

身份认证可信度研究

张明德¹ 郑雪峰¹ 吕述望² 张清国¹

(北京科技大学信息工程学院 北京 100083)¹ (信息安全国家重点实验室 北京 100039)²

摘 要 身份认证过程存在很多不确定因素,导致认证服务的结果并不绝对可信;而现有研究成果主要集中在身份认证的某些方面,不具有通用性。基于对身份认证的形式化描述和其安全性的逻辑分析,将身份认证过程中不确定因素分为4个方面;通过引入信任分类、不可信因子和安全度,提出一种具有通用性的身份认证可信度计算方法;并对基于静态口令和数字证书的身份认证模型进行实例分析。

关键词 身份认证,认证凭证,不可信因子,安全度,可信度

中图法分类号 TP301.6,TP309 **文献标识码** A

Research on Trust Degree of Authentication

ZHANG Ming-de¹ ZHENG Xue-feng¹ LV Shu-wang² ZHANG Qing-guo¹

(School of Information Engineering, University of Science and Technology Beijing, Beijing 100083, China)¹

(State Key Laboratory of Information Security, Beijing 100039, China)²

Abstract There are several uncertain factors in authentication procedure, so authentication services are not absolutely credible. However existing researches focused on not whole but some aspects of authentication. Based on formalized description for authentication and logical analysis on security of authentication, uncertain factors in authentication procedure were divided into four categories. Meanwhile a common approach on trust degree of authentication was proposed through the introduction of trust classification, non-trust factor and security degree. Two examples were given to demonstrate how to use this approach.

Keywords Authentication, Authentication voucher, Non-trust factor, Security degree, Trust degree

1 引言

身份认证构建于认证机制(如口令、证书、指纹等)和认证协议(如 Radius^[1]、Kerberos^[2]等)之上,为各种应用系统提供认证服务^[3]。由于受其复杂性和多样性的影响,身份认证过程存在多种不确定因素,导致认证服务的结果并不绝对可信。

为了度量身份认证的信任关系,业界提出了一些方法或模型。Thomas Beth 等最早提出一种基于经验值的信任度计算方法^[4];该方法适用于各种开放式网络,但并没有考虑身份认证的自身特点和复杂性。Ueli Maurer 通过定义 PKI 信任逻辑推理模型,给出了 PKI 信任值推理算法^[5];张明德等通过分析 PKI 证书及私钥签发过程和使用过程中的安全风险,提出了一种密钥可信度计算方法^[6];但该方法只适用于 PKI 机制,不适用于其它的认证机制。汪伦伟等将认证过程中不确定因素总结为3类:认证机制的不确定性、认证规则的不确定性和认证结论的不确定性,并借鉴专家系统中不确定性推理思想,提出认证可信度的思想,并给出了认证可信度因子模型^[7];但该模型没有考虑认证机制、认证协议及认证凭证的差异性,也没有分析访问实体的不确定性对认证服务结果

的影响。

本文对身份认证进行形式化描述,并对其安全性进行逻辑分析;以此为基础,将身份认证过程中不确定因素分为4个方面;通过引入信任分类、不可信因子和安全度,提出一种具有通用性的身份认证可信度计算方法;并对两类身份认证模型进行实例分析。

2 身份认证描述

针对身份认证,本文假设如下:

1)只提供访问实体的身份验证服务,不考虑访问实体在应用系统中的标识;

2)只研究身份认证系统对访问实体身份的验证,不考虑访问实体对身份认证系统身份的验证。

对身份认证涉及的基本组成要素进行定义。

定义 1(访问实体) 访问实体是指访问信息系统的最终对象,只有身份验证合法后才允许访问。

访问实体涉及两类对象:物理实体和数字实体;物理实体是指物理世界中对信息系统进行访问的对象,属于物理世界范畴;数字实体是指物理实体在数字世界中的虚拟映射,属于

到稿日期:2010-12-19 返修日期:2011-03-05

张明德(1972—),男,博士生,主要研究方向为信息安全,E-mail:rickchina@263.net;郑雪峰(1951—),男,研究员,博士生导师,主要研究方向为网络自控、信息安全;吕述望(1941—),男,教授,博士生导师,主要研究方向为密码学、信息安全;张清国(1966—),男,博士生,主要研究方向为信息安全。

数字世界范畴。

访问实体集合表示为 $E=\{e_1, e_2, \dots\}$, 物理实体集合表示为 $PE=\{pe_1, pe_2, \dots\}$, 数字实体集合表示为 $DE=\{de_1, de_2, \dots\}$ 。 $e=(pe, de)$ 表示访问实体, 其中 pe 表示 e 对应的物理实体, de 表示 e 对应的数字实体。

$pe(e)$ 表示访问实体 e 对应的物理实体, $de(e)$ 表示访问实体 e 对应的数字实体, $inf(pe)$ 表示物理实体 pe 的特征信息。

定义 2(认证凭证与认证机制) 认证凭证是指访问实体向信息系统证明身份的专有数据。认证凭证由凭证标识和凭证秘密组成, 凭证标识和凭证秘密一一对应。凭证标识主要由唯一性编码及物理实体特征信息等组成; 凭证标识一般不保密, 但凭证秘密必须保密。物理实体可能有多个认证凭证, 但每个认证凭证对应的数字实体不同。

认证机制是指认证凭证产生及验证的基本方法。认证协议是基于对认证凭证进行合法性验证从而实现身份认证的通讯协议。

认证凭证实际是认证机制的具体表现; 如静态口令机制下, 认证凭证为口令标识和静态口令; 动态口令机制下, 认证凭证为口令标识和动态口令(包括用户端安全设备, 如硬件令牌); PKI 机制下, 认证凭证为数字证书和私钥(包括用户端安全设备, 如 USB Key)。相同的认证机制, 可能有多种认证凭证。

认证凭证集合表示为 $V=\{v_1, v_2, \dots\}$; $v=(iv, sv)$ 表示认证凭证, 其中 iv 表示凭证标识, sv 表示凭证秘密; $v(e)=(iv(e), sv(e))$ 表示访问实体 e 的认证凭证。

$V(E)$ 表示集合 E 中所有访问实体的认证凭证集合。

定义 3(身份管理方) 身份管理方是指对认证凭证进行管理的功能组件。

身份管理方集合表示为 $AM=\{am_1, am_2, \dots\}$ 。 $Adm(am, v(e))$ 表示存在事实“组件 am 给访问实体 e 新增认证凭证 $v(e)$ ”。

定义 4(身份验证方) 身份验证方是对认证凭证进行验证的功能组件, 主要基于认证协议对认证凭证进行合法性验证。相同的认证凭证, 可能选择不同的认证协议。

身份验证方集合表示为 $AV=\{av_1, av_2, \dots\}$ 。 $Ver(av, v(e))$ 表示存在事实“访问实体 e 的认证凭证 $v(e)$ 通过组件 av 的合法性验证”。

定义 5(身份依赖方) 身份依赖方是指其行为操作依赖于身份验证方结果的功能组件, 可能是业务服务功能, 也可能是访问控制组件。

身份依赖方集合表示为 $RP=\{rp_1, rp_2, \dots\}$ 。

定义 6(身份认证域) 身份认证域是指处于同一管理职权边界内的一个身份认证组成部分。

每个身份认证域可定义为一个五元组, 即: $D=\{E, V(E), am, av, RP\}$, 如图 1 所示。

仅包含单个身份认证域的系统称为单域身份认证系统, 包含多个身份认证域的系统称为多域身份认证系统。

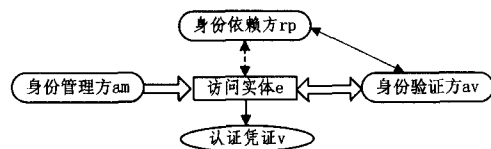


图 1 身份认证域

根据上述定义, 可以得到如下引理。

引理 1 $\forall e_1, e_2 \in E, e_1 \neq e_2 \Rightarrow de(e_1) \neq de(e_2)$ 。

该引理说明, 不同的访问实体, 其对应的数字实体也不同。物理实体和数字实体之间只存在一对一或一对多关系, 不存在多对一或多对多关系。

引理 2 $\forall e=(pe, de) \in E \Rightarrow v(e)=v(de)$ 。

该引理说明, 认证凭证属于数字世界范畴, 实质是颁发给数字实体的。

引理 3 $\forall e_1, e_2 \in E, e_1 \neq e_2 \Rightarrow v(e_1) \neq v(e_2)$ 。

证明: $e_1 \neq e_2 \Rightarrow de(e_1) \neq de(e_2) \Rightarrow$

$$v(de(e_1)) \neq v(de(e_2)) \Rightarrow v(e_1) \neq v(e_2)$$

该引理说明, 认证凭证与访问实体存在一一映射关系。

引理 4 $\forall e_1, e_2 \in E, v(e_1) \neq v(e_2) \Rightarrow iv(e_1) \neq iv(e_2)$ 。

该引理说明, 不同的认证凭证, 其凭证标识也不同。

3 身份认证的安全性

基于身份认证的基本组成要素, 现对身份认证涉及的安全性元素进行定义。

定义 7(凭证物理实体) 凭证物理实体是指凭证标识中物理实体特征信息 $inf(pe)$ 所对应的物理实体。 $pe(v)$ 表示认证凭证 v 的凭证物理实体。

定义 8(凭证持有者) 凭证持有者是指实际持有认证凭证的物理实体。凭证持有者不一定是凭证物理实体。 $vh(v)$ 表示认证凭证 v 的凭证持有者。

定义 9(信任, Trust In) $Trust(rp, x)$: 表示 rp 相信“ x 是可信的”或“ x 的行为与 rp 所期望的完全一致”。 x 可以是访问实体 e 、物理实体 pe 、数字实体 de 、组件 am 或组件 av 。

定义 10(控制, Control) $Ctrl(rp, pe(e) @sv(e))$: 表示 rp 相信“物理实体 $pe(e)$ 对凭证秘密 $sv(e)$ 是可控的”, 即“只有物理实体 $pe(e)$ 才能使用或操作凭证秘密 $sv(e)$ ”。用 $pe(e) @sv(e)$ 表示“只有物理实体 $pe(e)$ 才能使用或操作凭证秘密 $sv(e)$ ”。

定义 11(安全, Security) $Sec(rp, x)$: 表示组件 rp 相信“ x 是安全的”。 x 可以是物理实体 $pe(e)$ 或凭证秘密 $sv(e)$ 。当 x 为 $pe(e)$ 时, 表示“物理实体 $pe(e)$ 在主观上能保证不泄露任何秘密信息”。当 x 为 $sv(e)$ 时, 表示“凭证秘密 $sv(e)$ 在技术上能保证不被伪造、不被窃取或不被劫持”。

定义 12(真实, Authenticity) $Auth(rp, x)$: 表示 rp 相信“ x 是真实的”。

根据上述定义, 可以得到如下引理。

引理 5 $Adm(am, v(e)) \Rightarrow pe(v(e)) = pe(e)$ 。

该引理说明, 身份管理方在签发新的认证凭证时, 将物理实体特征信息加入认证凭证中。

引理 6 $Trust(rp, am), Adm(am, v(e)) \Rightarrow Auth(rp, vh(v(e)) = pe(e))$ 。

该引理说明, 凭证管理过程如果存在安全隐患, 可能会导致凭证物理实体与凭证持有者不一致。

引理 7 $Sec(rp, pe(e)), Sec(rp, sv(e)) \Rightarrow Ctrl(rp, pe(e) @sv(e))$ 。

该引理说明, 当物理实体和凭证秘密同时都安全时, 物理实体就能实现对凭证秘密的可控性。反之, 则不成立。

引理 8 $Trust(rp, av), Ver(av, v(e)) \Rightarrow Trust(rp, de$

(e))。

该引理说明,身份验证方实质上属于数字世界范畴,只能对数字实体的身份进行合法性验证,并不能对物理实体的身份进行合法性验证。

引理 9 $Trust(rp, de(e)), Auth(rp, vh(v(e))) = pe(e), Ctrl(rp, pe(e) @sv(e)) \Rightarrow Trust(rp, pe(e))$ 。

该引理说明,只有凭证持有者与凭证物理实体保持一致且实现对凭证秘密的可控时,对数字实体的信任才能转化为对物理实体的信任。该引理还说明,身份认证通过两个环节将数字世界与物理世界进行耦合:认证凭证的管理过程和物理实体对凭证秘密的控制过程;只有当这两个环节均保证完全耦合时,数字世界与物理世界的身份及信任才能保持一致性。

4 身份认证的可信度

身份认证的目的是在数字世界中实现对物理实体身份的合法性验证。但从引理 6—引理 9 发现,身份认证过程存在一些不确定因素,具体体现为 4 类关键对象的不确定性:认证机制的不确定性、身份管理方的不确定性、身份验证方的不确定性和访问实体的不确定性;这些不确定性因素可能会影响身份认证验证结果的可信度。

认证机制的不确定性主要包括认证凭证是否被破解(如 PKI 机制下,若 RSA 算法被破解,则从公开的数字证书就可计算出私钥)等;这些不确定性可能会导致认证凭证被泄露的安全风险。

身份管理方的不确定性主要包括信息系统是否安全、管理流程是否安全等;这些不确定性可能会导致认证凭证被泄露(凭证秘密被窃取)、被伪造(违规或过失签发认证凭证)等安全风险。

身份验证方的不确定性主要包括信息系统是否安全、认证协议是否安全等;这些不确定性可能会导致认证凭证被泄露(凭证秘密被窃取)、被伪造(假冒认证凭证通过合法性验证)等安全风险。

访问实体的不确定性主要包括物理实体是否可靠、信息系统是否安全、认证凭证存储是否安全等,这些不确定性可能会导致认证凭证被泄露(凭证秘密被窃取或被物理实体主动泄露)、被劫持(木马程序控制认证凭证)等安全风险。

定义 13(信任分类, Trust Classification 或 TC) 鉴于身份认证组成要素的复杂性和多样性,全面分析其行为与预期是否完全一致是非常困难的;当只需其实现有限功能时,没有必要信任其所有行为^[8]。基于对身份认证过程各种不确定性的分析,从避免安全风险角度,将身份认证相关的信任元素分为 3 类:

- 1) 保证认证凭证不被泄露,简称防泄露类或 AL 类(anti-leakage)。
- 2) 保证认证凭证不被伪造,简称防伪造类或 AF 类(anti-forge)。
- 3) 保证认证凭证不被劫持,简称防劫持类或 AH 类(anti-hijack)。

定义 14(不可信因子, Non-Trust Factor) 不可信因子是指,身份认证过程中,关键对象中各种不确定性导致认证凭

证被泄露、被伪造或被劫持等安全风险发生的影响程度。关键对象主要包括:凭证管理方 am 、凭证验证方 av 、访问实体 e 和认证机制 m 。不可信因子的取值范围为 $[0, 1]$, 缩写为 NTF。

为方便使用,用 χ 表示对象的防泄露类不可信因子,用 ω 表示对象的防伪造类不可信因子,用 ψ 表示对象的防劫持类不可信因子。关键对象 o 的不可信因子可用三元组 $NTF(o) = (\chi, \omega, \psi)$ 表示。

定义 15(安全度, Security Degree 或 SD) 安全度是指关键对象保证认证凭证不被泄露、不被伪造或不被劫持的可能性,用概率表示。

关键对象安全度定义如下:

$$S_{TC}(o) = 1 - \alpha^{l(o)}$$

其中:

- (1) o 表示关键对象, $o = am$ 或 av 或 e 或 m 。
- (2) TC 表示信任分类, $TC = AL$ 或 AF 或 AH 。
- (3) α 表示关键对象的不可信因子, $\alpha = \chi$ 或 ω 或 ψ 。
- (4) λ 表示经验函数,与成功经验次数 ns 和失败经验次数 nf 有关,且 $\lambda \geq 0$ 。

$$\lambda = \begin{cases} 0, & \text{如果 } nf > 0 \\ 1, & \text{如果 } nf = 0 \text{ 且 } ns = 0 \\ f(ns), & \text{如果 } nf = 0 \text{ 且 } ns > 0 \end{cases}$$

当 λ 与 ns 呈线性关系时,则有:

$$f(ns) = a * ns + 1 \quad (a \geq 0)$$

用 $ns(o)$ 与 $nf(o)$ 分别表示对象 o 的成功经验次数和失败经验次数。鉴于认证机制、身份管理方和身份认证方不可分离,本文假设 $ns(am) = ns(av) = ns(m)$ 、 $nf(am) = nf(av) = nf(m)$ 。

关键对象 o 的安全度可用三元组 $S(o) = (S_{AL}(o), S_{AF}(o), S_{AH}(o))$ 表示。

定义 16(身份认证可信度) 可信度是指一个事物或现象为真的可能性或相信程度,用概率表示。

认证凭证可信度是指 $vh(v(e)) = pe(e)$ 为真的可能性,用 $T(v(e))$ 表示。

凭证秘密可信度是指 $pe(e) @sv(e)$ 为真的可信度,用 $T(sv(e))$ 表示。

数字实体可信度是指 $de(e)$ 为真的可能性,记作 $T(de(e))$ 。

物理实体可信度是指 $pe(e)$ 为真的可能性,记作 $T(pe(e))$ 。由于身份认证的目的是在数字世界中实现对物理实体身份的合法性验证,因此物理实体可信度又称作身份认证可信度。

根据上述定义,可以得到如下引理。

引理 10 $NTF(m) = (\chi_m, 0, 0)$ 、 $NTF(am) = (\chi_{am}, \omega_{am}, 0)$ 、 $NTF(av) = (\chi_{av}, \omega_{av}, 0)$ 、 $NTF(e) = (\chi_e, 0, \psi_e)$ 。

引理 11 $S(m) = (S_{AL}(m), 0, 0)$ 、 $S(am) = (S_{AL}(am), S_{AF}(am), 0)$ 、 $S(av) = (S_{AL}(av), S_{AF}(av), 0)$ 、 $S(e) = (S_{AL}(e), 0, S_{AH}(e))$ 。

引理 12 $T(v(e)) = S_{AF}(am)$ 。

证明:设事件 $A =$ “身份管理方不确定性导致认证凭证 $v(e)$ 被伪造”,事件 $G =$ “ $vh(v(e)) = pe(e)$ 为假”,依据概率理论

和引理 6,则有:

$$P(G)=P(A), P(G)=1-T(v(e)), P(A)=1-S_{AF}(am) \\ \Rightarrow 1-T(v(e))=1-S_{AF}(am) \Rightarrow T(v(e))=S_{AF}(am)$$

引理 13 $T(sv(e))=S_{AL}(m)S_{AL}(am)S_{AL}(av)S_{AL}(e)S_{AH}(e)$ 。

证明:设事件 A ="认证机制不确定性导致认证凭证 $v(e)$ 被泄露",事件 B ="身份管理方不确定性导致认证凭证 $v(e)$ 被泄露",事件 C ="身份验证方不确定性导致认证凭证 $v(e)$ 被泄露",事件 D ="访问实体不确定性导致认证凭证 $v(e)$ 被泄露",事件 E ="访问实体不确定性导致认证凭证 $v(e)$ 被劫持",事件 G =" $pe(e)@sv(e)$ 为假",且事件 A, B, C, D, E 相互独立,依据概率理论,则有:

$$P(G)=P(A+B+C+D+E) \\ =1-(1-P(A))(1-P(B))(1-P(C))(1-P(D))(1-P(E))$$

$$P(G)=1-T(sv(e)), P(A)=1-S_{AL}(m), P(B)=1-S_{AL}(am), P(C)=1-S_{AL}(av), P(D)=1-S_{AL}(e), P(E)=1-S_{AH}(e) \\ \Rightarrow 1-P(G)=(1-P(A))(1-P(B))(1-P(C))(1-P(D))(1-P(E)) \Rightarrow T(sv(e))=S_{AL}(m)S_{AL}(am)S_{AL}(av)S_{AL}(e)S_{AH}(e)$$

引理 14 $T(de(e))=S_{AF}(av)$ 。

证明:设事件 A ="身份验证方不确定性导致认证凭证 $v(e)$ 被伪造",事件 G =" $de(e)$ 为假",依据概率理论和引理 8,则有:

$$P(G)=P(A), P(G)=1-T(de(e)), P(A)=1-S_{AF}(av) \\ \Rightarrow 1-T(de(e))=1-S_{AF}(av) \Rightarrow T(de(e))=S_{AF}(av)$$

引理 15 $T(pe(e))=T(v(e))T(sv(e))T(de(e))$ 。

证明:设事件 A =" $vh(v(e))=pe(e)$ 为假",事件 B =" $pe(e)@sv(e)$ 为假",事件 C =" $de(e)$ 为假",事件 G =" $pe(e)$ 为假",且事件 A, B, C 相互独立,依据概率理论,则有:

$$P(G)=P(A+B+C)=1-(1-P(A))(1-P(B))(1-P(C))$$

$$P(G)=1-T(pe(e)), P(A)=1-T(v(e)), P(B)=1-T(sv(e)), P(C)=1-T(de(e)) \\ \Rightarrow 1-P(G)=(1-P(A))(1-P(B))(1-P(C)) \Rightarrow T(pe(e))=T(v(e))T(sv(e))T(de(e))$$

5 实例分析

5.1 基于静态口令的身份认证模型

1) 主要假设

认证机制 m :认证凭证由标识 uid 和口令 pwd 组成;静态口令 pwd 随机产生;通过比对 pwd 和摘要值验证其合法性;

身份管理方 am :分配 uid 给访问实体; uid 和 pwd 对应关系存储在数据库中; pwd 只保存其摘要值;

身份验证方 av :使用口令认证协议对访问实体合法性进行验证;网络中只传输 pwd 摘要值;

访问实体 e :物理实体记忆 pwd ;

$$NTF(m)=(0, 1, 0, 0), NTF(am)=(0, 0.05, 0.02, 0), \\ NTF(av)=(0, 0.05, 0.05, 0)$$

$NTF(e)=(0, 0.05, 0, 0)$;认证凭证不使用硬件,不存在劫持的安全风险

$$f(m)=f(am)=f(av)=f(e)=ns+1$$

$$ns(m)=ns(am)=ns(av)=1, ns(e)=0$$

$$nf(m)=nf(am)=nf(av)=nf(e)=0$$

2) 身份认证可信度计算

$$T(v(e))=S_{AF}(am)=1-0.02^{1+1}=0.9996$$

$$T(sv(e))=S_{AL}(m)S_{AL}(am)S_{AL}(av)S_{AL}(e)S_{AH}(e) \\ =(1-0.1^{1+1})(1-0.05^{1+1})(1-0.05^{1+1})(1-0.05^1)(1) \\ =0.935803378125$$

$$T(de(e))=S_{AF}(av)=1-0.05^{1+1}=0.9975$$

$$T(pe(e))=T(v(e))T(sv(e))T(de(e)) \\ =0.9996 * 0.9975 * 0.935803378125 = 93.3\%$$

5.2 基于数字证书的身份认证模型

1) 主要假设

认证机制 m :认证凭证由数字证书和私钥组成;通过私钥签名验证其合法性;

身份管理方 am :为访问实体签发数字证书;数据库不保存证书和私钥对应关系,也不保存私钥;

身份验证方 av :使用 SSL/TLS^[9] 协议对访问实体合法性进行验证;网络中不传输私钥;

访问实体 e :公私钥对由 USB Key 产生,且私钥允许导出 USB Key;USB Key 通过口令对私钥进行保护;

$$NTF(m)=(0, 0.01, 0, 0), NTF(am)=(0, 0, 0.02, 0), NTF(av)=(0, 0, 0.01, 0)$$

$$NTF(e)=(0, 0, 0, 0.01);$$

$$f(m)=f(am)=f(av)=f(e)=ns+1$$

$$ns(m)=ns(am)=ns(av)=1, ns(e)=0$$

$$nf(m)=nf(am)=nf(av)=nf(e)=0$$

2) 身份认证可信度计算

$$T(v(e))=S_{AF}(am)=1-0.02^{1+1}=0.9996$$

$$T(sv(e))=S_{AL}(m)S_{AL}(am)S_{AL}(av)S_{AL}(e)S_{AH}(e) \\ =(1-0.01^{1+1})(1)(1)(1)(1-0.01^1) \\ =0.989901$$

$$T(de(e))=S_{AF}(av)=1-0.01^{1+1}=0.9999$$

$$T(pe(e))=T(v(e))T(sv(e))T(de(e)) \\ =0.9996 * 0.9999 * 0.989901 = 98.9\%$$

结束语 由于受复杂性和多样性的影响,身份认证过程存在很多不确定因素,导致认证服务的结果并不绝对可信;但现有研究成果主要集中在身份认证的某些方面,不具有通用性。本文基于对身份认证的形式化描述和其安全性的逻辑分析,将身份认证过程中不确定因素分为 4 个方面:认证机制的不确定性、身份管理方的不确定性、身份验证方的不确定性和访问实体的不确定性;通过引入信任分类、不可信因子和安全度,提出一种具有通用性的身份认证可信度计算方法;并对基于静态口令和数字证书的身份认证模型进行实例分析。

参考文献

- [1] Rigney C, Rubens A, Simpson W, et al. Remote Authentication Dial In User Service (RADIUS) [S]. IETF, RFC 2138. April 1997
- [2] Neuman C, Yu T, Hartman S, et al. The Kerberos Network Authentication Service (V5) [S]. IETF, RFC 4120. July 2005

- [3] 任传伦. 分布环境下身份认证和授权管理的研究[D]. 北京: 北京邮电大学, 2007
- [4] Beth T, Borchering M, Klein B. Valuation of trust in open systems[C] // Gollmann D, ed. ESORICS' 94, Lecture Notes in Computer Science, vol. 875. Berlin: Springer-Verlag, 1994, 3-18
- [5] Maurer U. Modelling a Public-Key Infrastructure Proc[C] // Bertino E, ed. 1996 European Symposium on Research in Computer Security(ESORICS' 96). Lecture Notes in Computer Science, vol. 1146, Berlin: Springer-Verlag, 1996, 325-350
- [6] Zhang Ming-de, Zheng Xue-feng, Yang Wen-sheng, et al. Re-

- search on Model of Trust Degrees for PKI[C] // The Fifth International Conference on Information Assurance and Security(IAS 2009). Volumes II. Xi'an, China, 2009, 647-650
- [7] 汪伦伟, 廖湘科, 王怀民. 认证可信度理论研究[J]. 计算机研究与发展, 2005, 42(3): 501-506
- [8] Yahalom R, Klein B, Beth T. Trust Relationships in Secure Systems-A Distributed Authentication Perspective[C] // Proc. IEEE Symp on Research in Security and Privacy. 1993, 150-164
- [9] Dierks T, Rescorla E. The Transport Layer Security(TLS) Protocol Version 1. 1[S]. IETF, RFC 4346. April 2006

(上接第 36 页)

初始条件下所有发送(或转发)概率和窃听概率都是相等的, 在相等情况下被窃听的概率不是最小, 随着 t 的增大, 被窃听的概率因发送概率和窃听概率的改变而变小。若惩罚次数 t 继续增大, 随机路径趋向于单一路径, 使被窃听的概率增大。

2) MGBR 策略前后窃听概率变化趋势及比较

通过 1) 验证了纳什均衡点的存在, 在纳什均衡条件下进行本次试验。通过该实验给出被窃听概率随节点的变化趋势, 并与基于最小跳数算法的路由协议^[15]下被窃听的概率进行比较。给出了节点 $N=4, 5, 6, 7, 8, 9, 10$ 时, 被窃听的概率的变化趋势, 如图 8 所示。

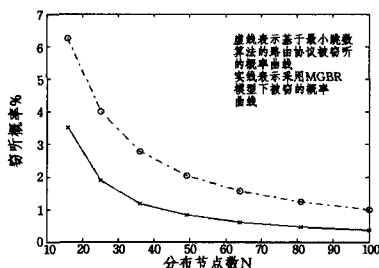


图 8 两种模型下被窃听概率随不同节点变化图

图中实线为 MGBR 策略下被窃听的概率, 虚线表示基于最小跳数算法的路由协议下被窃听的概率。两种情况下曲线变化趋势都表明随着节点的增加, 信息被窃听的概率减少, 并且变化趋势逐渐趋于平缓。基于最小跳数算法的路由协议, 由于没有采用概率传输, 其节点被窃听的概率明显比 MGBR 策略下被窃听的概率高。采用 MGBR 策略可以有效降低信息被窃听的概率, 提高网络的安全性。

结束语 本文针对 WSN 的路由寻址问题, 给出了 MGBR 模型。定义了博弈双方, 采用混合策略, 通过概率转化进行模型的状态转移。模型针对网络中的窃听问题, 给出了最优策略, 使用 PRISM 工具进行仿真实验, 得出了最优策略下的纳什均衡点, 通过比较给出 MGBR 模型下信息被窃听的概率变化曲线。在传统路由中, 窃听者具有记忆功能, 在窃听数据之后, 若发现该路径上的信息具有窃听价值, 将记录该路径, 并进行实时窃听, 这给信息的保密带来威胁。在本文给出的 MGBR 模型中, 路径的选择具有随机性, 降低了路径被连续窃听的概率, 提高了信息传输的安全性。

参 考 文 献

- [1] Heinzelman W R, Chandrakasan A, Balakrishnan H. Energy ef-

- ficient communication protocol for wireless micro sensor networks[C] // Proc of the 33rd Hawaii International Conference on System Sciences, Maui, 2000, 3005-3014
- [2] Sohrabi K, Gao J, Ailawadhi V, et al. Protocols for self-organization of a wireless sensor network[J]. IEEE Personal Communications, 2000, 7(5): 16-27
- [3] De S, Qiao C M, Wu H Y. Meshed multipath routing: An efficient strategy in sensor networks[J]. Computer Networks (Special Issue on Wireless Sensor Networks), 2003, 43(4): 482-497
- [4] Estrin D, Govindan R, Heidemann J, et al. Next century challenges: Scalable coordinate in sensor network[C] // Proc of the 5th AC-M/IEEE International Conference on Mobile Computing and Networking. Seattle, 1999, 263-270
- [5] Manjeshwar A, Agrawal D P. TEEN: A routing protocol for enhanced efficiency in Wireless Sensor Networks[C] // Proc of the 15th Parallel and Distributed Processing Symposium. San Francisco, 2001, 2009-2015
- [6] 徐许亮, 董荣胜, 刘亮龙, 等. 无线自组网中基于定价机制的节点协作性研究[J]. 系统仿真学报, 2009, 21(18): 5914-5918
- [7] 徐许亮, 董荣胜, 刘亮龙. 无线自组网中节点协作的纳什均衡研究[J]. 计算机工程, 2010, 36(4): 107-109
- [8] 曾加, 慕春棣. 基于不完全信息博弈的传感器网络能量平衡路由[J]. 自动化学报, 2008, 34(3): 317-322
- [9] 汪洋, 林闯, 等. 基于非合作博弈的无线网络路由机制研究[J]. 计算机学报, 2009, 32(1): 54-68
- [10] Qiu Li-li, Yang Y R, Zhang Yin, et al. On Selfish Routing in Internet-Like Environments[C] // Proc. ACM SIGCOMM '03. 2003, 151-162
- [11] La R, Anantharam V. Optimal Routing Control; Repeated Game Approach[J]. IEEE Trans. Automatic Control, 2002, 47: 437-450
- [12] Kannan R, Sarangi S, Iyengar S S. Sensor-Centric Energy-Constrained Reliable Query Routing for Wireless Sensor Networks [J]. J. Parallel and Distributed Computing, 2004, 64: 839-852
- [13] Bohacek S, Hespanha J P, Junsoo L, et al. Game theoretic stochastic routing for fault tolerance and security in computer networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2007, 9: 1227-1240
- [14] Fudenberg D, Tirole J. Game Theory[M]. 黄涛, 郭凯, 龚鹏, 等译. 北京: 中国人民大学出版社, 2006
- [15] 张喆. 基于最小跳数的无线传感器网络改进路由算法设计[D]. 南京: 南京理工大学, 2008(10)