# 基于标签树的自动信任协商策略分析

夏冬梅 曾国荪 陈 波 鲍 宇
(同济大学计算机科学与技术系 上海 201804)
(同济大学嵌入式系统与服务计算教育部重点实验室 上海 201804)

**摘 要** 网络实体间的信任建立是彼此进行安全交互的前提,自动信任协商为分布式环境下陌生实体的信任建立提供了方法。但现有的信任协商默认协商中访问控制策略正确,而策略本身很可能存在某些问题,导致协商失败。重点分析协商策略的性质,首先针对可能存在的冲突策略、平凡策略等策略不一致问题,构建了一种基于标签树的逻辑证明方法,进行策略一致性的检测,并证明了此证明方法的可靠性、完备性;其次,通过对策略树进行化简以求得最小证书集,并对其进行一次性披露和匹配,尽快达成成功协商,从而避免策略环问题,提高协商效率及成功率。

**关键词** 自动信任协商,访问控制策略,一致性,策略环
**中图法分类号** TP301 **文献标识码** A

## Analysis of Automated Trust Negotiation Policy Based on Label Tree

XIA Dong-mei ZEN Guo-sun CHEN Bo BAO Yu
(Department of Computer Science and Technology, Tongji University, Shanghai 201804, China)
(Tongji Branch, National Engineering & Technology Center of High Performance Computers, Shanghai 201804, China)

**Abstract** In the virtual computing environment the securing co-operation is based on the trust between the strangers, automated trust negotia-tion provides a mean to establish strangers in distributed situation. However, the current negotiation takes it for granted that the access control policy of negotiation is correct, which will probably has many problems to lead negotiation to fail. This paper emphasized on analyzing the characters of negotiation policy. Firstly, aiming at the inconsistency problems such as inconsistent policy and trivial policy, this paper established a logic proving method based on label binary tree in order to test policy consistency, so as to prove the soundness and completeness of this method. Secondly, this paper gained the minimal credential set by predigesting the policy tree, then successful negotiation was achieved through one-off discovering the minimal credential set, which will avoid the policy circle and improve the efficiency and the probability of negotiation.

**Keywords** Automated trust negotiation, Access control policy, Consistency, Policy circle

## 1 引言

在分布式计算环境中,如何在通信和交易主体间建立信任关系是一个重要问题。传统的访问控制技术主要基于请求方的身份进行授权,需要设定统一的安全管理域。然而,在开放的互联网中,基于身份的访问控制技术在跨多安全域进行授权及访问控制时暴露出许多弱点。

因此,1996年,AT&T实验室的Blaze等人提出了信任管理[1,2]的概念,为开放网络环境下建立信任提供了新思路。Winsborough等人称这类信任管理系统为基于能力(capability-based)的授权系统。Blaze等人开发了具有代表性的两个信任管理系统PolicyMaker和KeyNote。Li等人又提出了一种基于角色的信任管理框架[3],但它们仍需要服务提供方预先为服务请求方颁发指定权限的属性证书,无法与陌生方建立动态的信任关系。为了不依赖第三方在陌生实体间建立动态的信任关系,在信任管理的基础上Winsborough等人提出了自动信任协商(automated trust negotiation,简称ATN)的概念[4],并成为当前的一个重要研究方向。它是"通过信任证、访问控制策略的交互披露,资源的请求方和提供方自动地建立信任关系"。ATN的方法和传统的基于身份的访问控制系统相比,区别于以下几个方面[5]:

1) 两个陌生实体间是基于属性建立信任的,而属性则是通过披露数字证书来得以证明的。其中,数字证书是证书发布方关于参与方的属性的一种可校验的、不可更改的(non-forgeable)数字断言。

2)协商双方都可以定义各自的访问控制策略,以控制外部访问者对其敏感资源的访问。

3)信任协商双方可以直接建立信任,无需第三方的参与。

到稿日期:2009-01-07 返修日期:2009-03-16 本文受863专项(2007AA01Z425),973课题(2007CB316502),国家自然基金项目(90718015,60673157)资助。

夏冬梅 博士生,主要研究方向为可信计算,E-mail:dongmei_98jb@163.com;曾国荪 博士,教授,博士生导师,主要研究方向为可信并行计算、信息安全;陈 波 博士生,主要研究方向为可信计算、软件验证;鲍 宇 博士生,主要研究方向为可信计算。

在 ATN 中，访问控制策略在未授权的访问中对资源保护方面起着关键的作用[6]。而对于现有的 ATN，一旦协商双方制定好访问控制策略，则默认策略的正确性。然而，访问控制策略本身可能存在某些问题，而这些问题在协商过程中也很难被检测出来。因此，如果不对策略加以分析就开始协商，就很可能导致不必要的资源浪费以及协商的失败。为此，本文提出应在协商开始之前对访问控制策略的性质进行分析，进而保证协商过程的正确率及减少资源浪费。本文总结了当前信任协商中的访问控制策略(以下简称协商策略)可能存在的问题：

**问题 1** 访问控制策略中的冲突。在 ATN 中，访问控制策略常被设计得复杂化，目的是保护敏感策略或者策略中的敏感内容。然而，过于复杂的策略使得双方都难于执行，特别地，这些策略可能导致不一致性。例如，一个复杂的策略可以描述成 $P=f(a,b)=(a\vee\neg b)\wedge(b\vee\neg a)\wedge(a\vee b)\wedge(\neg a\vee\neg b)$，则无论 $a,b$ 取 true 或者 false，都有 $P=$false，即策略本身存在冲突。在这种情况下，协商过程必定失败。

**问题 2** 访问控制策略中存在策略环。在 ATN 中，协商双方根据访问控制策略进行证书披露。如果协商双方证书和策略的披露都相互依赖，则存在死锁，因而也会导致协商失败。

考虑到以上这些问题，在协商之前对其访问控制策略进行分析是不可或缺的。在以往的文献[7]中，也有试图利用 0-1 表以及策略矩阵的方法解决上述问题，但是没有证明这些方法的可靠性、完备性，且这些方法不易应用实现。因此本文以标签树的方式来表示访问控制策略，对策略进行分析和化简，从而避免上述问题。总体说来本文的贡献在于以下几点：

1) 总结了 ATN 中访问控制策略存在的若干问题，而在以往文献中都默认策略的正确性。

2) 定义了冲突策略、平凡策略两种问题策略；构造了一种基于标签二叉树的逻辑证明方法，据此进行策略一致性分析，并且证明了此分析方法的可靠性、完备性。

3) 对策略进行化简，求得最小证书集，通过证书的一次性披露达成成功协商，从而避免了策略环，并提高了协商效率，避免了不必要的协商失败。

## 2 自动信任协商基本概念

### 2.1 动信任协商流程

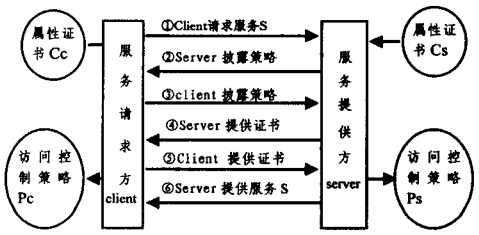


图 1 自动信任协商流程

开放网络环境中，陌生实体之间自动建立信任的组成和协商流程如图 1 所示。其中，Client/Server 是协商双方，它们分别具备一些属性证书以及保护这些证书的访问控制策略。在 ATN 中，协商由请求方发起后，提供方开始只披露那些形如 Si←True 的、没有条件直接可以披露的非敏感策略，待双方证书的不断深入披露，许多敏感策略的条件得到满足，再不断披露这些策略，直到请求方达成对服务 S 的访问，协商成功，否则协商失败。

### 2.2 信任协商的基本概念

造成协商失败的原因有两方面：一是双方持有的证书不足以达到对方的需求；另一方面可能在策略制定的时候就已经存在诸如策略冲突、策略环等问题，注定协商失败。本文着重分析后者，这里给出了相关的定义。

**定义 1**(证书集) $C=\{c_1,c_2,\cdots,c_n\}(1\leqslant i\leqslant n)$，其中 $c_i$ 表示证书，是由协商双方各自持有的、包含属性信息的、由权威中心签名的数字断言，令 $Cc$ 和 $Cs$ 分别代表服务请求方和提供方的证书集，则 $C=Cc\cup Cs$。

**定义 2**(策略集) $P=Pc\cup Ps$，其中 $Pc$ 是用来保护请求方证书的策略，$Ps$ 是保护提供方证书的策略。策略类型分成元策略和复合策略。元策略是对某一类属性的保护策略，复合策略则是元策略的集合。例如，$Ps$ 是用来保护资源或服务 $S$ 的，形如 $Ps:S\leftarrow f_s(p_1,p_2,\cdots,p_k)$，其中 $p_i$ 是对某一类属性证书的保护策略，形如 $p_i:s_i\leftarrow c_i$，而 $f_s(p_1,p_2,\cdots,p_k)$ 是对元策略 $p_i$ 进行 $\wedge$，$\vee$，$\neg$ 等操作的函数，且其值取 True 或 False。例如，给定一个证书集 $C$ 以及策略函数 $f_s(p_1,p_2,p_3)=p_1\vee(p_2\wedge p_3)$，则有 $f_s(p_1,p_2)=$True，$f_s(p_2,p_3)=$False。当且仅当 $f_s(C)=$True 时，称证书集 $C$ 满足策略 $Ps$。在协商过程中，请求方不断披露证书，直到其披露的证书集 $C'$ 满足 $f_s(C')=$True，则协商成功，可以对服务 $S$ 进行访问；否则协商失败，且过程终止。

**定义 3**(自动信任协商) 协商由请求方对某个资源或服务 $S\in Cs$ 的请求开始，其目标是寻找证书披露序列 $(c_1,c_2,\cdots,c_n=s)$，其中 $c_i\in Cc\cup Cs(1\leqslant i\leqslant n)$ 且对于每个 $c_i$ 对应的访问控制策略都是被满足的，即 $f_{ci}(\cup_{j<i}c_j)=$True。如果协商双方找到了一条这样的证书序列，则协商成功，否则失败。而证书序列的选择取决于双方的决策，即什么时候披露那个证书以及何时结束协商等。

**定义 4**(冲突策略) 设 $Cs$ 和 $Ps$ 分别代表服务提供方的证书集和策略集。协商由服务请求方对于证书 $S\in Cs$ 的请求开始。为了更好地保护访问控制策略的重要信息，$Ps$ 一般都有较复杂的表达式，以要求请求者能够披露更多的证书。然而复杂的访问控制策略加大了协商双方的协商难度，同时一些策略可能会出现不一致的情况。设 $Ps:S\leftarrow f_s(p_1,p_2,\cdots,p_n)$。如果 $f_s(p_1,p_2,\cdots,p_n)\equiv$False，无论 $p_i=$True or $p_i=$False，则称此策略是冲突策略。

**定义 5**(平凡策略) 通常 $f_s(p_1,p_2,\cdots,p_n)$ 在 $\{p_i\}$ 取不同值，即对应不同的证书序列时，可能取值 True 或者 False。而以下情况出现时，即 $f_s(p_1,p_2,\cdots,p_n)\equiv$True，则无论请求者是否持有相应证书，访问控制策略总会满足。此策略仍是不合法的策略，我们称之为平凡策略。

**定义 6**(策略一致性) 当自动信任协商中的访问控制策略 Policy 满足既不是冲突策略，也不是平凡策略，则称此策略满足策略一致性。

**定义 7**(策略环) 设 $Cc$ 和 $Cs$($Pc$ 和 $Ps$)分别代表请求方和提供方的证书集(策略集)，协商由请求方对服务 $S\in Cs$ 的请求开始，当在协商过程中存在如下情况 $Pci:c_i\leftarrow g_{ci}(s_j)$ 且 $Psj:s_j\leftarrow h_{sj}(c_i)$，即双方披露的依据都是相互依赖的，则称此访问控制策略中存在环，此协商过程是死锁的。

## 3 信任协商策略的一致性检测

### 3.1 策略描述

一个复合的访问控制策略 $P$ 可以通过若干元策略 $P_i(i=1,2,\cdots,n)$的$\langle\wedge,\vee,\rightarrow\rangle$方式来组合 $P=f(p_1,p_2,\cdots,p_n)$。例如，某书城有提供给在校师生的打折政策。如果某人能提供由 TJU 大学颁发的教师证或者有由 TJU 颁发的学生证，且其在校期间都必须没有不良记录，则满足这些条件的人就可以享受打折优惠。这条访问控制策略如图 2 所示。

```
Policy_discount=f(p1,p2,p3)= (p1∨ p2) ∧¬ p3
P1:{c1: TJU.teacher←x},
P2:{c2: TJU.student←x},
p3:{C3: TJU.Badrecord←x},其中x是变量。
```

图 2

### 3.2 基于标签二叉树的一致性证明方法的构造

本节构造一种可以构造命题证明的逻辑方法，用来证明访问控制策略的一致性。此类证明都是标签二叉树的形式，树上的标签是标号命题，即开头标有 $T$ 或 $F$（给命题指定了一个假定真值）的命题。对于命题 $\alpha$，$T(\alpha)$表示假定命题 $\alpha$ 是正确的；$F(\alpha)$表示假定命题 $\alpha$ 是错误的。对于命题 $\alpha$ 的证明可以通过对 $T(\alpha)$或 $F(\alpha)$构造标签二叉树的思路，将其分解成原子树来完成。对于任意命题 $\alpha,\beta$ 以及任意命题字母 $A$，原子树的基本情况如图 3 所示。

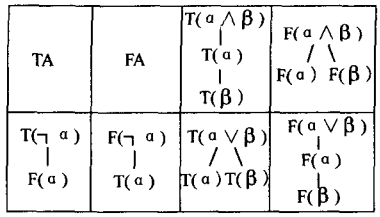


图 3

例如，若证明命题$((p1\vee(p2\wedge\neg p3))$的正确性，则证明此命题的真值假设 $T((p1\vee p2)\wedge\neg p3))$正确即可。证明方法是将其不断分解，直到所有结点都分解成原子树（称完全树）。如果命题正确，则由它分解出来的完全树中到达根节点的路径至少有一条是不矛盾的。在本例中，先把 $T((p1\vee p2)\wedge\neg p3))$分解到 $T(p1\vee p2)$和 $T(\neg p3)$，若$((p1\vee p2)\wedge\neg p3))$真，则 $p1\vee p2$ 真或者 $\neg p3$ 真；接下来把 $T(\neg p3)$分解到 $F(p3)$（$T(\neg p3)$，意味着 $F(p3)$），以及将 $T(p1\vee p2)$分解到 $T(p1)$或 $T(p2)$（若$(p1\vee p2)$真，则 $p1$ 真或者 $p2$ 真），则全部分解成原子树，如图 4 所示。此两条路径都不存在矛盾，所以命题$((p1\vee p2)\wedge\neg p3)$正确。

上述过程是构造命题证明的一种方法，其主要思路如下：从某个标号命题，如 $T(\alpha)$或 $F(\alpha)$出发，以其做树的根，利用上述过程把它分解到各分支，找到导出矛盾的那一支分解（对应树上的一条路径），对于 $T(\alpha)$，若存在有一条非矛盾的路径，则可证明 $\alpha$ 的正确性；对于 $F(\alpha)$，若存在有一条矛盾的路径，则说明 $\neg\alpha$ 的正确性。

### 3.3 一致性检测

**定理 1**（策略一致性证明） 当自动信任协商中的访问控制策略 Policy 经如下证明不是平凡的和冲突的，则称访问控制策略具有策略一致性，其中 b 证明策略是平凡的，若 c 证明此策略是冲突的：

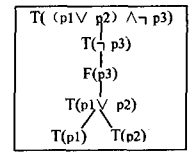


图 4

a）策略 Policy 可描述为 $f(p_1,p_2,\cdots,p_n)$，其中 $f$ 是一个对元策略 $p_i$ 进行交、并、非组合运算的布尔函数，其返回值为 True 或 False；

b）以 $F(P)$为根，将其分解成原子树，若所有到达根结点的路径都矛盾，则此策略是平凡策略；

c）以 $T(P)$为根，将其分解成原子树，若所有到达根结点的路径都矛盾，则此策略是冲突策略。

例如，对于策略 $P=p_1\wedge\neg p_1$ 以及策略 $P'=p_1\vee\neg p_1$，其一致性检测方法分别如图 5(a)及图 5(b)所示，则策略 $P$ 是冲突的，而策略 $P'$是平凡的，它们都不满足策略的一致性。

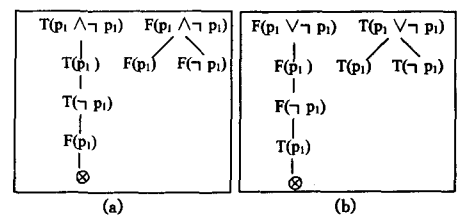


图 5

### 3.4 一致性检测的完备性、可靠性证明

对于策略的一致性，前面给出了上述检测方法。而对于一种证明方法，其证明有效性的语义概念应和可证性的语法概念相互等价。因此，需要分别证明所有无效策略/冲突策略都是永真的/永假的（证明的可靠性）、所有永真的/永假的命题都是无效的/冲突的（证明的完全性）。这里只给出其中平凡策略的可靠性完备性证明，冲突策略的可靠完备性证明与之类似。

**定理 2**（可靠性） 如果 $P$ 是平凡策略（即以 $F(P)$ 为根分解成的完全树，所有到达根结点的路径都矛盾），那么 $P$ 是永真的，即 $\vdash P\Rightarrow\vdash P$。

证明：采用反证法。假设 $P$ 非永真。根据定义，存在一个赋值 $\gamma$，指派真值 $F$ 给 $P$。在以下两种情况下，我们称赋值 $\gamma$（对元策略赋真值）与标号命题 $E$ 相一致：如果 $E$ 是 $T(P)$且 $\gamma(P)=T$，或者如果 $E$ 是 $F(P)$且 $\gamma(P)=F$。由引理 1 知，对任意的赋值 $\gamma$，如果它与某个树的根相一致，那么它必与该表中某条路径上的所有元策略真值相一致。对矛盾表中的任何一条路径，都不存在赋值与其相一致（由于每条路径都有形如 $F(p_i)$，$T(p_i)$的同时存在，因而无法给 $p_i$ 赋值），所以 $F(P)$不可能分解成每条路径都矛盾的完全树，即 $P$ 不是平凡策略，与前提矛盾，因此假设不成立，命题得证。

**引理 1** 设 $\tau$ 是逻辑标签二叉树 $\cup\tau_n$，$\gamma$ 是与 $\tau$ 的根值相一致的赋值，那么 $\tau$ 中存在一条路径 $W$，其上所有元策略的真值都与 $\gamma$ 相一致。

证明（归纳证明）：根据假设 $\gamma$ 与 $\tau$ 的根相一致，易知归纳法的基本情形成立，即对于所有根表值 $\tau$ 是原子表的情形，总有赋值 $\gamma$ 与 $\tau$ 的根相一致。例如根表值是 $T(\alpha\wedge\beta)$的情形，对应赋值 $\gamma(\alpha)=T,\gamma(\beta)=T$ 与其中一条路径一致。对归纳

步，假设已经构造了 $\tau_n$ 中的路径 $W_n$，它的所有表值都与 $\gamma$ 相一致。如果 $\tau_{n+1}$ 是 $\tau_n$ 扩展而来的，但未扩展其中的路径 $W_n$，那么令 $W_{n+1}=W_n$。如果 $\tau_{n+1}$ 扩展了 $\tau_n$，那么即对出现在 $\tau$ 中的某个标签值 $E$，将以其做根的原子树添加到 $W_n$ 的末端。由归纳假设知 $\gamma$ 与 $E$ 相一致，类似于对基本情形的分析，得到 $\gamma$ 必与 $W_n$ 的某条扩展路径相一致，记作 $W_{n+1}$。

**定理 3**(完备性)　如果策略 $P$ 永真，那么 $P$ 是平凡的(即以 $F(P)$ 为根分解成的完成树，所有到达根结点的路径都矛盾)，即 $\models P \Rightarrow \vdash P$。

证明：假设 $P$ 永真，即对每个赋值 $\gamma$，$\gamma(P)=T$。考虑以 $F(P)$ 为根的任意已经分解的完成树 $\tau$。如果 $\tau$ 有一条非矛盾路径 $W$，则由引理 1 知，存在一个赋值 $\gamma$，它与 $P$ 上所有元策略的真值相一致，所以也与 $F(P)$ 相一致。这就给出了一个赋值，使得 $\gamma(P)=F$，与 $P$ 的永真性相悖。因此 $\tau$ 中的每条路径都是矛盾的，从而 $P$ 是平凡的。

## 4　最小证书集消解策略环

### 4.1　策略简化

在 ATN 中，访问控制策略的设计很可能影响到协商的成功率和效率。过多的证书披露过程以及过于复杂的策略，都会降低协商的效率，甚至导致协商失败。特别地，如果证书披露过程中存在环，则按照策略环的证书披露序列进行证书披露，协商必定失败。因此，本文在前面所述标签树的基础上，提出了对策略进行约简的方法，从而找到 ATN 中达到协商成功的最小证书集。协商时，只需披露最小证书集，即可一次性达成协商。此法一方面提高了协商的效率及成功率，同时避免了策略环造成的死锁情况。

由于策略可以通过逻辑运算化成析取范式 $\Sigma(\Pi(pi,pj))$ 的形式[7]，为了方便对策略的化简，已有的方法将析取范式表示成策略矩阵[8]的形式。但这些方法不够直观，且在策略的分析、化简上不易操作实现[9]。因此，本文将访问控制策略先化成析取范式，再用策略标签树(ACP-LTree)的形式来描述。

每一个策略都可以描述成 ACP-LTree 的形式，它表示了元策略和受复合策略保护的访问资源之间的关系。根节点的标签表示复合的访问控制策略，它控制资源 R 的访问；其它结点标签表示元策略，每一条由叶子结点到达根结点的路径都表示访问资源 R 必须满足的元策略的集合。如 $p1 \wedge (p2 \vee \neg p3)$ 可以化成析取范式 $(p1 \wedge p2) \vee (p1 \wedge \neg p3)$，再将析取范式形式的策略表示成 ACP-Ltree，如图 6 所示。

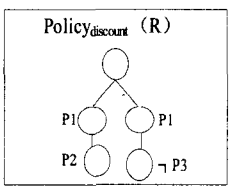


图 6

对于 ACP-Ltree 表示的策略，则可以根据以下规则对其进行化简：

1) 若某元策略是 true，遍历整个树，消去树上所有此策略。

2)若某元策略是 false，则消去所有通过该结点到达根结点的所有路径(包括边)。

3)若一条到根节点的路径上有重复的结点，则只保留一个，消去重复的。

4)依次遍历每条到根节点的路径。如果找到和其相同的一条，则消去这条路径(消去冗余路径)。

5)若一条到根节点的路径，其节点都包含在另一条中，则消去另一条路径，如图 7(a)所示(吸收)。

6)若一条到根节点的路径同另一条路径有相同的节点和相反的节点，则消去其中一条路径，且另一条路径删去其中相反节点，如图 7(b)所示(合并)。

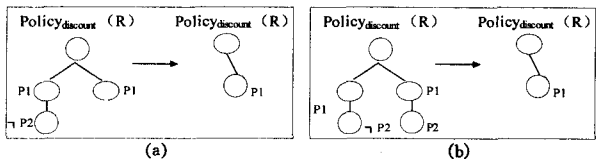


图 7

### 4.2　最小证书集

当一个访问控制策略描述成 ACP-LTree 的形式，按照前述规则对其约简后，每一条由叶子结点到根结点的路径所包含的证书集就是最小证书集的一个元素，所有路径则构成了满足此访问控制策略的最小证书集 $C_M$。

**定义 8**(最小证书集)　若 $Ps=\bigcap Ps_i=Ps_1 \wedge Ps_2 \wedge \cdots \wedge Ps_n$，且 $S_i \leftarrow f_{si}(c_i)$，则 $if\ \exists i(1 \leqslant i \leqslant n), \{\bigcup c_i \mid \bigcap Ps_i=\text{true}\} \Rightarrow \bigcup c_i \subseteq C_E$，即使得 $Ps$ 是 true 的所有证书序列都被列入有效证书集 $C_E$。而最小证书集 $C_M$ 是对 $C_E$ 简化的子集，也可以使得 $Ps$ 是 true。

ATN 中，协商的目标是找到一个证书披露序列，从而满足服务请求。然而在协商过程中，服务提供和请求方的证书要求依次披露，这就有可能造成策略环、协商失败等问题。本文利用最小证书集来计算证书披露的序列，以有效避免策略环问题，提高协商的效率。

### 4.3　策略环的消解

最小证书集可以帮助计算服务请求端应该提供的证书披露序列，协商过程根据证书检测算法检测客户是否持有最小证书集内的证书即可判断协商是否成功，不再需要披露具有敏感信息的访问控制策略，只需披露最小证书集。方法如下：

在协商前，请求方将自己持有的证书 $C_C$ 拿来分别与 $C_M$ 匹配(匹配算法如图 3 所示)。若在 $C_M$ 中找到一个元素，使得其包含在 $C_C$ 中，则可以达成成功协商，否则提供方拒绝请求方的访问。此方法通过一次性的证书匹配，即可达成协商结果，一方面可以提高协商效率和成功率，另一方面可以解决逐步披露证书中可能造成的证书循环依赖的死锁问题。例如，

| Client | Server |
|---|---|
| $p_{c1}: c1 \leftarrow s2 \wedge s3$ | $p_s: s \leftarrow (c1 \wedge c4) \vee c5$ |
| $p_{c2}: c2 \leftarrow s2$ | $p_{s2}: s2 \leftarrow c2$ |
| | $p_{s3}: s3 \leftarrow c4$ |

易知策略 $p_{c2}$，$p_{s2}$ 之间存在策略环。若按照这两个策略的要求进行证书披露，则可造成死锁。而经过对策略的分析与化简，对于服务 $S$ 的策略 $p_s$ 的最小证书集 $C_M=\{\{c_1,c_4\},\{c_5\},\{c_2,c_4\}\}$，如图 8 所示。这样在协商前，服务提供方就把请求方应满足的最小证书集发送给请求方，而请求方将自己

(下转第 175 页)

gions with Indeterminate Boundaries[C]// Proceeding of GISDATA Specialist Meeting on Geographic Objects with Indeterminate Boundaries. London: Taylor and Francis, 1996: 171-187

[3] Clementini E, DiFelice P. Approximate Topological Relations [J]. International Journal of Approximate Reasoning, 1997, 16 (2): 173-204

[4] 虞强源，刘大有，刘亚彬. 一种不确定区域的扩展蛋黄模型[J]. 电子学报，2004，32(4)：610-615

[5] Schockaert S, Cornelis C, Cock M D, et al. Fuzzy Spatial Relations Between Vague Regions[C]// 3rd IEEE Conference on Intelligent Systems. Berlin: Springer Verlag, 2006: 221-226

[6] Schockaert S, Cock M D, Cornelis C, et al. Fuzzy Region Connection Calculus: Representing Vague Topological Information[J]. International Journal of Approximate Reasoning, 2008, 48(1): 314-331

[7] 高振记，邬伦，杨俭. 基于RCC及粗糙模型的模糊地理对象拓扑关系表达[J]. 北京大学学报，2008，44(4)：597-603

[8] Egenhofer M, Clementini E, Felice P D. Topological Relations between Regions with Holes[J]. International Journal of Geographical Information Systems, 1994, 8(2): 129-144

[9] 邓敏，李志林，李光强. 简单面目标与带孔洞面目标间拓扑关系的层次表达方法[J]. 测绘学报，2008，37(3)：330-337

[10] Gau W L, Buehrer D J. Vague Sets[J]. IEEE Transactions on Systems, Man and Cybernetics(Part B), 1993, 23(2): 610 -614

[11] 刘一松，詹永照，孙亚民. 基于区域伸缩的空间关系表示[J]. 计算机科学，2008，35(4)：211-215

(上接第 157 页)

持有的证书与之匹配，若包含$\{c_1, c_4\} \subseteq C_C$ 或$\{c_5\} \subseteq C_C$ 或$\{c_2, c_4\} \subseteq C_C$ 成立，则协商成功。

```
Function: Match
Input: LTree T: 表示最小证书集的 ACP-LTree
       CC[n]: 服务请求方持有的证书集
Output: True/False
Descripton:
  Boolean Match(LTree T, CC[n])//依次遍历策略树中的每条根到
                                叶子的路径，若存在一条路径
                                使得其包含的策略都在请求方
                                所持有的策略集中，则返回
                                True，否则返回 False;
  {Boolean flag=False;//匹配成功的标志;
  L=T. firstchild;//从根结点的第一个孩子结点开始遍历;
  While( L! =NULL)//所有根到叶子的路径都遍历到，则循环结束;
  { for (int i=0;i<n;i++)//路径上每个结点都在请求方证书集里找一遍，找到则循环结束;
      { if (L. label! = CC[i]) flag=False;
    else { flag=True;
           break; } }
    if (flag= =True) L=L. child;
    else break;
  L=T. nextchild;//考虑下一条根到叶子的路径 }
return flag; }
```

图 8　证书策略匹配算法

**结束语**　ATN 的目标是在不同安全域中的陌生实体间建立信任，从而实现资源共享。而如何提高协商效率，增加协商成功率，以及保护敏感信息(策略和证书)，是 ATN 要解决的问题。本文针对访问控制策略可能造成协商失败的情况，提出了一种对访问控制策略进行逻辑分析的方法，判断策略的一致性，并且证明了此法的可靠性、完备性，避免在不一致的策略上进行协商造成的资源浪费；同时，本文根据对访问控制策略的化简，找到最小证书集，通过最小证书集的匹配，达成协商，避免协商死锁，提高协商效率与成功率。

## 参 考 文 献

[1] Blaze M, Feigenbaum J, Lacy J. Decentralized trust management [C]// Proc. of the 1996 IEEE Sypm. on Security and Privacy. Washington: IEEE Computer Society Press, 1996: 1664-173

[2] Li N H, Winsborough W H, Mitchell J C. Distributed credential chain discovery in trust management[C]// Herbert A S, ed. Proc. of the IEEE Symp. on Computing and Communications Security. New York: ACM Press, 2001: 156-165

[3] Li N H, Mitchell J C, Winsborough W H. Design of a role-based trust management framework[C]// Heather H, ed. Proc. of the IEEE Symp. on Security and Privacy. Washington: IEEE Computer Society Press, 2002: 114-130

[4] Winsborough W H, Seamons K E, Jones V E. Automation trust negotiation[C]// DARPA Information Survivability Conf. and Exposition. New York: IEEE Press, 2000: 88-102

[5] Yu T, Winslett M. A Unified Scheme for Resource Protection in Automated Trust Negotiation[C]// Proceedings of IEEE Symposium on Security and Privacy. 2003: 245-257

[6] 李建欣，怀进鹏，李先贤. 自动信任协商研究[J]. 软件学报，2006，17(1)：124-133

[7] Jin H, Liao Z, Zou D, et al. A New Approach to Hide Policy for Automated Trust Negotiation[C]// Proceeding of 1st International Workshop on Security. LNCS 4266, Springer-Verlag, 2006: 168-178

[8] Liao Zhensong, Jin Hai. A Logic Predicate Automated Trust Negotiation Model[C]// Proceedings of the 2nd International Conference on Communications and Networking in China (ChinaCom 2007). IEEE Press, Aug. 2007

[9] Zou Deqing, Liao Zhensong. A New Approach for Hiding Policy and Checking Policy Consistency [C] // Second International Conference on Information International Conference on Information Security and Assurance (ISA 2008). Busan, Korea: IEEE Computer Society, April 2008: 231-236

[10] Yu T, Winslett M, Seamons K E. Interoperable strategies in automated trust negotiation[C]// Proceedings of the 8th ACM Conference on Computer and Communications Security. ACM Press, 2001: 146-155

[11] Winsborough W H, Li N. Towards practical automated trust negotiation[C]// Proceedings of the 3rd International Workshop on Policies for Distributed Systems and Networks. 2002: 92-103