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人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。本文提出了一种新的协商模型，将信任建立在信任的双方，信任评估模块用于评估结点的互信评级。根据模型，首先判断双方是否存在直接可用的信任评估，若存在，则直接通过验证信任建立信任；若无直接可用的信任评估，则先建立信任，然后通过验证信任建立信任。在协商过程中，协议提供了有效的协商手段，提高了协商效率。试验结果表明，本协议能够有效地提高系统的安全性，为服务端上的安全攻击提供了有效的防护。

关键词 自动信任协商，信任评估，信任安全，协商安全，协商效率

中图分类号 TP393.08 文献标识码 A

Security and Efficiency Negotiation Model

LI Jianli, 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, so that contradictory situations make safety and efficiency become the main concerned 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, firstly query if there is available trust file to be directly used. If it exists, verify if 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 negotiation. 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, it is able to protect negotiation form 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交换信任建立信任的一种访问控制方法。本文提出了一种自动信任协商模型，自动信任协商模型，首先判断双方是否存在直接可用的信任评估，若存在，则直接通过验证信任建立信任；若无直接可用的信任评估，则先建立信任，然后通过验证信任建立信任。在协商过程中，协议提供了有效的协商手段，提高了协商效率。试验结果表明，本协议能够有效地提高系统的安全性，为服务端上的安全攻击提供了有效的防护。
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授权问题。在此基础上，提
出了一种高效率且安全的协商模型。

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
的生成过程，具体如下定义。

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，假定证书序列可以
描述为：(1) C_{\text{ClientCreds}} = C_{0}, C_{1}, ..., C_{m}, 其中
n \in \mathbb{N}, 有 C_i \subseteq ClientCreds, C_{m} \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。此次协商的证书请求序列如下：

3 协商模型

Winsborough 等人在提出自动信任协商的同时，对协商
模型也进行了描述。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
储存储拥有者的本地数字证书，一个 CAP 库，用来跟踪对方需
要提供的数字证书，以解密其保护的本地证书，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，协商方认为所
有的访问控制策略都不可以传递。因此，协商模型由协商安全代理、数字证书库和访问控制策略库。

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 = 
(R_{\text{Issuer}}, S_{\text{Issuer}}, F_{\text{Issuer}}, \text{Count}, \text{Fcount}, \text{Sig})，其中 R_{\text{Issuer}} 表示的是被
请求的资源，S_{\text{Issuer}} 表示的是关于资源 R_{\text{Issuer}} 上一次协商成功时
的时间，若两结果没有成功的协商历史，则 S_{\text{Issuer}} 的值为 0。F_{\text{Issuer}} 表示的是关于资源 R_{\text{Issuer}} 上一次协商失败时的时间，若两
结果没有失败的协商历史，则 F_{\text{Issuer}} 的值为 0。\text{Count} 表示的是关于资源 R_{\text{Issuer}} 成功的总协商次数，若两结果没有成功的协商
历史，则 \text{Count} 的值为 0。\text{Fcount} 表示的是关于资源 R_{\text{Issuer}} 失败的
总协商次数，若两结果没有失败的协商历史，则 \text{Fcount} 为
0。\text{Sig} 表示的是该信任票证的数字签名。

资源提供方为资源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 k 和 k^{-1} 表示，它们可以
相互用于加密和解密。

(1) 加密函数 BEM_{\text{Issuer}} = En\left(M\text{ess}, E\text{key}\right)

用加密密钥 E\text{key} 对信息 M\text{ess} 进行加密，返回密文
BEM。M\text{ess} 表示的是未加密的信息签名。

(2) 解密函数 M\text{ess} = De\left(BEM, E\text{key}\right)

用解密密钥 E\text{key} 对密文 BEM 进行解密。当且仅当解
密密钥 E\text{key} 与生成密文 BEM 的加密密钥 E\text{key} 是一对时，
返回被加密的信息 M\text{ess}。否则无法对 BEM 进行解密。

对 M\text{ess} 解密后，Sig 满足 Sig = En\left(M\text{ess}, E\text{key}\right)。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环
境代理中，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，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资源的
协商历史信息，在协商过程中，可以通过该信任票证来加
快协商的速度，以及通过该信任票证中的信息来加快协
商的速度。

3.2 信任评估模块

(1) 信任票证中记录了协商方双方对某一资源的协商次数
和协商失败次数，协商成功率表明协商方双方曾经拥有访问资
源需要的全部数字证书，可以认为协商方成功次数越多，协
商方对协商方的信任，即协商方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，证书之
间环形依赖，协商方协商策略不一致等情况的发生，则可以认
为协商方失败次数越多，协商方对协商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方双方的信任等级进行评估，同时，由于信任的动态性，即使信任随着时间的推移而衰减，在进行评估时，还考虑了时间对双方信任关系的影响。

对于信任票证的使用有效期，借鉴了 TrustX 框架中对信任票证有效期的定义，规定为 
\begin{align*}
\text{Validity} = n - t,
\end{align*}
其中，n 为信任票证不可使用有效期，t 为信任票证使用信任评估模块，评估方法如下：
定义 2 $T_{wu}$ 表示当前协商的起始时间，$T_{wu}$ 表示上次协商失败的时间。$\delta(T_{wu}, T_{ru})$ 表示协商时衰减系数。当 $T_{wu} - T_{ru} \leq 48h$ 时，满足 $\delta(T_{wu}, T_{ru}) = 1$，当 $T_{wu} - T_{ru} > 48h$ 时，满足 $\delta(T_{wu}, T_{ru}) > 0$，所以时间衰减系数满足：

$$\delta(T_{wu}, T_{ru}) = \frac{1}{1 + \frac{48}{T_{wu} - T_{ru}}}$$

定义 3 协议节点 A 和协商节点 B 的 $\lambda_s$ 表示节点 A 对节点 B 的初始信任等级，$\lambda_s$ 表示节点 B 对节点 A 的初始信任等级。信任证书中记录的节点 A 对节点 B 资源成功的协商次数为 $\tau_1$，失败的协商次数为 $\tau_2$。则经过评估模型评估后，节点 A 对节点 B 的信任度 $\lambda_A$ 满足 $\lambda_A = a \delta_{\tau_1}/(\tau_1 + \tau_2) - (1-a) \tau_1/(\tau_1 + \tau_2) + \lambda_s$，节点 B 对节点 A 的信任度 $\lambda_B$ 满足 $\lambda_B = a \delta_{\tau_2}/(\tau_1 + \tau_2) - (1-a) \tau_2/(\tau_1 + \tau_2) + \lambda_s$。

3.3 访问控制策略生成

在基于 X.509 的数字证书形式中，证书中没有包含描述证书权益者的属性信息，因此如何在协商过程中反映协商双方信任关系对于数字证书披露的影响成为本节需要考虑的问题。在自主信任算法中，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反映信任关系变化的管理过程的影响。

定义 4 对于任意的策略 $\mathcal{P}$，其形式可转换为 $e^{-\mathcal{P}} = E_1 \cdot V \cdot \ldots \cdot V_n$，其中 $E_i = S_1 \ldots \cdot S_n$ 表示 $\mathcal{P}$ 的一个子句，$S_i$ 表示 $\mathcal{P}$ 中的一个子策略。

定义 5 数字证书对请求者的相对敏感度越高，对于保护该证书的访问控制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 $p_j$，则子句数为 $1$，则访问控制策略被满足的概率为 $P = \prod \limits_{i=1}^{m} p_j$，可知子句中元策略个数 $m$ 越大，则 $P$ 越小，表明该策略保护的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 $P = \prod \limits_{i=1}^{m} p_j$，可知子句中元策略个数 $m$ 越小，则 $P$ 越小，表明该策略保护的证书相对请求者越敏感。

定义 6 假设访问控制策略 $\mathcal{P}$，子句中的元策略个数为 $P$，子句个数为 $P_{num}$，是节点认为与保护资源相关的证书数量，则 $\mathcal{P}$ 与数字证书满足的关系为 $P \cdot P_{num} \in \{0, N \} \cdot P_{num} \cap \{0, A \}$。经过认证评估后，资源相对请求者的信任等级为 $\Delta k(0 \leq k \leq 4)$，根据定理 1，满足 $P \cdot P_{num} \in \{0, N \} \cdot P_{num} \cap \{0, A \}$ 同时证书的策略满足 $e^{-\mathcal{P}} = E_1 \cdot V \cdot \ldots \cdot V_n$，当子句数 $m$ 越大，则 $P$ 越小，表明该策略保护的证书相对请求者越敏感。

4 模型分析

4.1 协商流程

分布式环境中的陌生节点 Client 和 Server，节点 Client 向节点 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

   ① ② ③ ④ ⑤ ⑥ ⑦ ⑧ ⑨ ⑩ ⑪ ⑫ ⑬ ⑭ ⑮ ⑯ ⑰ ⑱ ⑲ ⑳ 321

把当前的时间作为 $\text{CardDate}$ 同一天发送。Server 收到该消息后询问 Client 是否已经做好协商准备，同时询问 $\text{Client}$ 是否拥有请求资源 $S$ 的有效信任信息。

2. Client 根据请求资源查询自己的信任证书库，若存在与请求资源对应的信任信息，则把该信任信息发送给 Server，否则立即进入步骤 ⑦。

3. Server 收到 Client 关于请求资源 $S$ 的信任信息后，若信任证书签名 $\text{Sig}$ 的有效性，若 $\text{Sig}$ 是有效的，进入步骤 ⑤，否则进入步骤 ⑦。

4. Server 检查信任证书中 $\text{Sdate}$ 和 $\text{Fdate}$ 的值，若 $\text{Sdate} < \text{Fdate}$ 或者 $\text{CardDate} < \text{Sdate}$ 且 $(\text{CardDate} - \text{Sdate}) < 48h$，则进入步骤 ⑤，否则进入步骤 ⑧。

5. 若 $(\text{Fdate} - \text{Sdate}) < 48h$ 且 $(\text{CardDate} - \text{Fdate}) < 48h$，则进入步骤 ⑤。

6. 通过定义 2 和定义 3，根据信任证书中 $\text{Sdate}$、$\text{Fdate}$、$\text{ScoutCount}$、$\text{Count}$、$\text{Count}$ 的值分别计算节点 Client 和节点 Server 的相对信任等级，然后根据定义 5 生成得到各节点的信任信息。

7. Client 和 Server 之间的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 $\text{S}$ 的访问控制策略，则进入步骤 ⑤，否则进入步骤 ⑩。

8. Server 向 Client 披露请求资源 $S$ 的协商情况，进入步骤 ⑪。

9. 协商失败，进入步骤 ③。

10. Server 给出协商的结果，更改信任证书中的内容，并生成请求资源 $S$ 的信任证书，发送给 Client，协商结束。

4.2 信任证书分析

信任证书中数字签名的加密采用公钥机制，私钥固定且只能由自己拥有，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发送信任证书时，它首先对 hash 函数生成证书的摘要，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证书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证书时，首先接收方提取数字签名，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，然后对证书中除
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被修改过, 这样就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) 是指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发送请求, 由于缺乏提供有效的数字证书, 会athing 目标被拒绝, 甚至会导致协商失败。如果请求者可以获取请求该资源, 服务提供者需要在此次花费大量时间拒绝请求者。恶意攻击者可以利用这一特性, 不足对资源提供者做 DoS 攻击, 使其需要重新获取大量的计算资源和时间来处理该攻击, 造成服务失败。据前, 提出的信任评估模块中, 有一条负责记录上一次协商失败时间的信息。在模型中, 某些服务请求失败后, 在规定时间内该请求者不能再次请求该服务, 否则提供方会直接拒绝该服务请求, 并重新记录失败时间。所以, 新的模型可以有效地解决现有自动信任协商中存在的潜在问题 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。

<table>
<thead>
<tr>
<th>表 1 实验环境</th>
</tr>
</thead>
<tbody>
<tr>
<td>操作系统：Windows 8</td>
</tr>
<tr>
<td>CPU：2.67GHz Q4608</td>
</tr>
<tr>
<td>内存：2G</td>
</tr>
<tr>
<td>开发语言：JAVA</td>
</tr>
<tr>
<td>运行平台：TrustBuilder2</td>
</tr>
</tbody>
</table>

由于协商过程中, 信任票证的交换和验证与数字证书相似, 因此实验中把信任票证看作一种特别的数字证书, 其交换与验证的总时间与数字证书相同, 实验模拟了 200 组自动信任协商。因本地证书库中包含 5000 个本地证书, 每个证书集中分别包含了 4 个证书, 其中的数字证书和一个资源, 其访问控制策略具有定义, 按照初始化, 协商时, 协商双方随机从证书集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, 包括与信任票证的协商, 包括利用自动信任协商的时间, 实验记录了在相同环境下利用自动信任票证的自动信任协商每分钟所消耗的时间。图 4、图 5 分别显示了历史备份序列的时序图, 以及每分钟所消耗的时间。在实验过程中, 信任票证直接使用效率小于 3 分钟, 信任票证不可直接使用, 基于信任评估的自动信任票证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信任投票票证的协商效率, 由于协商过程中对数字证书的引用和匹配的时序差异, 因此造成了每次的协商时间都不完全相同, 而图中星号的折线表示基于信任评估和信任票证的自动信任协商, 由于在协商阶段需要检查信任票证, 导致了协商时间的不一致性。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, 从而降低协商的效率, 所以结果中出现了多次协商时间远小于传统协商的时间。

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时利用信任评估的协商中, Aver (Exist-H) = 559.8ms, Aver (non-Exist-H) = 688.2ms。信任票证不可直接使用时, 利用信任票证的协商中, Aver (Exist-H) = 286.8ms, Aver (non-Exist-H) = 688.0ms。利用信任票证的自动信任协商的耗时平均时间为 41.6%。证明了该模型在加入信任评估模块和对协商效率有大幅度提升。实验结果如表 2 所列, 历史备份序列的有效期与协商效率有关。在实际应用中, 规定其为 48h。

<table>
<thead>
<tr>
<th>表 2 实验结果</th>
</tr>
</thead>
<tbody>
<tr>
<td>信任票证可直接使用</td>
</tr>
<tr>
<td>利用信任票证的协商, Aver (Exist-H) = 286.8ms, Aver (non-Exist-H) = 688.0ms</td>
</tr>
<tr>
<td>效率提升</td>
</tr>
</tbody>
</table>

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效率。利用 TrustBuilder2 框架进行实验, 证明了提出的模型是有效的。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攻击。
分段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 $a=0.8$ 的 On-Off 攻击, 3 个节点在每 3 个时间段的正常通信信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评估值如图2 所示.

由图2 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, 该节点虽然不能被准确
地判断出正常数据和异常数据, 而合谋给定值仍然可以准确地
检出这几类异常节点的可信评估值也通过图2 所示, 基准云校验作为
的初步可信评估手段, 准确度较好, 计算复杂度较低, 且综合
信頼值计算可以进一步地对每个节点的可信行为进行评估, 以不相
应的计算复杂度较高, 对其节点的计算能力有一定要求.

二者的结合可以形成对WSN 节点的可信度评估方案, 可
以根据实际需求对这两类评估手段进行不同程度的侧重来兼
顾评价的准确性和实时性.

结束后, 本文针对分布式WSN 同轴节点采集数据的空
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传
播的WSN 节点信任评价方案, 建构了双重信任评估系
统, 利用零信任模型进行基准云数据, 基准云数据的准确度
综合信任评估进行动态更新, 该模型计算复杂度低但准确度
率, 基准云校验, 由节点自身信任和邻居节点之间共同
的综合评估体系更为准确地反映节点的可信行为可控制.

二者的结合可以形成对WSN 节点的可信度评估体系, 可
以根据实际需求对这两类评估手段进行不同程度的侧重来兼
顾评价的准确性和实时性.

参考文献

[1] 斛琦, 留礼平, 陈仲, 无线传感器网络中的信任管理[J]. 传感
学报, 2008, 18(7): 1716-1730
[2] 邵宾, 基于模糊综合评价的主观信任模型研究[J]. 通信技术,
2009, 42(12): 98-100

[3] 王长新, 张亚鹏, 王伟平, 等, 移动自组织网络基于声誉机制的分析
framework for high integrity sensor networks[J]. ACM Transac-
tions on Sensor Networks(TOSN), 2008, 4(3): 15
[5] 马守明, 王建武, 丁时平, 基于信任度的邻居节点的WSN 信
[6] 肖德华, 冯晓华, 张勇, 等, 基于模糊控制的网络信任模型研
[7] 刘沁, 王培, 陈建超, 等, 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): 61-66
[8] 刘沁, 陈建超, 等, 无源通信WSN 中一种具有激励机制的
信任管理模型[J]. 武汉大学学报, 2013, 6: 578-582
[9] Houwang D, Zhigang X, Xiaodong D. An entropy-based trust modell-
ing and evaluation for wireless sensor networks[C]// International
Conference on Embedded Software and Systems (ICESS' 05), IEEE,
2008, 27-31
[10] 马影, 崔晓勇, 无线传感器网络信任模型[J]. 计算机科学,
2010, 37(3): 128-132
[12] 徐晓斌, 王光卫, 王长武, 等, 基于信任模型的WSN 不确定性
[13] 徐晓斌, 王光卫, 王长武, 等, 基于信任模型的WSN 不确定性
[14] 李志杰, 瞿军, 道德威慑和伦理等值的计算[J]. 计算机研究与发
展, 2005, 45(2): 15-20
[16] 冯清, 李东明, 轨迹模型的特征值[J]. 计算机研究与发
展, 2005, 45(2): 15-20
rabilities in distributed networks[J]. Communications Maga-
azine, IEEE, 2008, 46(2): 112-119

(上接第 381 页)

foundations[R]. Mitre Corp Bedford, MA, 1973
control[M]. Artech House; 2003
[C]// Proceedings, 1996 IEEE Symposium on Security and Pri-
[8] Berrino E, Ferrari E, Squicciarini A C. Trust- & Xacr: 1, 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 es-
tablishment[C]// International Conference on Multimedia Infor-
mation Networking and Security, 2009 (MINES' 09). IEEE,
2009, 1: 135-139
for E-services[C]// International Conference on e-Education, e-
Business, e-Management and e-Learning, 2010 (ICE’ 10). IEEE,
2010: 141-145
tion over TrustBuilder framework[C]// 2012 8th International
Conference on Computing Technology and Information Manage-
ment(NCM and ICNIT), 2012, 1: 105-105