第43卷 第8期 西 安 交 通 大 学 学 报 Vol. 43 №8
2009年8月 JOURNAL OF XI′AN JIAOTONG UNIVERSITY Aug. 2009

面向属性约束的自动信任协商模型

官尚元，伍卫国，董小社，梅一多
（西安交通大学电子与信息工程学院，710049，西安）

摘要：针对已有自动信任协商系统策略语言粒度粗糙、不能生成所有信任序列且缺乏评估与择优机制等问题，提出一种面向属性约束的自动信任协商模型——ACATN. 其具有如下特点：利用属性约束细化策略语言粒度，不仅有效地保护了敏感服务和证书，而且提高了系统的灵活性；使用全局访问控制策略终止不会成功的协商请求，从而提高协商效率；采用信任序列搜索树描述信任序列的生成过程，基于此树的宽度、深度优先搜索算法在快速生成一个信任序列的同时，能够生成所有的信任序列；通过属性证书披露代价和通信开销评估信任序列，以便于系统选择最优信任序列. 结合具体实例对ACATN模型的使用进行了说明.

关键词：访问控制；自动信任协商；协商系统策略；属性约束
中图分类号：TP309 **文献标志码**：A **文章编号**：0253-987X(2009)08-0001-05

An Attribute-Constraints-Oriented Automated Trust Negotiation Model

GUAN Shangyuan, WU Weiguo, DONG Xiaoshe, MEI Yiduo
(Department of Computer Science and Technology, Xi′an Jiaotong University, Xi′an 710049, China)

Abstract: The existing automated trust negotiation systems suffer from the following drawbacks: the policy languages are coarse-grained, the negotiation strategy cannot generate all trust sequences, and the mechanism to evaluate and select trust sequences is absent. To address the above problems, an attribute-constraint-oriented automated trust negotiation (ACATN) model is proposed. The policy language is refined by using attribute constraint, which can not only effectively protect sensitive services and certificates, but also enhance its flexibility. The global access control policy is used to terminate impossible negotiation in advance so that the negotiation efficiency can be improved. The process of generating trust sequence is described by trust sequence searches tree. Based on the tree, the breadth-first and depth-first searches generate not only a trust sequence quickly, but also all trust sequences. Trust sequences are evaluated via disclosure cost and communication overhead so that the optimal one can be selected. ACATN is illustrated using a typical example.

Keywords: access control; automated trust negotiation; negotiation system strategy; attribute constraint

自动信任协商即是通过证书、访问控制策略的交互披露，使得资源请求方和提供方自动建立信任关系[1-3]. TrustBuilder[4-5]的访问控制策略采用“证书←证书”的形式，策略语言粒度粗糙，采用的算法也不能生成所有信任序列且缺乏评估和择优机制. Trust-χ[6]是一种适合P2P应用的ATN系统，其利用协商树来描述信任序列的生成过程并采用了宽度优先搜索算法，但缺乏信任序列的评估和择优机制. 为此，本文提出一种面向属性约束的自动信任协商模型——ACATN.

收稿日期：2009-03-10. 作者简介：官尚元(1979—)，男，博士生；伍卫国(联系人)，教授，博士生导师. 基金项目：国家自然科学基金资助项目(60773118)；国家高技术研究发展计划资助项目(2006AA01109).

1 ACATN模型

参与信任协商的双方实体可分为服务提供者和服务请求者. ACATN模型如图1所示,其中:证书库保存属性证书和身份证书等;策略库保存访问控制策略等;树管理器建立和维护信任序列搜索树;一致性检测器查找最小满足证书集,检测接收证书的有效性及该证书是否满足相关访问控制策略.

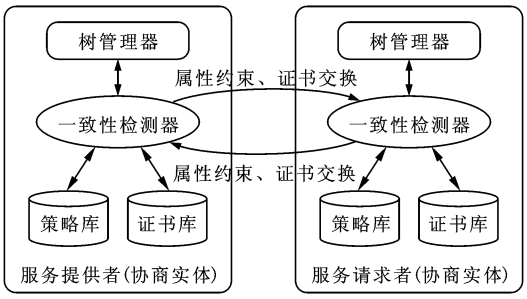


图1 ACATN模型

1.1 基本定义

为了解决策略语言粒度粗糙问题,ACATN引入属性约束细化策略语言粒度,即采用"证书|服务←属性约束"的形式描述访问控制策略.

定义1 属性约束为 $r(1*(\text{attr}\ [\text{op expr}]))$,其中attr为属性名,op为比较运算符(如=、≠、<、>等),expr为表达式或常量(类型必须与attr兼容).

在定义1中,$1*(\cdot)$表示()中的内容至少出现一次,$[\cdot]$表示其中的内容可以选择. 通过调整访问控制策略中的属性约束,证书持有者或服务提供者能够灵活地限定证书或服务的权限委托范围,从而有效地保护敏感证书和服务.

定义2 设属性证书集 $C=\{c_1,c_2,\cdots,c_k\}(k\in N)$满足属性约束 r,则称 C 是 r 的满足证书集,记为 C_r. $\forall C'\subset C$,C 满足 r 而 C' 不满足 r,则称 C 是 r 的最小满足证书集,记为 $C_{\min|r}$.

设有属性约束 r_1 和 r_2,如果 r_1 的所有最小证书集均满足 r_2,则称 r_2 包含 r_1,记为 $r_1\subseteq r_2$. 属性约束的最小满足证书集不惟一,不仅增加了协商成功的概率,而且为协商实体提供了保护其隐私的机会,故细化后的策略语言能够提高系统的灵活性.

定义3 设 $r_1,r_2,\cdots,r_n(n\geqslant 1)$为属性约束. 当且仅当 $r_i\subseteq r_j$ 或 $r_j\subseteq r_i(1\leqslant i,j\leqslant n$ 且 $i\neq j)$均不成立,$p_g(E\leftarrow r_1\vee r_2\vee\cdots\vee r_n)$是全局访问控制策略,简称为全局策略,其语义为:协商对方满足 $r_1,r_2,\cdots,r_n$ 中之一即可进入信任协商过程.

定义4 设 $r_1,r_2,\cdots,r_n(n\geqslant 1)$为属性约束. 当且仅当 $r_i\subseteq r_j$ 或 $r_j\subseteq r_i(1\leqslant i,j\leqslant n$ 且 $i\neq j)$均不成立,$p_k(c|S\leftarrow r_1\vee r_2\vee\cdots\vee r_n)$是局部访问控制策略,简称为局部策略. 其语义为:协商对方满足 $r_1,r_2,\cdots,r_n$ 中之一即可向对方披露证书 c 或提供服务 S.

可将访问控制策略分为全局策略和局部策略. 前者的作用与其他ATN系统的访问控制策略相同;后者根据协商对方的属性确定是否进入协商过程,且能够预先终止根本不会成功的协商请求,从而确保协商结果的有效性,提高协商效率.

定义5 设服务提供者的属性证书集为 C_{sp},访问控制策略集为 P_{sp};服务请求者的属性证书集为 C_{sr},访问控制策略集为 P_{sr}. C_{sp} 和 C_{sr} 幂集分别为 $P(C_{\text{sp}})$、$P(C_{\text{sr}})$. 证书集序列 $\langle C_i\rangle_{i\in[0,2n-1]}(n\in N)$是信任序列,但需满足下列条件.

(1)$((C_{2i}\in P(C_{\text{sr}}))\wedge(C_{2i}\neq\varnothing)\wedge(C_{2i+1}\in P(C_{\text{sp}}))\wedge(C_{2i+1}\neq\varnothing))$,$0\leqslant i<n$ 成立.

(2)如果 $\forall c\in C_{2i}$,则 $c\notin C_{2k}$;如果 $\forall c\in C_{2i+1}$,则 $c\notin C_{2k+1}$,$0\leqslant i<k<n$.

(3)如果 $c\in C_{2j}$,相应访问控制策略为 $p_c\in P_{\text{sr}}$,证书集 $C=\{c\mid c\in C_{2k+1},0\leqslant k<j<n\}$,则 C 满足 p_c;如果 $c\in C_{2j+1}$,相应访问控制策略为 $p_c\in P_{\text{sp}}$,证书集 $C=\{c|c\in C_{2k},0\leqslant k\leqslant j<n\}$,则 C 满足 p_c.

定义6 设属性证书为 c,披露代价为 $f(c)$,通信开销为 $g(c)$,则信任序列 $\Gamma=\langle C_i\rangle_{i\in[0,2n-1]}(n\in N)$的代价为

$$h(\Gamma)=\sum_{i=0}^{2n-1}\sum_{j=0}^{\text{Card}(C_i)}(\alpha f(c_j)+\beta g(c_j))$$

式中:$\text{Card}(C_i)$为集合 C_i 的势且 $c_j\in C_i$;α 和 $\beta(0\leqslant\alpha,\beta\leqslant 1)$是用户设定的比例因子,$\alpha+\beta=1$.

ACATN利用披露代价和通信开销来评估信任序列,以便于协商双方选择最优信任序列.

1.2 信任协商过程

协商过程如下:首先,协商双方检查对方是否满足本地全局策略,进而确定信任协商是否继续进行;其次,通过属性约束交换、生成信任序列;最后,协商双方根据信任序列规定的顺序发送并接收证书,接收方将验证证书的有效性并检查是否满足相关策略.

2 ACATN信任序列的生成

2.1 信任序列搜索树

ACATN利用信任序列搜索树来描述信任序列的生成过程. 信任序列搜索树由3类节点组成:证书节点、属性约束节点和最小满足证书集节点. 根节点

是特殊的证书节点,表示服务. 设 V_l 是信任序列搜索树中由叶子节点组成的集合,V_t 是终止节点组成的集合,终止节点指无须任何信息即可向协商对方披露节点中包含信息的节点,易知 $V_t \subseteq V_l$.

定义 7　设 $T(V,R)$是以 R 为根节点的树. $T(V,R)$是信任序列搜索树,但需满足下列条件.

(1)V 是树的节点集,每个节点可形式为 $v_{\mathrm{id}}(\sigma, l,t,s,o,p)$.

v_{id}是信任序列搜索树中节点的标识符.

σ 是节点 v_{id}所包含的属性证书、属性约束和最小满足证书集.

$l \in \{0,1,2,3,\cdots\}$是节点所在的层次,根节点为 0,其子节点为 1,孙子节点为 2,依次类推.

$t \in \{\mathrm{AND}, \mathrm{OR}\}$,其中类型 AND 表示与节点, OR表示或节点,其取值满足如下规则:当 $l \in \{k \mid (k=3n-3) \vee (k=3n-2), n \in N\}$时,$t=$OR(节点为或节点);当 $l \in \{k \mid k=3n-1, n \in N\}$时,$t=$AND(节点为与节点).

$s \in \{\mathrm{UNKN}, \mathrm{CLOS}, \mathrm{DISC}\}$,其中状态 UNKN 表示节点未知,CLOS 表示节点不可披露,DISC 表示节点可披露. 任何新建节点的状态均为 UNKN. 设节点为 v,其子节点集为 V_c.

如果节点 v 满足下列条件之一,则 $s_v=$DISC:①$v \in V_t$;②$t_v=$OR,存在 $v_c \in V_c$,有 $s_{v_c}=$DISC;③$t_v=$AND,任意 $v_c \in V_c$,有 $s_{v_c}=$DISC.

如果节点 v 满足下列条件之一,则其状态为 CLOS:①$v \in V_l$ 且 $v \notin V_t$;②$t_v=$OR,任意 $v_c \in V_c$,有 $s_{v_c}=$CLOS;③$t_v=$AND,存在 $v_c \in V_c$,有 $s_{v_c}=$CLOS.

$o \in \{\mathrm{PROV}, \mathrm{REQU}\}$,其中 PROV 表示节点信息保存在服务提供端,REQU 表示节点信息保存在服务请求端. o 取值满足下列规则:①$l \in \{k \mid (k=0) \vee (k=6n) \vee (k=6n-1) \vee (k=6n-2),\ n \in N\}$,$o=$PROV;②$l \in \{k \mid (k=6n-3) \vee (k=6n-4) \vee (k=6n-5),\ n \in N\}$,$o=$REQU.

p 表示父节点.

(2)$R=v_0(A,0,\mathrm{OR},\mathrm{UNKN},\mathrm{PROV},\mathrm{NULL})$是树的根节点.

信任序列搜索树中非叶子节点的状态完全由其子节点确定. 利用状态为 DISC 的节点确定先辈节点状态为 DISC 的过程称为可披露标记过程(USD);利用状态为 CLOS 的节点确定先辈节点状态为 CLOS 的过程称为不可披露标记过程(USC).

定义 8　设 $T(V,R)$为信任序列搜索树,V_l 为叶子节点集,$T(V_1,R_1)$为子树. $T(V_1,R_1)$是 $T(V,R)$的完备子树,即 $T(V_1,R_1) \preceq T(V,R)$,但需满足下列条件.

(1)$R_1=R$ 且 $V_1 \subseteq V$.

(2)任意 $v \in V_1$,如果 $t_v=$AND 且 $v \notin V_l$,则有 $\{v' \mid (v' \in V) \wedge (p_{v'}=v)\} \subseteq V_1$;如果 $t_v=$OR 且 $v \notin V_l$,则存在 $v' \in V_1$ 且 $p_{v'}=v$.

设 $T(V_1,R) \preceq T(V,R)$,如果 $V_1 \subset V$,则称 $T(V_1,R)$是 $T(V,R)$的完备真子树,即 $T(V_1,R) \prec T(V,R)$.

定义 9　设 $T(V,R)$为信任序列搜索树,$T_1(V_1,R)$是最小有效子树,但需满足下列条件.

(1)$T_1(V_1,R) \preceq T(V,R)$.

(2)$T_1(V_1,R)$的叶子节点均为终止节点,由叶子节点通过 USD 推出其余节点的状态均为 DISC.

(3)任意 $T_2(V_2,R)$,如果 $T_2(V_2,R) \prec T_1(V_1,R)$,则 $T_2(V_2,R)$不满足定义 9 的条件(2).

定义 10　设 $T(V,R)$为信任序列搜索树,$T_1(V_1,R)$是最大有效子树,但需满足下列条件.

(1)$T_1(V_1,R) \preceq T(V,R)$.

(2)$T_1(V_1,R)$的叶子节点均为终止节点,由叶子节点通过 USD 推出其余节点的状态均为 DISC.

(3)任意 $T_2(V_2,R)$,如果 $T_1(V_1,R) \prec T_2(V_2,R) \preceq T(V,R)$,则 $T_2(V_2,R)$不满足定义 10 的条件(2).

定理 1　给定信任序列搜索树,如果存在最小和最大有效子树,则有:①最小有效子树不惟一;②最大有效子树惟一.

证明　用举例法容易证明定理 1 中的①,故省略. 用反证法证明定理 1 中的②. 设 $T(V,R)$存在最大有效子树 $T_1(V_1,R)$和 $T_2(V_2,R)$且二者不同.

因 $T_1(V_1,R) \preceq T(V,R)$、$T_2(V_2,R) \preceq T(V,R)$,故二者能够合并为一棵树 $T(V^*,R)$且 $T(V^*,R) \preceq T(V,R)$. $T_1(V_1,R)$和 $T_2(V_2,R)$满足定义 10 中的条件(2),故 $T(V^*,R)$满足定义 10 中的条件(2). 假设 $T_1(V_1,R) \neq T_2(V_2,R)$,故 $T_1(V_1,R) \prec T(V^*,R)$或 $T_2(V_2,R) \prec T(V^*,R)$成立. 如果 $T_1(V_1,R) \prec T(V^*,R)$,则 $T(V^*,R) \preceq T(V,R)$,而 $T(V^*,R)$满足定义 10 中的条件(2),这与 $T_1(V_1,R)$是最大有效子树的定义相矛盾,故本假设不成立,即 $T_1(V_1,R)=T_2(V_2,R)$. 换言之,最大有效子树是惟一的.

定理 2　给定 $T(V,R)$,设其最小有效子树为 $T_1(V_1,R)$,最大有效子树为 $T_2(V_2,R)$,则有

$T_1(V_1,R)\leqslant T_2(V_2,R)$.

定理2的证明与定理1相似,故不再证明.

信任序列搜索树的有效子树可能是1个或多个信任序列,最小有效子树是一个信任序列,而最大有效子树包含所有信任序列.信任序列搜索算法的目的是,在信任序列搜索树中搜索出一个最小或最大有效子树,然后根据最小或最大有效子树生成1个或多个信任序列.ACATN的搜索算法包括宽度优先及深度优先.由定理1知,给定信任序列搜索树,采用宽度/深度优先搜索出的最大有效子树一定相同,而最小有效子树未必相同.因此,采用宽度优先还是深度优先搜索算法应根据实际情况而定.

由定理2知,给定信任序列搜索树,其最小有效子树一定是最大有效子树的完备子树,所以最大有效子树包含所有的最小有效子树.因此,通过搜索最大有效子树,能搜索出所有的最小有效子树,从而获取全部信任序列.

2.2 宽度优先搜索算法及信任序列生成算法

设信任序列 $\Gamma_1=\langle C_1,C_2,\cdots,C_k\rangle$ 和 $T_2=\langle D_1,D_2,\cdots,D_l\rangle$,$l\leqslant k$,$\Gamma_1+\Gamma_2=\langle C_1,C_2,\cdots,C_k,D_1,D_2,\cdots,D_l\rangle$,$\Gamma_1\bigcup\Gamma_2=\langle C_1\bigcup D_1,C_2\bigcup D_2,\cdots,C_l\bigcup D_l,C_{l+1},\cdots,C_k\rangle$,其中 $\Gamma_1|\Gamma_2$ 表示二者功能相同.

宽度优先搜索算法(算法1)如图2所示,它利用宽度优先的思想从信任序列搜索树中搜索最小有效子树或最大有效子树.信任序列生成过程(算法2)如图3所示,其根据最小或最大有效子树生成1个或多个信任序列.通过调用算法1和算法2,可以根据信任序列搜索树生成信任序列.

2.3 协商效率分析及搜索算法比较

定理3 假设信任协商过程涉及到协商双方的证书数 m、属性约束数 n,则ACATN的宽度/深度优先搜索算法的通信复杂度为 $O(mn)$.

证明 在信任序列生成阶段,ACATN主要包括3类消息:请求、满足和拒绝.根据强力回溯策略,每个属性约束最多发送2次请求属性约束的消息,且每次请求涉及的属性数不超过 n(每个属性约束的长度不会大于某个常数),此类消息的通信复杂度为 $O(mn)$;每个属性约束仅发送一次满足属性约束的消息,且消息包括属性约束的标识符(标识符长度不会大于某个常数),此类消息的通信复杂度为 $O(n)$;与满足消息相类似,拒绝消息的通信复杂度亦为 $O(n)$.

在属性证书交换阶段,消息数最多为 m,消息大小与证书大小有关(证书大小均不会大于某常数).因此,ACATN在证书交换阶段的通信复杂度为 $O(m)$.综上所述,ACATN的宽度/深度优先搜索算法的通信复杂度为 $O(mn)$.

定理3主要讨论了ACATN的宽度/深度优先搜索算法的通信复杂性,由于ACATN在用全局访问控制策略后能够提前终止不会成功的协商请求,从而提高了协商效率.

3 实例及分析

实例服务提供者的属性证书集为 $C_{sp}=\{d_1(4),d_2(3),d_3(5)\}$,括号内的值为证书的披露代价值,策略集为 $P_{sp}=\{p_g(E\leftarrow r_{\mathrm{I}}),p_1(S\leftarrow r_1\vee r_2\vee r_3),p_2(d_1\leftarrow r_8),p_3(d_2\leftarrow r_9),p_4(d_3\leftarrow r_3),p_5(d_4\leftarrow\varepsilon)\}$;服务请求者的属性证书集为 $C_{sr}=\{c_1(4),c_2(5),c_3(3),c_4(2),c_5(2)\}$,策略集为 $P_{sr}=\{p_g(E\leftarrow r_{\mathrm{II}}),p_1(c_1\leftarrow r_4\vee r_5),p_2(c_2\leftarrow r_6),p_3(c_3\leftarrow r_7),p_4(c_4\leftarrow\varepsilon),p_5(c_5\leftarrow\varepsilon)\}$.$r_{\mathrm{I}}$、$r_{\mathrm{II}}$、$r_1\sim r_9$ 的最小满足证书集惟一且分别为 $\{c_4\}$、$\{s_4\}$、$\{c_1,c_2\}$、$\{c_3\}$、$\{c_4\}$、$\{d_1\}$、$\{d_2,d_3\}$、$\{d_3\}$、$\{d_2\}$、$\{c_1\}$ 和 $\{c_5\}$,此外 $\alpha=\beta=0.5$.

输入 信任序列搜索树 $T(V,R)$
输出 如果搜索成功,返回TRUE,否则返回FALSE

步骤1 设队列 $Q_{\mathrm{Open}}=\varnothing$ 和 $Q_{\mathrm{Close}}=\varnothing$,变量 $\gamma\in\{\mathrm{TRUE,FALSE}\}$ 且 $\gamma=\mathrm{FALSE}$,把根节点 $v_0(A,0,\mathrm{OR,UNKN,PROV,NULL})$ 插入到 Q_{Open} 中.
步骤2 如果 $Q_{\mathrm{Open}}=\varnothing$,转步骤5,否则从 Q_{Open} 中取出一个节点插入 Q_{Close} 中,设取出节点为 v_i,$V_{ci}=\{v|(v\in V)\wedge(p_v=v_i)\}$.
步骤3 如果 $V_{ci}\neq\varnothing$,则:①扩展节点 v_i,根据定义7对子节点每一项赋值并将子节点插入到 Q_{Open} 中;②$V_{ci}\cap V_t\neq\varnothing$,$\forall v\in(V_{ci}\cap V_t)$,令 $s_v=\mathrm{DISC}$,然后调用USD标记 v_i 及其先辈节点的状态;③转步骤2.
步骤4 如果 $V_{ci}=\varnothing$,则:①如果 $v_i\in(V_l-V_t)$,$S_{v_i}=\mathrm{CLOS}$,然后调用USC标记 v_i 及其先辈节点的状态,如果 $S_{v_i}=\mathrm{CLOS}$,转步骤5,否则从 Q_{Open} 和 Q_{Close} 中删去本身或先辈状态为CLOS的节点;②转步骤2.
步骤5 如果 $S_{v_i}=\mathrm{DISC}$,则 $\gamma=\mathrm{TRUE}$,否则 $\gamma=\mathrm{FALSE}$,返回 γ.

图2 宽度优先搜索算法

输入 有效子树 $T(V,R)$
输出 信任序列

步骤1 $\Gamma=\varnothing$,$V_c\{v|(v\in V)\wedge(p_v=R)\}$.
步骤2 如果 $V_c=\varnothing$,则转步骤5.
步骤3 对任意 $v_i\in V_c(0\leqslant i<l,l=\mathrm{Card}(V_c))$,假设 v_i 是根节点子树 $T(V',v_i)$,则有 $\Gamma_i=\mathrm{TrustSeqGen}(T(V',v_i))$.
步骤4 如果 $t_R=\mathrm{OR}$,则 $\Gamma=\Gamma+\Gamma_1|\Gamma_2|\cdots|\Gamma_l$,否则 $\Gamma=\Gamma+\Gamma_1\cup\Gamma_2\cup\cdots\cup\Gamma_l$.
步骤5 如果 $l_R\in\{k|k=3(n-1),n\in N\}$,则 $\Gamma=\Gamma+\sigma_R$.
步骤6 返回.

图3 信任序列生成算法

首先，协商双方检查对方是否满足本地全局策略. 服务请求者发送属性证书 c_4 以满足服务提供者的全局策略 $p_g(E\leftarrow r_1)$；服务提供者向服务请求者发送 d_4 以满足其全局策略 $p_g(E\leftarrow r_{II})$. 通过全局策略检测后，协商双方已建立基本的信任关系，于是 ACATN 进入信任序列产生阶段.

其次，协商双方生成信任序列. 将协商双方的访问控制策略和属性证书转换成信任序列搜索树 T（见图 4a），调用算法 1 搜索出最大有效子树 T_M（见图 4b），然后调用算法 2 可生成$\langle\langle\{c_4,c_5\},\{d_2,d_3\},\{c_1,c_2\}\rangle|\langle\{c_5\},\{d_2\},\{c_3\}\rangle|\langle\{c_4\}\rangle,\{S\}\rangle$，进而得到下面 3 个信任序列

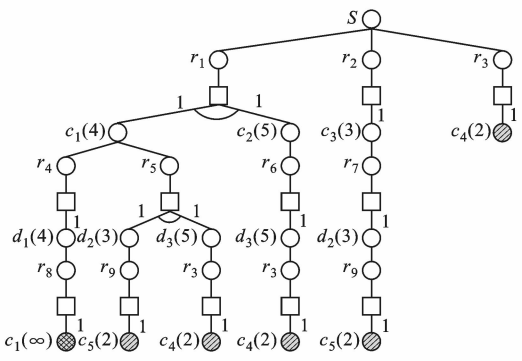
$$\Gamma_1=\langle\{c_4,c_5\},\{d_2,d_3\},\{c_1,c_2\},\{S\}\rangle$$

$$\Gamma_2=\langle\{c_5\},\{d_2\},\{c_3\},\{S\}\rangle$$

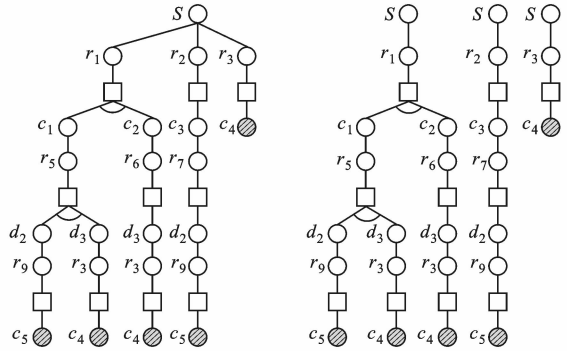
$$\Gamma_3=\langle\{c_4\},\{S\}\rangle$$

最后，协商双方选择信任序列代价（$h(\Gamma_1)=13.5$、$h(\Gamma_2)=5.5$、$h(\Gamma_3)=1.5$）中的一个进行证书交换. 如果采用宽度/深度优先搜索算法搜索最小有效子树，前者搜索出最小有效子树 T_3（见图 4c），后者搜索出最小有效子树 T_1（见图 4c），然后调用算法 2 生成 1 个信任序列.

综上所述，宽度/深度优先搜索算法不仅能快速搜索出最小有效子树（T_1、T_2 或 T_3），而且能搜索出最大有效子树（T_M）. 当生成多个信任序列时，可选择信任序列代价中的一个最优序列进行证书交换，这样不仅能够减小传输和认证开销，而且可以保护协商双方的隐私信息.



(a)信任序列搜索树 T



(b)最大有效子树 T_M　(c)最小有效子树 T_1、T_2 和 T_3

括号中的数值表示披露代价值；未标注的代价为 0

图 4　信任序列搜索树和最大或最小有效子树

4　结束语

本文提出一种面向属性约束的自动信任协商模型——ACATN，其特点是：①引入了属性约束细化策略语言粒度，有效地保护了敏感服务和证书，增加了协商机制的灵活性；②使用全局策略终止不会成功的协商请求，确保协商结果的有效性；③利用信任序列搜索树描述了信任序列生成的过程，基于此树给出了宽度/深度优先搜索算法；④定义了信任序列的代价，以便于选择最优序列. 在未来的工作中将实现 ACATN 并应用于真实的网格环境.

参考文献：

[1] SKOGSRUD H, MOTAHARI-NEZHAD H R, BENATALLAH B, et al. Modeling trust negotiation for web services [J]. Computer, 2009, 42(2): 54-61.

[2] 陈书义，孙锦山，赵宏，等. NSIS 下通用访问控制信令协议的设计与验证 [J]. 西安交通大学学报，2009，43(4)：34-38.
CHEN Shuyi, SUN Jinshan, ZHAO Hong, et al. Design and validation of universal access control signaling protocol based on next steps in signaling [J]. Journal of Xi'an Jiaotong University, 2009, 43(4): 34-38.

[3] WINSBOROUGH W H, SEAMONS K E, JONES V E. Automated trust negotiation [C]// DARPA Information Survivability Conference and Exposition. Los Alamitos, CA, USA: IEEE Computer Society, 2000: 88-10.

[4] YU Ting, WINSLETT M, SEAMONS K E. Supporting structured credentials and sensitive policies through interoperable strategies for automated trust negotiation [J]. ACM Trans on Information and System Security, 2003, 6(1): 1-42.

[5] YU Ting, MA Xiaosong, WINSLETT M. PRUNES: an efficient and complete strategy for automated trust negotiation over the internet [C]// ACM Conference on Computer and Communications Security. New York, USA: ACM, 2000: 210-219.

[6] BERTINO E, FERRARI E, SQUICCIARINI A C. Trust-χ: a peer-to-peer framework for trust establishment [J]. IEEE Trans on Knowledge and Data Engineering, 2004, 16(7): 827-841.

（编辑　苗凌　赵大良）