一种基于模糊策略的自动信任协商方案

马小信 曾国荪

(同济大学计算机科学及技术系 上海 201804)

(国家高性能计算机工程技术中心同济分中心 上海 201804)

摘 要 自动信任协商是一种在开放网络环境下陌生实体之间通过披露属性证书建立双方信任关系的重要手段。针对传统信任协商中协商规则描述较为严格、协商成功率和效率较低的问题,提出了一种基于模糊逻辑的自动信任协商方案,它通过将模糊逻辑引入信任协商,对信任协商规则进行模糊化处理,可以更简单而灵活地描述协商规则,并由此优化协商路径选择。分析表明,这种协商方案能够在一定程度上提高协商成功率和效率。

关键词 自动信任协商,模糊逻辑,属性证书,协商规则,协商策略

中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.12.047

Scheme of Automated Trust Negotiation Based on Fuzzy Logic

MA Xiao-xin ZENG Guo-sun

(Department of Computer Science and Technology, Tongji University, Shanghai 201804, China)

(Tongji Branch, National Engineering & Technology Center of High Performance Computer, Shanghai 201804, China)

Abstract Automated trust negotiation (ATN) is an important method for establishing the trust between strangers in open network environment by disclosing attribute certificates. Because it is difficult to use tranditional trust negotiation to describe the credential access control policies and establishing the trust is inefficient, a fuzzy logic-based scheme was proposed. By modeling the credential access control policies in fuzzy logic formula, the description will be more concise and flexible, and negotiation path will be optimized. The analysis shows that efficiency and success rate of this negotiation scheme can be improved to some extent.

Keywords Automated trust negotiation, Fuzzy logic, Attribute certificate, Negotiation rule, Negotiation strategy

1 引言

近年来,随着计算机网络技术的迅猛发展,越来越多的新兴开放计算模式,如网格计算、普适计算、对等计算、协同计算、云计算等,取代了传统封闭集中式的计算模式。基于网络的服务,包括电子商务、社交网络、微博、网上银行等,因其方便快捷的用户体验,被人们广为接受。与传统计算模式相比,在开放的计算模式和服务中,参与交互的实体之间往往完全陌生,故无法通过基于身份的认证系统保护自身的安全与隐私。这类分布式系统无法严格确定和控制参与实体的行为,增大了协同交互的风险。自动信任协商(Auto Trust Negotiation)能够自动为陌生实体之间建立起一定信任关系,以降低交互中存在的大量不确定、不可控、信息不完备等因素的影响,在一定程度上提高了系统的安全性和可靠性。

自动信任协商的本质是通过交互证书逐步披露参与者的隐私信息来建立信任关系的,因此披露证书的方式会极大影响信任协商的成功率和效率。传统的提高信任协商性能的途径之一是改进信任协商策略。信任协商策略(Trust Negotiation Strategy)是协商双方在建立信任关系中所采取的暴露证书和访问规则的方式,包括如何开始协商、暴露证书和访问规则的时机和判断协商何时终止,是自动信任协商研究的核心内容之一。经典的信任协商策略包括积极策略(Eager Strategy)与谨慎策略(Parsimonious Strategy)[1]。两者均由 W. H. Winshorough 等人首次提出,采取了贪心的思想,前者尽可能暴露可公开的证书以推进协商进行,但会暴露大量与协商无关的证书;后者则尽量少暴露证书,保护了部分隐私信息,但协商交互次数过多,且具有不可控性,协商往往不能成功或成本过高。Seamons 等人在此基础上引入了策略图,并提出了两种策略:RCS 策略(Relevant Credentials Set Strategy)和 ARP 策略(All Relevant Policis Strategy)[2],它们分别是积极策略和谨慎策略的发展。在此基础上,Yu 等人提出了一种基于策略搜索树的策略 PRUNES(Prudent Negotiation Strategy),基本思想是按深度优先方式对证书披露序列空间进行搜索,其通信复杂度为 $O(n^2)$,计算复杂度为 $O(nm)$,其中 m 为双方拥有的访问规则数量,n 为双方拥有的信任证书数目。此外,还有基于信任对象图(Trust Target Graph)的协商策略[4]、基于披露树(Disclose Tree)的协商策略[5]、基于协商树(Negotiation Tree)的协商策略[6]、基于契约(Contract)的协商策略[7]以及基于保护树(Protection Tree)的协商策略[8]等。

到稿日期:2014-11-26 返修日期:2015-02-02

马小信(1990—),男,硕士生,主要研究方向为网络安全、内容信任,E-mail:maxiaoxin2014@sina.com;**曾国荪**(1964—),男,博士,教授,博士生导师,CCF 高级会员,主要研究方向为异构计算、并发理论与并行处理、网格计算。

可以看出，传统的信任协商方案对协商性能的改进着重于如何建立一种更高效的协商策略，忽略了协商规则本身对协商成功率和效率的影响。事实上，协商规则本身对 ATN 的性能影响是巨大的：一方面，传统的协商规则描述语言过于严格，需要对方严格遵守信任规则，这将导致双方在可能达成共识的情况下因为某些细节不符合约束而延缓协商过程，甚至协商失败；另一方面，协商规则通常较为复杂，参与者很难据此找到较优的交互方式。因此，降低协商规则的复杂度、让协商规则更为灵活，不失为一种可行的解决方案。而作为一种能够模糊描述命题真值的逻辑系统，将模糊逻辑[11]引入自动信任协商能够在一定程度上解决以上问题。

2 模糊信任协商的基本概念

2.1 信任协商中的模糊需求

信任协商是双方（或多方）通过互相披露证书达成某种共识。这一过程的合理性来自于证书包含了证书持有者的隐私信息，即参与者通过不断暴露隐私从而完成信任协商。在传统的信任协商中，协商参与者披露证书前，需要对方先提供严格满足此证书的协商规则的证书集，如果提供的证书不能满足要求，协商就无法继续。因此协商规则的制定，对协商效率和成功率有很大影响。从这个角度上讲，更准确地量化证书所包含的隐私这一模糊的用户属性，意味着协商参与者能够制定出更合理的协商方案，从而提高协商的成功率和效率。

（1）模糊化对成功率的影响：实际协商中某些属性不适合用“真”或“假”的二元逻辑表述，例如商家某一优惠活动的对象是“年龄大于 60 岁的老年人”，而想表达的原始语义是“年龄很大的人”。很显然，10 岁的孩子和 59 岁的老人应该区别对待，对于后者，应酌情放宽限制。因此，模糊地考虑证书属性的满足程度，能够提高协商的成功率。

（2）模糊化对效率的影响：协商参与者在制定协商规则时，本意不一定要求对方满足所有要求，可以适当放宽某些属性的要求。例如医生在检测视力时，往往不要求对方回答正确某一行的全部开口方向，回答正确一个或几个就可以认为满足这一行的视力水平，即协商成功。因此，模糊化对提高协商效率是有帮助的。

另外，模糊量化用户的属性证书也在一定程度上有助于保护用户的隐私信息：在可以选择的情况下，可以尽量披露所含隐私信息较少的证书。综上所述，信任协商中存在大量的模糊现象和模糊需求，因此将模糊逻辑引入信任协商很有必要。

2.2 模糊信任协商的基本过程

本文所提出的信任协商框架与传统的自动信任协商框架基本相同。将传统的自动信任协商（Automated Trust Negotiation，ATN）中的证书、访问规则及协商策略模糊处理后，得到模糊信任协商的基本工作原理，如图 1 所示。

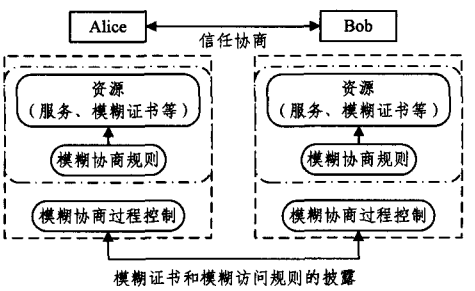

图 1 模糊信任协商的基本工作原理

本文所讨论的模糊信任协商限为两者协商，如图 1 所示，协商参与者为 Alice 和 Bob，他们的地位是对等的。协商参与者分别持有各自的资源（包括目标服务和模糊证书），对资源的合法访问需要满足相应的模糊协商规则。协商双方的协商过程表现为模糊证书及其访问规则的披露，而如何披露则取决于双方所采取的模糊协商策略。同时，模糊协商策略也决定了协商过程如何开始以及何时终止，它极大地影响了信任协商的效率和成功率。

2.3 模糊证书及信任协商规则

从上文讨论可以看出，属性证书是信任协商的核心，其定义如下。

定义 1（属性证书） 又称信任证书，是由权威机构（或称信任证书颁发机构）签名的数字断言，且具有可存储性和可验证性。所有的属性证书的集合可表示为 $C=\{c_1,c_2,\cdots,c_n\}$，其中 $c_i(1\leqslant i\leqslant n)$ 表示单个属性证书。

属性证书包含了协商者的一系列属性，例如一个与协商者身份相关的属性证书可以包含姓名、性别、年龄、居住地址、收入情况等敏感信息。为了方便讨论，本文将属性证书所含信息看成一个整体（即只包含一种属性信息的证书）。对这些信息进行模糊化处理，可以得到模糊属性证书，其定义如下。

定义 2（模糊属性证书） 模糊属性证书是一种属性证书，同时还具有表征证书敏感度及重要程度的隶属度，记为 $c.\lambda$。其中，c 是属性证书，λ 是属性证书隶属度，它表征了属性证书 c 的敏感程度、重要程度。

与传统的属性证书相比，模糊属性证书在此基础上引入了属性证书隶属度 λ，它的取值依赖于属性证书本身的信息及具体的应用场合。例如，一个包含了“用户年收入 30 万元”的属性证书，在贷款买房这一场景下，其隶属度 λ 可以达到 0.8，而“用户年收入 10 万元”的属性证书的隶属度可能只有 0.5。为了方便讨论，本文假定在某一协商过程中，模糊属性证书的隶属度是可以确定的，并且在此期间取值是唯一的。

信任协商中，证书不是无条件披露的，需要满足信任协商规则，信任协商规则定义如下。

定义 3（信任协商规则） 在网络环境中，信任协商的双方为了保护资源或服务（包括受保护的信任证书和协商信任规则等）的存取安全，各自制定的允许访问资源或服务的条件是指导每一步协商进行的规则，也是协商双方最终达成信任的终止准则。

信任协商规则可看作证书集到逻辑真值{1，0}上的一个映射关系。对于仅含单个证书的证书集，它的协商规则可记作 $s\leftarrow c$，其中 s 是受保护的资源和证书，c 是要求对方提供的证书，即当对方披露的证书中包含 c 证书描述的属性时，s 可以被披露。这种仅含单个证书的协商规则称为元信任规则。通过逻辑运算符 $\wedge$、$\vee$、$\neg$ 和括号，可以将元信任规则扩展为更一般的情况。

与传统的信任协商规则类似，模糊化的属性证书也有类似的协商规则，其定义如下。

定义 4（模糊信任协商规则） 模糊协商规则是信任协商规则的推广，记作 $P_s:s\leftarrow f_s(c_1,c_2,\cdots,c_n),\tau$，其中 s 为受保护的资源或证书，$(c_1,c_2,\cdots,c_n)$ 为要求对方提供的模糊证书集，f_s 为作用在该证书集上的模糊逻辑函数，τ 为门限隶属度。当且仅当 $f_s(c_1,c_2,\cdots,c_n)\geqslant\tau$ 时，s 可被合法披露。特别地，当证书集 C 满足 $f_s(C)\geqslant\tau$ 时，称 C 满足协商规则 P_s，记作 $satisfy(P_s,C)$。

在模糊协商规则中，证书不再被看作命题逻辑真值，而用该证书的隶属度 λ 参与计算证书集的模糊逻辑真值。同时，逻辑运算符 $\vee$、$\wedge$ 的语义也相应地变为取大和取小。例如，对于协商规则 $p_s \leftarrow (c_1 \vee c_2) \wedge c_3, \tau=0.45$，证书 c_1, c_2, c_3 对应的隶属度 λ_i 分别为 0.4，0.5，0.6，则此证书集整体的隶属度为 $\min(\max(0.4,0.5),0.6)=0.5 \geqslant 0.45$，因此当对方披露了此证书集后，证书 s 可以被披露。

3 模糊信任协商的协商过程控制方法

3.1 协商过程控制的一般描述

在形式化定义了模糊证书及其协商规则后，可以进一步讨论应当如何进行协商。假设协商参与方分别为 Alice 和 Bob，他们分别持有证书集 C_A 和 C_B。Bob 发起协商，向 Alice 请求资源 R。每个证书或资源有其相应的模糊协商规则。双方在协商过程中不断地轮流披露证书集并请求证书集，直到资源 R 的模糊协商规则满足或者被证明不可能被满足为止，即分别表示协商成功或协商失败。

进一步，假设在协商的某一步中，Alice 已向 Bob 请求的证书集为 $C_{ARequest}$，向 Bob 披露的证书集为 $C_{ADisclosed}$，拒绝向 Bob 披露的证书集为 $C_{ADecline}$，类似地可定义 $C_{BRequest}$、$C_{BDisclosed}$ 和 $C_{BDecline}$。同时，一方需要向另一方进一步索取证书集并披露证书集及其协商规则。并且，在一次协商中，一方向另一方最多请求 $Count_{MaxRequest}$ 个证书，最多披露 $Count_{MaxDisclose}$ 个证书。

在具体协商过程中，协商参与者需要根据双方披露的证书集来决定此时应该向对方请求哪些证书，以及披露哪些证书，即证书的请求准则和证书披露准则。本节将对这两方面具体展开论述。

3.1.1 证书请求准则

在协商开始时，由于目标资源 R 的模糊协商规则 P_R 未满足，此时 Alice 需要根据 P_R 判断向 Bob 请求何种证书。一般地，设协商中 Bob 向 Alice 请求了单个证书 s，其模糊协商规则为 $P_s: s \leftarrow f_s(C), \tau$，那么当 $C_{BDisclosed}$ 满足模糊协商规则 P_s 时，Alice 可以披露证书 s。否则，可以将 $f_s(C)$ 改写为析取式 $f_s(C)=\bigvee_{i=1}^{n}\bigwedge_{j=1}^{m_i} c_{ij}, c_{ij} \in C$，其中，对于证书集 $C_i=\{c_{ij}, 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m_i\}$，$f_s(C_i)$ 的模糊真值 $f_s(C_i)=\bigwedge_{j=1}^{m_i} c_{ij}=\min_{j=1}^{m_i}(\lambda_{ij})$。值得注意的是，若存在证书 $c_{ij} \in C_{BDisclosed}$，有 $\lambda_{ij}<\tau$，或 $c_{ij} \in C_{BDecline}$，那么该合取分支必然无法满足。

由于析取式满足的条件是任意合取支能够满足的，因此可以根据这一性质，进一步讨论 Alice 应当披露哪一个合取支（即向 Bob 请求哪些证书）。一种可行的做法是选择那些看起来容易满足的合取支，即选择 k 个合取支 $f_s(C_1)$，$f_s(C_2)$，…，$f_s(C_k)$，满足 $\forall k<l \leqslant n, |C_i - C_{BDisclosed} - C_{ARequest}| \leqslant |C_k - C_{BDisclosed} - C_{ARequest}|$，即本次协商 Alice 应当向 Bob 请求证书集 $\bigcup_{i=1}^{k} C_i - C_{BDisclosed} - C_{ARequest}$。

3.1.2 证书披露准则

与此同时，在本次协商中，Alice 应当向 Bob 披露证书（如果有可能的话）。设 Alice 可以披露的证书集为 $S=\{s \mid satisty(P_s, C_{BDisclosed})\}$，一方面，模糊证书 s 的隶属度 λ 越高，披露之后越容易满足 Bob 所持证书的协商规则；另一方面，s 距离目标资源 R 的协商请求距离越小，信任协商越容易成功。其中，协商请求距离的定义如下。

定义 5（协商请求距离） 协商请求距离是证书（或资源）c_A 和 c_B 之间请求依赖的一种描述，若存在最短的请求关系链：

$$c_A \xleftarrow{request} C_1 \xleftarrow{request} C_2 \xleftarrow{request} \cdots \xleftarrow{request} C_{n-1} \xleftarrow{request} C_B,$$

$c_n \in C_B$

则 c_A 和 c_B 的协商请求距离为 n，记作 $dis(c_A, c_B)=n$。

通常情况下，需要权衡证书的隶属度和协商请求距离对协商成功的影响。假设每一个未满足的证书得以成功披露的概率相同（为 ω_0），则证书的披露优先级可定义为

$$priority(c_B)=(1-\bar{\omega}_0^{|C_1-C_{Disclosed}|})(1-\bar{\omega}_0^{|C_2-C_{Disclosed}|})\cdots(1-\bar{\omega}_0^{|C_n-C_{Disclosed}|})\times\lambda_B, \bar{\omega}_0=1-\omega_0$$

ω_0 的取值可以预先假定，或在协商中动态更新。在有了每个证书的披露优先级后，就可以优先披露那些优先级较高的证书，从而更有可能达成协商。

3.1.3 协商停止判断准则

显然，当且仅当目标资源 R 得以披露时，信任协商成功；当协商双方均无法向对方请求或披露更多的证书时，协商无法进行，即协商失败。

导致证书无法披露的原因很多，可能是协商参与者没有或不愿披露一些证书，也可能是双方在协商过程中发现这些证书的协商规则无法满足，或证书之间存在循环依赖关系。例如，Bob 向 Alice 请求了证书 $c1$，根据 $c1$ 的协商规则，Alice 向 Bob 请求证书 $c2$，而 Bob 进一步根据 $c2$ 的协商规则向 Alice请求证书 $c1$。在这种情况下，双方均无法向对方进一步请求更多的证书，即 $C_{ARequest}$ 和 $C_{BRequest}$ 保持不变，故协商失败。

3.2 协商的算法设计

根据 3.1 节，可以得到协商过程某一步中 Alice 的证书请求及披露算法的伪代码描述（Bob 方类似）。

算法 1（证书请求算法） requestCredsAlgorithm

```
Input: C_ARequest, C_ADisclosed, C_ADecline, C_BRequest, C_BDisclosed, C_BDecline,
       Count_MaxRequest: 见 3.1 节
Output: C_newRequest: 本次 Alice 请求的证书集
requestCredsAlgorithm ()
{ C_newRequest = ∅;
  C_CList = ∅; // 保存能够进一步协商所需的证书集的集合
  for ∀s ∈ C_BRequest − C_ADecline − C_ADisclosed // 遍历 Bob 向 Alice 请求的
  证书
  { if (satisfy(P_s, C_BDisclosed)) continue; // Alice 已可以向 Bob 披露 s,
    不必根据 s 请求证书
    for ∀C_Branch ∈ ConjBranches(P_s) // ConjBranches(P_s)为 s 的模糊
    规则的所有合取分支
    { if (may_satisfy(P_s, C_Branch)) // 如果此合取支有可能得到满足
      C_CList = C_CList ∪ {C_Branch − C_ARequest − C_BDisclosed};
    }
  }
  while ((|C_newRequest| < Count_MaxRequest) ∧ (C_CList ≠ ∅)) // 选择 C_CList
  中含证书较少的证书集作为请求
  { C_min = {C_min | C_min ∈ C_CList, 对∀C ∈ C_CList, 有 |C_min| ≤ |C|};
    C_newRequest = C_newRequest ∪ C_min;
    C_CList = C_CList − {C_min};
  }
  return C_newRequest
}
```

算法 2(证书披露算法) discloseCredsAlgorithm

```
discloseCredsAlgorithm (){
    C_newDisclose = {s | s∈C_BRequest − C_ADecline − C_ADisclosed ∧ satisfy(P_s, C_BDisclosed)}
    while(|C_newDisclose| > Count_MaxDisclose)
    { s_min = {s_min | s_min ∈ C_newDisclose, 对∀s ∈ C_newDisclose, 有 priority(s_min) ≤ priority(s)}
      C_newDisclose = C_newDisclose − {s_min}
    }
}
```

其中证书 s 的优先级计算函数如下：

```
Input: C_ARequest, C_ADisclosed, C_ADecline, C_BRequest, C_BDisclosed, C_BDecline, R, ω0,
       Count_MaxDisclose: 见 3.1 节
Output: C_newDisclose: 本次 Alice 披露的证书集
priority(s)
{ priority = λ_s;
  for ∀C_i ∈ request_chain(R,s)// 证书 s 到 R 的请求链上的证书集的集合
      priority = priority * (1−ω0)^|C_i − C_ADisclosed − C_BDisclosed|;
  return priority;
}
```

4 模糊自动信任协商的性能分析

4.1 性能指标

信任协商的目的是为协商参与者之间建立信任关系。对于一种信任协商策略而言，要求相关协商规则和协商过程控制具有一定特性和要求[9]，概括起来，包括以下几个方面。

(1)完备性：若存在一种可能的证书披露方式使得信任规则能成功建立，那么协商策略能够保证协商成功。

(2)正确性：协商过程中不应暴露未满足协商规则的证书。

(3)隐私性：协商过程中不应该暴露协商方不愿披露的证书或协商规则，也不应披露与协商无关的证书。

(4)高效性：协商应尽量少地披露证书，并且尽量减少请求和披露证书的步骤，从而保证协商能快速进行。

(5)可终止性：协商过程中参与者能够主动停止协商，以免协商无限循环执行。

在满足以上基本特性后，还需要对信任协商策略的性能做出评价，以定量判断协商策略的优劣。常见的评价指标包括以下几个方面：

(1)协商效率。协商效率是指双方建立协商的开销，即在信任协商过程中，协商双方披露证书与协商信任规则，以建立信任关系所需要的各类开销，包括网络开销、通讯开销以及计算开销等。通常情况下，协商效率是由网络状况决定的，当网络带宽较大时，协商效率正比于协商步骤；当网络带宽较小时，协商效率则主要由证书的数量和大小决定。

(2)协商成功率。协商成功率是指协商者包括资源服务请求方、提供方之间协商成功次数与进行协商的次数的比值。

设 Alice、Bob 双方根据协商策略，协商了 S_{all} 次，成功了 S_{fact} 次，则协商成功率：

$$Success=\frac{S_{fact}}{S_{all}}$$

本文所讨论的模糊信任协商的主要目的是加速协商过程、提高协商效率，因此本节主要从协商的效率入手，评价模糊信任协商的性能。

4.2 协商效率分析

协商效率定量描述了达成协商所需要的总开销。影响协商效率的因素包含两方面：协商总步骤和披露证书的数量。假设本地计算时间相比于网络开销可忽略不计，所有的证书大小相近，因此协商效率主要由协商步骤和披露证书总数决定，其中协商的任一步骤带来的额外时间开销为 t_s，披露一个证书的时间为 t_c。

根据文献[3]，可以将协商过程展开成一个协商搜索树(Negotiation Search Tree)。协商搜索树是证书协商规则的直观描述形式。在将证书的协商规则写成析取范式后，如图 2 所示，树中的节点分为两种，圆形节点表示证书，每个子节点是方形节点，表示此证书协商规则的一个合取支，合取支中的每个证书在树中表示为此方形节点的直接子节点。显然，一个证书能被披露，当且仅当它的协商规则为永真式，或它的任意子树能够满足。例如，若证书 B3 和 A6 可以直接被披露，则 B4 可以被披露，进而 A1 可以被披露。

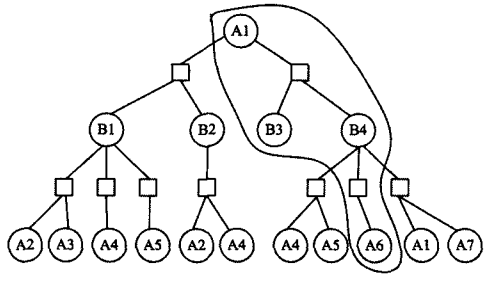

图 2 协商搜索树示例

显然，当且仅当存在一个包含根节点的子树，其所有叶节点的证书均可直接披露时，协商可以成功；协商的最小步骤等于这些子树中深度最小的子树的深度，而最小披露证书集为这些子树中所含圆形节点最少的子树的节点数。与传统的信任协商类似，最理想情况下，模糊协商中每一步骤都使得协商更进一步，因此模糊协商与传统的信任协商的步骤及披露证书数是一样的。最坏情况下，需要遍历整个搜索树才能找到一条合法的披露路径，故与传统的积极协商策略(Eager Strategy)相比，模糊协商策略所披露的证书数量相同，协商步骤会多于前者。

接着讨论模糊协商的平均效率。本文所描述的模糊信任协商对于效率的提升主要表现在对单个证书的协商成功率的提升上。由于我们用模糊逻辑描述证书的协商规则，使得在传统信任协商方案下无法成功披露的证书有可能得以披露，而在平均意义下单个证书协商成功率的提升意味着协商效率的提升，因此需要计算平均意义下协商成功率的提升。

设元证书 c(即协商规则 P_c 恒为真的证书)的隶属度为 λ，对方对此证书要求的门限隶属度为 τ，c 的属性在其取值域上连续均匀分布，则 λ 的取值概率为 $Prob(\lambda)=\begin{cases}\alpha, & \lambda=0\\ 1-\alpha-\beta, & 0<\lambda<1\\ \beta, & \lambda=1\end{cases}$。其中，$\alpha$ 和 β 分别为证书属性必然不满足或必然满足对方要求的概率，因此，对于元证书 c 而言，模糊化后的协商成功率为 $\beta'=\frac{1-\tau}{1-\alpha-\beta}+\beta$，比传统的属性证书提高了 $\frac{1-\tau}{1-\alpha-\beta}$。

设证书 s 的协商规则 P_s 写为析取式后包含了 n 个合取

(下转第 239 页)

cations Security. ACM,2010:426-439

[13] Caballero J, Poosankam P, Kreibich C, et al. Dispatcher: Enabling active botnet infiltration using automatic protocol reverse-engineering[C]//Proceedings of the 16th ACM Conference on Computer and Communications Security. ACM,2009:621-634

[14] Wikipedia Contributors. Mealy machine [EB/OL]. 2013-11-13 [2014-11-10]. http://zh.wikipedia.org/wiki/Mealy%E6%9C%BA

[15] 肖明明,余顺争. 基于文法推断的协议逆向工程[J]. 计算机研究与发展,2013,50(10):2044-2058
Xiao M M, Yu S Z. Protocol Reverse Engineering Using Grammatical Inference[J]. Journal of Computer Research and Development,2013,50(10):2044-2058

[16] 潘璠,洪征,杜有翔,等. 基于递归聚类的报文结构提取方法[J]. 四川大学学报(工学版),2012,44(6):137-142
Pan F, Hong Z, Du Y X, et al. Recursive Clustering Based Method for Message Structure Extraction [J]. Journal of Sichuan University (Engineering Science Edition),2012,44(6):137-142

[17] Comparetti P M, Wondracek G, Kruegel C, et al. Prospex: Protocol specification extraction[C]//2009 30th IEEE Symposium on Security and Privacy. IEEE,2009:110-125

[18] Bossert G, Guihéry F. Security Evaluation of Communication Protocols in Common Criteria[R]. Paris: ICCC,2012

[19] Postel J. RFC821: Simple Mail Transfer Protocol [S]. IETF, 1982

[20] Myers J, Rose M. RFC1939: Post Office Protocol-Version3[S]. IETF,1996

[21] 潘璠,洪征,周振吉,等. 语义层次的协议格式提取方法[J]. 通信学报,2013,34(10):162-173
Pan F, Hong Z, Zhou Z J, et al. Protocol format extraction at semantic level [J]. Journal on Communications,2013,34(10):162-173

(上接第 223 页)

支,每个合取支包含且仅包含了 m 个元证书,元证书满足门限隶属度 τ 的概率为 β'_{ij},则任意合取支得以满足的概率为 $\prod_{j=1}^{m}\beta'_{ij}$,整个析取式能够满足的概率为 $1-\prod_{i=1}^{n}(1-\prod_{j=1}^{m}\beta'_{ij})$。若所有元证书能够满足的概率均为 β',则证书 s 能够成功披露的概率为 $Prob(s)=1-(1-\beta'^{m})^{n}$。一般地,证书 s 距离元证书的平均距离为 $k(k=0,1,2,\cdots)$,若平均每个证书的协商规则包含了 n 个合取支,每个合取支包含了 m 个平均距离为 $k-1$ 的证书,则 s 得以成功披露的概率为

$$Prob(s_k)=\begin{cases}\beta', & k=0\\ 1-(1-Prob^{m}(s_{k-1}))^{n}, & k=1,2,\cdots\end{cases}$$

类似地,目标资源 R 被成功披露的概率为 $Prob(R)$,故协商成功率为 $Prob(R)$。例如,当 $\beta=0.7$,$\beta'=0.71$,$m=3$,$n=3$,$k=4$ 时,传统的信任协商成功率为 88.7%,而模糊协商的成功率提高到了 95%。可以看出,模糊协商对协商成功率影响非常大。

由于当且仅当找到一个能够披露的根节点的子树时协商可以成功,而双方的协商过程可以看作对这个搜索树的深度优先遍历。若在协商搜索树中目标资源 R 有 n 个子节点,每个子节点在传统的信任协商中成功率均为 $Prob_r$,在模糊信任协商中成功率均为 $Prob_r'$,每个子节点因协商失败造成的效率损失平均为 t_0,则模糊协商比传统的信任协商效率提升了 $t_0\sum_{i=0}^{n}Prob_r'-Prob_r$。由于模糊协商中会根据当前各个证书的模糊隶属度优先披露更有可能成功的证书,因此实际应用中其效率会略高一些。

结束语 自动信任协商为开放网络环境中的用户提供了一种有效而可靠的资源共享方式。针对传统的协商方式存在由于协商规则制定较严格而导致协商成功率和效率有所下降的问题,本文提出了一种基于模糊逻辑的信任协商方案,即协商双方可以通过制定更为合理的信任规则,来尽可能地降低协商的失败率,提高协商效率;同时也简单分析了模糊协商方案下效率的提升。在进一步的工作中,可以针对证书的隶属度做进一步的优化,以提高协商的成功率和效率。

参 考 文 献

[1] Winsborough W H, Seamons K E, Jones V E. Automated trust negotiation[C]//Proceeding of the DARPA Information Survivability Conference and Exposition. 2000:88-10

[2] Seamons K E, Winslett M, Yu T. Limiting the disclosure of access control policies during automated trust negotiation[C]//Network and Distributed System Security Symp (NDSS 2001). Internet Society Press,2001

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

[4] Winsborough W H, Li N H. Towards practical automated trust negotiation[C]//Proc of the 3rd International Workshop on Policies for Distributed Systems and Networks. Monterey, CA, USA,2002:92-103

[5] Yu T, Winslett M, Seamons K E. Supporting structured credentials and sensitive policies through interoperable strategies for automated trust negotiation[J]. ACM Transactions on Information and System Security,2003,6(1):1-42

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

[7] 李建欣,怀进鹏. COTN:基于契约的信任协商系统[J]. 计算机学报,2006,29(8):1290-1300
Li Jian-xin, Huai Jin-peng. COTN: A Contract-Based Trust Negotiation System[J]. Chinese Journal of Computers, 2006, 29(8):1290-1300

[8] Guan S Y, Dong X S, Mei Y D, et al. Towards automated trust negotiation for grids[C]//Proc of the IEEE International Conference on Networking, Sensing and Control. 2008:154-159

[9] 李建欣,怀进鹏,李先贤. 自动信任协商研究[J]. 软件学报,2006,17(1):124-133
Li Jian-xin, Huai Jin-peng, Li Xian-xian. Research on Automated Trust Negotiation[J]. Journal of Software,2006,17(1):124-133

[10] 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
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

[11] Zadeh L A. Fuzzy sets[J]. Information and Control, 8(3):338-353