第38卷第11期
2010年11月

同济大学学报(自然科学版)
JOURNAL OF TONGJI UNIVERSITY(NATURAL SCIENCE)

Vol.38 No.11
Nov. 2010

文章编号：0253-374X(2010)11-1682-07

DOI:10.3969/j.issn.0253-374x.2010.11.023

基于动态阈值的陌生网络实体间信任建立方法

鲍　宇[1,2]，曾国荪[1]，陈　波[1]，夏冬梅[1]

(1.同济大学 计算机科学及技术系，上海 201804；2.中国矿业大学 计算机学院，江苏 徐州 221116)

摘要：不完全信息的自动信任协商中存在如披露最少证书获得对方最大信任、协商效率等优化问题.利用博弈分析信任协商过程中的协商方的收益，给出权衡资源比重方法，量化了信任协商的计算过程，提出基于动态阈值的信任协商建立方法.动态阈值具有随证书披露与信息完整而进行自主变化的能力，可以减少协商过程的隐私披露.样例分析和仿真试验表明：使用动态阈值方法可以限制证书披露的数量，提高不完全信息下信任建立的效率.

关键词：信任协商；协商策略；信任建立；动态阈值

中图分类号：TP 393　　**文献标识码**：A

Dynamic Threshold Method of Establishing Trust in Open Environment

BAO Yu[1,2]，*ZENG Guosun*[1]，*CHEN Bo*[1]，*XIA Dongmei*[1]

(1. Department of Computer Science and Technology, Tongji University, Shanghai 201804, China; 2. Department of Computer Science and Technology, China University of Mining & Technology, Xuzhou 221116, China)

Abstract: In incomplete information environment, there are many optimization problems in the process of automated trust negotiation (ATN) based on exchanging digital credentials, like how to disclose minimum credentials and obtain maximum authorized, negotiation optimization, et al. Based on an analysis of the ATN process by game theory, a quantitative approach of trust is proposed to compute trust value of each credential in the ATN process a trust negotiation system is established on the basis of the dynamic strategy. The dynamic-threshold, fluctuating with the negotiation process, is proposed for further optimization to reduce credentials disclosure. The case analysis and simulations show that the dynamic-threshold strategy can restrict the amount of disclosed credentials and improve efficiency of the negotiation process in the incomplete information environment.

Key words: automated trust negotiation; trust negotiation strategy; trust establishment; dynamic-threshold

开放网络环境下，自动信任协商(automated trust negotiation，ATN)机制适合处理请求用户和网络服务处在不同安全域时的信任问题，包括披露各自的访问控制策略、证书的交换、协商消息传递、隐私保护等内容[1-3].其特点体现在：①陌生者实体之间信任关系通过属性证书交换进行确立；②协商双方都可定义访问控制策略，以规范对方对其资源的访问；③不需要可信第三方的参与[1].

在基于属性证书信任协商中，协商焦点是控制访问某种资源，策略通过访问控制来具体实现.William[4]针对协商策略提出了热心协商策略和吝啬协商策略，热心协商策略具有较高的效率，而吝啬协商策略的隐私保护较为出色.Yu等[3]认为，在信任协商中访问控制保护的资源不仅仅包括用户最终访问的需求资源，还应当包含证书本身.Bonatti[5]提出利用原语谓词过滤来约减访问控制策略，提高协商效率.Nicola[6]设计了迹算子和匹配算子，通过处理条件和接受条件的限制，提出了ATN中的容错机制，并设计了具有容错功能的协商Agent.Hristo[7]通过支持策略分级、溯因推理、细粒度的访问控制，提供了一个自引导的协商框架.Chen[8]讨论了披露最小证书问题.田立勤等[9]利用贝叶斯网络对用户的行为信任进行预测，试图使用博弈论建立信任.PRUNES[10]和TrustBuilder[11]信任系统使用谨慎协商策略试图综合热心和吝啬协商策略的优点.Trust

收稿日期：2009-10-10

基金项目：国家“八六三”高技术研究发展计划资助项目(2007AA01Z425，2009AA012201)；国家“九七三”重点基础研究发展规划资助项目(2007CB316502)；国家自然科学基金资助项目(90718015)；NSFC-微软亚洲研究院联合资助(60970155)；教育部高等学校博士学科点专项科研基金资助项目(20090072110035)；上海优秀学科带头人计划资助项目(10XD1404400)；高效能服务器和存储技术国家重点实验室开放基金(2009HSSA06)；中央高校基本科研业务费专项资金资助项目(2008A039，2009A052)

作者简介：鲍　宇(1977—)，男，博士生，主要研究方向为信息安全与模型检测.E-mail:baoyucumt@126.com

曾国荪(1964—)，男，教授，博士生导师，工学博士，主要研究方向为网格计算与信息安全.E-mail:gszeng@tongji.edu.cn

－X[12]协商策略使用了信任票和信任记忆，使得协商的效率得到提高.这些研究表明：一个合理的信任协商是在隐私保护的基础上进行信任建立，并综合考虑协商效率、容错等多个要求.但这些策略缺乏体现协商过程前期和后期的信任不同的特征，而这一点可使协商效率得到加强.本文考虑了协商交换证书的隐私性和敏感性，通过分析协商过程的信任动态变化情况，引入动态阈值以适应此动态过程，提出陌生网络实体间建立信任的一种机制和方法.

1　陌生网络实体间的信任协商要求

1.1　信任协商的过程

信任协商是交换证书、选择合适策略、获取访问授权的一种不完全信息博弈过程[9].通常协商策略有[8]：谨慎协商策略(prudent strategies)，热心协商策略(eager strategies)，阈值协商策略(threshold strategies).(协商策略表示用 Strategy；访问控制策略用 Policy，简称策略，下文同.)协商过程中，可根据信任的水平分为 3 个阶段，如图 1 所示.协商方 A 和 B 在协商开始之后，是陌生的网络实体，没有对方相关的信息，处于不信任状态.A，B 首先采取谨慎协商策略.然后通过证书交换，协商方 A 和 B 之间逐步建立了信任关系(阶段 2).在对方有一定的信任之后，则可采用改善协商效率的热心协商策略.在阶段 3，协商成功后，信任成功建立，策略和证书的敏感度降低，协商策略应当进一步改进，为下一次协商的优化策略做准备，提高后续协商的效率.

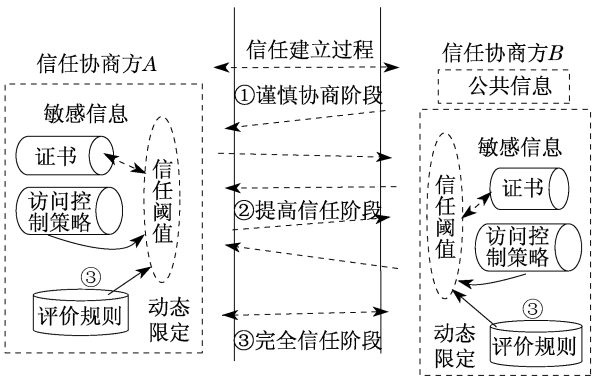

图 1　自动信任协商中信任变化的不同阶段

Fig.1　Trust changing in different phrases of ATN

为了表述方便，记 A 为协商请求方，B 为协商响应方，访问控制策略为 P，获取的效益为 V，请求资源 R 为 $Q(R)$，释放自己的策略/证书为 $U(P_A/C_A)$，并将其披露给对方为 $D(P_A/C_A)$，A 对 B 的信任为 $T_A(B)$.B 授权给 A，记 $G_B(A,R)$.下面进一步给出相关概念.

定义 1　信任协商的参与者：是一个 5 元组，即 $M_N=(N,A,C,R,P)$.其中 N 是信任协商参与者公共标识名集合；A 是属性有限集，该属性集合包含参与者所承认的属性，是协商双方都认可的属性的集合；C 是证书有限集，该集合包含参与者所有承认和接受的合法证书，是协商双方都认可的证书集合，记 C_A 为参与者 A 拥有的证书集；R 是参与者所拥有的资源可数集，$R_A\in R$ 表示参与者 A 拥有一个资源 R_A；P 是参与者的访问控制策略集，解释为关于 A 定义的逻辑公式描述，即这些公式的解释称为策略.

设 $p\in P$ 为其中一个策略，若 C 满足 p，记为 $C\vdash p$.文中策略的描述采用文献[3,8]中形式，策略表示如 $p_c:y\leftarrow\Phi(C_1,C_2,\cdots)$ 的形式.前缀 y 可以是资源、策略或证书，后缀 Φ 是 $2^C\rightarrow y$ 的映射，$C_i\in C$ 表示要求对方提供的证书.

定义 2　协商消息序列：假设在没有重复发送消息的一次协商过程中，由协商双方交替向对方发送每一个消息为 μ_i，则协商消息序列定义为 $\mu=\langle\mu_0,\mu_1,\mu_2,\cdots,\mu_n\rangle$.

在协商交换过程中，假设没有重复发送的消息，μ_k 为双方交替发送所产生的消息序列，则当 $k\in\{2i\mid i=0,1,\cdots,n\}$ 时为请求方消息，μ_0 为请求信息，即 $\mu_0=Q_A(R_B)$.协商结束时，消息 μ_n 应为服务方授权 $G_B(A,R)$，或者拒绝服务 $Z_B(A,R)$.如消息 μ_i 中包含证书 C_i，记为 $C_i\in\mu_i$.从消息 μ_i 中抽取包含的属性证书，使用函数 $M(\mu_i)\rightarrow 2^C$.另外，当接收到的消息没有新的内容，即 $\mu_i=\varnothing$ 或 $\mu_i=\mu_{i-2}$ 时，称之为空消息.空消息可以作为协商是否继续进行的标志，记为 msg Ø.

定义 3　证书可满足[8]：设自动信任协商中服务方 B 拥有 C_B，P_B，请求方 A 证书集和策略集分别为 C_A 和 P_A，设协商产生的消息序列为 μ.记 $g(\Phi)$ 为证书可满足函数，如果 $\Phi(C_A\cap(\bigcup\limits_{1\leqslant j<i}M(\mu_j))$ 相对应的策略 $p_B\in P_B$ 可满足，即 $C_A\cap(\bigcup\limits_{1\leqslant j<i}M(\mu_j))\vdash p_B$ 则 $g(\Phi)=1$，否则 $g(\Phi)=0$.

1.2　信任协商的优化问题

为保护敏感信息，通常需要加入信息访问控制策略[13]，它们也是访问控制策略.通过信息敏感度的评价，可以对敏感信息分级，决定披露的顺序.记证书 c_i 上的敏感评价为 $K(c_i)=X_i$，$X_i\rightarrow[0,1]$ 为

评价值.例,设有策略 $p_c: C_1 \leftarrow T.K(C_1)=0$ 表明证书 C_1 的敏感度为0,任何陌生人都可以访问.由于策略的表达通常为析取范式.协商策略的选择可被描述为一个披露敏感信息最小的MSC(minimum sensitivity cost)问题[8],这是一个Non-polynomial(NP)完全问题.

定义4 单方MSC问题:在信任协商中,假设用户 d 属于协商参与者集合 N,并拥有证书集 C_d 和策略集 P_d,对于每一个证书或策略 $c_i \in C_d \cup P_d$ 有 $K(c_i)=X_i$,μ 为消息序列,则信任协商结束时,d 为获得资源 R 必须披露的证书集合 $\{c \mid c \in M(\mu)\}$ 所对应的 $\sum X_i$ 最小化问题,称为单方MSC问题.单方MSC问题可表示如下:

$$\min f(\mu, C_d) = \sum_{i=1}^{n} K(C_d \cap M(\mu_i)),\ d \in N \tag{1}$$

定义5 协商信任度评估:信任协商过程中,协商方 A 拥有证书集 C_A 和策略集 P_A,B 对 A 所披露的属性证书、策略以及协商行为等所作出的评估,用以判断 A 的可信程度,称为 B 对 A 的信任度评估.记作 $T_B(A)$,下标 B 表示信任主体,参数 A 表示信任客体.

如果考虑到协商策略的效率问题,则信任协商过程可描述为一个披露证书和可信问题的综合优化问题:假设在信任协商中,用户 d 属于协商参与者集合 N,且拥有证书集 C_d 和策略集 P_d,对于每一个证书或策略 $c_i \in C_d \cup P_d$ 有 $K(c_i)=X_i$,μ 为消息序列,则信任协商结束时,满足

$$\max\{T(d), \min\{(|\mu|), f(\mu, C_d)\}\},\ d \in N \tag{2}$$

式中:$|\mu|$ 表示消息序列的长度;$\min(|\mu|)$ 表示协商步数最少;$T(d)$ 需要数值化,将在后面讨论.

命题1 在信任协商中,假设 d 属于协商参与者集合 N,且拥有证书集 C_d 和策略集 P_d,对于每一个证书或策略 $c_i \in C_d \cup P_d$ 有 $K(c_i)=X_i$,μ 为消息序列,协商过程生成的策略树为Tree,则在不完全信息情况下信任协商结束时,d 为获得对方信任,必须披露的证书集合 $\{c \mid c \in M(\mu)\}$ 所对应的 $\sum X_i$ 最小化问题是一个NP完全问题.(证明略)

命题2 基于敏感度的不完全信息的信任协商综合优化问题是一个NP完全问题.(证明略)

2 动态信任协商量化机制

2.1 信任协商动态阈值

在协商过程中,阈值是用以控制证书披露的门槛,阈值的引入试图结合热心协商策略和谨慎协商策略的优点,采用的是一种介于谨慎协商策略和热心协商策略中的披露方法.

定义6 信任协商阈值:记信任协商证书 c_i 的敏感信息评价 $K(c_i)=X_i$,$X_i \in [0,1]$,给定 $\varphi_0 \in [0,1]$,在披露证书时规定 $X_i \leqslant \psi_0$,称 ψ_0 为信任协商的阈值.阈值协商策略便是使用固定值 ψ_0 的信任协商策略.

定义7 信任支付:设信任协商参与者 d 的证书 c_i 的敏感信息评价 $K(c_i)=X_i$,d 披露证书 c_i 的敏感信息损失为 X_i,称敏感信息损失为信任支付,记为 $O(c_i)=X_i$.d 在信任协商过程中协商方总的信任支付为 $O(C_d)=\sum X_i$,$c_i \in C_d$.

定义8 信任协商二元效益:设信任协商参与者集合为 $N=\{d, d_{opp}\}$,d 在信任协商中的收益表示为二元效益,记为一个二元组 $V_d=(O,T)$,其中 O 表示协商方 d 的信任支付 $O(C_d)$;T 表示 d 对其对手 d_{opp} 的信任 $T_d(d_{opp})$.

使用 V 作为信任协商中的信任阈值.协商发送第 k 个消息时,称协商进行到 k 步.V 将协商方的不同特征的收益分离出来,包含了不同策略的不同方面的效益.用函数 f 表示计算 V 的函数.变量 p,t 分别表示特征向量的相应分量的变量.

定义9 信任二元效益函数:设 V 是信任协商二元效益,f 是 V 的效益计算函数,则 f 定义为:$f(V)=(u(p), u(t))$.其中 $u(p)$ 是将要披露的证书和策略的敏感度的叠加,$u(t)$ 是对方所披露的消息对信任对方程度的提升.

动态阈值采用信任的二元效益函数,体现了协商交互过程中信任不断加深的过程.协商的阈值在每一次信息交换之后,由于证书和策略披露,将引起阈值的变化.

2.2 敏感信息的量化计算

本文给出一个权重评价方法,其主要思想是依据信任协商过程中所生成的策略树.假设策略树满足[3]:根节点是协商的最终资源 R,除了根节点的节点分别表示一个属性证书(使用证书名称作为节点的名称),每个节点的子节点表示披露该节点上的证书所需要的条件.策略树上证书满足 $C_i > C_j$,即 C_j 是 C_i 的后继,则 C_j 在 C_i 之前披露.相同层次的节点能够同时披露.l 表示树的层次,第 l 层节点所代表的证书协商为 $l-1$ 层披露所必需的,代表协商参与者在该步骤时的策略选择.

记信任协商生成策略树的深度为 N_p,树的层次为 l,第 l 层节点集为 C_l,策略树的任一节点为 C_i 处于 l_i 层,C_i 第 k 个子树 sub $T_{i,k}$ 节点数目为 $|\text{sub } T_{i,k}|$,根据权重均等规则,第 l 层节点属性证书权重计算公式如下:

$$K(C_i) = \sum_{j=1}^{|l_i|} \sum_{k=1}^{|\text{sub } T_{i,j}|} K(C_k) + K(C_i) \quad (3)$$

满足 $\sum_{k=1}^{|\text{sub } T_{i,m}|} K(C_k) = \sum_{k=1}^{|\text{sub } T_{i,j}|} K(C_k)$,若 $C_m \in C_l, C_j \in C_l$,则

$$K(C_i) = \sum_{j=1}^{|l_i|} \sum_{k=1}^{|\text{sub } T_{i,j}|} K(C_k),\ 0 < l < N_p$$

公式(3)用于属性权重的建立,是一个递归的计算公式.

2.3　信任阈值的量化计算

在协商策略描述中,$\Phi(C_1, C_2, \cdots)$可以转换为析取范式公式[3],子项是合取形式,其选择导致协商收益不同.假设服务方所披露的策略 p_i 后缀中包含 N_s 个子项,请求方所选择的子项中包含要求披露的 j 个证书,其中请求方 $K(C_i) = X_i$,则该子项的敏感度效应为各项和:$u(p)_{c_i} = \sum_j X_i$.当披露 C_i 时,相对应的策略为 $p_{c_i}: C_i \leftarrow \Phi(C_k)$,策略敏感度为 Y_i,则请求方的敏感度支付为

$$u(p)_{c_i \cup p_i} = \sum_j X_i + \sum_j Y_i$$

则在协商过程中协商方 d 的敏感度支付为

$$u(p)_d = \sum_{|\mu|/2} u(p)_{c_i \cup p_i},\ d \in N \quad (4)$$

$u(t)$是可观行为的评估,评估函数的好坏决定了是否符合客观事实.计算不仅包含对方提供的证书本身支持的信任,还包括交互过程中索要对方的证书已经满足的比例,以及对方交换证书时行为是否符合规范,可通过消息格式、$g(c)$和非空新消息等来判断.

定义 10　消息可用性:当消息 μ_n 从信任协商方发送到接收方之后,消息 μ_n 可以被协商方正确解析,并引发消息 μ_{n+1},称消息 μ_n 为可用的,记 $H_\mu(\mu) = 1$,否则 $H_\mu(\mu) = -1$.

用函数 $h(C_i)$表示证书 C_i 本身提供的信任程度,C_{dis}表示对方已经披露的证书集,C_{need}表示需要对方披露的证书集,$g(C_i)$表示证书 C_i 可满足集,则未披露证书集为 $C_{\text{und}} = C_{\text{need}} - C_{\text{dis}}$,$g(C_i)/|C_{\text{need}}|$表示证书满足的比例,令 $|C_{\text{need}}| = m$.使用函数 H_{act} 表示行为信任评测函数,则

$$H_{i,\text{act}} = \sum_i g(C_i)/m + \sum_i H_\mu(\mu_i)/|\mu| \quad (5)$$

另外,协商提供 k 次消息容错,错误发生时,$H_\mu(\mu_i) < 0$,则式(5)修正为

$$H_{i,\text{act}} = \sum_i g(C_i)/m + \sum_i \max\{H_\mu(\mu_i), \min\{\max\{(e-k),0\},1\} \cdot H_\mu(\mu_i)\}/|\mu| \quad (6)$$

计算 $h(C_i)$时涉及两个方面,分别使用 $h_1(C_i)$和 $h_2(C_i)$表示,即信任评价公式:$h(C_i) = \omega_4 h_1(C_i) + \omega_5 h_2(C_i)$.

综合上述参数,引入权重对其量纲一化处理,可得

$$u(t) = \sum_i^{|\mu|} (\omega_1 h(C_i) + \omega_2 g(C_i)/|C_{\text{need}}| + \omega_3 H_{i,\text{act}}) = \omega_1 \sum_i^m h(C_i) + \omega_2 g(C_{\text{dis}})/|C_{\text{need}}| + \omega_3 H_{\text{act}}$$

其中$\sum \omega_i = 1$.　(7)

在确定 ω 时,需要保证 $\omega_3 < \omega_2 < \omega_1$,因为证书的披露是其中权重最大的.$\omega_3 = 0$ 时,所有形如 $p_c: r \leftarrow T$ 的策略将不受保护,可以直接披露.

3　基于动态阈值的信任协商建立方法

3.1　动态阈值协商策略描述

信任协商策略要求:①能够发现存在的解决方案,②能够成功终止,③在敏感度存在情况下,找到综合优化问题的最优解,④有一个高效的诱导机制,使协商迅速成功.

要求③是一个 NP 完全问题.为此,利用空消息使协商终止,当协商方不再接收到新消息时,则认为对方不能提供一个有效的策略使协商进行下去,协商终止.其次,尽管一次寻找确定的综合优化问题最优解和诱导机制是不可能的,但通过设定一个有效的阈值,可以部分满足要求③和④.

定义 11　占优选择:在信任协商中,如果协商方 A 选择策略 p 的析取范式子项 δ 获得效益 V_A,和在同等条件下,协商方选择任意 $\delta'(\delta' \neq \delta)$所获得效益 V'_A,满足 $V_A \geqslant V'_A$,即 $u(p) \geqslant u(p')$,$u(t) \geqslant u(t')$,则称子项 δ 为协商策略 p 的占优选择,记 $\Delta(p) = \delta$.

协商过程中的状态包含协商参与者,双方使用的证书集 C,协商涉及的资源集合 R,以及控制协商过程的阈值,从而根据协商的状态可以定义如下的协商策略模型.

定义 12 协商策略模型:是一个 8 元组 $M_S=(S,M,v,\rightarrow_v,\rho,S_0,S_q,\pi)$. 其中:$S$ 为可数状态集,$s\in S$ 表示其中的一个状态;M 为可数消息集;μ_i 表示其中的第 i 个消息;v 为阈值协商策略中当前参与者的阈值,$v\in[0,1]$;$\rightarrow_v$ 为 $M\times S\rightarrow M\times S$ 状态行为函数,由消息激发从一个状态到下一个状态,当某个状态接收到消息后,在阈值 v 作用下向另一个状态转化,并产生应答消息;ρ 为标记映射函数,定义状态到标记集合的映射;S_0 为初始状态集;S_q 为终止状态集;π 为阈值功能函数,用于计算和控制 $\rightarrow_v$ 中的阈值,在固定阈值是常数函数.

可以描述信任协商的动态阈值协商策略为:

算法:信任协商的动态阈值协商策略

输入:信任协商策略;输出:协商授权

```
S:C×C×R×v×P   ρ:S→2^(C∪R∪v∪P)
M:P×C   v:v=V∈[0,1]
ρ:F(V)
S0:if(player} = client){          //初始化
    μ0 = msg Ø
    S0←〈Ø,Ø,null,0,Q(R)〉          //R∈R
    oppCunlock = Ø
  }else(player} = server){
    μ1 = msg(pR,null)
    If(pR is satisfied) { S0←〈Ø,Ø,R,0,G(R)〉,
        S→Succ.}
    else {S0←〈Ø,Ø,R,0,pR)〉,oppCunlock = Ø}
  }
Sq:{Fail,Succ}
→v: if (msg Ø & oppCunlock = Ø & errortimes > errTolerance){S→Fail}   //判断容错次数
    if(msg Ø & oppCunlock = Ø)μi+1 = μi-2,v = F(V)
  //计算阈值
    else{
      if(μi = msg(deadlock))μi+1 = msg(Δ(pold/δold)with v,null).   //防止死锁
      if(ExitDeadlock(Δ(p) selected by opponent
          player)) {
        μi+1 = msg(deadlock,null),v = F(V)}
      else{
        Cdis = μi.C∪Cdis,Cund = Cund/μi.C
        if(μi.C satisfied pR & R≠Ø)S→Succ
        v = F(V)
        if(v.u(t)<errorThreshold)S→Fail
        recreat oppCunlock,oppCundis according to μi.C & P
        for each Ci in oppCunlock
          if(K(Ci)<v.u(t) & Ci∉oppCundis)
            {oppCdis = Ci∪oppCdis}
          if (oppCdis = Ø & oppCundis≠Ø) oppCdis =
            Min(K(Ci))
        oppCundis = oppCundis/oppCdis
        pnew is combined with all K(p)<v.u(t) &
            p is needed by μi.P
        μi+1 = msg(Δ(pnew) with v,oppCdis)
      }
      return μi+1
  }
```

上述算法描述中,msg Ø 表示空消息,ExitDeadlock 函数用于判断对方所选择的策略子项是否在策略选择的路径上存在死锁,opp C_{unlock} 是已经满足 Unlock 条件的 C_i,opp C_{undis} 是已经 Unlock 但没有向对方披露(Disclose)的证书集,opp C_{dis} 所生成的证书集合是将向对手披露的证书集.

根据命题 2,动态阈值协商算法最优化过程是一个非多项式算法,最好情况是出现热心协商策略的情况,最差情况时间复杂度将变成谨慎协商策略的策略证书的查找是有序队列查找,时间复杂度为 $O(\lg N)$,$N=|C_{dis}|$. 策略树的生成与策略、证书的传输息息相关. 在算法最好的情况下,时间复杂度为 $O(1)$;在最坏的情况下,需要判断死锁,时间复杂度为 $O(N^2)$,其中 $N=|C_{dis}|,|P_{dis}|=|C_{dis}|$.

3.2 信任协商策略安全性

定义 13 证书披露安全:对于一个信任协商策略 p,如果满足:① $\forall C_i, U(C_i)\geqslant D(C_i)$,即证书的披露之前 p_{C_i} 总是被满足的;② $\forall C_i$,无论何时披露,所涉及的证书披露策略 p_{C_i} 都可以被满足;③使用该协商策略协商的两个协商方所发起的协商都是证书披露安全的. 则称该协商策略是证书披露安全的.

命题 3 基于策略树和敏感信息评价的动态阈值协商策略是满足证书披露安全的.

证明 证明③只要证明①和②对协商策略中涉及的任意策略和任意证书都成立即可. 先证②,对于②中 player 的对手披露的任意 C_i,将被保存在本次协商使用的公共集合 C_{dis} 中,判断任意 p 是否满足,可依据 C_{dis} 集合中存放的证书,所以任意 C_i 只需要披露一次. 而协商方向对手披露的任意 C_i 将被保存在 opp C_{undis} 集合中,opp C_{undis} 集合将存放所有对手满足的证书,已经向对手披露的 C_i 将从 opp C_{undis} 集

合中删除,从而保证 C_i 只需要披露一次,由此说明②得证.另外,μ_i 中证书所满足后 Unlock 的任意 C_i 将存放在 opp C_{unlock} 中,v 的作用是限制证书披露的数量.C_i 只有被满足后才能存放 opp C_{unlock} 中,才能够披露.所以 C_i 满足 $U(C_i) \geqslant D(C_i)$.证毕.

证书披露安全并不能保证协商策略的安全.例如通过对方是否持有某一个证书推断持有者的属性,这些安全性将在后期的工作进行研究.

4　样例分析

4.1　样例研究

通过一个电子支付平台购书服务的实例,分析信任动态阈值协商策略在不完全信息信任协商过程中的应用.使用式(5)作为信任评价函数 $h(C_i)$.假设一个客户和一个售书商,双方的证书和策略的敏感度评测如表 1,2 所示.

表 1　客户与售书商的证书集的符号表

Tab.1　The token of client and server

客户证书名称	符号	售书商证书名称	符号
校园卡电子支付证书	C_1	第三方担保电子证书	S_1
淘宝网支付宝支付证书	C_2	网店实名证书	S_2
客户电子信用证书	C_3	电子营业执照证书	S_3
客户电子身份证书	C_4	图书正版验证证书	S_4
客户购物网络用户证书	C_5	售书商电子信用证书	S_5
学生证(学校电子证书)	C_6	售书商购物网络用户证书	S_6
eBay 国际信用支付证书	C_7	客户预买的电子书	R

表 2　客户和售书商的策略及其敏感度

Tab.2　The policies and sensitivity of client and serve

客户			售书商		
策略	X_i	Y_i	策略	X_i	Y_i
$C_1 \leftarrow S_1$	0.2	0.2	$R \leftarrow (C_1 \wedge C_4) \vee C_2 \vee C_7$	0.5	0
$C_2 \leftarrow S_3 \vee S_4$	0.7	0	$S_1 \leftarrow C_2 \vee (C_5 \wedge C_6)$	0.3	0.1
$C_3 \leftarrow S_2 \vee S_5$	0.2	0.1	$S_2 \leftarrow C_3$	0.2	0.1
$C_4 \leftarrow S_2$	0.1	0	$S_3 \leftarrow C_5$	0.1	0
$C_5 \leftarrow T$	0	0.1	$S_4 \leftarrow T$	0	0.1
$C_6 \leftarrow T$	0	0.1	$S_5 \leftarrow T$	0	0.1
其他	∞	∞	$S_6 \leftarrow T$	0	0.2

对于证书评测函数的计算公式 g,使用公式 $H_\mu(\mu)$中消息 μ_i 能够满足 $U(\mu_{i+1})$作为评测标准.如图 2,$S_4 \rightarrow S_5$,消息发送引起下一个新消息的开始,并提供相关的符合要求的消息,则 $H_\mu(\mu_i)=1$,$g(C_i)=1$.如果某个证书所提供的信息足以使协商方完全相信对方,则协商阈值迅速提升,以使得协商方提供完全策略集和相关证书集,迅速达到信任协商结果.客户权重的设置为 $\omega_1=0.6$,$\omega_2=0.3$,$\omega_3=0.1$.售书商的权重为 $\omega_1=0.5$,$\omega_2=0.4$,$\omega_3=0.1$.由图可见,在 $S_5 \rightarrow S_6$ 步骤时,由于售书商对客户的信任水平达到 0.426 7,但 S_2 披露条件没有完全满足,所以只披露了 S_1,S_5,所以协商的效率比开始的谨慎协商策略有所提高.如果发生错误,例如在 S_7 前售书商收到 3 次错误消息,V.u(t)将降为 0.224 7,S_1 将不会在 $S_5 \rightarrow S_6$ 步骤披露,将在信任继续增加之后的 $S_7 \rightarrow S_8$ 步骤披露.

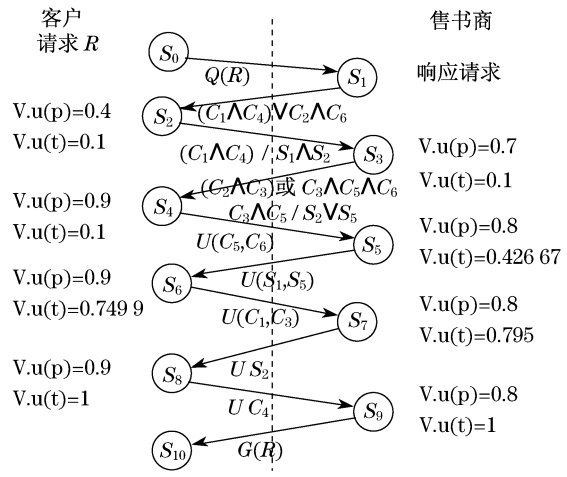

图 2　客户和售书商协商步骤信任变化

Fig.2　ATN process of Client and Server

4.2　仿真实验分析

利用软件仿真实验来模拟协商策略的控制,访问控制策略的选择,访问控制策略中证书的数目、分支数目等对协商策略的影响.为体现实验效果,选择热心协商和谨慎协商策略进行对比.

在仿真实验中,策略的随机性更能体现协商策略的实际效果.使用伪随机数对相关证书的数目、证书的序列等进行随机选取.同时,为提高策略分支选取对协商效果的影响,实验时假设参与协商方的证书数目为 n,含有分支的访问控制策略的比例为 0.2,概率密度服从参数为($\lceil n/2 \rceil$,0.2)的二项分布.任一访问控制策略中包含的证书数目 m 满足 $m \geqslant 1$,不妨假设每条访问控制策略包含的证书数目的分布在区间[1,3]上.在含有分支的访问控制策略中,假设访问控制策略包含的证书数目的概率密度不受策略证书集的影响,每条策略包含的证书数目服从参数为(2,1)的正态分布.对于不含分支策略的访问控制策略,由于存在合取项的可能,假设策略含有合取项的概率为 0.1,则访问控制策略服从参数为($\lceil n/2 \rceil$,0.1)的二项分布.

协商效率分析如图3所示.协商的步骤在 $n\leqslant 5$ 的情况下差别不是特别大,但随着证书数目的增多,动态阈值协商策略开始明显优于谨慎协商策略,但热心协商策略的效率仍然是最高的.热心协商策略不使用协商策略树,从协商效率来说,节省了协商步骤.而动态阈值协商策略在协商涉及的策略增多后,特别是协商后期,迅速提高交换证书的频率,从而提高了效率.

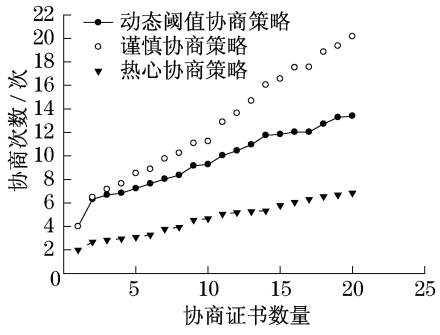

图3 协商策略效率对比

Fig.3 Comparison of ATN strategy efficiency

披露证书数量分析如图4所示.动态阈值协商策略披露的证书总体上比热心协商策略要少.这是因为热心协商策略对证书的披露只要满足条件就释放,使得协商在策略树比较平衡的情况下,泄露的信息比必要的信息要多得多,这也造成了曲线的震荡.

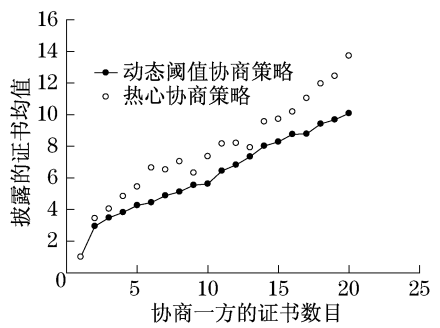

图4 协商披露证书数目对比

Fig.4 Comparison of disclosed credentials

分支对协商过程的影响如图5所示.策略树的分支比较少(<3)的情况下,协商效率的提高非常低.这是由于动态阈值协商策略在前期需要证书提供信任的支撑,在信任度提高的情况下,协商才能够提高效率.在协商策略树的分支>5时,由于协商的信任度有所提高,协商的效率明显提高.另外,从图4也可以看出,在图形后半部分,动态阈值协商策略的步骤均值比较小.

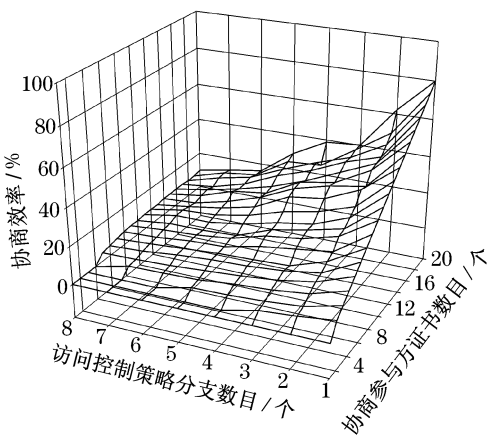

图5 协商策略分支对协商过程影响分析

Fig.5 Influence of the negotiation strategy branch

5 结语

本文针对信任协商中的信任敏感度的得益分析和信任在协商过程中的变化,提出动态阈值信任协商策略,根据协商方的交互行为和证书提供的过程,判断对方不断变化的可信程度,决定所要采取的协商策略.论文表明,该协商策略适用于在协商中的访问控制策略含有较多分支且对敏感信息披露又限制的情况.动态阈值协商策略可以同协商保护策略[3]、信任票[12]相兼容,进一步地提高协商的效率.该部分工作将在后续工作中研究.

参考文献:

[1] 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.
LIAO Zhensong, JIN Hai, LI Chisong, et al. Automated trust negotiation and its development trend[J]. Journal of Software, 2006,17(9):1933.

[2] Baselice S, Bonatti P A, Faella M. On interoperable trust negotiation strategies [C] // The 8th IEEE International Workshop on Policies for Distributed Systems and Networks. Bologna: IEEE Computer Society Press, 2007: 39-50.

[3] 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. New York: ACM Press, 2001: 146-155.

[4] William H W, Kent E S, Jones V E. Negotiating disclosure of sensitive credentials[C]// The Second Conference on Security in Communication Networks. Amlfi: ACM Press, 1999.

[5] Bonatti P, Olmedilla D. Driving and monitoring provisional trust negotiation with metapolicis [C] // Proceedings of the 6th IEEE International Workshop on Policies for Distributed Systems and NetworksStockholm: IEEE Computer Society Press, 2005: 14-23.

(下转第1693页)