0,m_1\in M$ 和一个授权公钥票据集，并且限制该授权公钥票据集中的元素未曾在 Phase 1 的抽取阶段出现过。挑战者挑选一个随机数 $b\in\{0,1\}$，使用方案中的加密算法以选取的授权公钥票据集对 m_b 进行加密，并将密文发送给敌手。

Phase 2：做 Phase 1 同样的操作，只要求授权私钥抽取查询不包含 Challenge 中授权公钥票据集对应的授权私钥集，解密查询不包含明文 m_b 对应的密文。

Guess：若敌手认为 Phase 2 结束，最后敌手输出一个猜测 $b'\in\{0,1\}$。如果 $b=b'$，则敌手赢得该游戏。

定理 2 假设 $\mathcal{F}$ 是 RBAC 中隐私保护方案的 IND-CCA2 攻击者，在运行时间 t 后，以 ε 的优势赢得定义 3 的游戏，并假设 $\mathcal{F}$ 分别可以访问 $q_{H_1},q_{H_2},q_{H_3},q_{H_4}$ 次随机预言机 H_1，H_2，H_3 和 H_4，以及 q_D 次解密预言机 D_{sim}，那么，我们便能够在时间 t' 内以 ε' 的成功概率求解 BDH 问题，并且有

$$t'\leqslant t+(q_{H_2}+q_{H_3}+q_{H_4})\cdot T$$

$$\varepsilon'\geqslant\varepsilon-\Pr[Bad]$$

$$=\varepsilon-2^{-|q|}(q_{H_1}+q_{H_3})+2^{-n}(q_{H_2}+q_{H_4})+2^{-2n-|q|}q_{H_2}\cdot q_{H_3}\cdot q_{H_4}\cdot q_D$$

式中，$|q|$ 表示素数 q 的二进制位数，T 为模幂运算的时间开销。

证明：假设系统参数为 $params=\langle q,G_1,G_2,\hat{e},n,P,H_1,H_2,H_3,H_4\rangle$，主密钥为 $s\in Z_q^*$，$\{e_i,\cdots,e_j\}$ 和 $\{d_i,\cdots,d_j\}$ 分别为授权公/私钥票据集。我们试图构造算法 $\mathcal{M}$，利用 $\mathcal{F}$ 的攻击优势来求解 BDH 问题。令主体标识 $Q_{ID}=aP$，授权公钥 $e_i=(r_{i,1}^s+\cdots+r_{i,m}^s)P=bP$，授权私钥 $d_i=(r_{i,1}^s+\cdots+r_{i,m}^s)Q_{ID}=bQ_{ID}=abP$，密文 $c=\langle Policy,U,V_1,\cdots,V_k,W\rangle$。根据信息交换协议，如果该密文正确，存在着 $V_s(s\in\{1,\cdots,k\})$，满足

$$m=W\oplus H_4(H_2(\hat{e}(bQ_{ID},U))\oplus V_s)$$

$$=W\oplus H_4(H_2(D)\oplus V_s)$$

为了使 $\mathcal{F}$ 能够完全发挥攻击优势，$\mathcal{M}$ 须精确仿真解密预言机 D 和随机预言机 H_1，H_2，H_3，H_4。我们用 D_{sim} 来表示解密预言机仿真算法，用 $H_{sim}^i,i\in\{1,2,3,4\}$ 来表示 4 个随机预言机仿真算法。

· 仿真随机预言机 H_{sim}^1

假设 $\mathcal{F}$ 能成功实施 IND-CCA2 攻击，那么 $\mathcal{F}$ 很可能提交 H_1 询问 *request*。如果确实询问过，那么将 $H_1(request)$ 直接返回给 $\mathcal{F}$。否则，$\mathcal{M}$ 随机选取 $r\leftarrow_R Z_p^*$，计算 rP 返回给 $\mathcal{F}$，并将 $(request,H_1(request))$ 加入 H_1-*List*。具体描述如下：

If $\exists(request,H_1(request))\in H_1$-*List* Then

  Return $H_1(request)$

Else

  $r\leftarrow_R Z_p^*$，$H_1(request)\leftarrow rP$

  Add $(request,H_1(request))$ To H_1-*List*

  Return $H_1(request)$

· 仿真随机预言机 H_{sim}^2

假设 $\mathcal{F}$ 能成功实施 IND-CCA2 攻击，那么 $\mathcal{F}$ 很可能提交 H_2 询问 *request*。如果确实询问过，那么将 $H_2(request)$ 直接返回给 $\mathcal{F}$。否则，$\mathcal{M}$ 随机选取 $y\leftarrow_R\{0,1\}^n$，返回 y 给 $\mathcal{F}$，并将 $(request,H_2(request))$ 加入 H_2-*List*。具体描述如下：

If $\exists(request,H_2(request))\in H_2$-*List* Then

  Return $H_2(request)$

Else

  $y\leftarrow_R\{0,1\}^n$，$H_2(request)\leftarrow y$

  Add $(request,H_2(request))$ To H_2-*List*

  Return $H_2(request)$

· 仿真随机预言机 H_{sim}^3

假设 $\mathcal{F}$ 能成功实施 IND-CCA2 攻击，那么 $\mathcal{F}$ 很可能提交 H_3 询问 (σ,m)。如果确实询问过，那么将 $H_3(\sigma,m)$ 直接返回给 $\mathcal{F}$。否则，$\mathcal{M}$ 随机选取 $u\leftarrow_R Z_p^*$，计算 uP，返回 u 给 $\mathcal{F}$，并将 (σ,m,u,uP) 加入 H_3-*List*。具体描述如下：

If $\exists(\sigma,m,H_3(\sigma,m),-)\in H_3$-*List* Then

  Return $H_3(\sigma,m)$

  Else

  $u\leftarrow_R Z_p^*$，$H_3(\sigma,m)\leftarrow u$

  Add $(\sigma,m,H_3(\sigma,m),uP)$ To H_3-*List*

  Return $H_3(\sigma,m)$

· 仿真随机预言机 H_{sim}^4

假设 $\mathcal{F}$ 能成功实施 IND-CCA2 攻击，那么 $\mathcal{F}$ 很可能提交 H_4 询问 r。如果确实询问过，那么将 $H_4(request)$ 直接返回给 $\mathcal{F}$。否则，$\mathcal{M}$ 随机选取 $x\leftarrow_R\{0,1\}^n$，返回 x 给 $\mathcal{F}$，并将 $(request,x)$ 加入 H_4-*List*。具体描述如下：

If $\exists(request,H_4(request))\in H_4$-*List* Then

  Return $H_4(request)$

Else

  $x\leftarrow_R\{0,1\}^n$，$H_4(request)\leftarrow x$

  Add $(request,H_4(request))$ To H_4-*List*

  Return $H_4(request)$

· 仿真解密预言机 D_{sim}

假设 $\mathcal{F}$ 能成功实施 IND-CCA2 攻击，那么 $\mathcal{F}$ 很可能曾提交 D_{sim} 询问 $request=\langle U,V,W\rangle$。如果确实询问过，那么将 $D_{sim}(request)$ 直接返回给 $\mathcal{F}$。如果 $\exists(\sigma,m,H_3(\sigma,m),uP)\in H_3$-*List* $\wedge uP=U$，返回 m 给 $\mathcal{F}$，并将 $(request,m)$ 加入 *D*-*List*。具体描述如下：

If $\exists(request, D_{sim}(request)) \in D\text{-}List$ Then

Return $(D_{sim}(request))$

Else

If $\exists(\sigma, m, H_3(\cdot, m), uP) \in H_3\text{-}List \wedge uP = U$ Then

$D_{sim}(request) \leftarrow m$

Add $(request, D_{sim}(request))$ To $D\text{-}List$

Return $(D_{sim}(request))$

下面进行概率分析。首先考虑 $\mathcal{M}$ 的仿真环境与真实世界相比会导致敌手的观察产生差异的事件，这些事件可能会影响敌手不能正常发挥他的攻击优势。

令 $HBad_i$ 表示算法 H^i_{sim} 中发生错误的事件，即 H^i_{sim} 中出现错误的情况，那么

$$\Pr[HBad_i] \leqslant 2^{-|q|} q_{H_i} \ (i=1,3), \Pr[HBad_i] \leqslant 2^{-n} q_{H_i} \ (i=2,4) \quad (1)$$

类似地，令 $DBad$ 表示算法 D_{sim} 中发生错误的事件，易知

$$\Pr[DBad] \leqslant \Pr[HBad_2] \cdot \Pr[HBad_3] \cdot \Pr[HBad_4] \cdot q_D = 2^{-2n-|q|} \cdot q_{H_2} \cdot q_{H_3} \cdot q_{H_4} \cdot q_D \quad (2)$$

定义 $Bad = HBad_1 \vee HBad_2 \vee HBad_3 \vee HBad_4 \vee DBad$。

$$\Pr[Bad] \leqslant \Pr[HBad_1] + \Pr[HBad_2] + \Pr[HBad_3] + \Pr[HBad_4] + \Pr[DBad] = 2^{-|q|}(q_{H_1} + q_{H_3}) + 2^{-n}(q_{H_2} + q_{H_4}) + 2^{-2n-|q|} \cdot q_{H_2} \cdot q_{H_3} \cdot q_{H_4} \cdot q_D \quad (3)$$

考虑事件 $\mathcal{F}$ wins $\wedge \neg Bad$。若此事件发生，$\mathcal{F}$ 将输出一个有效的明文 m。可以看出，对于密文 $c=\langle U, V, W\rangle$，其中 $U=uP$，求解 u 是一个椭圆曲线离散对数问题，所以只能通过后两项来构造。而为了得到密文，需要得到 $H_4(\sigma)$ 的值，即得到 σ。为了得到 σ，需要求解 $H_2(g'_{ID})$，即得到 $\hat{e}(d_{ID}, U)$，即求解 $\hat{e}(P,P)^{ab}$。那么，若仿真结束时成功解密，便能成功求解 BDH 问题。也就是说，该问题能被唯一地规约到 BDH 问题。

我们用 $\mathcal{M}$ invert 表示成功求解 $\hat{e}(P,P)^{ab}$，根据以上分析有

$$\varepsilon' = \Pr[\mathcal{M} \text{ invert}] \geqslant \Pr[\mathcal{F} \text{ wins} \wedge \neg Bad] \quad (4)$$

由于 $\varepsilon = \Pr[\mathcal{F} \text{ wins}] \leqslant \Pr[Bad] + \Pr[\mathcal{F} \text{ wins} \wedge \neg Bad]$ (5)

那么根据式(1)—式(7)可得

$$\varepsilon' \geqslant \varepsilon - \Pr[Bad] = \varepsilon - 2^{-|q|}(q_{H_1} + q_{H_3}) + 2^{-n}(q_{H_2} + q_{H_4}) + 2^{-2n-|q|} \cdot q_{H_2} \cdot q_{H_3} \cdot q_{H_4} \cdot q_D \quad (6)$$

最后，由式(6)知定理结论成立。

3.2 性能分析

由上一节的分析可以看出，本文提出的隐私保护方案是 IND-CCA2 语义安全。众所周知，安全和性能是一对矛盾体，安全性得到满足的情况下，性能势必会降低。通过与传统 RBAC 模型的性能进行对比的模拟实验证实了支持隐私保护的 RBAC 模型的执行效率和应用效果。实验环境设定为主体 A 与客体 B 进行交互，A 作为服务提供方，B 作为服务请求方。由 B 向 A 发起访问请求，考察执行效率。根据资源访问事务的差异，在访问过程中采用不同的安全策略。改变安全策略导致执行效率不同，反过来也可以根据执行效率来优化安全策略的配置。模拟实验在 Windows 2000 环境下采用 visual c++ 6.0 编程实现。模拟实验得到的结果如图 2 所示。从实验结果中可得出以下结论：通过配置合理的安全策略，支持隐私保护的 RBAC 模型与传统模型相比，在执行效率方面影响很小，但安全性方面大大优于基本模型。

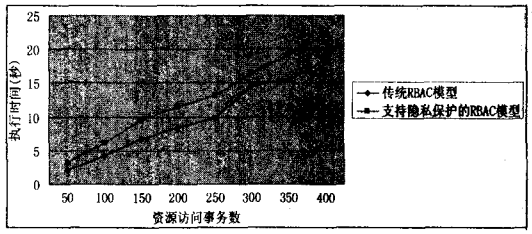


图 2 支持隐私保护的 RBAC 模型与传统 RBAC 模型的执行性能比较

结束语 本文在传统基于角色的访问控制模型的基础上，以角色布尔变元来描述策略表达式，将策略表达式转化为析取范式，建立访问控制决策与策略布尔表达式取值之间的映射，以策略表达式的元素作为授权公钥分量，用户拥有的角色作为授权私钥分量，提出了一种基于身份加密的 RBAC 模型隐私保护方案。该方案不需要在线的可信第三方，不披露除用户 ID 以外的其它信息。在实施资源的访问控制的同时，避免了隐私资源的泄漏。在资源请求者与资源拥有者进行交互时，一次通信就完成了信息交换，具有通信量较低的优点。通过随机预言模型证明本方案满足 IND-CCA2 语义安全。仿真实验表明，该方案具有良好的执行效率和应用效果，很好地解决了多域以及 P2P 等环境下资源共享所存在的隐私泄漏的问题，但在隐私资源保护的策略完整性等方面需要进一步研究。

参 考 文 献

[1] Gong L, Qian X. Computational Issues in Secure Interoperation [J]. IEEE Transactions on Software Engineering, 1996, 22(1): 43-52

[2] Ajayi O, Sinnott R, Stell A. Trust Realisation in Multi-domain Collaborative Environments[C]// Proceedings of the 6th IEEE/ACIS International Conference on Computer and Information Science (ICIS'07). Melbourne, Australia, 2007: 906-911

[3] 夏鲁宁，荆继武. 一种基于层次命名空间的 RBAC 管理模型[J]. 计算机研究与发展，2007，244(12)：2020-2027

[4] 杨秋伟，洪帆，杨木祥，等. 基于角色访问控制管理模型的安全性分析[J]. 软件学报，2006(8)：1804-1810

[5] Snyder L. Formal Models of Capability-based Protection Systems[J]. IEEE Transactions on Computers, 1981, 30(3): 172-181

[6] Winsborough W H, Seamons K E, Jones V E. Automate trust negotiation[C]// DARPA Information Survivability Conf. and Exposition. 2000: 88-102

[7] Li Ninghui, Winsborough W H, Mitchell J C. Beyond Proof-of-Compliance: Safety and Availability Analysis in Trust Management[C]// Proceedings of IEEE Symposium on Security and Privacy. 2003: 123-139

[8] Irwin K, Yu Ting. Preventing Attribute Information Leakage in Automated Trust Negotiation[C]// Proceedings of the 12th ACM Conference on Computer and Communications Security. 2005: 36-45

[9] 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

[10] Li N, Du W, Boneh D. Oblivious signature-based envelope[C]// Proceedings of the 22nd ACM Symposium on Principles of Distributed Computing (PODC 2003). 2003: 182-189

[11] Frikken K, Atallah M, Li J. Hidden Access Control Policies with Hidden Credentials[C]// Proceedings of the 3rd ACM Workshop on Privacy in the Electronic Society. 2004: 130-131

(下转第 121 页)

间几方面来验证算法的有效性。设初始节点数量为 m_0，局域世界节点个数为 M，插入节点 t。$M=m$，网络中每次增加一个节点，先从整个网络中选取一个小的局域世界，然后新增节点都是随机与局域世界中的节点相连；$M=m_0+t$，该模型把整个网络作为一个局域世界，每次增加节点都是从整个网络中按照度的概率选择节点连接，其中局域世界树选举参照文献[8]中的方法。

实验通过网络结构的演化判据的三大统计属性之一的顶点度分布($P(k)$)来检验网络是否具备幂律特性。

图 2 实验结果表明在不同初始网络状态下，$M\approx t+m_0$ 时的 $P(k)$曲线趋于幂律分布，当 $M=m$ 时分布曲线相似。由此可知，点强度优先的连接算法对网络初始状态并不敏感，均可以有效地将网络演变成一个具有幂律分布特性的小世界网络。当初始网络的规模很小(如 100 个节点)时，初始网络是否连通作用不明显，但是随着初始网络规模的增加，在曲线右下部渐渐突现出一个连接数目众多的独立尾部，考察尾部中的节点，发现全部来自初始网络，说明当网络最终规模和初始规模的比例没有达到一定程度时，全连通的初始网络将会因为其先入优势，而成长为网络的核心，从中还可知当模型连接数量和网络规模达到一定比例之后，网络的无标度性特性越明显。

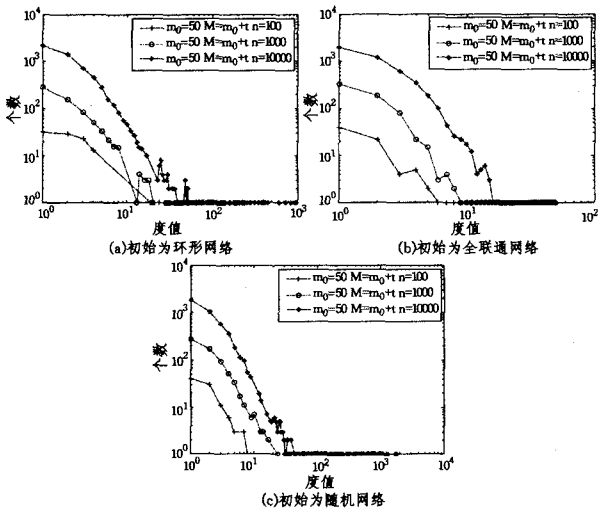
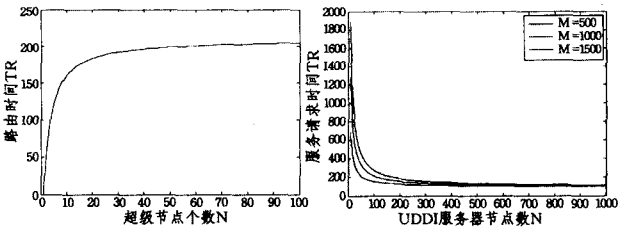


图 2　不同初始网络在 $M=m_0+t$ 时 $P(k)$分布图

为了反映模型在服务响应时间上与节点的关系，模型对路由时间与超级节点数量的关系和平均服务响应时间与网络节点的关系进行了实验，以分析节点数量与服务时间的关系。

图 3(a)实验结果表明，服务信息的路由时间在超级节点数量超过 20 之后基本维持在一个常量，其时间取决与网络时延。本文主要讨论较大规模的网络，超级节点数量较多，因此为了简化问题的讨论，将路由时间定为常量 δ。图 3(b)实验结果表明节点数量在 200 个以内，请求响应时间与网络中的节点数量关系密切，增加服务注册中心的数量可以有效减少整体服务响应时间；当节点大于 200 时，服务注册中心数量的增加对提高服务响应时间不明显，因此，200 节点以上，与服务注册中心所包含的信息量关系不明显。



(a)路由时间与超级节点数量的关系　(b)平均服务响应时间与网络节点关系

图 3　平均服务查询时间和超级节点数量的关系

结束语　本文通过在密集区投放服务点的指导思想，提出了一种具有超级节点的语义路由 UDDI 模型 SPSR-UDDI，网络演化表现为节点对选举出让自己服务查询最快的区域超级节点以及维护网络连接所做出的权衡，通过节点边权优先连接原则让部分节点动态调整连接策略，使得全局服务响应时间较短。本文提出的节点点强度优先连接模型，克服了当前部分模型只考虑随机性连接而没有考虑择优性的连接等不太符合真实世界网络的复杂性与多样性的不足，同时建立了网络演化和服务响应时间模型，实现了网络自组织演化过程，并进行了仿真实验，证实了其有效性。

参 考 文 献

[1] Clement L. Universal Description Discovery & Integration(UDDI 3.0). 2004. http//uddi.org/pubs/uddi_v3.htm

[2] Tran D A, Hua K A. A peer-to-peer architecture for media streaming[J]. IEEE Journal on Selected Areas in Communications, 2004, 22(1): 1-14

[3] Condie T, et al. Adaptive peer-to-peer topologies[C]// 4th Int. Conf. on Peer-to-Peer Computing. New York: IEEE Press, 2004: 53-62

[4] 杜宗霞，怀进鹏. 主动分布式 Web 服务注册机制研究与实现[J]. 软件学报，2006(03)：454-462

[5] 董攀，朱培栋，卢锡城. 一种网络自组织演化的数学模型[J]. 软件学报，2007，18(12)：3071-3079

[6] Chen QH, et al. The modeling of scale-free networks[J]. Phys A, 2004, 335: 240-248

[7] 方锦清，毕桥，等. 复杂动态网络的一种和谐统一的混合择优模型及其普适特性[J]. 中国科学(G 辑)，2007(2)：230-249

[8] 赵海，袁韶谦，等. 一种局部集聚的网络演化模型[J]. 东北大学学报：自然科学版，2007(11)：1548-1551

[9] 刘道群，刘写. 一种 P2P 网络安全动态的信任模型[J]. 重庆工学院学报：自然科学版，2009，23(11)：90-94

(上接第 50 页)

[12] Matthew P, Patrick T, Patrick M, et al. Secure Attribute Based Systems[C]// Proceedings of the 13th ACM Conference on Computer and Communications Security. 2006: 99-112

[13] 刘志远，杨秋伟，洪帆，等. 一种基于标识的隐私资源保护方案[J]. 计算机应用，2008，28(2)：418-421

[14] Sandhu R, Coyne E J, Feinstein H L, et al. Role-based Access Control Models[J]. IEEE Computer, 1996, 29(2): 38-47

[15] Shamir A. Identity-based cryptography and signature schemes [A]// Advances in Cryptology, CRYPTO'84, Lecture Notes in Computer Science[C]. Berlin: Springer-Verlag, 1985, 196: 47-53

[16] Boneh D, Franklin M. Identity-based encryption from the Weil pairing[A]// Advances in Cryptology, CRYPTO 2001, Lecture Notes in Computer Science [C]. Berlin: Springer-Verlag, 2001, 2139: 213-229