软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2016,27(2):451−465 [doi: 10.13328/j.cnki.jos.004840]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

安全高效的异构无线网络可控匿名漫游认证协议*

周彦伟[1,2,3], 杨 波[1,2,3], 张文政[2]

[1](陕西师范大学 计算机科学学院,陕西 西安 710062)

[2](保密通信重点实验室,四川 成都 610041)

[3](信息安全国家重点实验室(中国科学院 信息工程研究所),北京 100093)

通讯作者: 杨波, E-mail: byang@snnu.edu.cn

摘 要: 分析传统的匿名漫游认证协议,指出其匿名不可控和通信时延较大的不足.针对上述不足,提出异构无线网络可控匿名漫游认证协议,远程网络认证服务器通过 1 轮消息交互即可完成对移动终端的身份合法性验证,当移动终端发生恶意操作时,家乡网络认证服务器可协助远程网络认证服务器撤销移动终端的身份匿名性.该协议在实现匿名认证的同时,还具有恶意匿名的可控性,有效防止了恶意行为的发生,且其通信时延较小.安全性证明表明,该协议在 CK 安全模型中是可证安全的.相对于传统漫游机制而言,该协议更适合于异构无线网络.

关键词: 异构无线网络;可控漫游;匿名认证;CK 安全模型;可证安全

中图法分类号: TP393

中文引用格式: 周彦伟,杨波,张文政.安全高效的异构无线网络可控匿名漫游认证协议.软件学报,2016,27(2):451−465. http://www.jos.org.cn/1000-9825/4840.htm

英文引用格式: Zhou YW, Yang B, Zhang WZ. Secure and efficient roaming authentication protocol with controllable anonymity for heterogeneous wireless network. Ruan Jian Xue Bao/Journal of Software, 2016,27(2):451−465 (in Chinese). http://www.jos.org.cn/1000-9825/4840.htm

Secure and Efficient Roaming Authentication Protocol with Controllable Anonymity for Heterogeneous Wireless Network

ZHOU Yan-Wei[1,2,3], YANG Bo[1,2,3], ZHANG Wen-Zheng[2]

[1](School of Computer Science, Shaanxi Normal University, Xi'an 710062, China)

[2](Science and Technology on Communication Security Laboratory, Chengdu 610041, China)

[3](State Key Laboratory of Information Security (Institute of Information Engineering, The Chinese Academy of Sciences), Beijing 100093, China)

Abstract: This paper analyzes the traditional anonymous roaming authentication protocol, and points out the deficiencies of their uncontrolled anonymity and communication delay. A controllable anonymous roaming authentication protocol is proposed in this paper for heterogeneous wireless networks. This protocol can complete verifying the legitimacy of the identity of the mobile terminal through one message interaction. If the mobile terminal has malicious operation, the home network authentication server can help remote network authentication server to revoke the identity anonymity of the mobile terminal. The protocol accomplishes anonymous authentication and

* 基金项目: 国家自然科学基金(61572303, 61272436, 61303092); 信息安全国家重点实验室(中国科学院信息工程研究所)开放课题(2015-MS-10); 保密通信重点实验室基金(9140C110206140C11050); 中央高校基本科研业务费专项资金(GK201504016); 陕西师范大学优秀博士论文项目(X2014YB01)

Foundation item: National Natural Science Foundation of China (61572303, 61272436, 61303092); Foundation of State Key Laboratory of Information Security (Institute of Information Engineering, The Chinese Academy of Sciences) (2015-MS-10); Foundation of Science and Technology on Communication Security Laboratory (9140C110206140C11050); Fundamental Research Funds for the Central Universities (GK201504016); Program of Excellent Doctoral Dissertation of Shaanxi Normal University of China (X2014YB01)

收稿时间: 2014-11-15; 修改时间: 2015-02-17; 采用时间: 2015-04-17

possesses controllability on malicious anonymity at the same time, thus effectively preventing the occurrence of malicious behavior and the communication delay. This protocol is safe in the CK security model.

Key words: heterogeneous wireless network; controlled roaming; anonymous authentication; CK security model; provably secure

随着网络信息技术的快速发展,无线网络已逐步向多种无线接入技术并存的全 IP 异构无线网络发展.异构无线网络有拓扑结构动态变化、开放链路、多种接入技术并存等特点,已使其成为下一代网络发展的趋势.多样化的、无处不在的服务特性,使异构无线网络相对于传统网络更容易受到攻击者的攻击,将面临窃听、重放攻击等安全威胁.为了保证异构无线网络的安全,需要部署安全认证、访问控制等安全措施.

异构无线网络中多种无线接入技术并存,因此,安全漫游是其关键服务之一.安全漫游使得移动终端的接入服务可不受家乡网络覆盖范围的限制,即,当漫游到远程网络(家乡网络之外的网络)时,移动终端在异构无线网络中仍然可以保持连接.漫游认证过程在完成移动终端身份合法性验证的同时,需关注用户隐私信息的匿名性保护问题,同时应防止移动终端的身份和位置等隐私信息被恶意实体跟踪,即安全漫游机制需具有匿名性和不可追踪性.

同时,网络技术的迅速发展,使得身份的合法性认证已不再是判断用户安全的充要条件,而应在身份合法的同时关注终端平台是否可信,即,终端平台的可信性已成为用户安全性验证的必要条件之一.用户对终端平台的可信性需求促进了可信计算技术的兴起及发展,可信计算工作组发布可信平台模块(trusted platform module,简称 TPM)规范和移动可信模块(mobile trusted module,简称 MTM)规范,旨在以硬件芯片为基础,构建安全、可靠、可信的终端平台(TPM 用于非移动终端,MTM 用于移动终端).因此,应在漫游认证过程中增加用户终端平台的可信性验证机制.

异构无线网络抽象模型主要由用户(user,简称 US)、US 家乡域认证服务器(home authentication server,简称 HS)和 US 访问的远程域认证服务器(remote authentication server,简称 RS)组成,同时还包括异构网络管理中心(management center,简称 MC).图 1 所示为异构无线网络抽象模型,其中,US 所使用的终端设备可以是 3G 等蜂窝通信设备、WLAN 终端、WiMAX 终端或者是支持多模的移动终端等.接入点(access point,简称 AP)是抽象的接入设备,可以是 3G 或 WiMAX 网络的基站,也可以是 WLAN 的接入点.

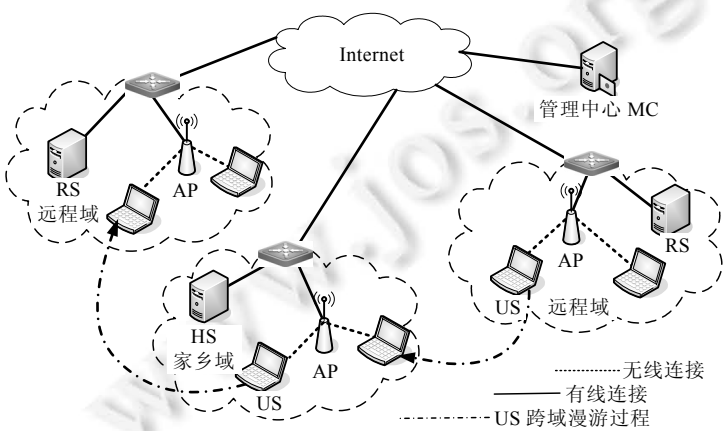


Fig.1 Roaming model for heterogeneous wireless network

图 1 异构无线网络漫游模型

通常在传统漫游认证机制中,家乡域和远程域(家乡域与远程域是相对而言的,以 US 为判定依据)之间预先签订了漫游协议,US 可接入远程服务域.但是,当且仅当 US 完全通过 RS 的认证时才允许其接入,并且为保护漫游用户的隐私信息,漫游认证机制需保证用户身份的匿名性和不可追踪性.同时,由于无线网络的特殊性,无线网络下移动终端的漫游认证机制还需兼顾以下两个方面:

① 移动终端的计算能力和能量通常是有限的,必须尽量减轻协议参与方,特别是移动终端的计算量.

② 无线网络的带宽相对较低,信道出错率较高,在降低消息长度的同时应减少协议的交互轮数.

从本质上讲,安全漫游主要完成跨域的身份认证、平台可信性评估、密钥协商及用户的隐私保护等.国内外研究人员对漫游认证协议进行了大量研究.文献[1]提出了一种基于对称加密的匿名认证协议,运算量较低.文献[2]指出,文献[1]存在匿名性缺陷,并提出了基于公钥的改进方案,但计算开销较大.文献[3]提出了两种匿名漫游协议,分别基于秘密分割和自验证公钥体制,但是两种方案仅具有匿名性而不具有不可追踪性.文献[4]分析了无线漫游的安全需求,并给出了设计匿名无线漫游协议的框架.在文献[4]的基础上,文献[5]进一步提出了具体基于 Diffie-Hellman 密钥交换和证书公钥的无线漫游协议.为了避免网络运营商两两之间签订漫游协议而造成管理的不便,文献[6]提出了基于代理的漫游认证和计费框架.文献[7]虽然提出了基于身份的漫游协议,但未提供匿名性服务.文献[8]提出了一种基于身份的多信任域认证方案,但其计算量较大,推广性较差.文献[9]提出了基于身份的匿名无线认证方案,并借助于公钥实现家乡认证服务器与外地认证服务器之间的认证.但在文献[9]中,接入认证服务器需要传输其为用户签发的临时身份证书以用于后续密钥的协商,增加了网络传输负载和移动终端数据的存储量,同时存在移动终端欺骗攻击、Rogue 网络攻击和密钥更新不满足前向安全的缺陷[10].文献[10]提出一种安全的匿名无线认证协议,弥补了文献[9]方案的不足.文献[11]提出了异构无线网络下的匿名认证和密钥协商协议,引入用户的临时认证身份和临时通信身份实现用户的身份匿名.文献[12]对异构网络通信实体进行抽象,建立了通用的接入认证模型.文献[13]提出了一种适用于异构无线网络的匿名漫游协议.该协议流程简化,且具有较强的匿名性.文献[14]在移动互联网下提出了可信移动平台的跨域服务接入机制,实现可信计算环境下可信移动终端的服务接入及跨域申请.文献[15]提出了组合安全的无线漫游协议.该协议兼顾安全性和实际应用的可行性,实现了漫游的轻量级身份认证,保护了漫游节点的隐私.文献[16]提出了移动网络下抗攻击的双向匿名密钥协商协议,并分析了该协议的身份匿名性和密钥协商公平性等安全属性.文献[17]提出了无线网络下抗攻击的匿名认证协议.该协议不仅可以抵抗现有的攻击,而且具有较高的执行效率,可适用于电池供电的无线通信系统.

在传统的漫游认证机制[8−17]中,当 US 向 RS 申请漫游时,由于 RS 并未掌握漫游用户的注册信息,因此 RS 需在 HS 的协助下完成 US 的合法性验证,即 RS 将 US 的漫游证明信息发给 HS,由 HS 负责验证 US 的合法性,RS 根据 HS 的验证反馈制定相应的决策.因此,传统的漫游认证机制往往需要 2 轮($US\leftrightarrow RS$,$RS\leftrightarrow HS$)消息交互才能完成 US 的漫游接入,导致 US 的计算负载较重,并且通信时延较大.同时,传统协议对 US 身份的匿名性不具有可控性,即,当 US 出现恶意行为时,RS 也无法撤销 US 的匿名性.因此,漫游认证机制在实现 US 身份合法性的同时,实现终端平台的可信性验证,降低参与方的执行负载和通信时延,具有可控的匿名性.

由于椭圆曲线上离散对数问题有更高的安全性,同时具有密钥短小、运算速度快等优点,因此,本文基于椭圆曲线提出异构无线网络可控匿名漫游认证协议.在该协议中,US 注册家乡域网络时可获得 HS 的漫游授权信息.在申请漫游服务时,US 基于授权信息生成漫游验证信息,则 RS 基于漫游验证信息的合法性完成对 US 身份合法性及终端平台可信性的验证,同时保证了 US 隐私信息的安全性和匿名性.本文协议仅通过 1 轮消息交互即可完成漫游认证,减少了漫游过程的消息交互轮数,降低了通信时延,提高了协议的执行效率,有效降低了用户终端的计算负载,同时对漫游用户的恶意匿名行为具有可控性.

1 基础知识

1.1 椭圆曲线

$GF(q)$为定义的有限域,其中,q 为有限域中的元素个数,E_ω为定义在有限域 $GF(q)$上的安全椭圆曲线,F 为 E_ω 上的一个公开基点,Q 是椭圆曲线上 F 的倍数点.即,存在 $d\in Z_q^*$, 满足 $Q=dF$.

定义 1(椭圆曲线离散对数问题). E_ω为定义在 $GF(q)$上的安全椭圆曲线,其中,F 为 E_ω的公开基点,Q 是椭圆曲线上 F 的倍数点.即,存在整数 $d\in Z_q^*$, 满足 $Q=dF$.将如何由 F 和 Q 求解 d 的问题称为椭圆曲线离散对数问题.

假设 1. 不存在任何算法能够在期望的多项式时间内,以不可忽略的概率解决(E_ω,F,Q)上的离散对数问题.

1.2 CK安全模型

CK 安全模型中定义了理想模型 AM 和现实模型 UM 两种模型[18−20].① 理想模型 AM 表示认证的链路模型,在 AM 中攻击者是被动的,并且具有调用协议运行、查询会话密钥、暴漏会话密钥、攻陷协议参与者以及测试会话密钥的能力,但是 AM 中攻击者只能忠实地传递同一消息 1 次,不能伪造、篡改或重放来自未被攻陷参与者的消息;② 现实模型 UM 表示未认证的链路模型,在 UM 中,攻击者除了能够执行 AM 中的所有攻击以外,还具有伪造、篡改和重放消息的能力,则在 UM 中攻击者能够控制协议事件的调度和通信链路,同时还能通过攻击者具体的攻击手段获知协议参与者存储器中的秘密信息.

定义 2[21]. 设Π是运行在 AM 中的 n 方消息驱动协议,Π'是运行在 UM 中的 n 方消息驱动协议.若对于任何 UM 敌手$\mathcal{Q}$,始终存在一个 AM 敌手$\mathcal{A}$使得两个协议的全局输出在计算上是不可区分的,则称协议Π'在 UM 中仿真了 AM 中的协议Π.

定义 3[21]. 编译器 C 是一种算法,其输入是协议的描述,输出也是协议的描述.若一个编译器 C 对于任何协议Π均有协议 $C(\Pi)$在 UM 中仿真Π,则这个编辑器称为认证器.因此,AM 中的安全协议可由认证器转化为 UM 中的安全协议.

定义 4[21]**(会话密钥安全)**. 对于 AM 中的任何敌手$\mathcal{A}$,当且仅当以下性质都满足时,该协议在 AM 中是会话密钥安全的:

性质 1. 未被攻陷的参与双方完整执行协议后,参与者获得相同的会话密钥.

性质 2. 敌手$\mathcal{A}$进行测试会话查询攻击,它猜中正确会话输出值的概率不超过$\frac{1}{2}+\varepsilon$,其中,ε是安全参数范围内可忽略的任意小数.

定理 1[18]. 假设λ是一个消息传输认证器,即λ在 UM 中仿真了简单消息传输协议.假设 C_λ是在λ的基础上定义的编译器,则 C_λ也是一个认证器.认证器是模块化方法中非常重要的机制,它可以确保将 AM 中的安全协议转化为 UM 中的安全协议.

定理 1 的证明详见文献[21].文献[18,21,22]详细介绍了 CK 安全模型的基本理论和基于该模型设计安全密钥协商协议的基本方法.限于篇幅,本文不再赘述.

2 可控匿名漫游认证协议

本文的异构无线网络可控匿名漫游认证协议由两个阶段组成.

① 注册家乡域.主要完成 HS 与 US 间的身份合法性认证及 HS 对 US 终端平台的可信性验证,并且完成会话密钥的协商和签名授权信息的分发.

② 漫游远程域.RS 基于漫游验证信息完成对 US 身份合法性和终端平台可信性的验证,实现 US 的安全漫游接入.

2.1 假设及符号

2.1.1 相关假设

本文协议的安全性基于以下假设:

假设 2. 各区域认证服务器均安全可信,既不会发送虚假信息,也不会利用已掌握的用户信息实施假冒攻击,更不会随意揭示用户的真实身份;同时,认证服务器均安全保存私钥,避免密钥泄露事件的发生.

假设 3. 各认证服务器获得管理中心 MC 签发的证书,证书包含 MC 的签名等信息,并通过安全途径对外公布相关参数.由 MC 协助各认证服务器完成彼此间安全信道及信任关系的建立.

假设 4. 各认证服务器间的时钟同步机制可保证消息时间戳的新鲜性和同步性.

2.1.2 符号定义

本文所使用相关符号的定义见表 1.

Table 1 Definition of relevant variables

表 1 相关变量的定义

变量	定义
ID_A	A 的身份标识
(PK_A,KS_A)	A 的公私钥对,秘密保存私钥 KS_A,防止泄漏
KS_A^{-1}	A 关于私钥 KS_A 的求逆运算值, KS_A^{-1} 是 A 的秘密信息
T_A	A 产生的时间戳
(AIK_{Priv},AIK_{Pub})	可信平台中 TPM 的身份证明密钥对
$Cert(AIK_{Pub})$	可信平台的 AIK 证书
$\|\|$	连接符
$\oplus$	异或运算

2.2 系统初始化

系统建立过程的主要操作有:

(1) 各区域认证服务器向管理中心 MC 注册,由 MC 管理各认证服务器的安全性及相关事宜.

(2) MC 选取满足条件的 q(q 为大素数,且 $q>2^k$,k 为安全参数)阶循环群 G,群 G 的一个生成元为 P;定义有限域 $GF(q)$,并选择有限域 $GF(q)$上的安全椭圆曲线 E_ω;定义抗碰撞的单向哈希函数:$H_1:GF(q)\rightarrow\{0,1\}^*$, $H_2:\{0,1\}^*\rightarrow Z_q^*$, $H_3:Z_q^*\rightarrow\{0,1\}^*$, $H_4:\{0,1\}^*\rightarrow\{0,1\}^*$;定义非对称密钥加/解密算法 $Enc()$和 $Dec()$及对称加/解密算法 $E()$和 $D()$;管理中心 MC 向各区域认证服务器发布基础公开参数:

$$Params=\{G,q,P,H_1,H_2,H_3,H_4,Enc,Dec,E,D,E_\omega\}.$$

(3) 各区域认证服务器分别产生本区域的主密钥和公开钥,妥善保管主密钥,并公开相应的系统参数.

如,HS 选取随机数 $KS_H=S_H\in Z_q^*$ 作为主密钥,其公钥为 $KP_H=S_HP$,则有等式 $KS_H^{-1}KP_H=S_H^{-1}S_HP=P$ 成立;HS 选择椭圆曲线 E_ω上的两个点 F_H和 Q_H,其中,F_H为公开基点,Q_H是 F_H的倍数点,即,存在 d_H,满足 $Q_H=d_HF_H$,其中,d_H为秘密信息需妥善保存,F_H和 Q_H为公开信息对外公布;HS 秘密保存主密钥 KS_H和秘密信息 d_H,公开系统参数 $\{G,q,P,H_1,H_2,H_3,H_4,Enc,Dec,E,D,KP_H,Q_H,F_H,E_\omega\}$.同理,RS 秘密保存主密钥 KS_R 和秘密信息 d_H,公开系统参数 $\{G,q,P,H_1,H_2,H_3,H_4,Enc,Dec,E,D,KP_R,Q_R,F_R,E_\omega\}$.

2.3 注册家乡域

如图 2 所示,家乡域注册阶段主要完成 US 在 HS 上的注册.注册过程中,HS 完成对 US 的身份合法性及终端平台可信性验证,为合法、可信的 US 派发漫游授权信息及临时身份信息等.

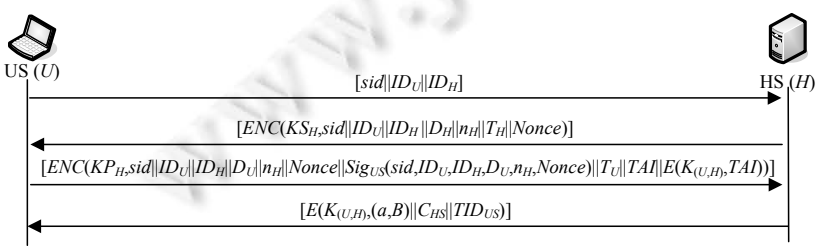


Fig.2 Registration home domain

图 2 注册家乡域

(1) US 向 HS 发送申请,注册家乡网络.

(2) HS 收到 US 的注册申请后,选取秘密随机数 $r_H\in Z_q^*$, 然后计算 $D_H=(r_H+KS_H)KP_U$,通过计算将秘密数 r_H

安全擦除.HS 选择随机数 $n_H \in Z_q^*$ 后,发送 $Enc(KS_H,sid||ID_U||ID_H||D_H||n_H||T_H||Nonce)$给 US,其中,$sid$ 为会话标识;时戳 T_H 和随机数 $Nonce$ 保证了消息的新鲜性,同时可防止重放攻击,并且,$Nonce$ 可用于标记通信消息是否得到相应的回复.

(3) US 收到 HS 的响应消息后,选取秘密随机数 $r_U \in Z_q^*$,然后计算 $D_U=(r_U+KS_U)KP_H$,通过计算将 r_U 安全擦除.计算协商密钥 $K_{(U,H)} = KS_U^{-1}(r_U + KS_U)D_H$ 和消息签名 $Sig_{US}(sid,ID_U,ID_H,D_U,Nonce)$.

根据 US 所持终端的类型,分以下两类讨论:

① US 持可信移动终端进行通信交互,终端的可信性验证信息包括平台可信性证明信息及证明信息的完整性验证信息.HS 通过身份验证信息和平台可信性验证信息,验证 US 身份的合法性和终端平台的可信性.

US 使用存储根密钥从安全芯片 MTM 中读取身份密钥 AIK_{Priv},并使用该密钥对平台配置寄存器值 $PCRs$ 和 n_H 进行签名,得到:$SIG_{TPM}(PCRs,n_H)=Enc(AIK_{Priv},PCRs||n_H)$,则 US 的平台可信性验证信息为 $TAI=SML||Cert(AIK_{Pub})||SIG_{TPM}(PCRs,n_H),SML$ 为完整性度量日志.US 计算 $E(K_{(U,H)},TAI)$,并发送 $Enc(KP_H,sid||ID_U||ID_H||D_U||n_H||Nonce||Sig_{US}(sid,ID_U,ID_H,D_U,n_H,Nonce)||T_U||TAI||E(K_{(U,H)},TAI))$给 HS.

② US 持普通移动终端进行通信,仅发送身份验证信息,HS 通过身份验证信息验证 US 的身份合法性.

US 发送 $Enc(KP_H,sid||ID_U||ID_H||D_U||n_H||Nonce||Sig_{US}(sid,ID_U,ID_H,D_U,n_H,Nonce)||T_U)$给 HS.

(4) HS 收到 US 的身份合法性及平台可信性验证请求后,首先验证签名 $Sig_{US}(sid,ID_U,ID_H,D_U,n_H,Nonce)$的合法性及参数的正确性,完成 US 的身份合法性验证,并且验证消息是否由 US 所发送.

验证通过后,HS 计算 $K_{(H,U)} = KS_H^{-1}(r_H + KS_H)D_U$,解密消息 $E(K_{(U,H)},TAI)$与接收到的 TAI 进行对比,检查 US 终端平台可信性验证信息的完整性,验证签名信息 $SIG_{TPM}(PCRs,S_H)$的合法性,即 $PCRs||n_H=Dec(AIK_{Pub},SIG_{TPM}(PCRs,n_H))$,基于随机数 n_H 判断可信性验证信息的新鲜性:若签名的合法性和新鲜性验证通过,则运用平台可信性验证策略对 US 终端平台的可信性进行验证;否则终止协议.若 US 持普通终端通信,则 HS 不进行上述可信性验证,仅进行身份合法性验证(下文只考虑用户持可信移动终端时的漫游情况).文献[19,20]对平台可信性验证策略及相关关键技术进行了详细研究,本文可使用该策略实现对 US 终端平台的可信性验证.限于篇幅,对终端平台的可信性验证策略及其关键技术不再赘述.

相关验证通过后,HS 为 US 生成漫游授权信息.HS 选取秘密随机数 $L \in Z_q^*$,产生 US 的漫游授权信息,具体过程如下:

① HS 计算 $B=LF_H$ 和 $a=d_HH_2(H_1(B))+L$;

② HS 为 US 计算临时的身份标识 $TID_{US}=S_{US}\oplus ID_{US}\oplus ID_{HS}$(其中,$S_{US}=H_4(ID_{US}||H_3(N_{HS}))$,$N_{HS}$ 为 HS 选取的随机数).

HS 保存$\langle S_{US},ID_{US},TID_{US},N_{HS}\rangle$为用户建立注册信息,便于提供 US 的匿名性撤销服务.HS 为 US 生成授权证书 C_{HS},并通过安全信道将授权信息(a,B)、授权证书 C_{HS} 和临时身份标识 TID_{US} 发送给 US,即 HS 发送消息 $E(K_{(U,H)},(a,B)\|C_{HS}\|TID_{US}\|T_H')$ 给 US.其中,$C_{HS}=Enc(KS_H,ID_{HS}||TID_{US}||T_{Begin}||T_{End})$主要包含 HS 的身份信息及授权范围和授权期限等相关信息,T_{Begin} 为授权起始时间,T_{End} 为授权的结束时间,则 $T_{End}-T_{Begin}$ 为授权证书的有效时长.

(5) US 收到漫游授权信息$\langle(a,B)\|C_{HS}\|TID_{US}\|T_H'\rangle$后,首先基于 HS 的公钥 PKH 及当前时戳验证授权证书 C_{HS} 的合法性及时效性,然后验证等式 $aF_H=Q_HH_2(H_1(B))+B$ 是否成立:若上述等式成立,则说明 HS 为 US 生成了合法、有效的漫游授权信息;否则终止协议.同时,在消息交互过程中,US 完成对 HS 的身份合法性验证,实现注册时 US 与 HS 间的双向身份认证.

授权证书 C_{HS} 的合法性及时效性验证过程如下:

① 用 HS 的公钥解密授权证书 C_{HS},判断接收到的身份标识是否与 C_{HS} 中封装的身份标识相一致:若一致,则进行第②步验证;否则终止,即,C_{HS} 是非法的授权证书.

② 根据当前时间 T_{Now} 与 T_{Begin} 间的关系,判断授权证书 C_{HS} 是否生效:若 $T_{Now}\geqslant T_{Begin}$,则进行第③步验证;

否则终止,即 C_{HS} 在当前时间未生效.

③ 根据当前时间 T_{Now} 与 T_{End} 间的关系,判断授权证书 C_{HS} 是否失效:若 $T_{End}\geqslant T_{Now}$,则认为授权证书 C_{HS} 是合法有效的;否则终止验证,即 C_{HS} 在当前时间已过期.

2.4 漫游远程域——安全漫游

US 获得 HS 的合法授权后,在漫游授权信息的有效时间($T_{End}\geqslant T_{Now}\geqslant T_{Begin}$)内,US 可多次向远程域认证服务器 RS 申请漫游服务.US 的一次漫游过程如图 3 所示.

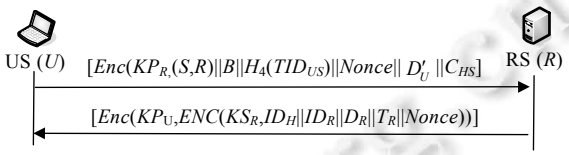


Fig.3 Roaming remote domain

图 3 漫游远程域

(1) US 选取秘密随机数 $r'_U\in Z_q^*$,然后计算 $D'_U=(r'_U+KS_U)PK_R$;选择秘密随机数 $b\in Z_q^*$,生成漫游验证信息 $R=bF_H$ 和 $S=aH_2(H_1(R)\oplus H_3(Nonce)\oplus H_4(TID_{US}))+b$,其中,$Nonce$ 为 US 选取的随机数,保证了验证信息的新鲜性.

US 生成当前时戳 T'_U,并发送签名认证消息 $Enc(KP_R,(S,R)\|B\|H_4(TID_{US})\|Nonce\|T'_U\|D'_U\|C_{HS})$ 给 RS,向远程服务域 RS 申请漫游服务.

(2) RS 收到 US 的漫游验证信息 $\langle(S,R)\|B\|H_4(TID_{US})\|Nonce\|T'_U\|D'_U\|C_{HS}\rangle$ 后,首先基于 HS 的公钥 PK_H 及当前时戳验证授权证书 C_{HS} 的合法性和有效性,若 C_{HS} 是合法且有效的授权证书,则继续验证等式 $SF_H=Q_HH_2(H_1(B)+B)H_2(H_1(R)\oplus H_3(Nonce)\oplus H_4(TID_{US}))+R$ 是否成立:若等式成立,则表明 US 持有真实有效的漫游验证信息,且其身份合法性已通过家乡域认证服务器 HS 的验证,即,US 是身份合法且平台可信的漫游申请者;否则终止协议.

RS 选取秘密随机数 $r_R\in Z_q^*$,然后计算 $D_R=(r_R+KS_R)KP_U$.RS 计算与 US 间的会话密钥 $K_{(R,U)}=KS_R^{-1}(r_R+KS_R)D_U$ 后,发送 $Enc(KS_U,Enc(KP_R,ID_H\|ID_R\|D_R\|T_R\|Nonce))$给 US.消息的加密传输确保通信消息仅能由 US 解密,保证了消息的机密性;同时,能够实现 US 对 RS 的身份认证.

(3) US 解密消息,首先验证消息的合法性;其次验证消息是否是由 RS 发送,并确认 RS 是否是其先前议定的远程域认证服务器,并验证 RS 的身份合法性,实现漫游认证过程中 US 和 RS 的双向身份认证;最后,US 计算会话密钥 $K_{(U,R)}=KS_U^{-1}(r_U+SK_U)D_R$,完成漫游服务申请.

2.5 匿名的可控性

当 RS 对 US 的验证信息产生怀疑或 US 漫游进入远程网络域后出现恶意匿名访问行为时,RS 可将漫游认证信息及相关公开信息提交给 HS 进行匿名身份追踪.HS 首先验证匿名追踪申请的合法性,然后,通过查询存储数据向 RS 提供 US 临时身份的哈希信息,则 RS 可获悉 US 临时身份的哈希值(记为 TID'_{US})及身份等隐私信息.RS 接收到 HS 的应答信息后,验证等式 $H_4(TID_{US})=TID'_{US}$(其中,TID_{US} 为 US 申请漫游服务时所提交的临时身份信息)是否成立:若成立,则 HS 提供了准确信息,即 RS 获知了 US 的真实身份;若等式不成立,则 HS 所提供的信息有误,RS 要求 HS 继续提供相关信息,即 HS 无法对恶意用户进行庇护.

本文基于用户行为的可信性检测机制控制恶意漫游用户的身份匿名性;然而行为的可信性检测并非本文的重点研究内容,因此本文未对该机制进行深入研究,仅仅对如何实现匿名的可控性进行了描述;由于行为可信性监测已是安全控制领域的研究热点,并且众多研究者[19,23,24]已在行为监测方面进行了相关研究,限于篇幅,本文对行为的可控性未作深入阐述,同时,下文对协议的可控性未作详细分析.

3 安全性证明

本节基于 CK 安全模型证明本文可控匿名漫游认证协议的安全性.

3.1 AM中的漫游协议

在本文协议中,RS 依赖 US 的漫游证明信息鉴别 US 的身份合法性及平台可信性.为简化协议证明过程,匿名漫游认证协议的两个阶段分别抽象描述为协议δ和φ,其中,δ为可信认证,φ为安全漫游.下面分别证明δ和φ是 AM 中的会话密钥安全的密钥交换协议.

协议δ描述如下:

① 注册请求.US 向 HS 发送注册请求消息,消息中包含相关参与者的身份标识$\{sid,ID_M,ID_H\}$.

② 注册响应.HS 收到 US 的注册请求后,选取秘密随机数 $r_H,n_H\in Z_q^*$,然后计算 $D_H=(r_H+KS_H)KP_U$.HS 发送消息 $Enc(KS_H,sid||ID_U||ID_H||D_H||n_H||T_H||Nonce)$给 US.

③ 可信性验证请求.US 收到 HS 的响应消息后,选取秘密随机数 $r_U\in Z_q^*$,然后计算 $D_U=(r_U+SK_U)KP_H$ 和 $K_{(U,H)}=KS_U^{-1}(r_U+KS_U)D_H$.生成验证信息 $TAI=SML||Cert(AIK_{Pub})||SIG_{TPM}(PCRs,n_H)$后,US 发送 $Enc(KP_H,sid||ID_U||ID_H||D_U||n_H||Nonce||Sig_{US}(sid,ID_U,ID_H,D_U,n_H,Nonce)||T_U||TAI||E(K_{(U,H)},TAI))$给 HS.

④ 可信性验证响应.HS 首先验证 US 签名及其参数的正确性,实现对 US 的身份合法性验证.验证通过后,HS 运用平台可信性验证策略对 US 平台的可信性进行验证.HS 为身份合法且平台可信的 US 发送漫游授权信息和临时标识号 TID_{US}.HS 发送消息 $E(K_{(U,H)},(a,B)\|C_{HS}\|TID_{US}\|T_H')$ 给 US.

协议φ描述如下:

① 漫游请求.US 在可信认证阶段获得漫游授权信息 $\langle(a,B)\|C_{HS}\|TID_{US}\|T_H'\rangle$,US 选取秘密随机数 $r_U'\in Z_q^*$,然后计算 $D_U'=(r_U'+KS_U)KP_R$,生成漫游验证信息(S,R).US 向 RS 发送消息:

$$Enc(KP_R,(S,R)\|B\|H_4(TID_{US})\|D_U'\|Nonce\|T_U'\|C_{HS}).$$

② 漫游响应.RS 收到 US 的漫游申请后,验证消息及参数的正确性,基于漫游验证信息(S,R)和授权证书 C_{HS}的合法性完成对 US 身份合法性和平台可信性的验证.RS 选取秘密随机数 $r_R\in Z_q^*$,然后计算 $D_R=(r_R+SK_R)PK_U$ 及与 US 间协商的会话密钥 $K_{(R,U)}=KS_R^{-1}(r_R+KS_R)D_U'$.RS 发送消息 $Enc(KP_U,Enc(KS_R,ID_H||ID_R||D_R||T_R||Nonce))$给 US.

③ US 验证 RS 的身份合法性,并计算会话密钥 $K_{(U,R)}=KS_U^{-1}(r_U'+KS_U)D_R$,完成跨域漫游服务申请.

定理 2. 当签名、非对称及对称加解密等算法均安全且难解时,协议δ和协议φ在 AM 中是会话密钥安全的.

证明:对δ协议而言,若 AM 中的协议δ满足会话密钥安全定义的两个性质,则δ在 AM 中是会话密钥安全的.

(1) 在协议δ交互过程中,由于消息参与者没有被敌手$\mathcal{A}$攻陷,协议执行完毕时,US 和 HS 得到没有篡改的 D_U和 D_H,则 US 和 HS 计算的会话密钥分别为

- $K_{(U,H)}=KS_U^{-1}(r_U+KS_U)D_H=KS_U^{-1}(r_U+KS_U)(r_H+KS_H)PK_U=(r_U+KS_U)(r_H+KS_H)P,$
- $K_{(H,U)}=KS_H^{-1}(r_H+KS_H)D_U=KS_H^{-1}(r_H+KS_H)(r_U+KS_U)KS_U=(r_U+KS_U)(r_H+KS_H)P,$

故 $K_{(H,U)}=K_{(U,H)}$,因此,协议δ满足会话密钥安全的性质 1.

(2) 对于会话密钥安全的性质 2 采用反证法证明.

假设 AM 中存在一个敌手$\mathcal{A}$能够以不可忽略的优势ε成功猜测会话密钥是真实的还是随机的,那么存在输入为 $(Params,D_U^*,D_R^*,K^*)$ 的算法$\mathcal{T}$,通过调用$\mathcal{A}$,能够以不可忽略的优势区分真实会话密钥和随机值,其中,*Params* 为本文协议的公开参数.

设猜测游戏的交互过程中$\mathcal{A}$发起会话的轮数为 L.具体交互过程如下:

① 选择随机数 $a\in\{1,2,\ldots,L\}$.

② 调用$\mathcal{A}$完成对 AM 中 US 与 RS 间匿名漫游认证协议的模拟,给$\mathcal{A}$提交 *Params* 作为协议执行的公共

参数.

③ 只要$\mathcal{A}$作为参与者,无论是参与一个新的会话密钥的建立(除第 a 次会话外)还是获得消息,都遵循匿名漫游认证协议中相应参与者的执行.当一个会话结束时,与之相关的密钥就要在参与者的内存中擦除;若参与者被攻陷或会话已暴漏(除第 a 次会话外),就把这个被攻陷的参与者或相应的会话密钥的所有信息提供给$\mathcal{A}$.

④ 在第 a 次会话中,输入(US,RS,a),调用 US 和 RS 的会话,设 US 向 RS 发送 (US,a,D_U^*).

⑤ RS 收到 (US,a,D_U^*) 后,向 US 发送 (RS,a,D_R^*).

⑥ 如果 US 选择会话(US,RS,a)作为最后一次测试会话,那么向$\mathcal{A}$提供 K^*作为询问应答.

⑦ 如果会话(US,RS,a)没有暴漏,或者选择了第 a 轮会话外的某一次会话作为最后一次测试会话,或者$\mathcal{A}$没有选择测试会话就终止了,那么$\mathcal{T}$输出 $b'\leftarrow\{0,1\}$,然后终止.

⑧ 如果$\mathcal{A}$终止并输出比特 b',那么$\mathcal{T}$终止,并且也输出比特 b'.

根据$\mathcal{A}$的测试会话是否与算法$\mathcal{T}$选择的一致,分两种情况讨论:

① 敌手$\mathcal{A}$选择的测试会话和$\mathcal{T}$随机选择的会话相同.

在测试会话中,给$\mathcal{A}$的应答为 K^*,若算法$\mathcal{T}$的输入为$(Params,D_U,D_R,K)$,即是真实的会话密钥协商参数和会话密钥,则给$\mathcal{A}$的询问应答就是US和RS在会话 a 中的真实会话密钥 K;若算法$\mathcal{T}$的输入为$(Params,D_U^*,D_R^*,K^*)$,即是随机值,那么询问的应答也是随机的.如果$\mathcal{A}$能够以 $\frac{1}{2}+\varepsilon$ 的概率猜对测试应答是真实值还是随机值,其中,ε是不可忽略的,那么这也等价于算法$\mathcal{T}$以 $\frac{1}{2}+\varepsilon$ 的概率猜对其输入是真实会话密钥还是随机值.

② 敌手$\mathcal{A}$的第 a 次会话没有被选作测试会话.

在这种情况下,算法$\mathcal{T}$通常输出一个随机比特,然后结束会话.因此,猜对输入分布的概率是 $\frac{1}{2}$. 令事件$\mathcal{E}$表示敌手$\mathcal{A}$选择的测试会话恰好是第 a 次会话, $\Pr[\mathcal{E}]=\frac{1}{L}$, 并且敌手$\mathcal{A}$能够以不可忽略的优势$\varepsilon$猜对测试应答是真实值还是随机值,则有 $\Pr[\mathcal{A}\text{ 猜测成功}]=\left(\frac{1}{2}+\varepsilon\right)\Pr[\mathcal{E}]+\frac{1}{2}(1-\Pr[\mathcal{E}])=\frac{1}{2}+\frac{\varepsilon}{L}$.

由于算法$\mathcal{T}$以敌手$\mathcal{A}$为子程序运行,则有 $\Pr[\mathcal{T}\text{ 猜测成功}]=\Pr[\mathcal{A}\text{ 猜测成功}]$,即算法$\mathcal{T}$能够以不可忽略的优势区分真实会话密钥和随机值.因此,协议δ满足会话密钥安全的性质 2.

在 AM 中,由于敌手不能对消息进行伪造、篡改和重放,只能真实地转发合法参与者产生的消息,US 和 HS 得到没有篡改的身份合法性及平台可信性验证信息,并协商了安全的会话密钥 $K_{(U,H)}$和 $K_{(H,U)}$,所以协议δ在 AM 中是安全的.

同理,协议φ在 AM 中是会话密钥安全的. □

3.2 认证器构造

本文从 HS 认证 US(协议δ)、RS 认证 US(协议φ)着手构造认证器.

(1) 对于 US 与 HS 间的认证信息流,采用基于时戳的签名认证器$\lambda_{Sig,T}$,其安全性、匿名性证明过程详见文献[22],具体过程如下:

① $\mathcal{A}$获取时间戳 T_A,计算签名 $Sig(m,T_A,ID_B)\rangle$,发送消息$\langle m,Sig(m,T_A,ID_B)\rangle$给$\mathcal{B}$.

② $\mathcal{B}$接收到消息后,检查时戳 T_A 的新鲜性及验证签名 $Sig(m,T_A,ID_B)\rangle$的合法性,若 T_A 新鲜且签名正确,则$\mathcal{B}$完成对$\mathcal{A}$的认证.

(2) 对于 US 与 RS 间的认证消息,由于 US 的验证信息既不能包含 US 的真实身份信息,又能够让 RS 验证 US 是否拥有真实身份和可信终端平台,故使用基于身份的匿名认证器$\lambda_{Enc,TID,T}$,其安全性、匿名性证明详见文献[21],具体过程如下:

① $\mathcal{A}$注册获得临时身份信息 TID_A,用$\mathcal{B}$的公钥加密产生密文消息 $Enc(KP_B,m||T_A||TID_A)$),最后将$\langle TID_A, Enc(KP_B,m||T_A||TID_A)\rangle$发送给$\mathcal{B}$.

② $\mathcal{B}$接收到消息后解密密文消息,验证 TID_A 是否合法:若为非法用户,则终止执行;否则,检查时间戳 T_A 的新鲜性,若验证通过,则$\mathcal{A}$通过$\mathcal{B}$的认证.

3.3 UM中的协议

首先,将上述认证器$\lambda_{Sig,T}$和$\lambda_{Enc,TID,T}$应用于本文 AM 中的协议消息流,在不影响协议可证安全性的前提下,将 US 的身份标识隐藏起来,使攻击者无法获得其真实有效的身份信息;最后,应用文献[18]中的方法优化 UM 中的协议,且该优化过程并不影响协议的安全性.图 4 所示为 UM 中的协议δ和协议φ.

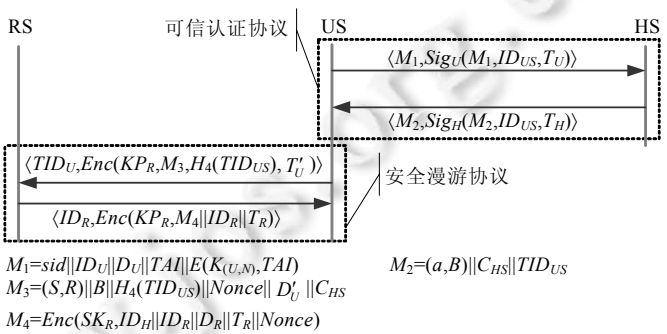


Fig.4 Protocols δ and φ in the UM

图 4 UM 中的协议δ和协议φ

定理 3. 当签名、非对称及对称加解密等算法安全且难解时,协议δ和协议φ在 UM 中是安全的,即,本文协议是安全的漫游协议.

证明:运用认证器$\lambda_{Sig,T}$和$\lambda_{Enc,TID,T}$把协议δ和协议φ直接转化为 UM 环境中会话密钥安全的密钥交换协议.由于所采用的认证器是可证安全的,可知 UM 中的协议δ和协议φ是可证安全的. □

对认证协议δ的一些说明:

① US 基于真实身份 ID_{US} 向 HS 注册,HS 密钥协商参数 D_H 及随机数 n_H 的加密传输,在保证消息完整性的同时,可使 US 验证 HS 是否是其合法的家乡域认证服务器,实现 US 与 HS 间的双向身份认证。

② US 基于 HS 发送的秘密随机数 n_H 生成平台可信性及身份合法性验证信息,随机数 n_H 确保了验证信息的新鲜性。

③ HS 为身份合法且平台可信的 US 生成授权证书 C_{HS} 和授权信息(a,B);同时,为 US 建立相应的注册信息,对恶意 US 进行匿名的控制操作.

对漫游协议φ的一些说明:

① 当 US 进行远程域漫游时,US 基于安全哈希函数 $H_4()$实现临时身份标识 TID_{US} 对远程域认证服务器 RS 的匿名性;利用 RS 的公钥加密不仅确保了漫游申请消息的安全性,而且实现了用户身份的保密;时戳及随机数的使用能够防止敌手进行重放攻击,并且保证协商密钥的新鲜性.

② RS 无需本地域认证服务器 HS 的协助,基于授权证书 C_{HS} 和漫游证明信息(S,R)的合法性直接完成对 US 的身份合法性验证;US 通过 RS 的签名应答消息对 RS 的身份进行验证,实现漫游过程中 US 与 RS 间的身份合法性双向认证.

③ 在 US 与 RS 间实现匿名漫游的同时,完成会话密钥的安全协商,由于双方均选取随机秘密数参与会话密钥的协商,保证了会话密钥的新鲜性,并且使得会话密钥具有较强的前后向安全性;同时,任何一方都无法伪造会话密钥.

④ 密钥协商过程中消息完整性的保证是必不可少的.在 US 与 RS 间的密钥协商过程中,消息的加密传输确保了密钥协商参数的完整性.

4 模型分析

本节对本文可控匿名漫游认证协议的匿名性等属性进行分析.

4.1 匿名性分析

漫游通信消息中均未出现 US 的真实身份,US 的真实身份 ID_U 被其临时身份标识 TID_U 替代.因仅有 HS 掌握秘密数 S_H,所以只有 HS 才能还原用户的真实身份 ID_U,因此,本文协议采用临时身份标识实现用户身份的匿名性保护,确保了用户身份的机密性,并且在漫游认证过程中保护用户匿名性的同时并未降低其安全性.

漫游验证信息仅能报告 US 的身份是否合法,平台是否可信,并未包含 US 的配置信息及其身份等隐私信息,即,验证信息具有匿名性,并且匿名性的强弱取决于授权证书 C_{HS} 有效时间的长短,越短则匿名性越强,同时,其匿名性是可控的,可控性依赖于漫游用户的临时身份标识,仅允许合法的用户与 RS 建立漫游服务.

特别地,本文为实现用户漫游过程的高效性,注册家乡域时,HS 基于 US 的真实身份为其产生临时身份标识 TID_U,并将其封装在授权证书 C_{HS} 中.对于 RS 而言,无法获知 US 的真实身份,但当 US 向同一 RS 多次申请漫游时,RS 可将多次漫游申请关联起来.由于 RS 是安全可信的,因此 RS 对漫游申请的关联并未对协议的安全性造成影响;若 US 追求漫游过程的强匿名性,则 US 每次漫游之前向 HS 申请凭证 C_{HS},保证 US 每次漫游时所持有的临时身份标识各不相同,确保 US 具有强匿名性和不可追踪性.

4.2 安全性分析

4.2.1 抗伪造性

由于 US 通过秘密随机数和临时身份标识生成漫游认证信息(S,R),而由于 HS 无法获悉随机数,则无法伪造 US 的漫游认证信息;若 HS 欲通过椭圆曲线上的已知点求解随机数,则将面临椭圆曲线离散对数难解问题.因此,HS 无法伪造 US 的漫游认证信息;同理可知,RS 和攻击者同样无法伪造 US 的漫游认证信息.即,除 US 外的任何人都无法产生有效的漫游验证信息.

4.2.2 可验证性

定理 4. US 可验证 HS 漫游授权信息的合法性.

证明:因为 $aF_H=[d_HH_2(H_1(B))+L]F_H=d_HF_HH_2(H_1(B))+LF_H$,已知 $Q_H=d_HF_H$ 和 $B=LF_H$,因此当等式 $aF_H=Q_HH_2(H_1(B))+B$ 成立时,HS 的漫游授权信息通过了 US 的验证. □

定理 5. RS 可验证 US 漫游认证信息的合法性.

证明:因为 $SF_H=aF_HH_2(H_1(R)\oplus H_3(Nonce)\oplus H_4(TID_{US}))+bF_F$,已知 $a=d_HH_2(H_1(B))+L$ 和 $R=bF_H$,则有:

$$SF_H=(Q_HH_2(H_1(B))+B)H_2(H_1(R)\oplus H_3(Nonce)\oplus H_4(TID_{US}))+bF_F;$$

因此,当等式 $SF_H=Q_HH_2(H_1(B)+B)H_2(H_1(R)\oplus H_3(Nonce)\oplus H_4(TID_{US}))+R$ 成立时,US 的漫游认证信息通过了 RS 的验证. □

4.2.3 不可否认性

由抗伪造性分析可知:除 US 外的任何人都无法产生有效的漫游验证信息;同时,漫游验证信息(S,R)中包含签名者的临时身份标识 TID_{US}.因此,US 不能否认已产生的漫游验证信息,并且通过漫游验证信息中的相关身份标识可判断漫游验证信息是由 US 生成的.

4.2.4 无关联性

US 基于随机数 *Nonce* 产生漫游验证信息(S,R),保证了验证信息的新鲜性,同时确保除 US 外的任何人都无法将 US 的不同验证信息进行关联.因此,攻击者无法将截获的漫游验证信息与已有信息相关联,确保了 US 身份和位置等隐私信息的不可跟踪性,可有效防止攻击者针对 US 实施跟踪、窃听等攻击行为.

4.2.5 抗替换攻击

若攻击者通过非法手段获得 US 的漫游验证信息(*S*,*R*)后,持(*S*,*R*)向 RS 证明其是 HS 的合法授权用户,由于临时身份标识将验证信息与 US 进行了绑定,然而攻击者无法提供正确的临时身份标识,导致其无法通过 RS 对(*S*,*R*)的合法性验证.

4.3 性能分析

本节将本文协议与其他相关漫游认证机制就漫游过程的通信消息和计算效率进行比较.为方便对本文协议进行性能分析,本节以文献[9]中经典的匿名漫游认证协议为例简要介绍传统漫游认证协议[11−16]的 2 轮交互认证模式的执行流程及认证特点.限于篇幅,具体过程详见文献[9].

传统漫游认证协议[9]的消息交互过程包含以下步骤:① 用户 US 向远程域申请漫游,发送申请消息给远程域的认证服务器 RS;② RS 收到 US 的漫游申请后,由于 RS 未掌握 US 的具体注册信息,因此无法独自完成对 US 的合法性验证,则 RS 生成认证信息,并发送认证询问消息给 US 的家乡域认证服务器 HS;③ HS 对 US 的合法性进行验证,并构造应答消息将验证结果返回给远程域认证服务器 RS;④ RS 根据 HS 对 US 的合法性验证结果,制定相应的漫游访问策略,并发送响应消息给 US.

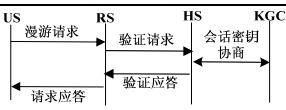
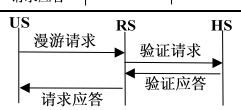
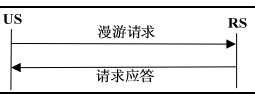
在传统的漫游认证协议中,当 US 向 RS 申请漫游时,由于未掌握漫游用户的注册信息,RS 需在 HS 的协助下完成 US 的合法性验证,即 RS 将 US 的漫游证明信息发给 HS,由 HS 负责验证 US 的合法性,RS 根据 HS 的验证反馈制定相应的决策.因此,传统的漫游认证协议采用 2 轮交互的认证模式完成对 US 的身份合法性验证.

4.3.1 通信效率

表 2 给出了本文漫游认证协议与其他相关漫游认证机制[8−17]就通信时延和漫游特点等方面的比较结果.

Table 2 Comparsion of communication time delay

表 2 漫游通信时延比较

	漫游认证模型	漫游特点	通信时延	可控性
文献[8]		RS 在 HS 的协助下完成对 US 身份合法性验证,并且通过 KGC 完成会话密钥的协商	大	未涉及可控性
文献[9−17]		RS 在 HS 的协助下完成对 US 身份合法性验证.验证由 2 轮消息交互完成	较大	未涉及可控性
本文协议		RS 通过 US 的验证信息直接完成对其身份合法性及终端平台可信性的验证.由 1 轮消息交互完成	小	具有可控性

在本文协议中,因 US 在向远程域 RS 申请漫游前已完成本地域的注册工作,即已获得 HS 的授权信息,因此无需 HS 的协助,基于漫游验证信息 US 与 RS 间通过 1 轮消息交互即可完成漫游服务的申请即验证,通信时延远远低于其他传统漫游认证机制[8−17],降低了漫游过程的通信负载和切换时延,提高了异构无线网络下 US 的切换速度和协议的执行效率.

本文协议将传统漫游协议的 2 轮交互认证模式改进为 1 轮交互认证模式;相对于传统漫游协议而言,本文协议降低了 RS 和 HS 的计算负载,减少了协议的消息交互轮数,降低了通信时延.

4.3.2 计算效率

本文协议中 RS 无需 HS 的协助,基于 1 轮消息交互即可完成对 US 合法性的验证,降低了用户终端的计算负载和通信时延,减少了协议的交互轮数.

表 3 给出了本文协议与部分传统漫游认证协议[8−13]在漫游过程中的计算开销比较结果.表 3 中仅对计算量较大的相关运算进行了统计对比,对计算量较小的相关运算(如异或运算、哈希运算等)并未统计.

从表 3 数据来看,每执行一次本文协议的漫游认证,US 和 RS 都进行一次椭圆曲线运算和一次非对称加密

运算,US 的计算量远小于文献[8,10,13],延续了文献[12,14]计算量小的优势.但在本文协议中,RS 无需 HS 的协助,基于 1 轮消息交互即可完成对 US 身份合法性和终端平台可信性的验证,在通信时延方面具有较大的优势.

Table 3 Comparsion of computation efficiency

表 3 计算效率比较

相关运算	本文协议	文献[13]	文献[12]	文献[11]	文献[10]	文献[9]	文献[8]
双线性运算(US/RS/HS)	–	1/0/1	–	–	0/0/1	0/0/1	4/4/4
椭圆曲线运算(US/RS/HS)	1/1/0	–	–	–	–	–	–
对称加解密(US/HS/RS)	–	2/4/2	1/1/0	0/0/1	1/1/1	2/1/1	2/0/2
非对称加解密(US/HS/RS)	1/1/0	3/3/2	1/1/2	2/2/1	2/1/1	0/3/3	0/1/1
指数运算(US/HS/RS)	–	–	–	–	–	2/1/2	–
MAC 次数(US/HS/RS)	–	–	–	1/0/0	–	–	2/2/2
信息交换次数(US-RS/RS-HS)	2/0	2/2	2/2	2/2	2/2	2/2	3/2

注:“–”表示该协议未涉及此操作

整体而言,本文协议具有消息交互轮数少、通信时延低和执行效率高的特点,并且本文协议对 US 的恶意匿名漫游具有可控性的特点.但由于安全性与计算开销间仅能寻求平衡,因此,为了确保通信过程的安全性,本文协议漫游过程中使用了非对称加解密、签名等运算量较大的算法,在实际应用中,可根据环境的具体要求减少对通信消息的加、解密及签名操作.

4.4 协议特点

4.4.1 直接性

US 从 HS 处获得注册授权信息后,无需 HS 的参与,US 就可直接向 RS 进行身份合法性证明,减少了漫游认证协议的消息交互轮数,即 RS 基于漫游证明信息直接完成对 US 身份合法性的验证.

4.4.2 认证性

在没有泄露 US 秘密信息及其注册信息的前提下,RS 可基于漫游证明信息的合法性完成对 US 的身份合法性验证;若合法性验证通过,RS 就认为 US 是 HS 上注册的合法移动节点,即 RS 对 US 的身份合法性鉴别通过.

4.5 实用性

本文协议可适用于 3G/4G 网络环境下移动用户 US 的漫游通信及资费服务,RS 为 US 提供服务且收取费用,若 US 每漫游移动一次就缴费一次,则将带来诸多不便.因此在 US 漫游身份认证过程中,RS 向 HS 收取服务费用,HS 再向 US 收取.因漫游过程中 US 持 HS 授权的漫游验证信息向 RS 证明其身份合法性及平台可信性,所以 US 无法否认因漫游而产生的费用,并且本文的漫游认证协议可满足基于 IP 的无线网络环境下移动用户的漫游认证需求,同时,本文协议不仅可完成可信移动终端的漫游认证工作,同时可在传统网络(非可信计算环境)中完成移动终端的漫游服务请求,因此,本文的漫游协议具有强兼容性.

5 结束语

由于椭圆曲线具有安全性高、密钥短小、运算速度快等优势,本文针对传统漫游认证机制无法满足可信计算环境下移动可信终端漫游服务时的平台可信性认证需求,并且不具备匿名的可控性的不足,提出了异构无线网络下可控匿名漫游认证协议.用户持移动可信终端申请漫游服务时,远程网络认证服务器基于用户验证信息的真实性及有效性,完成对移动可信终端的合法性验证.采用临时身份标识实现用户的匿名性保护,不仅使远程网络和攻击者无法获知用户的真实身份,而且保证了用户身份和位置等隐私信息的机密性;同时,攻击者无法将截获的验证信息与已有的通信信息相关联,确保了用户身份和位置等隐私信息的不可跟踪性,可有效防止攻击者针对用户实施跟踪、窃听等攻击行为.本文的协议在实现可信漫游的同时并未降低安全性,同时具有匿名性、扩展性及匿名的可控性等特点,并且具有安全性高、执行效率高、兼容性强和应用广泛的优势.所以,相对于传统的漫游机制而言,本文协议更适合于异构无线网络.为方便对本文漫游认证协议基本工作原理的介绍,我们以

异构无线网络为应用场景对本文漫游认证协议进行了详细介绍,但是本文协议同样适用于基于 IP 的无线网络环境.

下一步,我们将在本文协议的基础上继续深入对轻量级漫游认证机制的研究,在满足匿名漫游认证安全性的基础上,进一步降低移动终端的计算负载;同时,将在更弱的安全性假设(如认证服务器的密钥会发生泄露)下,对安全漫游机制进行研究.

References:

[1] Zhu JM, Ma JF. An efficient authentication protocol with anonymity for wireless IP networks. Journal on Communications, 2004, 25(6):12−18 (in Chinese with English abstract).

[2] Peng HX, Feng DG. Security flaws and improvement to a wireless authentication protocol with anonymity. Journal on Communications, 2006,27(9):78−85 (in Chinese with English abstract).

[3] Jiang YX, Lin C, Shen XM. Mutual authentication and key exchange protocols for roaming services in wireless mobile networks. IEEE Trans. on Wireless Communications, 2006,5(9):2569−2577. [doi: 10.1109/TWC.2006.05063]

[4] Yang GM, Wong DS, Deng XT. Anonymous and authenticated key exchange for roaming networks. IEEE Trans. on Wireless Communications, 2007,6(9):3461−3472. [doi: 10.1109/TWC.2007.06020042]

[5] Yang GM, Wong DS, Deng XT. Formal security definition and efficient construction for roaming with a privacy-preserving extension. Journal of Universal Computer Science, 2008,14(3):441−462.

[6] Shi MH, Rutagemwa H, Shen XM. A service-agent-based roaming architecture for WLAN/cellular integrated networks. IEEE Trans. on Vehicular Technology, 2007,56(5):3168−3181. [doi: 10.1109/TVT.2007.900525]

[7] Jiang J, He C, Jiang L. On the design of provably secure identity-based authentication and key exchange protocol for heterogeneous wireless access. In: Proc. of the Int'l Conf. on Communications, Networking and Mobile Computing. Berlin, Heidelberg: Springer-Verlag, 2005. 972−981. [doi: 10.1007/11534310_102]

[8] Peng HX. An identity-based authentication model for multi-domain. Chinese Journal of Computers, 2006,29(8):1271−1281 (in Chinese with English abstract).

[9] Zhu H, Li H, Shu WL, Wang YM. ID-Based wireless authentication scheme with anonymity. Journal on Communications. 2009,30(4):130−136 (in Chinese with English abstract).

[10] Jiang Q, Li GS, Ma JF. Security flaws and improvement of an ID-based wireless authentication scheme with anonymity. Journal on Communications, 2010,31(9A):209−216 (in Chinese with English abstract).

[11] Hou HF, Ji XS, Liu GQ. Identity-Based anonymity authentication protocol in the heterogeneous wireless network. Journal on Communications, 2011,32(5):153−161 (in Chinese with English abstract).

[12] Hou HF, Ji XS, Liu GQ, Zhang QW. Provable security authentication scheme based on public key for heterogeneous wireless network. Journal of Electronics & Information Technology, 2009,30(10):2385−2391 (in Chinese with English abstract).

[13] Jiang Q, Ma JF, Li GS, Liu HY. Identity-Based roaming protocol with anonymity for heterogeneous wireless networks. Journal on Communications, 2010,31(10):138−145 (in Chinese with English abstract).

[14] Wu ZQ, Zhou YW, Qiao ZR. Access mechanism of trusted mobile platform under mobile network. Journal on Communications, 2010,31(10):158−169 (in Chinese with English abstract).

[15] Wang LM, Jiang SR, Guo YB. Composable-Secure authentication protocol for mobile sensors roaming in the Internet of things. Scientia Sinica (Informationis), 2012,42(7):815−830 (in Chinese with English abstract). [doi: 10.1360/112011-1081]

[16] Xu J, Zhu WT, Feng DG. An efficient mutual authentication and key agreement protocol preserving user anonymity in mobile networks. Computer Communications, 2011,34(3):319−325 (in Chinese with English abstract). [doi: 10.1016/j.comcom.2010.04.041]

[17] Yoon EJ, Yoo KY, Ha KS. A user friendly authentication scheme with anonymity for wireless communications. Computers and Electrical Engineering, 2011,37(3):356−364. [doi: 10.1016/j.compeleceng.2011.03.002]

[18] Tin YST, Boyd C, Nieto JG. Provably secure key exchange: An engineering approach. In: Proc. of the Australasian Information Security Workshop. Adelaide: Australian Computer Society, 2003. 97−104.

[19] Wu ZQ, Zhou YW, Qiao ZR. A controllable and trusted anonymous communication scheme. Chinese Journal of Computers, 2010, 33(9):1686−1702 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2010.01686]

[20] Zhou YW, Wu ZQ, Jiang L. Cross-Domain mechanism of anonymous attestation for distributed network. Journal of Computer Applications, 2010,30(8):2120−2124 (in Chinese with English abstract). [doi: 10.3724/SP.J.1087.2010.02120]

[21] Canerri R, Krawczyk H. Analysis of key-exchange protocols and their use for building secure channels. In: Proc. of the Eurocrypt. Berlin, Heidelberg: Springer-Verlag, 2001. 453−474. [doi: 10.1007/3-540-44987-6_28]

[22] Jiang Q, Ma JF, Li GS, Ma Z. Security integration of WAPI based WLAN and 3G. Chinese Journal of Computers, 2010,33(9): 1675−1685 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2010.01675]

[23] Liu WW, Han Z, Shen CX. Trusted network connect control based on terminal behavior. Journal on Communications, 2009,30(11): 127−134 (in Chinese with English abstract).

[24] Li XY, Gui XL, Mao Q, Leng DQ. Adaptive dynamic trust measurement and prediction model based on Behavior Monitoring. Chinese Journal of Computers, 2009,32(4):664−674 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2009.00664]

附中文参考文献:

[1] 朱建明,马建峰.一种高效的具有用户匿名性的无线认证协议.通信学报,2004,25(6):12−18.

[2] 彭华熹,冯登国.匿名无线认证协议的匿名性缺陷和改进.通信学报,2006,27(9):78−85.

[8] 彭华熹.一种基于身份的多信任域认证模型.计算机学报,2006,29(8):1271−1281.

[9] 朱辉,李晖,苏万力,王育民.基于身份的匿名无线认证方案.通信学报,2009,30(4):130−136.

[10] 姜奇,李光松,马建峰.基于身份的匿名无线认证方案的安全缺陷及改进.通信学报,2010,31(9A):209−216.

[11] 侯惠芳,季新生,刘光强.异构无线网络中基于标识的匿名认证协议.通信学报,2011,32(5):153−161.

[12] 侯惠芳,季新生,刘光强,张秋闻.基于公钥的可证明安全的异构无线网络认证方案.电子与信息学报,2009,30(10):2385−2391.

[13] 姜奇,马建峰,李光松,刘宏月.基于身份的异构无线网络匿名漫游协议.通信学报,2010,31(10):138−145.

[14] 吴振强,周彦伟,乔子芮.移动互联网下可信移动平台接入机制.通信学报,2010,31(10):158−169.

[15] 王良民,姜顺荣,郭渊博.物联网中移动 Sensor 节点漫游的组合安全认证协议.中国科学:信息科学,2012,42(7):815−830.

[19] 吴振强,周彦伟,乔子芮.一种可控可信的匿名通信方案.计算机学报,2010,33(9):1686−1702. [doi: 10.3724/SP.J.1016.2010.01686]

[20] 周彦伟,吴振强,蒋李.分布式网络环境下的跨域匿名认证机制.计算机应用,2010,30(8):2120−2124. [doi: 10.3724/SP.J.1087.2010.02120]

[22] 姜奇,马建峰,李光松,马卓.基于 WAPI 的 WLAN 与 3G 网络安全融合.计算机学报,2010,33(9):1675−1685. [doi: 10.3724/SP.J.1016.2010.01675]

[23] 刘巍伟,韩臻,沈昌祥.基于终端行为的可信网络连接控制方案.通信学报,2009,30(11):127−134.

[24] 李小勇,桂小林,毛倩,冷东起.基于行为监控的自适应动态信任度测模型.计算机学报,2009,32(4):664−674. [doi: 10.3724/SP.J.1016.2009.00664]

周彦伟(1986－),男,甘肃通渭人,博士生,工程师,主要研究领域为密码学,匿名通信技术,可信计算.

杨波(1963－),男,博士,教授,博士生导师,主要研究领域为密码学,信息安全.

张文政(1966－),男,研究员,主要研究领为密码学,信息安全.