

一种高效安全的自动信任协商模型

李健利 邓 潇 王艺谋 谢 悦

(哈尔滨工程大学计算机科学与技术学院 哈尔滨 150001)

摘 要 自动信任协商是分布式环境中陌生结点建立信任的有效方法。协商过程中,协商结点既要隐藏自身敏感信息,又要相互暴露信息以增强彼此信任,这种矛盾的局面使得效率和安全成为研究者主要关注的问题。提出了一种新的协商模型,在传统模型的基础上加入了信任票证库和信任评估模块。其中,信任票证用于记录历史协商的信息,信任评估模块用于评估结点的相互信任等级。在协商时,首先判断双方是否存在直接可用的信任票证,若存在,则直接通过验证信任票证而省略数字证书的交换过程。反之,则利用票证中记录的协商双方的成功协商次数和失败协商次数,以此评估协商双方的信任等级。信任等级的提高降低了双方数字证书对对方的敏感性,进而减少了协商过程中访问控制策略和数字证书交换的次数,缩短了整个协商消耗的时间,从整体上提高了协商的效率。由在 TrustBuilder2 上的实验可知,提出的模型能有效地提高协商的效率,通过分析可知,利用记录的协商失败时间信息,可以有效地防止恶意结点对服务方的拒绝服务攻击,从而证明了该模型是高效安全的。

关键词 自动信任协商,信任票证,信任评估,协商安全,协商效率

中图法分类号 TP393.08 文献标识码 A

Security and Efficiency Negotiation Model

LI Jian-li DENG Xiao WANG Yi-mou XIE Yue

(College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China)

Abstract Automated trust negotiation is a way to establish trust for strange peers in the distributed environment. During negotiation, peers have to not only conceal sensitive information, but also reveal information to strengthen mutual trust, that contradictory situation makes safety and efficiency become the main concern problem for researchers. We proposed a new negotiation model which adds trust file repository and trust evaluation module into the traditional model. Trust file is used to record historical negotiation information of two peers and trust evaluation module is used to evaluate the trust level of two peers. When negotiation starts, it firstly queries if there is available trust file to be directly used. If it exists, verify it to omit the process of exchanging credentials. Otherwise, it uses the success and fail negotiation times to evaluate their trust level of two peers. Since the trust level of the two negotiators has increased and the sensitivity to the digital credential to each other has decreased, the exchange times of the access control policy and the digital credential will be decreased during the negotiating. Furthermore, it will shorten the time spent and increase the efficiency. By doing experiment in Trustbuilder2, the proposed model is able to increase negotiation efficiency. By analyzing, it is able to protect negotiation from denial of service by using the recorded fail negotiation time. Therefore, the proposed model is safe and efficient.

Keywords Automated trust negotiation, Trust file, Trust evaluation, Negotiation safety, Negotiation efficiency

1 引言

自动信任协商^[1,2]是分布式网络环境中的陌生双方在协商策略和协商协议的共同引导下通过轮流相互交换数字证书建立信任的一种访问控制方法^[3-7]。由于数字证书本身包含着敏感信息,证书拥有者并不愿意披露给陌生方。因此,协商利用了访问控制策略来管理数字证书的安全披露。协商过程中,协商双方在相互交换信息的同时,还要保证敏感信息不会被泄露,这种矛盾使得协商过程变得复杂。因此,如何使协商

变的高效且安全成为研究自动信任协商的主要内容之一。

2000年,Winsborough等人^[1]提出了两种经典协商策略:积极策略和谨慎策略。在积极策略中,只要一方的访问控制策略被满足,它会立即把证书披露给另一方,该策略具有非常高的效率,却不安全。在谨慎策略中,协商者只会披露满足了访问控制策略并且被请求的证书,该策略具有很好的安全性,效率却很低。这之后,研究者利用双方的协商历史来提高协商效率^[8-11],在已经提出的相关研究中,以 Bertino 等人^[8]提出的验证权证最具代表性,然而它的不足之处是如果权证过

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,主要研究方向为信息安全、自动信任协商;邓 潇(1989—),男,硕士,主要研究方向为自动信任协商;王艺谋(1990—),男,硕士,主要研究方向为自动信任协商;谢 悦(1989—),男,硕士,主要研究方向为自动信任协商。

期,将无法运用其他的办法提高效率。为了解决上述问题,引入了信任评估机制来处理权证过期的问题。在这基础上,提出了一种高效且安全的协商模型。

2 自动信任协商

Winsborough 等人把自动信任协商定义为一组证书序列披露的过程。满足如下定义:

定义 1 假设 $ClientCreds$ 是资源请求方的数字证书, $ServerCreds$ 是资源提供方的数字证书,则证书披露序列可以描述为: $\{C_i\}_{i \in [0, 2n+1]} = C_0, C_1, \dots, C_{2n+1}$, 其中 $n \in N$, 有 $C_{2i} \subseteq ClientCreds, C_{2i+1} \subseteq ServerCreds$ 。其中证书集合 C 满足 $C = ClientCreds \cup ServerCreds$ 。

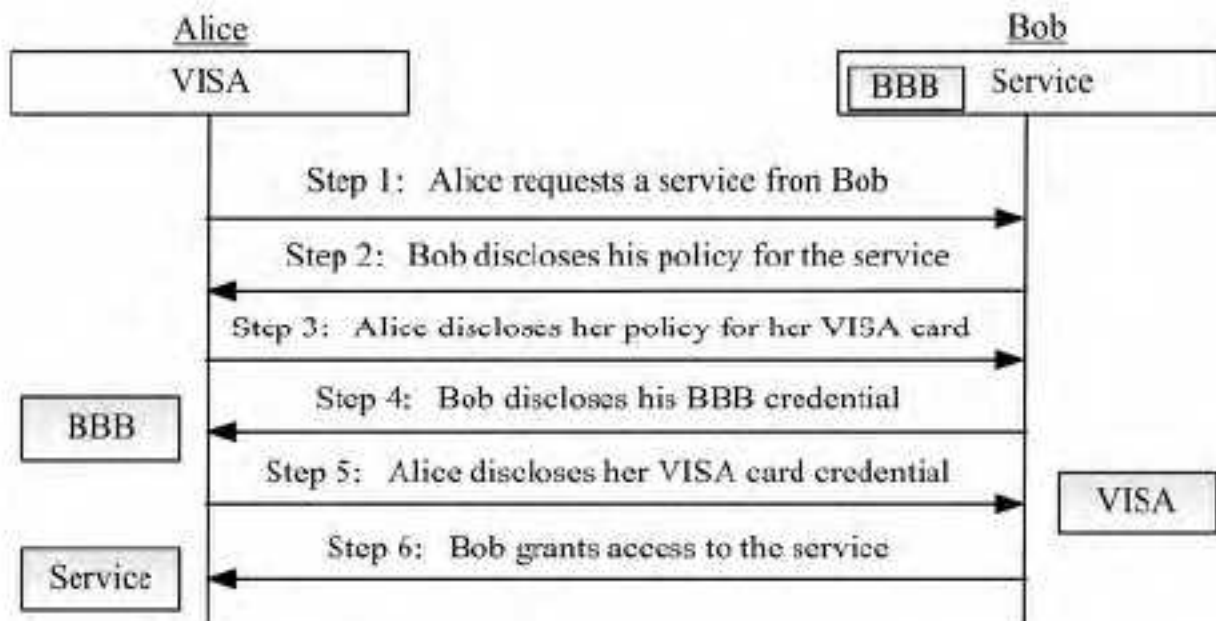


图 1 Alice 与 Bob 的协商过程

如图 1 所示, Alice 和 Bob 是两个协商实体,其中 Alice 向 Bob 请求服务。此次协商的证书披露序列为: $\{BBB\ Credential, VISA\ Card, Service\}$ 。

3 协商模型

Winsborough 等人在提出自动信任协商的同时,对协商的模型也做了描述。在其描述的协商模型中,协商方各自包含一个协商安全代理,协商方还包含一个数字证书库用来存储结点拥有的本地数字证书;一个 CAP 库,用来指明对方需要披露的数字证书,以解锁其保护的本地证书;一个 SGP 库 (SGP 和 CAP 形式上相同),协商方通过发送 SGP 以告知对方其所需的数字证书。CAP 和 SGP 都是访问控制策略,不同之处是 SGP 可以作为请求发送给对方,如今的自动信任协商认为所有的访问控制策略都是可交换的。因此,传统的协商模型包括协商安全代理、数字证书库和访问控制策略库。

本节提出了一种新的自动信任协商模型,该模型是在传统模型的基础上做了改进,引入了信任票证库和信任评估模块,如图 2 所示。

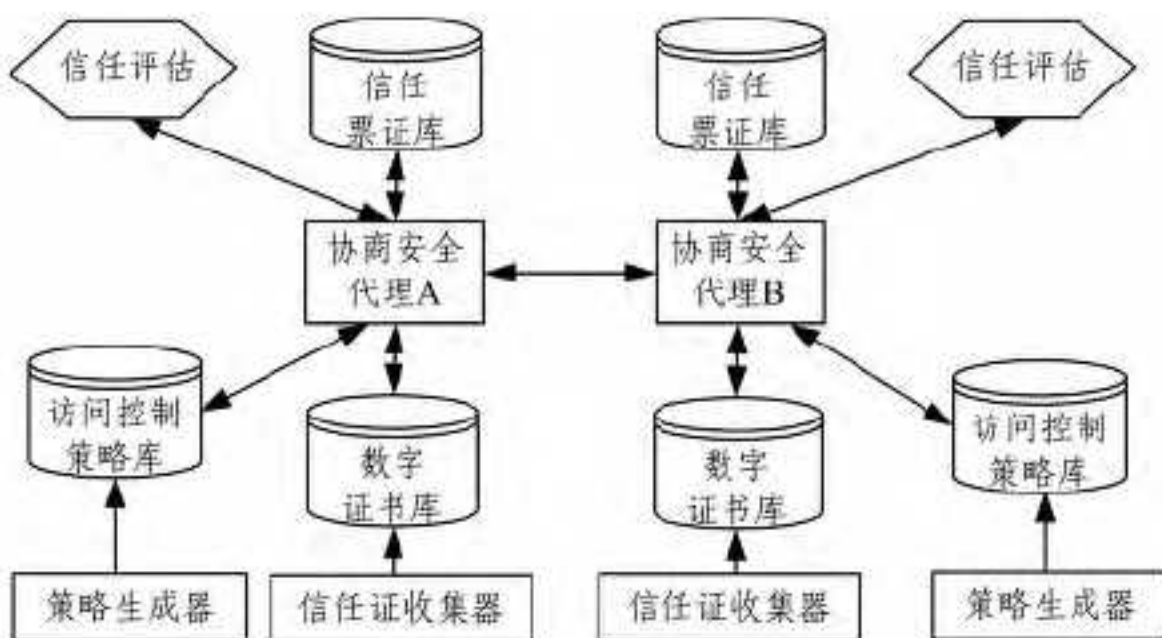


图 2 协商模型

3.1 信任票证

信任票证是双方协商结束后,资源提供方为资源请求方

颁发的文件,该文件存储着一个六元组信息。信任票证 $T = \{Rs, Sdate, Fdate, Scount, Fcount, Sig\}$, 其中 Rs 表示的是被请求的资源; $Sdate$ 表示的是关于资源 Rs 上一次协商成功时的时间,若两结点没有成功的协商历史,则 $Sdate$ 的值为 0; $Fdate$ 表示的是关于资源 Rs 上一次协商失败时的时间,若两结点没有失败的协商历史,则 $Fdate$ 的值为 0; $Scount$ 表示的是关于资源 Rs 成功的总协商次数,若两结点没有成功的协商历史,则 $Scount$ 的值为 0; $Fcount$ 表示的是关于资源 Rs 失败的总协商次数,若两结点没有失败的协商历史,则 $Fcount$ 为 0; Sig 表示的是对该信任票证的数字签名。

资源提供方为请求方颁发信任票证时,通过密钥生成器来生成一对密钥,公钥和私钥,分别用 κ 和 κ^{-1} 表示,它们可以相互用于加密和解密。

①加密函数 $BEM = En(Mess, Ekey)$

用加密密钥 $Ekey$ 对信息 $Mess$ 进行加密,返回密文 BEM 。 $Mess$ 表示的是未加密的数字签名。

②解密函数 $Mess = De(BEM, Dkey)$

用解密密钥 $Dkey$ 对密文 BEM 进行解密。当且仅当解密密钥 $Dkey$ 与生成密文 BEM 的加密密钥 $Ekey$ 是一对时,返回被加密的信息 $Mess$ 。否则,无法对 BEM 进行解密。

对 $Mess$ 加密后 Sig 满足: $Sig = En(Mess, \kappa^{-1})$, 数字签名 Sig 加密后被添加在信任票证的尾部,然后把该信任票证发送给资源的请求者。信任票证以独立文件的形式存储在循环队列当中,请求者设定队列最大长度 Max 的值。每次接收到的信任票证存储在队列的队头,当队列满时,则删除队尾的文件后,再把其加入到队头,最后遍历队列,删除与接收到的信任票证中访问资源相同的信任票证。

综上所述,信任票证的作用是记录协商双方对某个资源的协商历史信息。在协商过程中,可以通过直接利用信任票证加快协商的速度,以及通过间接利用其中记录的信息来加快协商的速度。

3.2 信任评估模块

为了达到利用票证中记录的信息提高协商效率的目的,模型中引入了信任评估模块。信任评估的作用是当协商双方无法直接利用信任票证获得请求的资源时,通过评估协商双方的信任等级,来减少低敏感性数字证书的披露。因为“在协商过程中,协商双方先暴露不太重要的数字证书,当达到一定的信任等级时,再暴露敏感的证书[12]”。

信任票证中记录了协商双方针对某一资源的协商成功次数和协商失败次数。协商成功表明协商双方曾经拥有访问资源需要披露的全部数字证书,则可以认为协商成功次数越多,协商双方对对方越信任,即协商双方的信任等级与协商成功次数正相关。协商失败表明协商过程中有数字证书缺失、证书之间环依赖、双方协商策略不一致等情况的发生,则可以认为协商失败次数越多,协商双方对对方越不信任,即协商双方的信任等级与协商失败次数负相关。因此,通过协商成功次数和协商失败次数来对协商双方的信任等级进行评估。同时,由于信任的动态性,即信任随着时间的推移而衰减,在进行信任评估时,还考虑了时间对双方信任关系的影响。

对于信任票证的直接使用有效期,借鉴了 Trust-X 框架[8]中对验证权证有效期的定义,规定为 48h。当信任票证不可直接使用时,协商双方使用信任评估模块,评估方法如下:

定义2 T_{cur} 表示当前协商的时间, T_{last} 表示上一次协商发生的时间, $\delta(T_{cur}, T_{last})$ 表示时间衰减系数。当 $T_{cur} - T_{last} \rightarrow 48h$ 时, 满足 $\delta(T_{cur}, T_{last}) \rightarrow 1$; 当 $T_{cur} - T_{last} \rightarrow \infty$ 时, 满足 $\delta(T_{cur}, T_{last}) \rightarrow 0$ 。所以时间衰减系数满足:

$$\delta(T_{cur}, T_{last}) = \begin{cases} 1, & \text{当 } 0 \leq T_{cur} - T_{last} \leq 48h \\ e^{-(T_{cur} - T_{last})/c}, & \text{当 } T_{cur} - T_{last} > 48h \end{cases}$$

定义3 协商结点 A 和协商结点 B , 设 λ_1 表示结点 A 对结点 B 的初始信任等级, λ_2 表示结点 B 对结点 A 的初始信任等级, 信任票证中记录的结点 A 请求结点 B 资源成功的协商次数为 τ_s , 失败的协商次数为 τ_f 。则经过评估模型评估后, 结点 A 对结点 B 的信任度 λ_A 满足 $\lambda_A = \alpha \delta_s \tau_s / (\tau_s + \tau_f) - (1 - \alpha) \tau_f / (\tau_s + \tau_f) + \lambda_1$, 结点 B 对结点 A 的信任度 λ_B 满足 $\lambda_B = \alpha \delta_s \tau_s / (\tau_s + \tau_f) - (1 - \alpha) \tau_f / (\tau_s + \tau_f) + \lambda_2$ 。

3.3 访问控制策略生成

在基于 X.509 标准的数字证书形式中, 证书内容中没有包含描述证书敏感度的属性信息, 因此如何在协商过程中反应协商双方信任度变化对数字证书披露的影响成为本节需要考虑的问题。在自动信任协商中, 数字证书的披露受到访问控制策略的保护, 所以, 可以把上述的问题转变为通过改变访问控制策略来反映信任关系变化对协商过程的影响。

定义4 对于任意的复合策略 $Policy$, 其形式都可转化为 $c \leftarrow Policy = D_1 \vee \dots \vee D_m$, 其中 $D_i = S_{i1} \wedge \dots \wedge S_{in}$ 表示 $Policy$ 的一个子句, $S_{ij} (0 < i < m, 0 < j < n)$ 表示资源 c 的一个元策略。

定理1 数字证书对请求者的相对敏感度越高, 对于保护该证书的复合策略的子句个数越多, 子句中的元策略个数越少。

证明: 假设访问控制策略中元策略被满足的概率为 p_{ij} 。极端情况下, 当子句个数为 1, 则访问控制策略被满足的概率为 $P = \prod_{j=1}^n p_{1j}$, 可知子句中元策略个数 n 越大, 则 P 越小, 表明该策略保护的数字证书相对请求者越敏感。当子句中元策略个数为 1, 则访问控制策略被满足的概率为 $P = \sum_{i=1}^m p_{i1}$, 可知子句的个数 m 越小, 则 P 越小, 表明该策略保护的数字证书相对请求者越敏感。

定义5 假设访问控制策略 $Policy$ 子句中的元策略个数为 $P.len$, 子句个数为 $P.num$, N 是结点认为与保护资源相关的证书数量。则 $Policy$ 与数字证书满足的关系为: $P.len \in [0, N], P.num \in [0, A_N^N]$ 。经过信任评估后, 资源相对请求者的信任等级为 $\Delta k (0 \leq k \leq 1)$, 根据定理1, 满足 $P.len = \lfloor \Delta k \cdot N \rfloor, P.num = A_N^{\lfloor \Delta k \cdot N \rfloor}$ 。同时证书 c 的策略满足 $c \leftarrow Policy = D_1 \vee \dots \vee D_m$, 当相对信任度为 i 和 j 且 $i \leq j$ 时, $P(i)$ 中出现的子句 D_i 与 $P(j)$ 中出现的子句 D_j 的关系是 $D_i \subseteq D_j$ 。

4 模型分析

4.1 协商流程

分布式环境中的陌生结点 $Client$ 和 $Server$, 结点 $Client$ 向结点 $Server$ 发送资源请求, 协商被触发, 其协商流程如图3所示:

①首先 $Client$ 向 $Server$ 发送关于资源 S 的请求消息, 并

把当前的时间作为 $Curdate$ 一同发送。 $Server$ 收到该消息后询问 $Client$ 是否已经做好协商准备, 同时询问 $Client$ 是否拥有请求资源 S 的有效信任票证。

② $Client$ 根据请求资源查询自己的信任票证库。若存在与请求资源对应的信任票证, 则把该信任票证直接发送给 $Server$, 进入步骤③。若不存在与请求资源对应的信任票证, 则告知给 $Server$, 进入步骤⑥。

③ $Server$ 收到 $Client$ 关于请求资源 S 的信任票证后, 验证数字签名 Sig 的正确性。若 Sig 验证是正确的, 进入步骤④, 否则进入步骤⑥。

④ $Server$ 检查信任票证中 $Sdate$ 和 $Fdate$ 的值, 把 $Sdate, Fdate$ 和步骤①中收到的 $Curdate$ 进行比较。若 $(Sdate > Fdate) \&\& (Curdate - Sdate \leq 48h)$, 则进入步骤⑦。若 $(Fdate > Sdate) \&\& (Curdate - Fdate \leq 48h)$, 则进入步骤⑧。若 $Curdate - Sdate > 48h$ 或者 $Curdate - Fdate > 48h$, 则进入步骤⑤。

⑤通过定义2和定义3, 根据信任票证中 $Sdate, Fdate, Scount, Fcount$ 的值分别计算结点 $Client$ 和结点 $Server$ 的相对信任等级。然后根据定义5生成得到各自的访问控制策略。

⑥ $Client$ 和 $Server$ 轮流交换访问控制策略和数字证书来完成对请求资源 S 的协商。若最后能满足 S 的访问控制策略, 则进入步骤⑦; 否则进入步骤⑧。

⑦ $Server$ 向 $Client$ 披露请求资源 S , 协商成功, 进入步骤⑨。

⑧协商失败, 进入步骤⑨。

⑨ $Server$ 根据协商的结果, 更改信任票证中的内容, 并重新生成资源 S 的信任票证, 发送给 $Client$, 协商结束。

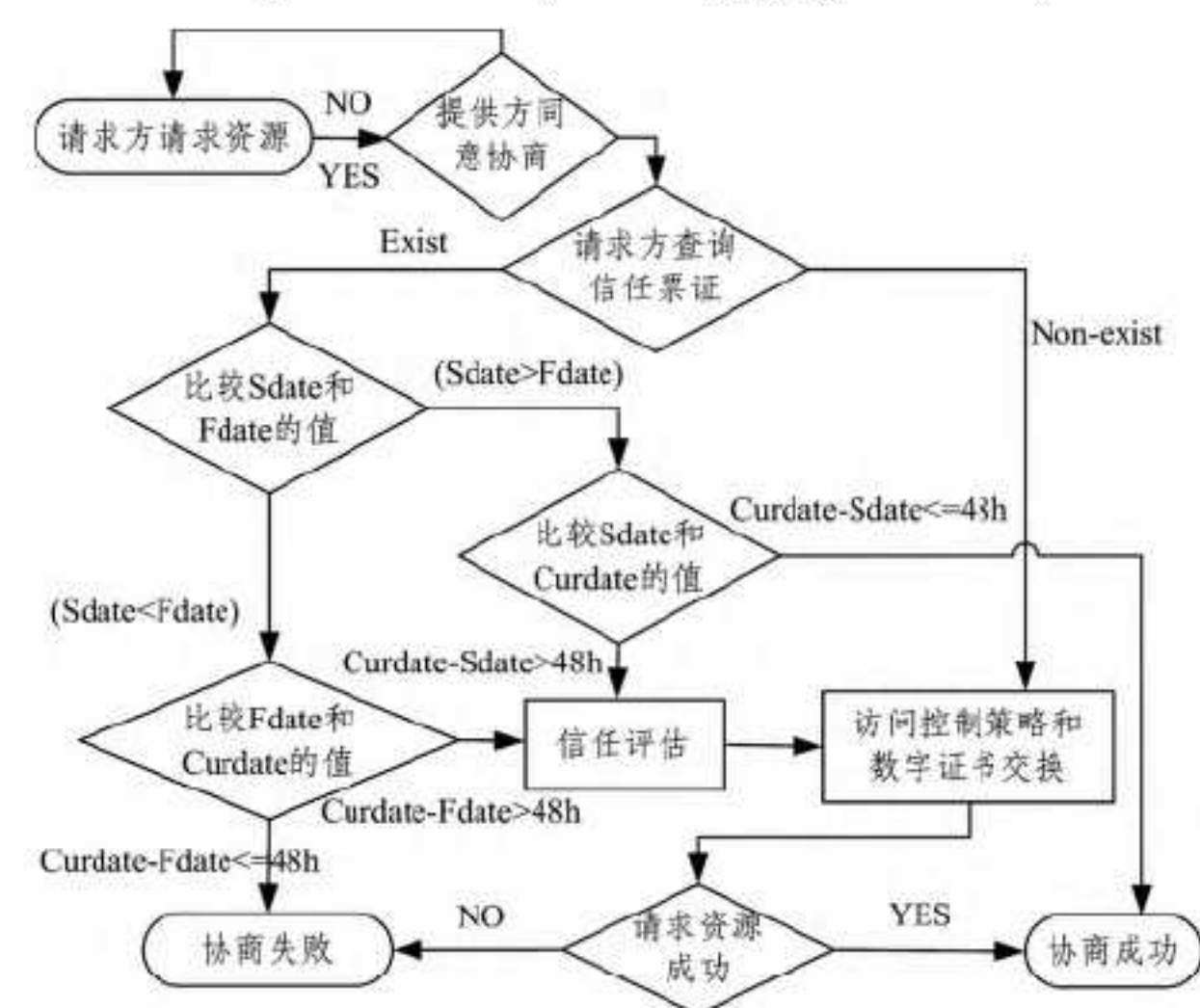


图3 协商流程

4.2 信任票证分析

信任票证中数字签名的加密采用公钥机制, 私钥固定且只能由自己独有, 与私钥对应的公钥通过本人进行公开。当协商结束后, 资源拥有者为资源请求者颁发信任票证时, 它首先用 hash 函数生成票证的摘要, 然后利用私钥对摘要进行加密生成数字签名, 最后将这个签名附在信任票证后发送给资源请求者。在协商过程中, 资源拥有者收到资源请求者发送的信任票证时, 首先接收方取下数字签名, 用自己的公钥解密得到摘要, 以此核实该文件是否由自己颁发, 然后对票证中除

签名以外的内容用 hash 函数计算,得到另外一份摘要,通过与收到摘要对比来确定信任票证是否被修改。这样既能保证信任票证不会被伪造,也能保证信任票证不会被修改,确保了信任评估模块中数据的正确性。

4.3 拒绝服务攻击

拒绝服务攻击 (Denial of Service, Dos) 主要是攻击者利用合理的服务请求来占用过多的服务资源,从而使合法用户无法得到相应的服务。自动信任协商中,服务请求者向资源提供者请求资源,由于缺乏提供有效的数字证书,协商最终以失败结束,然而请求者可以继续请求该资源,服务提供者需要在此花费大量时间拒绝请求者。恶意结点可以利用协商的上述不足对资源提供者做 Dos 攻击,使提供者需要暂用大量的计算资源和时间来处理该结点的请求,甚至造成服务方的崩溃。提出的信任票证中,有一条负责记录上一次协商失败时间的信息。在此模型中,某次服务请求失败后,规定在 48h 之内该请求者不能再次请求该服务,否则提供方直接拒绝该服务请求,并重新记录失败时间。所以,新的模型能有效地解决原有自动信任协商中存在的恶意结点 Dos 攻击的问题。

4.4 仿真实验

实验选择了 TrustBuilder2 作为仿真平台,实验环境如表 1 所列。

表 1 实验环境

机器配置	操作系统	Window 8
	CPU	2.67GHz Q8400
	内存	2G
开发语言	JAVA	
运行平台	TrustBuilder2	

由于协商过程中,信任票证的交换和验证与数字证书类似,因此实验中把信任票证看成一种特别的数字证书,其交换与验证的总时间与一张数字证书相同。实验模拟了 200 组自动信任协商,证书库中包含 5 对本地证书集,每对证书集中分别包含了 4 个左右的数字证书和一个资源,其访问控制策略根据定义 1 随机生成。协商时,协商双方随机从证书库中抽取一对证书集和对应的访问控制策略作为协商时的数字证书和访问控制策略。每半分钟模拟一次协商,实验结果记录了每次协商所消耗的时间,为了与传统的自动信任协商做比较,实验记录了在相同环境下未利用协商历史的自动信任协商每次协商所消耗的时间。图 4、图 5 分别显示了历史披露序列有效期为 3 分钟和 5 分钟时(在实验模拟中发现,信任票证直接使用有效期小于 3 分钟时,信任票证不可直接使用),基于信任评估和信任票证的自动信任协商与传统的自动信任协商的协商时间(单位为 ms)。

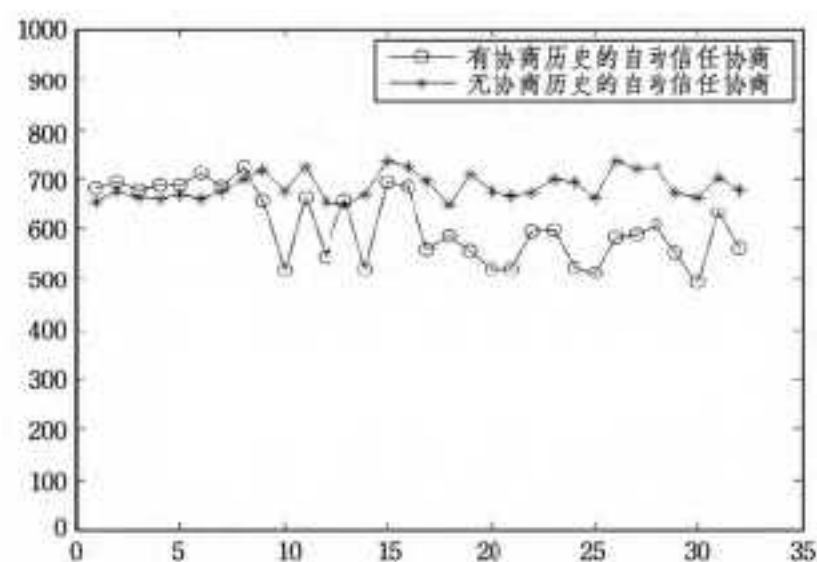


图 4 信任票证可直接使用

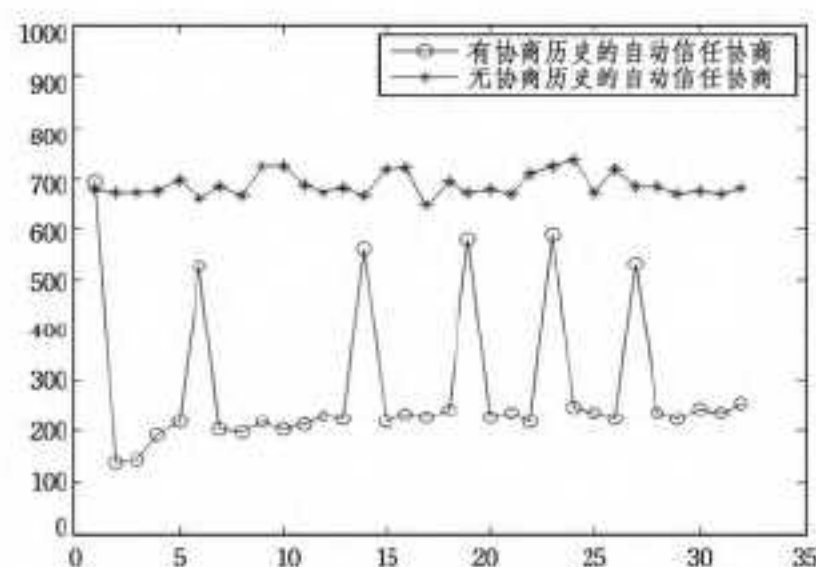


图 5 信任票证不可直接使用

由图可知,带星号的折线表示传统的自动信任协商的协商时间分布,由于每次协商过程中进行数字证书选择和匹配的时间差异,因此造成了每次的协商时间都不完全相同,然而可以看到时间大致稳定在一个范围内,带圈的折线表示基于信任评估和信任票证的自动信任协商,由于在每次协商前都需要检索信任票证,导致了除协商时间外,整个过程还需要额外的时间消耗,因此可以发现某些协商的时间大于传统协商的时间。然而,协商历史的加入减少了协商次数,进而降低协商的时间,所以结果中出现了多次协商时间远小于传统时间的情况。

通过观测实验结果发现,协商的成功率大约在 80% 左右。通过计算协商的平均时间,在信任票证不可直接使用仅利用信任评估的协商中, $Aver(Exist-H) = 559.8ms$, $Aver(non-Exist-H) = 686.2ms$ 。信任票证不可直接使用时,通过利用协商历史信息对协商双方做信任评估,自动信任协商的整体协商时间相对于不利用协商历史的自动信任协商的整体协商时间缩短了 8.1%,证明了该模型中加入信任评估模块后相对于 Trust-X 框架的优势。在信任票证可直接使用且利用信任评估的协商, $Aver(Exist-H) = 286.6ms$, $Aver(non-Exist-H) = 688.0ms$,利用协商历史的自动信任协商的整体协商时间相对于不利用协商历史的自动信任协商的整体协商时间缩短了 41.6%,证明了该模型较传统协商模型对协商效率有大幅度提升。实验结果如表 2 所列,其中历史披露序列的有效期与协商频率有关,在实际应用中,规定其为 48h。

表 2 实验结果

	信任票证可直接使用	信任票证不可直接使用
不利用协商历史的 ATN	686.2ms	688.0ms
利用协商历史的 ATN	559.8ms	286.6ms
效率提升	8.1%	41.6%

结束语 本文针对协商效率和安全问题提出了一种新的自动信任协商模型,通过将直接使用信任票证和利用历史协商信息做信任评估两种方法相结合来加快协商的速度。利用 Trustbuilder2 框架进行实验,证明了提出的模型是高效的。同时,新的模型还可以利用记录协商失败的时间来防止恶意结点的拒绝服务攻击。

参考文献

- [1] Winsborough W H, Seamons K E, Jones V E. Automated trust negotiation[C]//Proceedings DARPA Information Survivability Conference and Exposition, 2000(DISCEX'00). IEEE, 2000, 1: 88-102P

(下转第 392 页)

分簇₃中节点₂₁、节点₂₄和节点₂₇同时作为恶意节点,发动攻击强度 $\delta=0.2$ 的On-Off攻击,3个节点均在每3个时间片的正常通信后在一个时间片内发送错误数据。其正常数据和合谋异常数据的基准云校验值和综合信任值如图5所示。

由图5可知,本文所提的基准云校验对于多个节点的合谋攻击有一定的误差,以节点₂₇为例,该校验并不能较准确地区分正常数据和异常数据,而综合信任值依然可以准确地将同簇内的多个异常节点准确地检测出来。基准云校验作为初步信任评估手段,准确性较差,计算复杂度较低,而综合信任值计算可以进一步地对节点的通信行为进行评价,但是相应的计算复杂度较高,对簇头节点的计算能力有一定要求。二者相结合可以形成对WSN节点的双重信任评价方案,可以根据实际需求对这两重评价手段进行不同程度的侧重来兼顾评价的准确性和实时性。

结束语 本文针对分簇WSN同簇节点采集数据的空间相关性和时间相关性,基于隶属云理论提出一种基于信任反馈云模型的WSN节点信任评价方案,构建了双重信任评价体系,利用轻量云模型进行基准云校验,基准云依据反馈的历史综合信任值进行动态更新,该校验计算复杂度低但准确度较低,除基准云校验外,由节点自身信任和邻近节点信任融合成的综合信任值可以更为准确地反映节点的通信行为可信程度。二者结合构成的双重信任评价体系可以根据外界环境变化调整隶属云模型,并实时准确地检测单节点异常和多节点合谋攻击。所提的评价方案是基于采集数据驱动的,基准云校验和信任计算均在簇头节点完成,簇头节点的计算资源需求较大,对于各成员节点间的数据转发行为并未予以考虑,下一步的研究工作为对于成员节点间有转发行为的WSN网络结合信任反馈隶属云模型进行信任评价研究。

参 考 文 献

- [1] 荆琦,唐礼勇,陈钟. 无线传感器网络中的信任管理[J]. 软件学报,2008,19(7):1716-1730
- [2] 邵斐. 基于模糊综合评判的主观信任模型研究[J]. 通信技术,2009,42(12):98-100

- [3] 王建新,张亚男,王伟平,等. 移动自组网中基于声誉机制的安全路由协议设计与分析[J]. 电子学报,2005,33(4):596-601
- [4] Ganeriwal S, Balzano L K, Srivastava M B. Reputation-based framework for high integrity sensor networks[J]. ACM Transactions on Sensor Networks(TOSN),2008,4(3):15
- [5] 马守明,王汝传,叶宁. 基于信誉度集对分析的WSN安全数据融合[J]. 计算机研究与发展,2011(9):1652-1658
- [6] 肖德琴,冯健昭,周权,等. 基于高斯分布的传感器网络信誉模型[J]. 通信学报,2008,29(3):47-53
- [7] 刘涛,熊焰,黄文超,等. 一种基于Bayes估计的WSN节点信任度计算模型[J]. 计算机科学,2013,40(10):61-64
- [8] 刘涛,关亚文,熊焰,等. 无人值守WSN中一种具有激励机制的信任管理模型[J]. 武汉大学学报:理学版,2013(6):578-582
- [9] Hongjun D, Zhiping J, Xiaona D. An entropy-based trust modeling and evaluation for wireless sensor networks[C]// International Conference on Embedded Software and Systems(ICESS'08). IEEE,2008:27-34
- [10] 马彬,谢显中. 无线传感器网络云信任模型[J]. 计算机科学,2010,37(3):128-132
- [11] 蔡绍滨,韩启龙,高振国,等. 基于云模型的无线传感器网络恶意节点识别技术的研究[J]. 电子学报,2012,40(11):2232-2238
- [12] 徐晓斌,张光卫,王尚广,等. 基于轻量云模型的WSN不确定性信任表示方法[J]. 通信学报,2014,35(2):63-69
- [13] 徐晓斌,张光卫,王尚广,等. 基于群体信任的WSN异常数据过滤方法[J]. 通信学报,2014,35(5):108-117.
- [14] 李德毅,孟海军. 隶属云和隶属云发生器[J]. 计算机研究与发展,1995,32(6):15-20
- [15] 李德毅,刘常昱. 论正态云模型的普适性[J]. 中国工程科学,2004,6(8):28-34
- [16] 冯清青,李弄野. 无线传感器网络节点分簇与非分簇性能比较[J]. 计算机应用研究,2009(11):4244-4247
- [17] 李捷,韩志杰. 一种基于预测的WSN非均衡分簇路由算法[J]. 计算机研究与发展,2010(8):1459-1465
- [18] <http://db.lcs.mit.edu/labdata/labdata.html>
- [19] Sun Y L, Han Z, Liu K J R. Defense of trust management vulnerabilities in distributed networks[J]. Communications Magazine, IEEE,2008,46(2):112-119

(上接第381页)

- [2] Winslett M. An introduction to trust negotiation [M]// Trust Management, Springer Berlin Heidelberg,2003:275-283
- [3] Harrison M A, Ruzzo W L, Ullman J D. Protection in operating systems[J]. Communications of the ACM,1976,19(8):461-471
- [4] Bell D E, LaPadula L J. Secure computer systems: Mathematical foundations[R]. Mitre Corp Bedford MA,1973
- [5] Ferraiolo D, Kuhn D R, Chandramouli R. Role-based access control[M]. Artech House,2003
- [6] Sandhu R S, Coyne E J, Feinstein H L, et al. Role-based access control models[J]. Computer,1996,29(2):38-47
- [7] Blaze M, Feigenbaum J, Lacy J. Decentralized trust management [C]// Proceedings. ,1996 IEEE Symposium on Security and Privacy,1996. IEEE,1996:164-173
- [8] Bertino E, Ferrari E, Squicciarini A C. Trust-𝒳;: a peer-to-peer framework for trust establishment[J]. IEEE Transac-

- tions on Knowledge and Data Engineering,2004,16(7):827-842
- [9] Liu B, Lu H. A peer-to-peer framework for accelerating trust establishment[C]// International Conference on Multimedia Information Networking and Security,2009 (MINES'09). IEEE,2009,1:135-139
- [10] Liu B, Lu H, Zhao Y, et al. A Framework: Trust Establishment for E-services[C]// International Conference on e-Education, e-Business, e-Management, and e-Learning,2010 (IC4E'10). IEEE,2010:141-145
- [11] Jianli L. Multi-negotiation targets in Automated Trust Negotiation over TrustBuilder framework[C]// 2012 8th International Conference on Computing Technology and Information Management(NCM and ICNIT). 2012,1:101-105
- [12] 廖振松. 虚拟组织中自动信任协商研究[D]. 武汉: 华中科技大学,2008