一个前向安全的基于 RSA 的多服务器的认证协议

杜浩瑞 陈建华 戚明平 彭 聪 范 青
(武汉大学数学与统计学院 武汉 430072)

摘 要 设计安全、实用的多服务器下密钥协商协议是当前信息安全领域研究的热点。基于设计协议的一般准则,讨论了 Wang 等[15]设计的一个匿名的基于生物特征的多服务器的密钥认证协议方案,指出了该协议无法抵抗服务器假冒攻击、智能卡丢失攻击、会话密钥泄露攻击;同时该方法因用户匿名性失效易造成用户隐私泄露的问题,所以不适用于实际应用。为了弥补这些缺陷,文中给出了一种基于 RSA 密钥的改进协议。在注册阶段,RC 和服务器共享不同的密钥、时间标记等来有效抵抗服务器假冒攻击和实现匿名性、不可追踪性等。在登录阶段,协议采用公钥技术来实现用户动态身份的登录和保证前向安全性等。在认证阶段,协议包括 3 次相互认证,并对消息做新鲜性检测等,实现相互认证以防止重放攻击等。最后,协议对可能存在的攻击进行安全分析和效率分析,证明了改进协议能抵抗丢失智能卡攻击、匿名性等攻击。同时,该协议尽量保持了简单的运算。

关键词 RSA,匿名,多服务器,密钥协商,前向安全
中图法分类号 TP309 **文献标识码** A

Forward-secure RSA-based Multi-server Authentication Protocol

DU Hao-rui CHEN Jian-hua QI Ming-ping PENG Cong FAN Qing
(School of Mathematics and Statistics, Wuhan University, Wuhan 430072, China)

Abstract The design of secure and practical key agreement protocol under multi-server is a hot topic in the field of information security. Based on the general principles of protocol design, this paper discussed the research of an anonymous multi-server key authentication protocol scheme based on biological characteristics designed by Wang et al. It pointed out that server counterfeiting attack, smart card loss attack and session key leakage attack can be realized in this protocol. At the same time, due to the failure of user anonymity, it is easy to leak user privacy, so it is not suitable for practical application. To remedy these shortcomings, a key improvement protocol based on RSA was proposed. In the registration stage, RC and server share different keys and time markers, which can effectively resist server counterfeiting attacks and achieve anonymity and untraceable ability. In the login phase, the protocol uses public key technology to realize the login and forward security of users' dynamic identity. In the authentication stage, the protocol includes three times of mutual authentication, does freshness detection of messages, and realizes mutual authentication to prevent replay attacks and so on. Finally, the security analysis and efficiency analysis of the possible attacks prove that the improved protocol can resist the attacks of losing smart card, anonymity and so on. At the same time, it maintains a simple operation.

Keywords RSA, Anonymity, Multi-server, Key agreement, Forward security

互联网的发展加快了人们进入信息时代的步伐,同时信息量也逐渐增大。特别地,智能手机的普及激发了人们对信息的获取,而且对信息的时效性有更高的要求。这就使得人们不得不在服务器之间来回切换以节约时间成本。另外,互联网的广泛应用促使生活方式发生改变,一部智能手机就可以完成商品交易。但在使用互联网的过程中,个人信息难免会无意泄露,从而让非法分子有可乘之机。产生这些问题很重要的一点是认证协议的不完善,因此,设计一种安全高效的认证协议迫在眉睫。2001 年 Tuaur[1]第一次将"口令+智能卡"应用于多服务器环境认证协议,用户使用一个口令即可登录多个不同的服务器。但传统的双因子认证协议[2-7]具有低熵这一缺点,攻击者可通过离线口令猜测攻击和窃听攻击来获得用户口令和身份。为了解决这一难题,2010 年 LI 等[8]提出基于生物特征值的身份认证协议,不幸的是该协议并非多服务器下的身份认证协议,同时也无法抵抗服务器拒绝服务等攻击。2011 年,Yoon 等[9]提出基于椭圆曲线的多服务器下匿名三因子认证协议。随后,Kim 等[10]提出 Yoon 的协议不能抵抗内部攻击、离线口令猜测等。同时,He 等[11]提出多服务器下认证密钥交换协议,但是被 Odelu 等[12]指出无法保证假冒攻击和重放攻击。2014 年 Chuang 等[13]提出一种仅使用 hash 运算的多服务器下三因子身份认证协议的高效协议。但是被 Mishar 等[14]提出此协议存在假冒攻击和服务器欺骗攻击等。至此,王瑞兵等[15]提出一个匿名性的密钥协商方案,宣称能抵抗各种攻击且提供匿名性。另外,Chaudhry 等[16]提出将椭圆曲线和生物特征值结合起来,并且在效率上做了很大的改进。但 Xia 等[17]提出该协议无法抵抗假冒攻

杜浩瑞(1994—),男,硕士,主要研究方向为数论与密码,E-mail:634064631@qq.com;**陈建华**(1963—),男,教授,博士生导师,主要研究方向为数论与密码,E-mail:chenjh_ecc@163.com(通信作者)。

击等，同时，提出自己的优化方案，并对常见攻击模型做出形式化得证明。之后，殷秋实等[18]在 Xia 方案的基础上提出一种更加高效的方案。汪定等[19-20]指出 Wan 等[21]协议无法实现离线口令猜测攻击、匿名性等，指出 Amin 等[22]的方案对抗前向安全攻击是脆弱的，以及 Reddy 等[23]不能抵抗用户假冒攻击且无法实现用户不可追踪性。

本文从实用性和安全性方面对文献[15]的方案深入分析，发现该方案并未实现匿名性，而且容易遭受服务器假冒攻击和智能卡丢失攻击等。本文回顾了文献[15]的认证方案，详细分析了方案中可能受到的攻击类型。同时，提出一个前向安全的基于 RSA 的多服务器的认证协议，并对安全性做了分析。

1 文献[15]的密钥认证协议方案

文献[15]提出一个匿名的基于生物特征的多服务器的密钥认证协议方案，该方案包含服务器注册阶段、用户注册阶段、登录阶段、认证阶段、口令修改阶段。本节回顾该认证方案，为使描述方便，统一使用该方案所使用的符号，同时增补了后文所用到符号，如表 1 所列。

表 1 符号说明

符号	说明	符号	说明
U_i	用户	y	RC 确定秘密数
ID_i	用户的身份	$h_i(),i=0,1,2,3$	hash 函数
PW_i	用户的口令	$\|$	字符串连接符
BIO_i	用户的生物特征	$\oplus$	异或服务器
RC	注册中心	$Treg$	时间标记
SID_j	服务器 S_j 的身份	ΔT	时间段
S_j	服务器 j	$Gen(,)$	随机生成函数
PSK,y_i	S_j 和 RC 之间共享的安全密钥	$Rep(,)$	确定性恢复函数
χ	系统主密钥	e,d,n	公钥、私钥、整数

1.1 服务器注册阶段

首先，应用服务器 S_j 向 RC 申请成为合法服务器，同时 RC 为服务器 S_j 分配密钥 PSK。

1.2 用户注册阶段

新用户想要获取应用服务器 S_j 的资源，首先要在 RC 上注册。注册过程如图 1 所示。

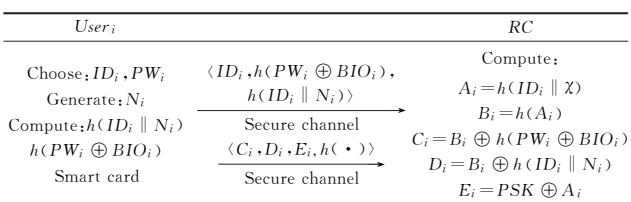

图 1 注册阶段

步骤 1 一个新的用户自主选择 ID_i 和口令 PW_i 同时选取随机数 N_i，并提取生物特征 BIO_i，计算 $h(ID_i\|N_i)$和 $h(PW_i\oplus BIO_i)$。最后，用户通过安全通道向 RC 提交信息 $\langle ID_i,h(PW_i\oplus BIO_i),h(ID_i\|N_i)\rangle$。

步骤 2 RC 收到消息后计算：$A_i=h(ID_i\|\chi)$，$B_i=h(A_i)$，$C_i=B_i\oplus h(PW_i\oplus BIO_i)$，$D_i=B_i\oplus h(ID_i\|N_i)$，$E_i=PSK\oplus A_i$。

步骤 3 RC 储存 U_i 注册信息，将参数$\langle C_i,D_i,E_i,h(\cdot)\rangle$保存到 Smart card 中，并通过安全通道把智能卡提交给用户。

步骤 4 用户收到智能卡后，将 N_i 置于智能卡中。最后，智能卡储存参数如下$\langle C_i,D_i,E_i,h(\cdot),N_i\rangle$。

1.3 登录阶段

步骤 1 用户登录服务器 S_j，将智能卡插入读卡器中，同时，输入身份 ID_i、口令 PW_i 和生物特征 BIO_i。智能卡计算 $B_i=C_i\oplus h(PW_i\oplus BIO_i)$ 并判断 $B_i\oplus h(ID_i\|N_i)$ 是否和智能卡中的 D_i 相等。如果通过验证，则用户合法；否则，停止协议。

步骤 2 智能卡产生一个随机数 N_1，计算 $M_1=h(B_i)\oplus N_1$，$AID_i=ID_i\oplus h(B_i\|N_1)$，$M_2=h(ID_i\|N_1\|E_i)$，然后给服务器发送消息：$\langle M_1,M_2,AID_i,E_i\rangle$，如图 2 所示。

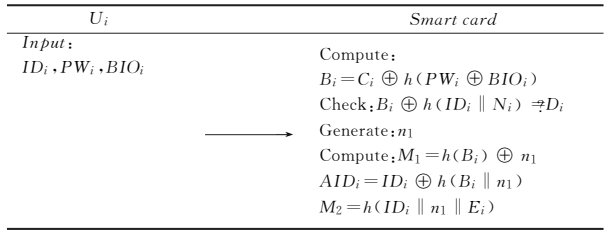

图 2 登录阶段

1.4 认证阶段

步骤 1 服务器 S_j 收到用户消息$\langle M_1,M_2,AID_i,E_i\rangle$后，利用 PSK 计算 $A_i=E_i\oplus PSK$，$B_i=h(A_i)$，$N_1=M_1\oplus h(B_i)$ 和 $ID_i=AID_i\oplus h(B_i\|N_1)$，验证 $h(ID_i\|N_1\|E_i)$是否等于 M_2。如果验证通过，服务器将继续执行；否则，终止协议。

步骤 2 服务器 S_j 随之产生随机数 N_2，计算 $SK_{ji}=h(ID_i\|SID_j\|N_1\|N_2)$，$M_3=N_2\oplus h(ID_i\|N_1)$和 $M_4=h(SID_j\|N_2)$。将消息$\langle SID_j,M_3,M_4\rangle$给用户。

步骤 3 用户收到服务器消息后，计算 $N_2=M_3\oplus h(ID_i\|N_1)$，并验证 M_4 和 $h(SID_j\|N_2)$是否相等。如果验证通过，则用户确定服务器 S_j 合法，同时计算 $SK_{ij}=h(ID_i\|SID_j\|N_1\|N_2)$，并将 $SK_{ij}\oplus h(N_2)$给服务器 S_j。

步骤 4 服务器 S_j 回复$h(N_2)$，如果 $h(N_2)$正确，则该用户合法，如图 3 所示。

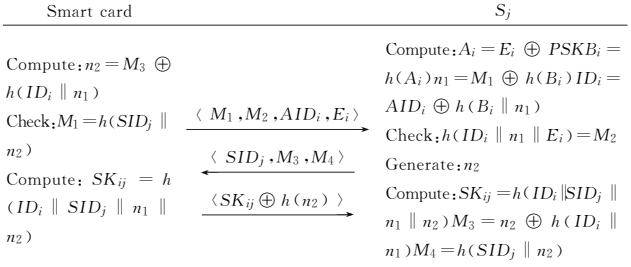

图 3 认证阶段

1.5 口令修改阶段

步骤 1 用户向智能卡输入身份 ID_i、口令 PW_i 和生物特征 BIO_i。

步骤 2 智能卡计算 $B_i=C_i\oplus h(PW_i\oplus BIO_i)$，并检验 $B_i\oplus h(ID_i\|N_i)$ 是否等于 D_i。如果智能卡相等，则用户输入新口令 PW_{new}；否则，拒绝修改。

步骤 3 智能卡计算 $C_{new}=C_i\oplus h(PW_i\oplus BIO_i)\oplus h(PW_{new}\oplus BIO_i)$，并用 C_{new} 替换 C_i，这样口令修改阶段完成，如图 4 所示。

U_i		smart card
		Compute: $B_i=C_i \oplus h(PW_i \oplus BIO_i)$ Check: $D_i=B_i \oplus h(ID_i \| N_i)$
	ID_i, PW_i, BIO_i →	Key in: PW_{new} Compute: $C_{new}=C_i \oplus h(PW_i \oplus BIO_i) \oplus h(PW_{new} \oplus BIO_i)$ Replace: C_i to C_{new}

图 4　口令修改

2　文献[5]所提协议的分析

2.1　匿名性失效

任意应用服务器 S_j，一旦收到用户消息$\langle M_1, M_2, AID_i, E_i\rangle$，计算 $A_i=E_i \oplus PSK$，$B_i=h(A_i)$，$N_1=M_1 \oplus h(B_i)$，$ID_i=AID_i \oplus h(B_i \| N_1)$，回复用户 U_i 的身份 ID_i。SK_j 可以随时跟踪用户的行为，则匿名性失效。

2.2　服务器假冒攻击

步骤 1　服务器 S_j 可以得到用户的 AID_i, E_i, A_i。接着，服务器 S_j 可以伪造任何合法用户的登录，完成与 S_k 的认证过程。

步骤 2　服务器 S_j 计算 $B_i=h(A_i)$，产生随机数 N_1'。

步骤 3　计算 $M_1=h(B_i) \oplus N_{1'}$，$AID_i'=ID_i \oplus h(B_i \| N_1')$，$M_2'=h(ID_i \| N_{1'} \| E_i)$，通过安全信道将$\langle M_1, AID_i', M_2', E_i\rangle$发送给 S_k。

步骤 4　服务器 S_k 收到消息后，利用 PSK 计算 $A_i=PSK \oplus E_i$，$N_1'=h(h(A_i)) \oplus M_1$，$AID_i'$，验证 $h(ID_i \| N_1' \| E_i)$是否等于 M_2'，S_k 误认 S_j 为合法用户。

步骤 5　服务器 S_k 随机产生随机数 N_2'，计算 $SK_{ij}'=h(ID_i \| SID_j' \| N_1' \| N_2')$，随后 S_k 通过公共信道发送消息$\langle SID_j, M_3', M_4'\rangle$给 S_j。

步骤 6　服务器 S_j 收到$\langle SID_j, M_3', M_4'\rangle$，发消息$\langle SK_{ij} \oplus h(N_2)\rangle$给 S_k。

步骤 7　服务器 S_k 使用会话密钥 $h(N_2)$。

S_j 成功地假冒服务器 S_K。

2.3　会话密钥泄露攻击

某个攻击者攻击合法服务器或者恶意服务器和攻击者联合，都可导致 PSK 的泄露。同时，通过非法窃听得到$\langle M_1, M_2, AID_i, E_i\rangle$，$\langle SID_j, M_3, M_4\rangle$以及$\langle SK_{ij} \oplus h(n_2)\rangle$，便可恢复会话密钥，解密用户和服务器之间的信息。具体步骤如下：

步骤 1　计算 $A_i=PSK \oplus E_i$，PSK 服务器泄露。

步骤 2　$h(ID_i \| N_i)=B_i \oplus D_i$，$N_2=M_3 \oplus h(ID_i \| N_i)$和 Sk_{ij}。

以上分析最核心的要点是 RC 和服务器之间的密钥 PSK 是相同的，这就导致一些非法服务器泄露信息，从而导致一系列可能的攻击。为了弥补该协议的缺陷，本文设计了更加安全和高效的协议。

3　改进方案

3.1　初始化阶段

RC 是可信第三方，负责系统建立、参数选取、用户注册，一旦攻破则无安全性可言。注册之前，RC 选取主密钥 χ，产生大素数 p 和 q，计算 $n=pq$，为了最大安全性，两数长度一样。最后，RC 公布所有参数：$\langle n, h(\cdot), h_0(), h_1(), h_2(), h_3()\rangle$。具体执行过程如图 5 所示。

服务器 S_j	服务器注册阶段	注册中心 RC
		计算 $h_0(SID_j)$，检查 hash 表
	$\langle SID_j, e\rangle$ 安全信道	RC 选取密密值 y_i, T_{reg}
选择 SID_j、 公钥 e，		计算 $h_0(SID_j \| y_i)$
	$\langle h_0(SID_j \| y_i), T_{reg}\rangle$ 安全信道	保存 $\langle SID_j, h_0(SID_j \| y_i), h_0(T_{reg})\rangle$
用户	用户注册	注册中心 RC
		计算 $h(ID_i)$，检查 hash 表
选择 ID_i 和 PW_i， 提取 Bio_i, a 计算： Gen $(Bio_i)=(\sigma_i, \theta_i)$， 键入 a, θ_i 到智能卡	$\langle ID, h(PW_i \| a), h(PW_i \| \sigma_i)\rangle$ →	$A_i=h_0(h_0(ID_i) \| \chi \| T_{reg}) \oplus h0(PW_i \| a))$， $B_i=h_0(h_0(ID_i) \| y_i \| T_{reg})$， $C_i=h_0(h_0(ID_i) \| h_0(y) \| h_0(PW_i \| \sigma_i))$， $D_i=A_i \oplus h_0(ID_i) \oplus h_0(h_0(PW_i \| \sigma_i))$， $E_i=h_0(A_i) \oplus h_0((SID_j \| y_i \| T_{reg}) \oplus h_0(A_i))$， $F_i=E_i \oplus h_0(h_0(ID_i) \| h_0(PW_i \| \sigma_i))$， $G_i=B_i \oplus h_0(PW_i \| a)$，
	← $\langle n, e, C_i, D_i, F_i, G_i, h_0(y), h_0(), h_1(), h_2(), h_3()\rangle$ 安全信道	
用户	登录认证阶段	服务器 S_j
输入 ID_i、PW_i、扫描 BIO_i 计算 $h_0(ID_i)$， $\sigma_i=Rep(BIO_i, \theta_i)$， $h_0(PW_i \| \sigma_i)$， $B_i=G_i h_0(PW_i \| a)$， $h_0(h_0(ID_i) \| h_0(y) \| h_0(PW_i \| \sigma_i))?=C_i$ $A_i=D_i \oplus h_0(ID_i) \oplus h_0(h_0(PW_i \| \sigma_i))$ $E_i=F_i \oplus h_0(h_0(ID_i) \| h_0(PW_i \| \sigma_i))$ $H_i=h_0(A_i) \oplus h_0(SID_j \| h_0(y))$ 产生 r_1， $C=r_1^e \bmod n$ $AID_j=h_0(ID_i) \oplus h_0(r_1) \oplus E_i$ $M_1=h_0(h_0(A_i) \| h_0(ID_i) \| r_1 \| T)$ $r_2=M_2 \oplus h_0(B_i \| r_1)$ 判断 $M_3?=h_1(h_0(ID_i) \| SID_j \| r_1 \| r_2 \| B_i \| T_3)$ 计算： $M_4=h_2(h_0(ID_i) \| SIDj \| r_1 \| r_2 \| B_i)$， $Sk_{ij}=h_3(h_0(ID_i) \| SID_j \| r_1 \| r_2 \| B_i)$	$\langle SID_j, AID_j, C, H_i, M_1, T_1\rangle$ →	检查新鲜性 $\Delta T=T_2-T_1$ 计算 $r_1=C^d \bmod n$， $h_0(A_i)=H_i h_0(SID_j \| h_0(y))$ $h_0(ID_i)=AID_j \oplus h_0(r_1) \oplus E_i$ 判断 $h_0(h_0(A_i) \| h_0(ID_i) \| r_1 \| T_1)?=M_1$ S_j 产生 r_2 计算： $B_i=h_0(h_0(ID_i) \| y_i \| T_{reg})$ $M_2=h_0(B_i \| r_1) \oplus r_2$ $M_3=h_1(h_0(ID_i) \| SID_j \| r_1 \| r_2 \| B_i \| T_3)$ S_j 判断 M_4 $Sk_{ij}=h_3(h_0(ID_i) \| SID_i \| r_1 \| r_2 \| B_i)$
	$\langle SID_j, M_2, M_3, T_3\rangle$ →	
	$\langle M_4\rangle$ →	

图 5　协议过程

3.2 注册阶段

3.2.1 服务器注册

首先,服务器 S_j 登录 RC 注册,S_j 选择自己身份 SID_j,选择公钥 e,计算出私钥 d 保密。同时,将〈SID_j,e〉通过安全信道发给 RC。收到消息后,计算 $h_0(SID_j)$并与储存的服务器 hash 数据库和服务器公钥数据库比对。若有相同,服务器重新注册。否则,RC 为服务器选取密密值 y_i,服务器 S_j 时间标记为 T_{reg}=服务器名称‖注册时间‖随机数填充,计算 $h_0(SID_j \| y_i)$。最后,通过安全通道,把〈$h_0(SID_j \| y_i)$,T_{reg}〉发送给服务器 S_j。服务器保存〈SID_j,$h_0(SID_j \| y_i)$,$h_0(T_{reg})$〉。

3.2.2 用户注册

步骤 1 用户选择 ID_i 并 PW_i,并提取生物信息 Bio_i,计算 $Gen(Bio_i)=(\sigma_i,\theta_i)$,$h_0(PW_i \| \sigma_i)$,选择一定长度随机数 a(注册完毕后,无须记忆)。最后,用户通过安全通道把〈ID_i,$h_0(PW_i \| a)$,$h_0(PW_i \| \sigma_i)$〉传给 RC。

步骤 2 RC 收到消息后,计算 $h_0(ID_i)$,对照用户 hash 数据库,检查是否被注册。若是,则返回重新注册;否则,计算:

$A_i=h_0(h_0(ID_i) \| \chi \| T_{reg}) \oplus h_0(PW_i \| a)$

$B_i=h_0(h_0(ID_i) \| y_i \| T_{\text{reg}})$

$C_i=h_0(h_0(ID_i) \| h_0(y) \| h_0(PW_i \| \sigma_i)))$

$D_i=A_i \oplus h_0(ID_i) \oplus h_0(h_0(PW_i \| \sigma_i))$

$E_i=h_0(A_i) \oplus h_0((SID_j \| y_i \| T_{reg}) \oplus h_0(A))$

$F_i=E_i \oplus h_0(h_0(ID_i) \| h_0(PW_i \| \sigma_i))$

$G_i=B_i \oplus h_0(PW_i \| a)$

RC 储存〈n,e,C_i,D_i,F_i,G_i,$h(y)$,$h_0()$,$h_1()$,$h_2()$,$h_3()$〉,并通过安全通道发送给用户。

步骤 3 用户收到智能卡后,键入 a,θ_i。最后智能卡中包含信息有:

〈n,e,a,$\theta_i C_i$,D_i,F_i,G_i,$h_0(y)$,$h_0()$,$h_1()$,$h_2()$,$h_3()$〉。

3.3 登录阶段

步骤 1 用户要登录服务器 S_j,将智能卡插入读卡器中,输入 ID_i,PW_i,扫描 BIO_i,智能卡计算 $h_0(ID_i)$,$\sigma_i=Rep(BIO_i,\theta_i)$,$h_0(PW_i \| \sigma_i)$,$B_i=G_i \oplus h_0(PW_i \| a)$,并判断 $h_0(h_0(ID_i) \| h_0(y) \| h_0(PW_i \| \sigma_i))$是否与 C_i 相等,若相同,则用户合法;否则,终止协议。如果连续几次都输入错误,则智能卡当天被锁住。

步骤 2 用户合法性得到确认后,计算:

$A_i=D_i \oplus h_0(ID_i) \oplus h_0(h_0(PW_i \| \sigma_i))$

$E_i=F_i \oplus h_0(h_0(ID_i) \| h_0(PW_i \| \sigma_i))$

$H_i=h_0(A_i) \oplus h_0(SID_j \| h_0(y))$

产生随机数 r_1,计算:

$C=r_1^e \bmod n$

$AID_j=h_0(ID_i) \oplus h_0(r_1) \oplus E_i$

$M_1=h_0(h_{01}(A_i) \| h_0(ID_i) \| r_1 \| T_1)$

通过安全信道将〈SID_j,AID_j,C,H_i,M_1,T_1〉。

3.4 认证阶段

步骤 1 服务器 S_j 收到用户消息后,检查身份、时间的新鲜性,若时间超过 $\Delta T=T_2-T_1$,则终止认证,T_2 为当前服务器时间戳。计算:

$r_1=C^d \bmod n$

$h_0(A_i)=H_i \oplus h_0(SID_j \| h_0(y))$

$h_0(ID_i)=AID_j \oplus h_0(r_1) \oplus E_i$

判断 $h_0(h_0(A_i) \| h_0(ID_i) \| r_1 \| T_1)$是否与 M_1 相等。若不成立,协议终止。

步骤 2 用户合法性得到确认后,服务器 S_j 随机产生 r_2,计算:

$B_i=h_0(h_0(ID_i) \| y_i \| T_{reg})$

$M_2=h_0(B_i \| r_1) \oplus r_2$

$M_3=h_1(h_0(ID_i) \| SID_j \| r_1 \| r_2 \| B_i \| T_3)$,$T_3$ 为当前时间戳。发送消息〈SID_j,M_2,M_3,T_3〉。

步骤 3 智能卡收到消息后,计算:

$r_2=M_2 \oplus h_0(B_i \| r_1)$

检查 $M_3=h_1(h_0(ID_i) \| SID_j \| r_1 \| r_2 \| B_i \| T_3)$是否成立,若不成立,协议终止。计算:

$M_4=h_2(h_0(ID_i) \| SID_j \| r_1 \| r_2 \| B_i)$

$Sk_{ij}=h_3(h_0(ID_i) \| SID_j \| r_1 \| r_2 \| B_i)$

给服务器发送 M_4。

步骤 4 服务器 S_j 检验 M_4 是否成立,若不成立则终止协议。最后,经过一系列步骤后,会话密钥为 $Sk_{ij}=h_3(h_0(ID_i) \| SID_i \| r_1 \| r_2 \| B_i)$。

3.5 口令修改阶段

当用户需要更新口令时,运行过程为:

步骤 1 运行登录和认证阶段。

步骤 2 如果运行结果顺利,智能卡计算:

$h(PWi^{\text{new}} \| \sigma_i)$,

$C_i^{\text{new}}=h_0(h_0(ID_i) \| h_0(y) \| h_0(PW_i^{\text{new}} \| \sigma_i))$

$D_i^{\text{new}}=A_i \oplus h_0(ID_i) \oplus h_0(h_0(PW_i^{\text{new}} \| \sigma_i))$

$F_i^{\text{new}}=E_i \oplus h_0(h_0(ID_i) \| h_0(h_0(PW_i^{\text{new}} \| \sigma_i))$

$G_i^{\text{new}}=B_i \oplus h_0(PW_i^{\text{new}} \| a)$

替换智能卡中 C_i,D_i,F_i,G_i。

4 安全分析

4.1 匿名性

文献[19-20]指出,匿名性两个层次的含义为:1)基本层次要求攻击者无法获得用户的真实身份。2)高级层次要求攻击者无法区分两个会话是同一用户参与,实现用户的不可追踪性。改进的协议中仍然使用动态身份 AID_i,用户在登录服务器 S_j 时,仅知道用户的 $h(ID_i)$,不能回复用户真实的身份,从而保证了用户真实身份的隐蔽性。同时,用户在不同时间登录相同的服务器 S_j,每次动态登录身份是不同的,实现了对用户隐私的保护。其次,实现了用户的不可追踪性。假设攻击者通过非法途径得到智能卡,并提取出智能卡中的相关参数如下:〈n,e,a,$\theta_i C_i$,D_i,F_i,G_i,$h_0(y)$,$h_0()$,$h_1()$,$h_2()$,$h_3()$〉。通过窃听得到了用户和服务器之间的交互信息〈SID_j,AID_j,C,H_i,M_1,T_1〉,〈M_2,M_3,T_3〉。

具体攻击过程为:计算 $h_0(A_i)=H_i \oplus h_0(SID_j \| h_0(y))$,其中 H_i,SID_j 从截获的消息,$h_0(y)$从智能卡中提取。可以注意到 A_i 与 ID_i,T_{reg} 和 PW_i 有关。若经常修改口令,攻击者则无法确定用户身份,从而实现对用户的不可追踪性。

4.2 智能卡丢失攻击

若用户的智能卡丢失,捡到用户智能卡的攻击者利用侧信道技术提取出智能卡中相关参数〈n,e,a,$\theta_i C_i$,D_i,F_i,G_i,

$h_0(y)$，$h_0()$，$h_1()$，$h_2()$，$h_3()$〉，但不知道用户的身份、口令、以及生物特征，从而无法正常登录。另外，假若攻击者窃听到用户和服务器之间的通信内容，仅仅恢复出 $h(A_i)$，无法解密 C，r_1，r_2，B_i，也就是无法解密会话密钥。

4.3　抗前向安全攻击

前向安全攻击是指一方或者多方的私钥长期泄露，此前的会话密钥依旧安全[19]。本文协议中，如果服务器 S_j 的私钥 d、秘密值 y_i 泄露，同时攻击者窃听到用户和服务器之间的消息，则攻击者可冒充服务器解密所有的消息，但是无法计算 $B_i=h_0(h_0(ID_i)\|y_i\|T_{reg})$，$T_{reg}$ 服务器时间标记是不被获取的，从而无法计算出会话密钥。若 RC 被攻破，仅仅是储存用户的 SID_j 和注册时间的 hash 表泄露，无法获取 T_{reg} 的值，进而无法计算出会话密钥，实现了前向安全。

4.4　抗已知密钥攻击

抗已知密钥攻击是指某次会话密钥的泄露不会导致其他密钥的安全性。这就要求每次会话密钥都是一次性的、随机的、独立的。在协议中，会话密钥参数 r_1 和 r_2 都是随机产生的；另一方面，不同会话密钥中产生相同的随机数的概率是非常小的。协议会话密钥 Sk_i 是满足以上要求的。

4.5　重放攻击

首先，协议在交互过程中对消息的新鲜性做了判断，一旦超出规定时间视为作废。其次，若攻击者窃听到用户登录服务器的消息〈SID_j，AID_j，C，H_i，M_1，T_1〉，并且在规定时间内重放消息，则服务器可以验证它的合理性。但服务器 S_j 产生一个新随机数 r_2'，返回消息〈SID_j，M_2'，M_3'，T_3〉，$M_2=h_0(B_i\|r_1)\oplus r_2'$，$M_3=h_1(h_0(ID_i)\|SID_j\|r_1\|r_2'\|B_i\|T_3)$，但是攻击者不知道 $h_0(ID_i)$ 和 r_1，无法计算出 SK_{ij}。因此，只有 M_1 重放得不到确认，M_2，M_3，M_4 则得不到服务器的检测。因此，改进方案能抵抗重放攻击。

4.6　抗服务器假冒攻击

协议指出 RC 与每个不同的服务器 S_j 都有不同的秘密值 y_i，这样可防止服务器欺骗。同时，假设某个恶意的服务器 Sk 保留了用户的登录消息试图发起假冒攻击，但是 Sk 不知道 y_i 和 T_{reg}，无法计算 $E_i=h_0(A_i)\oplus h_0((SID_j\|y_i\|T_{reg})\oplus h_0(A))$ 和 B_i，所以无法造出合法的会话密钥。

4.7　抵抗合法用户拒绝服务攻击

由于生物特征的不稳定性，会把合法用户视为非法用户而拒绝服务。但是，本文采用文献[17]所采用的模糊提取技术，对稍有不同的生物特征信息提供预处理，从而解决了合法用户非法访问问题。

5　效率分析

本协议大部分采用 hash 和异或操作，在认证阶段考虑到不可追踪性问题和智能卡的计算能力有限问题后，把计算量较大的问题留给服务器 S_j。为了表述方便，采用以下符号表示不同运算的需要的时间，‖ 和⊕不计时间、T_h 表示一次 hash 运算所需时间、T_m 为椭圆曲线点乘时间、T_e 表示指数模幂运算时间。通过与文献[9-10，13，15]比较发现本协议改进了协议必备的几项内容，如匿名性、服务器假冒攻击、抗前向攻击等，为了解决各项安全问题，将不可避免地增加时间和经济成本。但是，总的来说本协议实践性较强，没有特别复杂的计算。详细性能分析如表 2、表 3 所列。

表 2　本协议和其他协议的安全性能分析

安全性能	文献[9]	文献[10]	文献[13]	文献[15]	本文方法
匿名性	×	×	×	×	√
会话密钥协商	×	√	√	√	√
丢失智能卡攻击	×	√	×	×	√
口令猜测攻击	√	√	√	√	√
重放攻击	√	√	√	√	√
服务器假冒攻击	√	√	×	×	√
前向安全性	×	×	×	×	√
抗密钥泄露仿冒攻击	√	√	√	√	√
抗已知密钥攻击	√	√	√	×	√
抵抗合法用户拒绝服务攻击	√	√	√	√	√

表 3　效率分析

阶段	协议				
	文献[9]	文献[10]	文献[13]	文献[15]	本文
注册	$2T_h$	$3T_h$	$3T_h$	$4T_h$	$13T_h$
登录	$2T_h+T_m$	T_m+3T_h	$4T_h$	$5T_h$	$10T_h+T_e$
认证	$15T_h+3T_m$	$4T_m+18T_h$	$12T_h$	$12T_h$	$10T_h+T_e$
修改	$2T_h$	$2T_h$	$2T_h$	$3T_h$	$6T_h$
总计	$21T_h+4T_m$	$23T_h+4T_m$	$21T_h$	$24T_h$	$39T_h+2T_e$

结束语　本文首先回顾了文献[15]的协议过程并分析其存在的问题。其次，针对这些安全漏洞，提出本文的方案来克服的安全漏洞。同时分析了协议中有可能存在的攻击，如匿名性、抗服务器假冒攻击、抗前向性等。通过对比分析，本文方案展示了更高的安全性能和实用性。

参 考 文 献

[1] TSUAR W J. A flexible user authentication scheme for multi-server internet services[C]// Proc. of the Int'l Conf. on Networking (ICN 2001). LNCS 2093，2001：174-183.

[2] LI C T. Secure smart card based password authentication scheme with user anonymity[J]. Information Technology & Control，2011，40(40)：157-162.

[3] WU Z Y，CHANG D L，LIN T C，et al. A reliable dynamic user-remote password authentication scheme over insecure network [C]// Processing of the 26th International Conference on Advanced Information Networking and Applications. Washington DC：IEEE Computer Society，2012：25-28.

[4] LI X，MA J，WANG W D，et al. A novel smart card and dynamic ID based remote user authentication scheme for multi-server Environments[J]. Mathematical & Computer Modelling，2013，58 (1/2)：85-95.

[5] CHEN B L，KUO W C，WU C L. Robust smart-card-based remote user password authentication scheme[J]. International Journal of Communication Systems，2014，27(2)：377-389.

[6] KUMARI S，KHAN M K. More secure smart card-based remote user pass-word authentication scheme with user anonymity[J]. Security & Communication Networks，2014，7(11)：2039-2053.

[7] XU L L. An improved and provable remote user authentication scheme based on elliptic curve cryptosystem with user anonymity[J]. Security & Communication Networks，2015，8(2)：245-260.

[8] LIC T，H WANG. An efficient biometric-based remoteuser authentication scheme using smart cards [J]. Journal of Net work and Computer Applications，2010，33(1)：1-5.

[9] YOON E J，YOO K Y. Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem[J]. The Journal of Supercomputing，2013，63(1)：235-255.

（下转第 437 页）

[J]. 清华大学学报(自然科学版)，2013(12)：1750-1760.
[2] 石波，谢小权. 基于 D-S 证据理论的网络安全态势预测方法研究[J]. 计算机工程与设计，2013，34(3)：821-825.
[3] 陈善学，杨政，朱江，等. 一种基于累加 PSO-SVM 的网络安全态势预测模型[J]. 计算机应用研究，2015，32(6)：1778-1781.
[4] 田庆安，郭玉锦，王文涛. 基于小波与 DBN 的负荷预测模型[J]. 兰州理工大学学报，2017，43(2)：110-114.
[5] ZHANG H，XU T，LI H. StackGAN：Text to Photo-Realistic Image Synthesis with Stacked Generative Adversarial Networks [C]// IEEE International Confernece on Computer Vision(ICCV)，2016：5908-5916.
[6] 吴昊. 随机森林预测与纳什均衡策略的高职英语教学模式研究[J]. 佳木斯职业学院学报，2017(2).
[7] CHANG J，SCHERER S. Learning representations of emotional speech with deep convolutional generative adversarial networks [C]// IEEE International Conference on Acoustics，Speech and Signal Processing. IEEE，2017：2746-2750.
[8] ZHAO Y，TAKAKI S，LUONG H T，et al. Wasserstein GAN Waveform Loss-based acoustic model training form Multi-speaker Text-toSpeechsynthesis systems using a wav Net rocoder[J]. IEEE Access，2017：7(1)：1-10.
[9] 王峰，何俊. 博弈论在通信对抗态势预测中的应用[J]. 运筹与管理，2011，20(2)：132-136.
[10] RADFORD A，METZ L，CHINTALA S. Unsupervised Representation Learning with Deep Convolutional Generative Adversarial Networks[J]. Computer Science，2015.
[11] 朱红春，黄伟，刘海英，等. 基于 KL 散度的面向对象遥感变化检测[J]. 国土资源遥感，2017，29(2)：46-52.
[12] 张妍，韩光威，陆宁云，等. 基于 JS 散度的轨道车辆门系统健康状态评估方法[J]. 机械设计与制造工程，2017，46(11)：122-127.
[13] SRIVASTAVA A，VALKOV L，RUSSELL C，et al. VEEGAN：Reducing Mode Collapse in GANs using Implicit Variational Learning[J]. arXiv：1705. 07761，2017.
[14] 王群，董文略，杨莉. 基于 Wasserstein 距离和改进 K-medoids 聚类的风电/光伏经典场景集生成算法[J]. 中国电机工程学报，2015，35(11)：2654-2661.
[15] ARJOVSKY M，CHINTALA S，BOTTOU L. Wasserstein GAN [J]. 2017.
[16] NAKAJO K. Improved gradient method for monotone and lipschitz continuous mappings in banach spaces[J]. Acta Mathematica Scientia(English Series)，2017，37(2)：342-354.
[17] 李南星，盛益强，倪宏. 基于 LM 算法的 MLP 模型及其应用[J]. 网络新媒体技术，2018，7(1)：59-63.
[18] MUKKAMALA M C，HEIN M. Variants of RMSProp and Adagrad with Logarithmic Regret Bounds[J]. IEEE Transactions Biomed Engineering，2017，5(6)：1220-1228.
[19] QIU Z，YAN Z，FEI Y，et al. RGB-DI Images and Fall Convolution Nuernal Network-Based Outdoor Scene Understanding for Mobile Robots[J]. IEEE Transactions on Instrumentation & Measurement，2018，1(99)：1-11.
[20] IOFFE S，SZEGEDY C. Batch Normalization：Accelerating Deep Network Training by Reducing Internal Covariate Shift[J]. arXiv：1502. 03167，2015.
[21] 陈秀真，郑庆华，管晓宏，等. 层次化网络安全威胁态势量化评估方法[J]. 软件学报，2006，17(4)：885-897.

(上接第 413 页)

[10] KIM H，JEON W，LEE K，et al. Cryptanalysis and improvement of a biometrics-based multi-server authentication with key agreement scheme[C]// Proc. of the 12th Int'l Conf. on Computational Science and Its Applications (ICCSA 2012). IEEE，2012：391-406.
[11] HE D B，WANG D. Robust biometrics-based authentication scheme for multi-serve environmental[J]. IEEE Systems Journal，2005，9(3)：816-823.
[12] ODELU V，DAS A K，GOSWAMI A. Crytanalysis on robust biometrics-based authentication scheme for multi-server environment [EB/OL]. http://eprint. iacr. org/2014/715.
[13] CHUANG M C，CHEN M C. An anonymous multi-server authenticated key agreement scheme based on trust computing suing smart cards and biometric [J]. Expert Systems with Applications，2014，41(4)：1411-1418.
[14] MISHRA D，DAS A，MUKHOPADHYAY S. A secure user anonymity-preserving biometric-based multi-sever authenticated key agreement scheme using smart cards [J]. Expert Systems with Applications，2014，41(18)：8129-8143.
[15] 王瑞兵，陈建华，张媛媛. 一个匿名的基于生物特征的多服务器的密钥认证协议方案的研究[J]. 计算机应用研究，2016，33(7)：2190-2196.
[16] CHAUDHRY S A. A secure biometric based based multi-server authentication scheme for social multimedia network [J]. Multimedia Tools & Applications，2016，75(20)：1-21.
[17] XIA P Z，CHEN J H. Three-factor authentication scheme for multi-servers environments based on elliptic curve cryptography [J]. Application Research of Computers，2017，34(10)：3061-3067.
[18] 殷秋实，陈建华. 多服务器环境下基于椭圆曲线密码的改进的身份认证协议[J]. 计算机科学，2018，45(6)：111-116.
[19] 汪定，李文婷，王平. 对三个多服务器环境下匿名认证协议的分析[J]. 软件学报，2018，29(7)：1937-1952.
[20] 汪定，马春光，翁臣，等. 一种适于受限资源环境的远程用户认证方案的分析与改进[J]. 电子与信息学报，2012，34(10)：2520-2526.
[21] WAN T，LIU Z X，MA J F. Authentication and key agreement protocol for multi-server architecture[J]. Journal of Computer Research and Development，2016，53(11)：2446-2453.
[22] AMIN R. Cryptanalysis and efficient dynamic ID based remote user authentication scheme in multi-server environment ssing smart card[J]. Int'l Journal of Network Security，2016，18(1)：172-181.
[23] REDDY A G，YOON E J，DAS A K，et al. Design of mutually authenticated key agreement protocol resistant to impersonation attacks for multi-server environment[J]. IEEE Access，2017，5：3622-3639.