一种基于多样化历史信息的自动信任协商策略

李健利 王艺谋 谢 悦 丁洪骞
(哈尔滨工程大学计算机科学与技术学院 哈尔滨 150001)

摘 要 针对自动信任协商的协商效率问题,提出了一种基于多样化历史信息的自动信任协商策略。本策略将历史信息作用于协商过程中,利用策略有向图来完成协商;利用票证来存储历史协商信息,并采用数字签名技术来保证信息的真实性和完整性。根据历史协商信息在产生方式上的不同,提出了信任票证和历史票证,并结合其特点设计了相关的格式以及验证和工作过程。最后进行了实验仿真,结果表明该模型可以提高重复协商的效率。

关键词 自动信任协商,协商效率,策略有向图,历史协商信息
中图法分类号 TP393.08 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.3.025

Automated Trust Negotiation Based on Diverse History Information

LI Jian-li WANG Yi-mou XIE Yue DING Hong-qian
(College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China)

Abstract For the problem of efficiency which appeares in the repeated automated trust negotiation, a negotiation strategy based on diverse history negotiation information was proposed. This strategy combines history information with negotiation by means of policy directed graph and ticket. The former one is used to finish the negotiation and the latter one is used to storage history negotiation information, meanwhile, digital signature technology is adopted to ensure the authenticity and integrity of the information. According to the different modes of history negotiation which is generated, trust-ticket and history-ticket were proposed. In addition, proper formation, verification and working procedure were designed in view of their characteristics. Finally, simulation results demonstrate that this model can improve efficiency in repeated negotiation.

Keywords Automated trust negotiation, Negotiation efficiency, Policy directed graph, Historic negotiation information

1 引言

自动信任协商(Automated Trust Negotiation, ATN)[1,2]是通过逐渐披露自身属性使处于不同安全域的陌生实体可针对请求的资源建立信任。在虚拟的网络环境中,传统安全域中使用的自主访问控制机制因设计的局限性,导致很难实现资源的跨域访问。自动信任协商通过交换用户的属性,为不同安全域中的陌生实体提供了建立信任关系的方法,也为虚拟网络环境提供了一种有效的资源共享方法。

ATN模型利用了基于属性的访问控制策略(Attribute Based Access Control, ABAC)[3]作为资源的保护策略,基于属性的访问控制策略具有更加灵活的特点,为用户提供了多样选择,这种设计更适合在分布式环境下使用;其利用属性证书(Attribute Certificate, AC)作为属性的载体,并严格遵从授权管理基础设施(Privilege Management Infrastructure, PMI)的规定来使用属性证书。协商策略是ATN模型的核心,协商策略规定了协商双方交互的具体方式,即需要交换哪些证书、何时交换证书以及信任建立的标准,因此协商策略的安全性和效率直接决定了自动信任协商模型的优劣。

2 相关研究

Winsborough等人在提出ATN概念的同时提出了吝啬策略和贪婪策略。吝啬策略以协商安全性为核心,通过增加协商轮次来避免披露无关的证书,但是协商中需要消耗很多时间;贪婪策略则以提高协商效率的思想为核心,尽量披露所有证书来减少协商轮数。这两种策略是从不同的侧重点来进行协商,为协商策略的研究提供了很好的参考。

围绕着安全性和效率这两个评估协商策略的关键因素,自动信任协商的研究人员提出了大量的方案。

以协商安全性为核心,间接提高协商效率,是目前协商策略的一种主流思想。Yu等人提出了一种削减协商策略PRUNES,首次将创建树的思想引入协商策略中,减少了无关证书的披露,同时提高了协商的安全性,但是在计算和通信方面都过于复杂[4];Yao Hui等人在树建模的基础上提出基于权重的协商策略,通过在证书上定义权重来有选择地披露证书,但是权重的定义并不符合一般性[5];鲁洪伟等人提出了一种高效的DFANS策略[6],将一条访问控制策略转变成有穷自动机的形式,使访问控制策略中证书之间的联系更强;其它

到稿日期:2015-02-09 返修日期:2015-04-10 本文受国家自然科学基金项目(61073042)资助。
李健利(1963-),男,硕士,副教授,硕士生导师,主要研究方向为信息安全,E-mail:lijanli@hrbeu.edu.cn;王艺谋(1990-),男,硕士,主要研究方向为信息安全;谢 悦(1989-),男,硕士,主要研究方向为信息安全;丁洪骞(1990-),男,硕士,主要研究方向为信息安全。

协商策略还有联合协商策略[7]、基于着色 Petri 网的自动信任协商[8]等,但以上介绍的协商策略都没有用到历史协商信息。

随着协商策略研究的深入,小部分研究者将视线转移到对历史协商信息的利用上。Elisa Bertino 等人设计的 Trust-X 协商模型最早引入对历史信息的应用[9],当用户获得请求的资源时,资源请求方会为用户提供短期内直接获取资源的能力,这种设计很好地减少了频繁请求资源的协商时间,但是 Trust-X 只限同一资源,忽略了请求多资源时,协商过程之间的联系。

历史信息还被用来与信任评估相结合以提高协商效率,刘百灵在以自动信任协商为基础的 P2P 协商框架中引入本地信任结点和声明权证[10],请求本地信任结点来获得声明权证,通过这种方法可在一定情况下提高协商效率,但由本地信任结点提供的声明权证的安全性和有效性却值得怀疑。邓潇等人将信任等级与资源敏感度相结合:信任等级越高,资源敏感度越低,信任等级由历史协商的成功与失败数决定。这种方法看似高效,但存在一定的安全问题,同时缺乏普遍性。刘博等人利用历史对不同用户提供的相同资源进行评估,并选择一个最适合的资源进行协商[11]。这一想法是很好的研究方向,但更侧重对用户安全性的评估,缺少对协商策略的研究。

因此,本文针对以上出现的协商效率低下、历史协商信息利用不足和安全性低等问题,提出了基于多样化历史信息的自动信任协商策略。从整体上来看,本策略将历史信息引入协商过程中,利用策略有向图来完成协商并产生可用的历史信息;根据历史信息产生过程的不同,提出了信任票证和历史票证的概念,并根据两种票证的特点设计了票证格式及验证和使用过程。安全方面,利用数字签名技术来保证票证内容的真实性和完整性;规定了严格的票证校验规则来保证票证的有效性,进而保证协商的安全性。

3 策略的整体设计

基于多样化历史信息的协商策略,在协商过程中利用策略有向图和历史信息来完成协商。当协商双方针对不同资源进行协商时,利用历史信息可以避免相同协商过程的重复执行,进而提高协商效率。同时,根据记录协商过程中产生的信息,可以得知已经被满足的资源和未被满足但已经知道其协商过程的资源,这两类资源可以看成两种不同的可重复利用的历史信息,将这两种信息作为历史信息保存并用于下次协商,可以增加协商的灵活性。

在自动信任协商中,资源与证书、证书与证书之间受访问控制策略的限制而存在相互的依赖关系,PRUNES 协商策略中使用创建树的方法来展现证书间的联系,但树型结构中父结点与子结点这种一对多的对应关系并不能灵活地展现证书间的联系。相反,图型结构中结点关系的任意性更能体现证书间复杂的关联性,因此本文通过设计策略有向图来完成协商。

为方便表达,定义如下符号:

Object:表示资源,该对象可能是服务、资源;

Negotiation_Object:表示针对资源的协商;

Policy_ Object:表示资源的访问控制策略;

SubPolicy:表示访问控制策略中的子策略;

Cred:表示协商过程中用到的属性证书。

自动信任协商中资源(包括属性证书)的访问控制策略可以表示成由逻辑运算符"∧"、"∨"和括号组成的属性证书逻辑表达式,标准格式可表示为:

$Policy=SubPolicy_0 \vee SubPolicy_1 \vee \cdots \vee SubPolicy_n$

$SubPolicy=Cred_1 \wedge Cred_2 \wedge \cdots \wedge Cred_n$

在访问控制策略中子策略之间是逻辑或的关系,这表明协商时只要满足一条子策略,访问控制策略就可以被满足;在子策略中,证书之间是逻辑与关系,所以必须提交所有证书,子策略才会被满足。

根据访问控制策略表达式,可以对资源 Object 或受保护证书 Cred 进行如下表示:

$lock(Object/Cred,(SubPolicy_0,SubPolicy_1,\cdots,SubPolicy_n))$

将无法披露或未拥有的资源表示为:$lock(Object/Cred,(false))$;可直接披露的资源表示为:$lock(Object/Cred,(true))$;已经被披露的资源表示为:$sat(Object/Cred,(Cred_0,Cred_1,\cdots,Cred_n))$,其中 $Cred_i$ 表示披露资源所用到的证书,其中既包括资源请求方的证书又包括资源提供方的证书,如果资源无法被披露,则表示为:$unsat(Object/Cred)$;未被验证但已经知道其披露序列的资源表示为:$seq(Object/Cred,(Cred_0,Cred_1,\cdots Cred_n))$。

3.1 策略有向图的设计

策略有向图包含 3 种类型的结点:属性证书结点、合取结点和布尔结点。属性证书和布尔结点用圆圈表示,并标注所代表的证书名或布尔值;合取结点用方形表示。

策略有向图的边用来表示结点之间的逻辑关系,边所指向的结点为受保护资源,另一端表示需要被满足的资源。指向合取结点的所有子结点之间为合取的逻辑关系,指向属性证书结点的所有子结点之间为析取的逻辑关系。布尔结点指向的结点一定是可直接披露或永远不会披露的属性证书结点。

根据以上定义来转换访问控制策略,如图 1 所示。

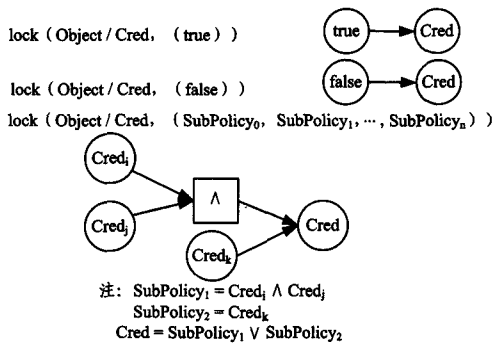

图 1 访问控制策略转换

图 2 给出了多个相关策略及与其对应的策略有向图。

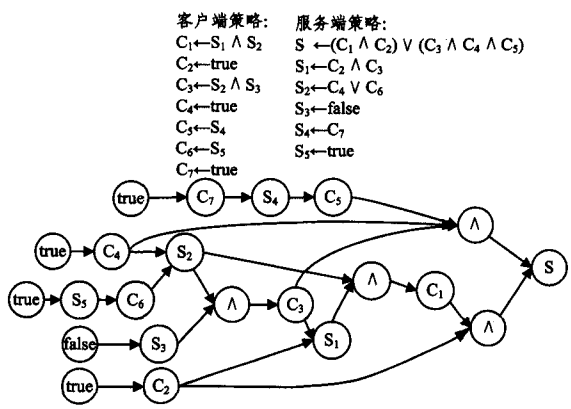

图 2 相关策略及与其对应的策略有向图

3.2 策略有向图的削减与分解

在策略有向图中，入度为 0 的结点一定是布尔结点，通过布尔结点可以知道哪些结点永远不会被披露，这些结点对证书披露序列的生成是无用的，可以被削减掉。在访问控制策略中有些属性证书存在必然的依赖关系，即：

If: $lock(Cred_i,(false))$

$SubPolicy_i = Cred_1 \wedge Cred_2 \wedge \cdots \wedge Cred_n(exit\ Cred_i)$

Then: $SubPolicy_i = false$

If: $lock(Cred_j,(SubPolicy_i))$

Then: $unsat(Cred_j)$

Elseif: $lock(Cred_j,(SubPolicy_i,SubPolicy_j))$

Then: $exchange\ lock(Cred_j,(SubPolicy_j))$

因此有如下削减规则：

从布尔值为 false 的结点开始削减，削减布尔结点指向的结点。如果该结点指向一个属性证书结点且属性证书结点的入度为 1，则削减该结点，并以此规律继续向前削减直到发现入度不为 1 的属性证书结点。当遇到入度不为 1 的属性证书结点，削减将不会继续进行。

如果被削减掉的属性证书结点指向合取结点，削减时将合取结点看作可以削减的属性证书结点，并按以上规则向前削减。削减合取结点后原本指向此结点的证书结点会与原图分离并形成子图，即：

If: $seq(Cred,(Cred_0,Cred_1,\cdots,Cred_n))$

$lock(Cred_j,(false))$

$SubPolicy_i = Cred_i \wedge Cred_j, SubPolicy_i \subseteq Policy\_Object$

Then: $Cred_i \not\subset Negotiation\_Object$

图 3 展示了对图 2 中策略有向图削减和分解后的结果图。

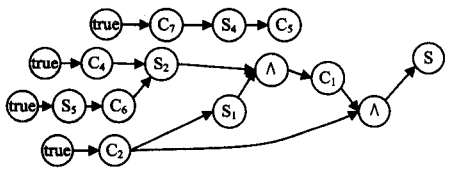

图 3 削减和分解后的策略有向图

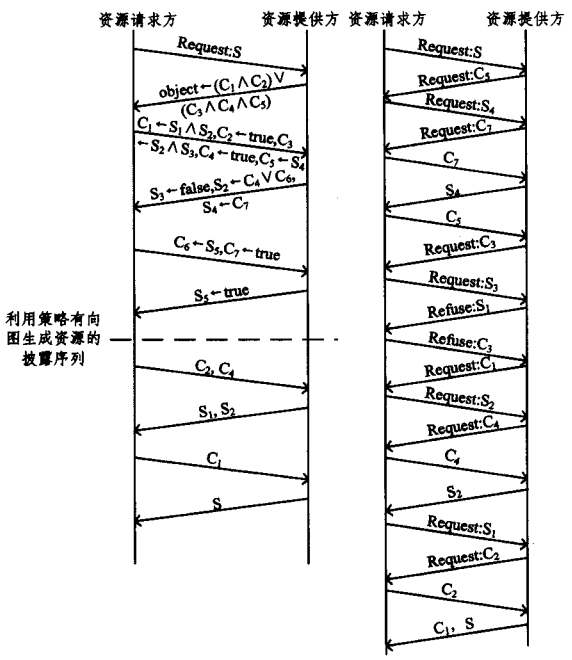

图 4 协商过程对比

图 4 展示了使用策略有向图的协商策略与 PRUNES 协商策略协商的过程。从图中可以看出，利用策略有向图的协商策略与 PRUNES 协商策略在协商双方交互的轮次上有明显的减少，这主要因为 PRUNES 协商策略是在协商的同时创建树，这样双方会针对一些与协商无关的证书进行交互。例如图中，披露资源 S 时，只需证书 C_2、C_4、S_2、S_1、C_1，但是，在利用 PRUNES 策略的协商过程中，协商双方针对证书 C_7、S_4、C_5、C_3、S_3 进行了交互，导致交互轮次增加，同时披露了与资源 S 无关的证书 C_7、S_4、C_5。而利用策略有向图的协商过程并不包括无用的证书交换。

3.3 历史信息的产生

削减后的策略有向图中存留的结点可以分为两大类：一类是与协商相关的证书；另一类是与协商无关的证书。协商双方会交换并验证与协商相关的证书来建立相互信任关系，对于与协商无关的证书不做任何处理。但是这两类证书在理论上都是可以被满足的。对于第一类证书，因为它已经被披露，所以当它再次被请求时，可以直接披露，无需根据其访问控制策略进行协商；对于第二类证书，因为其披露序列已经生成，当再次被请求时，直接根据已有的披露序列交换证书。因此，以上两种证书所产生的信息都可以作为历史信息来存储。

根据以上介绍的两类证书并结合图 3 中的策略有向图可以看出，当协商双方针对 S 建立信任后，会得到如图 5 所示的历史信息。

第一类历史信息：	第二类历史信息：
$Sat(S,(C_2,C_4,S_2,S_1,C_1))$	$Seq(C_5,(C_7,S_4))$
$Sat(C_1,(C_2,C_4,S_2,S_1))$	$Seq(C_6,(S_5))$
$Sat(S_2,(C_4))$	$Seq(S_4,(C_7))$
$Sat(S_1,(C_2))$	

图 5 协商后的历史信息

4 历史信息的存储

根据两类历史信息，提出了两种票证，分别是信任票证和历史票证。

4.1 信任票证

用户通过与资源对应的信任票证，证明自己曾经通过协商获得过资源，而如今可以直接获得资源。

虽然信任票证可以作为信任延续的载体，但是根据证书的使用原则，在每次使用证书时，都需要向证书颁发者验证证书是否被撤销。因此使用信任票证的同时还需向证书的颁发者验证证书的有效性，在信任票证的设计上需要记录相关证书的编号和颁发者 ID。图 6 展示了信任票证的格式。

```
〈!DOCTYPE TrustTicket [
〈!ELEMENT Type (Trust_ticket)〉
〈!ELEMENT Rescourse (#PCDATA)〉
〈!ELEMENT Sender ID (#PCDATA)〉
〈!ELEMENT Receiver ID (#PCDATA)〉
〈!ELEMENT CertificateSequence(Certificate+)〉
〈!ELEMENT Certificate(Certificate ID,Issuer ID)〉
〈!ELEMENT Certificate ID (#PCDATA)〉
〈!ELEMENT Issuer ID (#PCDATA)〉
〈!ELEMENT Effective Time (#PCDATA)〉
〈!ELEMENT Signature (#PCDATA)〉
]〉
```

图 6 信任票证的基本格式

信任票证定义包含 7 种元素（type、sender、receiver、re-

source、certificate_sequence、effective_time、signature)，其中type表示票证类型；sender是票证发送方，表明此票证是由谁签发的；receiver是票证的接收方，表明此票证的拥有者；resource表示此票证针对的是哪一个资源，此资源包括服务器提供的服务，也包括受保护的属性证书；certificate_sequence记录了获得资源所交换的属性证书，certificate_sequence中包含多个certificate元素，certificate元素中记录了相关属性证书的信息，其中包含属性证书序列号certificate_num和颁发者信息sender_id；effective_time是有效时间，用来描述信任票证的有效期；signature是数字签名，用于证明票证的有效性和安全性。

将信任票证与第一类历史信息转换，则有：

$sat(Object/Cred,(Cred_0,Cred_1,\cdots,Cred_n))$

$\rightarrow Trust\_ticket(Object/Cred,Certificate\_sequence,Effective\_time)$

对票证中的certificate_sequence与effective_time有如下规定：

$Effective\_time\_T_A=Min(Limit\_time\_Cred_0,\cdots,Limit\_time\_Cred_n)$

$Certificate\_sequence=\{(Cred_i\_num,Cred_i\_sender\_id)\mid \forall i\subseteq(0,n)\}$

4.2 历史票证

历史票证主要记录资源的证书披露序列。当需要请求受保护的资源时，双方可以根据历史票证中记录的披露序列交换并验证属性证书。

历史票证作为记录披露序列的媒介，其中只记录了资源的历史披露序列，协商双方根据历史票证中的披露序列交换相关属性证书，所以无需记录证书颁发者信息；考虑到加密对时间的消耗，历史票证无需数字签名技术来保证内容的有效性和安全性，不同于信任票证跳过访问控制策略直接获得资源，历史票证只是避免了披露序列生成过程，但最终还需要满足访问控制策略才能获得资源。历史票证的格式如图7所示。

```
〈!DOCTYPE HistoryTicket [
〈!ELEMENT Type (History_ticket)〉
〈!ELEMENT Rescourse (#PCDATA)〉
〈!ELEMENT Sender ID (#PCDATA)〉
〈!ELEMENT CertificateSequence〉
〈!ELEMENT Effective Time (#PCDATA)〉
]〉
```

图7 历史票证的基本格式

定义历史票证包含5种元素(type、sender、resource、credentials_sequence、effective_time)，type、sender、resource、effective_time 4个字段与信任票证相同，credentials_sequence字段记录了满足此资源需要披露的证书序列。

将信任票证与第二类历史信息转换，则有：

$Seq(Object/Cred,(Cred_0,Cred_1,\cdots,Cred_n))$

$\rightarrow History\_ticket(Object/Cred,Certificate\_sequence,Effective\_time)$

其中$Certificate_sequence=(Cred_0,Cred_1,\cdots,Cred_n)$。

5 历史信息的工作过程

5.1 历史信息的验证

对于票证的验证主要分为两个时期，分别是获得对方签发的票证时和使用票证时。但是根据信任票证和历史票证的存储内容与使用方式的不同，两种票证的验证过程也有差异。

信任票证作为证明信任延续的媒介，当用户收到对方发送的信任票证时，需要验证信任票证的证书序列和有效时间是否与实际协商中交换的证书序列和有效时间一致。因为当用户使用信任票证时，需要验证对方的相关属性证书未被撤销，如果对方签发的信任票证中记录的证书序列不全，将无法对全部的相关证书进行有效验证。同理，如果对方在签发信任票证时刻意地将信任票证的有效期延长，当用户使用信任票证时，对方可能已处于非可信状态，这将影响用户的安全。同时，对方收到信任票证后，首先查看票证的有效期，接着查看信任票证是否是由自己签发的并且内容是否被修改，最后验证信任票证中记录的用户的相关属性证书的有效性。信任票证的验证过程如图8所示。

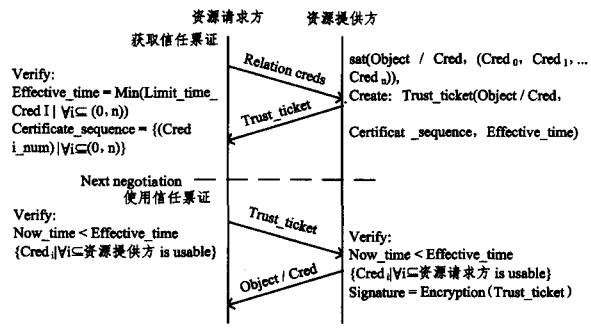

图8 信任票证的验证过程

历史票证作为记录披露序列的媒介，无需与信任票证一样的验证过程，因为历史票证中只记录了资源的披露序列，所以在接收和使用历史票证时只需验证其有效期。

5.2 策略有向图与票证的结合过程

协商实体在建立信任的过程中可将信任票证和历史票证共同作用于策略有向图中。同时资源被披露后，其对应的历史票证也可转化为信任票证。

访问控制策略中存储了协商方想获得资源所要提交的属性证书，当协商双方交换访问控制策略时，分别将己方已有的与具体属性证书对应的信任票证和历史票证发送给对方。设资源请求方拥有证书$Cred_i$，资源提供方拥有与此证书对应的信任票证$Trust_ticket(Cred_i,Certificate_sequence,Effective_time)$，当请求方请求资源$S$后，提供方参考自己拥有的信任票证，将$S$对应的访问控制子策略$SubPolicy=Cred_1\wedge Cred_2\wedge\cdots\wedge Cred_i$修改成$SubPolicy=Cred_1\wedge Cred_2\wedge\cdots\wedge Trust_ticket_i$并发送给请求方；资源提供方如果拥有证书$Cred_i$对应的历史票证$History_ticket(Cred_i,Certificate_sequence_i,Effective_time)$，则将访问控制策略修改成$SubPolicy=Cred_1\wedge Cred_2\wedge\cdots\wedge Certificate_sequence_i$。通过对访问控制表达式的转换，将信任票证和历史票证融入由相关访问控制表达式生成的策略有向图中，以减少双方的协商轮次，进而提高协商效率。

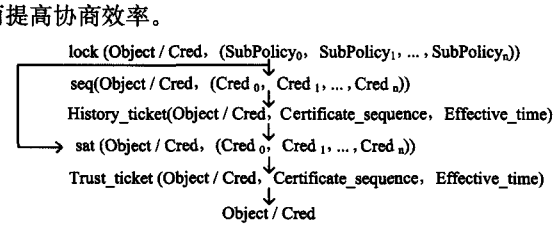

图9 历史票证与信任票证的转化过程

当资源经过双方协商被披露后，资源拥有方签发信任票

证并发送给请求方，如果请求方先前拥有相应资源的历史票证，则历史票证被信任票证替换。历史票证与信任票证的转化过程如图 9 所示。

5.3 协商实例

下面用实例说明采用基于多样化历史信息的协商策略的协商过程，以图 2 中的协商作为双方的首次协商，协商结束后产生的信息作为历史信息。此时，资源提供方又提供了资源 object，协商请求方将针对 object 与资源提供方建立信任。协商具体过程如图 10 所示。

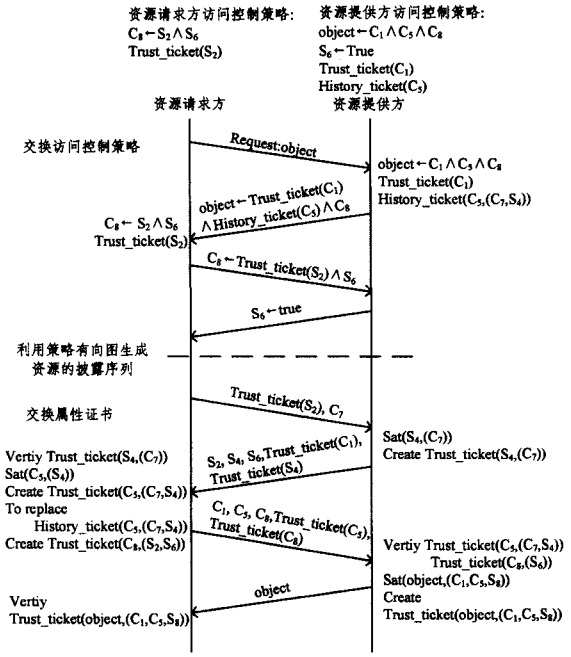

图 10 实例协商过程

从上图中可以看出，双方在协商中使用了信任票证 *Trust_ ticket*（S_2）、*Trust_ticket*（C_1）和历史票证 *History_ ticket*（C_5），避免了针对证书 S_2、C_1 和 C_5 的协商，减少了协商轮数。在证书和访问控制策略的使用量上有明显的减少，这样直接降低了策略有向图的复杂程度，加快了图的削减过程和针对资源 object 的证书披露序列的产生。

6 仿真和分析

仿真实验主要验证基于多样化历史信息的协商策略相对于经典的 PRUNES 协商策略在协商效率上的提升。本实验仿真平台应用了 Trust Builder2 这款开源软件。

实验 1 在服务端开辟 8 个资源，分别编号 1 到 8 作为变量，设置 8 个资源的访问控制，使其具有一定程度的相似性，先对 PRUNES 协商策略进行仿真，客户端分别访问 8 个资源，同时记录消耗的时间。再对基于多样化历史信息的协商策略进行仿真，并分别记录客户端获得 8 个资源所消耗的时间，具体的实验结果如图 11 所示。

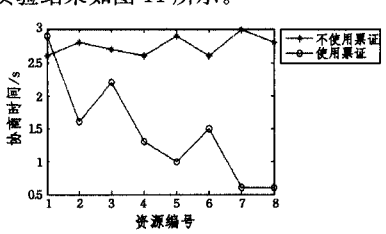

图 11 协商时间对比图

通过以上数据可以看出，利用 PRUNES 协商策略分别请求 8 个资源所消耗的时间相差无几，但是利用基于多样化历史信息的协商策略后，只有在请求第一个资源时消耗的时间略长，其他几个资源的协商时间都少于使用 PRUNES 协商策略所消耗的时间。并且随着协商次数的增加，前几次协商会出现协商时间的波动，到对第 7、8 个资源进行协商时，时间消耗趋于稳定，出现这种现象的主要原因在于使用信任票证的数量，开始的几次协商中信任票证对证书的覆盖率不大，因此前几次请求在协商的过程中用到的信任票证较少，在效率上的提高不明显，随着信任票证对证书的覆盖率的提高，协商时间会稳步缩短，当覆盖率为 100%时，无论访问控制策略怎样变化，只要协商能够成功，协商时间都不会改变且时间消耗非常少。值得注意的是第一个资源的协商时间略长于 PRUNES 协商策略，因为协商的过程中包含了信任票证的生成阶段。

实验 2 同样是服务器端开辟 8 个资源，利用基于多样化历史信息的协商策略进行仿真实验，客户端对 8 个资源分别进行 3 组请求，3 组请求中 8 个资源的访问控制策略的相似度分别为 0、50%、100%，记录每组获得资源所消耗的时间，结果如图 12 所示。

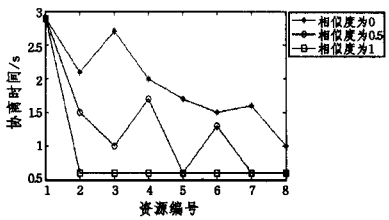

图 12 相似度不同情况下的协商时间对比

通过以上数据可以看出，访问控制策略相似度越高，协商时间减少的速度越快。资源的访问控制策略相似度为 0 时，随着请求次数的增加，虽然前几次的协商时间会有所波动，但是从整体上来看仍是呈减少的趋势，因为即使相似度为 0，随着协商的深入总会使用到相同证书；资源的访问控制策略相似度为 50%时，意味着一半的协商过程可以用信任票证取代，所以协商的时间减少明显，但是，最终还是达到稳定状态，即信任票证对证书的覆盖率为 100%；资源的访问控制策略相似度为 100%时，由图可知从第二次开始，就呈现稳定状态，但是需要注意造成稳定的原因不是信任票证对证书的覆盖率为 1，而是每次协商使用的是相同的信任票证。通过以上分析可以看出，服务端为资源设置的访问控制策略相似度越高，完成协商所消耗的时间越少。

实验 3 将传统的协商策略与使用信任票证的协商策略进行对比，记录 20 次协商实验中敏感信息的披露条数，结果如图 13 所示。

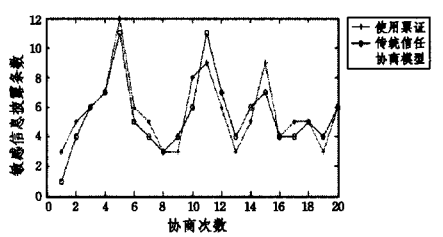

图 13 敏感信息的披露条数对比

因为传统的信任协商策略也有对证书和策略的加密保护机制，所以与本文提出的基于信任票证的协商策略披露的敏感信息数量相差不大，因此信任票证具有很好的安全性。

（下转第 144 页）

cy Preserving Approach on Road Network[J]. Chinese Journal of Computers,2011,34(5):865-878(in Chinese)
薛姣,刘向宇,杨晓春,等.一种面向公路网络的位置隐私保护方法[J].计算机学报,2011,34(5):865-878

[11] Sun Lan,Luo Zhao,Wu Ying-jie,et al. An Algorithm for protection location privacy in road network[J]. Journal of Shandong University(Engineering Science),2012,42(5):96-101(in Chinese)
孙岚,罗钊,吴英杰,等.面向路网限制的位置隐私保护算法[J].山东大学学报(工学版),2012,42(5):96-101

[12] Zhao Ping,Ma Chun-guang,Gao Xun-bing,et al. Protecting Location Privacy with Voronoi Diagram over Road Networks[J]. Computer Science,2013,40(7):116-120(in Chinese)
赵平,马春光,高训兵,等.路网环境下基于 Voronoi 图的位置隐私保护方法[J].计算机科学,2013,40(7):116-120

[13] Shun K G,Ju X,Chen Z,et al. Privacy protection for users of location-based services[J]. IEEE Communications Society,2012,19(1):30-39

[14] Chow C Y,Mokbel M F,Liu X. A peer-to-peer spatial cloaking algorithm for anonymous location-based service[C]// Proceedings of the 14th Annual ACM International Symposium on Advances in Geographic Information Systems. ACM,2006:171-178

[15] Hu H,Xu J. 2PASS:Bandwidth-optimized location cloaking for anonymous location-based services[J]. IEEE Transactions on Parallel and Distributed Systems,2010,21(10):1458-1472

[16] Wang Lu,Meng Xiao-feng. Location Privacy Preservation in Big Data Era:A Survey[J]. Journal of Software,2014,25(4):693-712(in Chinese)
王璐,孟小峰.位置大数据隐私保护研究综述[J].软件学报,2014,25(4):693-712

[17] Brinkhoff T. A framework for generating network based moving objects[J]. Geo Informatic,2002,6(2):153-180

[18] Sousa M, Techmer A, Steinhage A, et al. Human tracking and identification using a sensitive floor and wearable accelerometers [C]//2013 IEEE International Conference on Pervasive Computing and Communications (PerCom). IEEE,2013:166-171

[19] Gedik B, Liu L. Protecting location privacy with personalized k-anonymity:Architecture and algorithms[J]. IEEE Transactions on Mobile Computing,2008,7(1):1-18

[20] Xu J,Tang X,Hu H,et al. Privacy-conscious location-based queries in mobile environments[J]. IEEE Transactions on Parallel and Distributed Systems,2010,21(3):313-326

[21] Pan X,Xu J,Meng X. Protecting location privacy against location-dependent attacks in mobile services[J]. IEEE Transactions on Knowledge and Data Engineering,2012,24(8):1506-1519

[22] Zhu Qing,Zhao Tong,Wang Shan. Privacy Preservation Algorithm for Service-Oriented Information Search[J]. Chinese Journal of Computers,2010,33(8):1315-1323(in Chinese)
朱青,赵桐,王珊.面向查询服务的数据隐私保护算法[J].计算机学报,2010,33(8):1315-1323

(上接第 126 页)

结束语 本文提出了一种基于多样化历史信息的协商策略,解决了传统协商策略在重复协商时出现的协商效率低下的问题。根据资源的使用情况分别提出了历史票证和信任票证,根据两种票证的具体用途及其对协商安全性的影响程度,分别设计了票证的格式及验证方法,并将票证的工作过程与协商过程融合,提高了同一用户多次访问相关资源的协商效率。最后进行了实验仿真,结果表明,当协商双方围绕多个资源进行协商时,相对于传统的协商策略,基于多样化历史信息的协商策略在协商效率上有明显的提高;随着资源之间访问控制策略相似度的提升,基于多样化历史信息的协商策略在协商效率上的优势更加突出。当信任票证对证书的覆盖率达到100%时,双方只需一轮协商即可建立针对具体资源的信任。

参 考 文 献

[1] Winsborough H,Seamons K E,Jones V E. Automated trust negotiation[C]// DARPA Information Survivability Conference and Exposition. 2000:88-102

[2] Liao Zhen-song,Jin Hai,Li Chi-song,et al. Automated trust negotiation and its development trend [J]. Journal of Software,2006,17(9):1933-1948(in Chinese)
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

[3] Shen Hai-bo,Hong Fan. Survey of research on access control model [J]. Application Research of Computers,2005,6(3):9-11(in Chinese)
沈海波,洪帆.访问控制模型研究综述[J].计算机应用研究,2005,6(3):9-11

[4] Yu T, Ma X, Winslett M. PRUNES: an efficient and complete strategy for automated trust negotiation over the Internet[C]// Proceedings of the 7th ACM Conference on Computer and Communications Security. ACM,2000:210-219

[5] Yao Hui,Gao Cheng-shi,Dai Qing,et al. Dynamic programming-based strategy for automated trust negotiation [J]. Computer Application,2009,28(4):892-895(in Chinese)
姚慧,高承实,戴青,等.一种基于动态规划的自动信任协商策略[J].计算机应用,2009,28(4):892-895

[6] Lu H,Liu B. DFANS:A highly efficient strategy for automated trust negotiation [J]. Computers & Security,2009,28(7):557-565

[7] Pikulkaew T, Kikuchi H. Improving Efficiency in Privacy-Preserving Automated Trust Negotiation with Conjunctive Policies [C]//2011 14th International Conference on Network-Based Information Systems (NBiS). IEEE,2011:679-684

[8] Yu D,Chen N. An automated trust negotiation model based on improved coloured timed Petri net [J]. International Journal of Sensor Networks,2014,16(2):61-69

[9] Squicciarini A,Bertino E,Ferrari E,et al. PP-trust-X:A system for privacy preserving trust negotiations [J]. ACM Transactions on Information and System Security (TISSEC),2007,10(3):12

[10] Liu B. Efficient trust negotiation based on trust evaluations and adaptive policies [J]. Journal of Computers,2011,6(2):240-245

[11] Li Jian-li,Gao Yong,Huo Guang-lei,et al. Reputation-based P2P trust system [J]. Computer Application,2011,31(1):147-150(in Chinese)
李健利,高勇,霍光磊,等.基于声誉的 P2P 信任系统[J].计算机应用,2011,31(1):147-150