何耀, 王以松, 张辉. 基于 ECC 的物联网三因素双向认证协议[J]. 智能计算机与应用,2024,14(6):27-34. DOI:10.20169/j.issn.2095-2163.240604

基于 ECC 的物联网三因素双向认证协议

何 耀[1,2], 王以松[1,2], 张 辉[3,4]

(1 贵州大学 公共大数据国家重点实验室, 贵阳 550025; 2 贵州大学 计算机科学与技术学院, 贵阳 550025;
3 贵州财经大学 信息学院, 贵阳 550025; 4 世纪恒通科技股份有限公司博士后科研工作站, 贵阳 550018)

摘 要: 为解决物联网中用户和服务器双方认证过程中存在的隐私泄露、非法攻击等安全问题,提出一种基于 ECC 的物联网三因素双向认证协议。首先,使用 ECC 算法和 Hash 函数将用户密码、生物特征和智能卡三者结合生成三因素认证码,以提高系统安全性并降低系统运算复杂度。其次,认证双方通过 2 次信息交互实现双向认证,并引入数字签名和时间戳来保障认证的准确性与时效性,进一步增强协议安全性。最后,在认证结束后,设计会话密钥自动更新机制以防止会话密钥泄露引起的安全问题。在 Ubuntu22.04 虚拟机环境中对协议的操作时间进行测试,实验结果及分析表明,该协议对各种已知攻击具有鲁棒性,与其他协议相比,该协议具有明显的安全优势和性能优势。

关键词: ECC 算法; 生物特征; 智能卡; 三因素双向认证
中图分类号: TP309.2 **文献标志码**: A **文章编号**: 2095-2163(2024)06-0027-08

Three-factor bidirectional authentication protocol for the Internet of Things based on ECC

HE Yao[1,2], WANG Yisong[1,2], ZHANG Hui[3,4]

(1 State Key Laboratory of Public Big Data, Guizhou University, Guiyang 550025, China; 2 School of Computer Science and Technology, Guizhou University, Guiyang 550025, China; 3 School of Information, Guizhou University of Finance and Economics, Guiyang 550025, China; 4 Postdoctoral Scientific Research Station, Shiji Hengtong Technology Co., Ltd., Guiyang 550018, China)

Abstract: In order to solve the security problems such as privacy disclosure and illegal attacks in the authentication process of users and servers in the Internet of Things, a three-factor bidirectional authentication protocol based on ECC is proposed. Firstly, elliptic curve cryptography algorithm and Hash function are used to combine user password, biometric characteristics and smart card to generate three-factor authentication codes, which can improve system security and reduce system computational complexity. Secondly, the authentication parties use two information exchanges to achieve bidirectional authentication. And digital signature and timestamp are introduced to ensure the accuracy and timeliness of authentication, so as to enhance the protocol's security. Finally, after completing the authentication, an automatic session key update mechanism is designed to prevent the security problems caused by session key disclosure. The operation time of the protocol is tested in the Ubuntu22.04 virtual machine environment. The experimental results and analysis show that the scheme is robust against various known attacks. Compared with other schemes, the proposed protocol has obvious security and performance advantages.

Key words: ECC algorithm; biometrics; smart card; three-factor bidirectional authentication

0 引 言

随着信息技术的发展以及物联网的广泛应用,移动程序已普遍存在于人类社会生活中,由于网络服务需求的快速增长以及分布式系统的发展,用户信息容易受到各种攻击,导致隐私信息泄露造成损失。身份认证技术可以在用户获得系统服务之前识别用户的身份真伪,从而防止非法用户威胁系统安

基金项目: 国家自然科学基金(U1836205, 61976065); 2022 年度贵州财经大学引进人才科研启动项目(2022YJ007); 贵州省科技计划项目(黔科合支撑[2023]一般 372); 贵州省教育厅 2023 年度贵州省高校科学研究项目(黔教技[2023]063 号)。

作者简介: 何 耀(1999-),男,硕士研究生,主要研究方向:信息安全; 张 辉(1985-),男,博士后,研究员,主要研究方向:数据安全。
通讯作者: 王以松(1975-),男,博士,教授,主要研究方向:人工智能安全。Email: yswang@gzu.edu.cn

收稿日期: 2023-04-27

全。同时,用户也可以识别服务器的合法性,防止受到服务器的欺骗攻击。因此,用户身份认证技术已成为确保身份认证系统安全最重要且最有效的方法之一。个人生物特征具有独特性和不可伪造性,以用户的语音、指纹、面部识别等生物特征作为身份认证的第三要素,可以保证在用户密码被泄露或智能卡信息被提取的情况下,整个系统仍然可以安全运行,因此基于个人生物特征的智能认证方式应运而生。图 1 为物联网设备多服务器认证系统架构,其中展示了用户、生物识别器、物联网设备、服务器之间的交互过程。

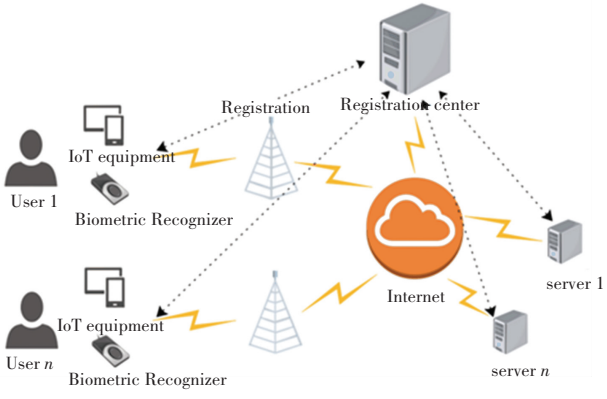

图 1 物联网设备认证图

Fig. 1 Diagram of IoT device authentication

2018 年,Ali 等学者[1]提出了一种基于椭圆曲线密码体制的三因素认证协议,该协议保证了用户匿名性,能够克服密码猜测、用户模拟、内部人员和智能卡盗窃攻击。但是,Wang 等学者[2]发现文献[1]中提出的协议容易受到用户模拟、服务器模拟、特权内部人和拒绝服务攻击等攻击,并且无法提供前向安全性和三因素保密性。2019 年,Wang 等学者[3]提出了一种可证明安全的、基于匿名生物特征的身份认证协议,该协议使用 ROR 模型和 BAN 逻辑证明了协议的安全性,但是该协议容易受到 KCI 攻击和 DoS 攻击。2020 年,Kumar 等学者[4]提出一种基于 ECC 的无线传感器网络安全三因素认证协议,与 Wang 等学者[3]的协议存在相同的问题:不支持用户撤销功能,并且存在时间戳检查延迟的问题,这会导致关键节点易遭受 KCI 攻击和 DoS 攻击。同年,Vinoth 等学者[5]提出了一个安全的多因素认证密钥协议方案,该方案使用访问结构和秘密共享来建立用户和传感器之间的会话密钥。但该方案容易遭受传感器节点捕获攻击、DoS 攻击、重传攻击以及去同步攻击。2021 年,Yu 等学者[6]提出了一种扩展混沌映射认证和密钥协议方案,并使用 AKE 逻辑证明了协议能够实现通信参与者之间的相互认证。Kumar 等学者[7]利用切比雪夫混沌映射的密码学特性,设计了一种支持服务器可扩展性的认证协议,但是该协议不提供用户不可追溯性。2023 年,李懿等学者[8]提出一种应用于远程医疗信息系统中的三因素匿名认证协议,该协议在 Dharminder 等学者[9]协议的基础上做了改进,将协议中的 RSA 方法替换成椭圆曲线算法和对称加解密算法。但是该协议使用的密钥长期固定,容易受到密钥泄露、服务器欺骗、中间人攻击。

在本研究中,发现了一个常见的安全问题,即这些协议中的服务器仅通过用户身份和共享密钥对用户进行身份认证,恶意服务器可以很容易发起用户假冒、重传、DoS 等攻击。为了克服上述协议问题,本文提出了一种基于 ECC 的物联网三因素双向认证协议。协议 ECC 算法和 Hash 函数加密用户密码、生物特征和智能卡数据,并引入数字签名和时间戳来增强系统安全性;认证双方通过 2 次信息交互实现双向认证,并引入数字签名和时间戳来保障认证的准确性与时效性;在认证阶段结束后设计会话密钥自动更新机制以防止会话密钥泄露带来服务器欺骗、重传、中间人攻击等非法攻击。本文提出的协议能够克服上述的安全问题。在 Ubuntu22.04 虚拟机环境中对协议的操作时间进行测试,结果表明,本文提出的协议能够抵抗常见的攻击,具有一定的安全优势和性能优势。

1 基础知识

1.1 模糊提取器

传统的散列函数对输入非常敏感,只有在输入不相同时才会返回不同的输出。由于生物特征信息很容易与各种噪声混合,不可能使用传统的散列函数来再现实际的生物特征,因此本文提出的协议使用一种通用的生物特征验证方法—模糊提取器[10-11]。在辅助字符串的帮助下,模糊提取器可以从生物特征输入中提取均匀随机字符串。只有当输入非常接近原始生物特征时,模糊提取器才能使用辅助字符串恢复原始生物特征数据。模糊提取器包括生成过程(Gen)和再现过程(Rep)。

(1)随机数生成算法 $Gen(BIO)=(P,R)$:输入生物特征 BIO,Gen 的概率算法将输出随机生物特征字符串 R 和辅助字符串 P。

(2)随机数再现算法 $Rep(BIO',P)=(R)$:输入生物特征 BIO',只要 BIO 和 BIO' 之间的距离满足

给定的验证阈值，*Rep* 的确定性算法就可以用辅助字符串 P 从生物特征数据 BIO' 中输出生物特征字符串 R。

1.2 ECC 密码算法

ECC 密码算法是一种轻量级公钥加密协议，是 Koblitz 在 1987 年提出的[12]，是建立在有限域的椭圆曲线代数上，提供了与传统的非对称密码体制相同的功能。设 q 为大素数，有限域 $GF(q)$ 上的椭圆曲线 E 是平面曲线 $y^2 = x^3 + ax + b$ 的解集，其中 a 和 b 在 $GF(q)$ 上且满足 $4a^3 + 27b^2 \neq 0 (\mathrm{mod}\ q)$。

如今，由于 ECC 与传统公钥密码算法相比具有参数更小、密钥更短、计算更快、密码复杂性更低和安全级别更高等优点而被用于许多应用和标准中。ECC 密码算法的安全性依赖于椭圆曲线离散对数问题（ECDLP）[13] 和 Diffie－Hellman 困难问题（ECDHP）[13]。

困难问题 1　椭圆曲线离散对数问题(ECDLP)

ECDLP 的定义如下：给定 $P, Q \in GF(q)$，找到一个标量 $d \in [1, n-1]$，计算 $Q = dP$（其中 $P, Q \in GF(q)$）是困难的。

困难问题 2　椭圆曲线 Diffie－Hellman 问题(ECDHP)

ECDHP 的定义如下：给定 $P \in GF(q)$ 和点 $A = aP$，$B = bP$，用多项式时间有界算法确定点 $C = abP$ 在计算上是困难的。

2　三因素双向认证协议

在本节中，将为多服务器环境提出一种新的三因素双向认证协议。该协议涉及注册中心、用户和服务器三个实体，包括 4 个阶段，分别是：注册、登录、认证和更新阶段。在所提出的三因素双向认证协议中，使用的符号和说明见表 1。

表 1　符号说明表

Table 1　Symbol description table

符号	描述
$H(\cdot)$	Hash 函数
$h(\cdot)$	生物 Hash 函数
$E(F_q)$	椭圆曲线上的有限域
P	椭圆曲线上的基点
ID_i	用户 U_i 的 ID
PW_i	用户 U_i 的密码
B_i	用户 U_i 的生物特征
B_i^*	生物特征关键数据
Q	公开辅助数据
(PK_i, SK_i)	用户 U_i 的公私钥对
SR	用户和服务器的会话密钥

2.1 注册阶段

注册过程详细步骤如下：

$Reg(ID_i, PW_i, B_i) \rightarrow (B_i^*, PW_i^*, SR, PK_i, SK_i, A_i, M_i)$：首先用户 U_i 选择并输入用户标识 ID_i、密码 PW_i 和生物特征 B_i，模糊提取器的 Gen 概率算法输出随机生物特征 B_i^* 和辅助字符串 Q，即 $Gen(B_i) = (B_i^*, Q)$。用户 U_i 再计算 $PW_i^* = H(PW_i \| h(B_i^*))$ 和 $A_i = H(ID_i \| PW_i^*)$。之后用户 U_i 通过安全通信信道将 $\{ID_i, PW_i^*\}$ 发送给服务器。服务器收到来自用户 U_i 的注册信息后，选择一个随机数 $SR \in Z_n^*$ 作为会话密钥，选择 (PK_i, SK_i) 作为用户的公私钥对，计算 $M_i = H(ID_i \| SR) \oplus PW_i^*$，并将信息 $\{(PK_i, SK_i) M_i, SR\}$ 存储在智能卡 SC_i 中发送给用户 U_i。用户和服务器的注册过程见表 2。

表 2　注册过程

Table 2　Process of registration

User U_i		Server
Select: ID_i, PW_i, B_i	$\xrightarrow{ID_i, PW_i^*}$	Select: $SR, (PK_i, SK_i)$
Calculates:		and calculates:
$Gen(B_i) = (B_i^*, Q)$		$M_i = H(ID_i \| SR) \oplus PW_i^*$
$PW_i^* = H(PW_i \| h(B_i^*))$		$SC_i = \{(PK_i, SK_i), SR, M_i\}$
$A_i = H(ID_i \| PW_i^*)$	$\xleftarrow{SC_i}$	Store $\{ID_i, PW_i^*, SR, (PK_i, SK_i), M_i\}$

2.2 登录与认证

登录与认证阶段主要分为用户登录、服务器认证用户、用户认证服务器三个步骤，具体如下：

(1) $Login(ID_i', PW_i', B_i') \rightarrow$ (Yes/No)：用户 U_i 插入智能卡 SC_i，并输入用户 ID_i'、密码 PW_i' 和生物特征 B_i'，智能卡 SC_i 使用模糊提取器中的函数再现 B_i^*，即 $Rep(B_i', Q) = B_i^*$，然后计算 $PW_i^{*\prime} = H(PW_i' \| h(B_i^*))$、$A_i' = H(ID_i' \| PW_i^{*\prime})$，并验证存储

的 A_i 与计算的 $A_i^{'}$ 是否相等。若二者相等,算法输出 Yes,用户 U_i 登录成功,继续进行认证阶段的操作;否则输出 No,登录不成功,会话终止。

(2) $Ver(r_i, ID_i, PW_i^*, SR, T_i) \rightarrow$ (Yes/No):用户 U_i 登录成功后,选择一个随机数 $r_i \in Z_n^*$,并产生当前时间戳 T_i,计算 $R_i = r_iP$,用私钥 SK_i 签名 $Sig = Sig_{SK_i}(H(ID_i \| R_i))$,用公钥 PK_i 加密 ID_i 得到 $E_i = Enc_{PK_i}(ID_i)$,然后计算验证消息 $Au = H(M_i \| R_i \| SR) + E_i$。用户将信息 $\{R_i, T_i, Sig, Au\}$ 发送给服务器,服务器收到 $\{R_i, T_i, Sig, Au\}$ 后,先验证时间戳 T_i 的有效性,即 $|T_s - T_i| \leqslant \Delta T$。若 T_i 无效,则会话终止,认证失败。若有效,服务器使用用户的公钥验证签名 Sig 的合法性,若 Sig 不合法,用户 U_i 的身份认证不通过,会话终止;若 Sig 合法,服务器 $E_i = Au - H(M_i \| R_i \| SR)$、$Dec(E_i) = ID_i^{'}$,并验证解密的 $ID_i^{'}$ 是否与数据库中存储的 ID_i 相等。若相等则服务器成功认证用户,若不相等,服务器认证用户失败,会话终止。

(3) $Ver(n, R_i, T_j) \rightarrow$ (Yes/No):服务器成功认证用户后,选择一个随机数 $n \in Z_n^*$,并产生当前时间戳 T_j,计算 $N = nR_i$、$As = H(ID_i^{'} \| (M_i \oplus PW_i^*) \| N)$,并将 $\{As, N, T_j\}$ 发送给用户。用户收到服务器发送的 $\{As, N, T_j\}$ 后,先验证时间戳 T_j 的有效性,即 $|T_u - T_j| \leqslant \Delta T$。若 T_j 无效,则会话终止,认证失败。若有效,计算 $As^{'} = H(ID_i \| (M_i \oplus PW_i^*) \| N)$,并与收到的 As 进行比较。若不相等,则认证失败。若相等,用户成功认证服务器。至此,用户和服务器之间完成相互认证,登录和认证过程见表 3。

表 3 登录和认证过程

Table 3 Process of login and authentication

User U_i	Insecure channel	Server
Inserts SC_i *into the card reader*		
Inputs: $ID_i, PW_i, B_i^{'}$		
Calculates: $Rep(B_i^{'}, Q) = B_i^*$		
$PW_i^* = H(PW_i \| h(B_i^*))$		
Check if $A_i = H(ID_i \oplus PW_i^*)$?	$\{R_i, T_i, Sig, Au\} \rightarrow$	Check if $\|T_s - T_i\| \leqslant \Delta T$?
If *so*, *choose* $r_i \in Z_n^*, T_i$		and use PK_i *verify* Sig
Calculates: $R_i = r_iP$		if *so calculates*:
$Sig = Sig_{SK_i}(H(ID_i \| R_i))$		$E_i = Au - H(M_i \| R_i \| SR)$
$E_i = Enc_{PK_i}(ID_i)$		$Dec(E_i) = ID_i^{'}$ and verify $ID_i^{'} = ID_i$?
$Au = H(M_i \| R_i \| SR) + E_i$		if verification holds, choose $n \in Z_n^*, T_j$
Check if $\|T_u - T_j\| \leqslant \Delta T$?	$\leftarrow \{As, N, T_j\}$	Calculates: $N = nR_i$ and
if *so*, *calculates*:		$As = H(ID_i^{'} \| (M_i \oplus PW_i^*) \| N)$
$As^{'} = H(ID_i \| (M_i \oplus PW_i^*) \| N)$		
Check if $As^{'} = As$?		
if *so*, *output success*		

2.3 更新阶段

当合法用户 U_i 出于某些安全原因想要更新其密码和生物特征,以及每次会话结束后服务器自动更新会话密钥 SR,可以在注册后的任何时间进行更改,更新阶段的具体步骤如下。

(1) $Update(ID_i, PW_i, B_i) \rightarrow (PW_i^{new}, B_i^{new}, A_i^{new})$:用户 U_i 插入智能卡 SC_i,输入标识 ID_i、密码 PW_i 和生物特征 B_i,与登录阶段一样,智能卡 SC_i 使用模糊提取器函数计算 $Rep(B_i^{'}, Q) = B_i^*$、$PW_i^* = H(PW_i \| h(B_i^*))$ 和 $A_i^{'} = H(ID_i \oplus PW_i^*)$,并验证存储的 $A_i^{'}$ 与 A_i 是否相等。若二者不相等,立即终止操作,否则用户 U_i 身份合法,可以继续更新操作。用户 U_i 输入新的密码 PW_i^{new} 和生物特征 B_i^{new},如果用户 U_i 不想更改生物特征,则仍可以保留旧的生物特征 B_i。智能卡 SC_i 计算 $Gen(B_i^{new}) = (B_i^{*new}, Q^{new})$、$Rep(B_i^{'new}, Q^{new}) = B_i^{*new}$、$PW_i^{*new} = H(PW_i^{new} \| h(B_i^{*new}))$、$A_i^{new} = H(ID_i \oplus PW_i^{*new})$,最后将智能卡中的 A_i 替换成 A_i^{new}。

(2) $Update(N, SR) \rightarrow (SR^{new})$:输入随机数 N 和会话密钥 SR,算法输出更新后的会话密钥 SR^{new}。服务器和用户同时更新,具体更新算法为:

① 用户更新:

$SR^{new} = H(R_i \| N \| SR)$

$M_i^{new} = H(ID_i \| SR) \oplus PW_i^*$

② 服务器更新：

$SR^{new} = H(R_i \| N \| SR)$

3　协议分析

3.1　安全性证明

本节使用随机预言模型分析所提三因素双向认证算法的安全性，证明该协议是否能够保证用户密码、智能卡、用户私钥和会话密钥的机密性。首先，假设敌手 A 具备以下能力：

Reveal 1：随机预言机能够通过椭圆曲线 $E(F_q)$ 给定的两点 P 和 $Q = dP$，计算出整数 d。

Reveal 2：随机预言机可以对哈希值 $h(x)$ 进行反向求解得出字符串 x，即从 $h(x)$ 中反推出 x 的值。

对抗模型：假设在模型中敌手 A 可以控制用户和服务器三者之间的不安全通道：

（1）敌手 A 能窃取到信道上传输的所有消息。

（2）敌手 A 能在信息传输过程中注入伪造信息。

（3）敌手 A 能拦截并篡改信道上传输的所有消息。

（4）敌手 A 能监测用户和服务器的动态。

定理 1　基于椭圆曲线离散对数问题和哈希函数单向性，该三因素双向认证算法可以防止敌手 A 泄露用户密码 PW_i 和私钥 SK_i。

证明 1　$Pro1_{A,\text{Protocol}}^{\text{ECDLP,Hash}}$

1.Eavesdrop (R_i, Sig, Au, T_i) on the insecure channel,

where $R_i = r_iP, Sig = Sig_{SK_i}(H(ID_i \| R_i)), Au = H(M_i \| R_i \| T_i) + E_i$

2.Call *Reveal* 1 on input M_i and Sig, let $(PW_i^{*'}, SK_i') \leftarrow Reveal\ 1\ (M_i, Sig)$

3.Call *Reveal* 2 on input $PW_i^{*'}$,let $(PW_i') \leftarrow Reveal\ 2\ (PW_i^{*'})$

4.Compute $\text{Dec}(E_i') = \{ID_i'\}$

if $ID_i' = ID_i$ and $PW_i' = PW_i$ then

　Accept PW_i' as the secret key PW_i of the server

　Accept SK_i' as the secret key SK_i of the shared key

　return 1

else return 0

end if

在建立的模型中，敌手 A 具备 Reveal 1 和 Reveal 2 以及泄露用户密码 PW_i 和私钥 SK_i 的能力。根据证明 1 的过程可知，敌手 A 若能破解 ECDLP 问题、逆向求解哈希函数，就能泄露、获取用户密码 PW_i。但是，根据困难问题 1 和困难问题 2 可知，敌手 A 很难从 M_i 和 Sig 中反推出 PW_i^* 和 SK_i，同时没有用户的生物特征 B_i^*，就不能从 PW_i^* 中计算出用户密码 PW_i，就无法破解传输信息来假冒用户和服务器骗取双方的信任。因此，所提算法能够防止用户隐私信息的泄露，抵抗用户假冒、服务器欺骗、中间人等攻击。

定理 2　基于椭圆曲线离散对数问题和哈希函数单向性，该三因素双向认证算法可以抵抗敌手 A 获取用户和服务器的会话密钥 SR。

证明 2　$Pro2_{A,\text{Protocol}}^{\text{ECDLP,Hash}}$

1.Eavesdrop (Au, As, Sig, R_i, N) on the insecure channel,

where $Au = H(M_i \| SR \| R_i) + E_i, As = H(ID_i' \| (M_i \oplus PW_i^*) \| N)$

2.Call *Reveal* 1 on input PK_i and P, let $(r_i', SK_i') \leftarrow Reveal\ 1\ (Sig, R_i)$

3.Compute $SK_i' = PK_iP$,let $E_i' = Enc_{PK_i}(ID_i')$

4.Call *Reveal* 2 on input Au,let $(M_i', SR') \leftarrow Reveal\ 2\ (Au)$

if $Au' = H(M_i' \| SR' \| R_i') + E_i' = Au$

　Accept SR' as the secret key SR of the user

　return 1

else return 0

end if

在建立的模型中，敌手 A 具备 *Reveal* 1 和 *Reveal* 2 以及获取会话密钥 SR 的能力。根据证明 2 的过程可知，敌手 A 若能破解 ECDLP 问题并反向求解哈希函数，就能从验证消息 Au、E_i 中获取用户私钥 SK_i 和会话密钥 SR。但是，根据困难问题 1 和困难问题 2，敌手很难从签名 Sig 中获取到用户私钥 SK_i，也很难从 Au 中获取会话密钥 SR。并且用户私钥 SK_i 和会话密钥 SR 都封装在智能卡中，每经过一次认证，用户和服务器的会话密钥 SR 都会自动更新，用户私钥 SK_i 和会话密钥 SR 封装在智能卡中，即使敌手 A 获取到了传输的认证消息，因为没有用户的生物特征 B_i^*，是无法得到会话密钥 SR 的。因此，本

文设计的算法能够防止敌手通过智能卡丢失、离线密码猜测、用户假冒等非法手段获取会话密钥 SR。

3.2 安全性分析

安全性分析是用于检测协议中可能存在的安全问题,本小节重点分析所提协议在实际应用过程中具有双向认证、前向安全性、匿名性和不可追溯性、三因素认证等安全性,能够抵抗智能卡丢失攻击、用户假冒攻击、服务器欺骗攻击、离线密码猜测攻击、重放攻击、中间人攻击等。这里将展开研究分述如下。

(1)双向认证。本协议通过采用挑战-应答的机制来实现双向认证的功能。只有合法的用户 U_i 通过使用自己的私钥 SK_i 才能生成正确的签名 Sig 供服务器进行验证,同时服务器还要验证用私钥解密得到的用户 ID_i ,以验证用户 U_i 的合法性;验证成功后,服务器的验证消息 $As = H(ID_i' \| (M_i \oplus PW_i^*) \| N \| T_j)$ 也需要通过用户 U_i 的验证,才能证明服务器的身份是合法的。因此,整个过程使用了 2 次认证实现了双向认证。

(2)前向安全性。在所提协议中,用户和服务器的会话密钥 SR 不以明文形式直接传输,并且用户和服务器之间的传输的认证信息包含了不同随机数,基于 ECDLP 困难问题和 Hash 函数的单向性特点,攻击者是得不到会话密钥的,因此也无法猜测与之前所有会话密钥相关联的秘密信息。

(3)匿名性和不可追溯性。由于用户 U_i 的真实密码和生物特征包含在 $PW_i{}^*$ 中,即使攻击者截获到登录信息,因为哈希函数的抗碰撞性和 ECDLP 困难问题攻击者无法计算出正确的密码 PW_i。同时,没有用户的公私钥,攻击者无法验证签名,也不能解密 E_i,并且每次登录请求消息和响应消息都包含随机数,即使攻击者截获所有传输的信息,用户和服务器隐私信息也不会受到影响。因此,本协议可以实现用户的匿名性和不可追踪性。

(4)三因素认证。在该协议中,用户 U_i 拥有合法的智能卡 SC_i,输入三因素 $\{ID_i, PW_i, B_i\}$ 且验证 $A_i = H(ID_i \oplus PW_i^*)$ 成功后才能进行后续操作。攻击者要对其进行攻击,需要得到这 3 个因素才能计算 $PW_i^* = H(PW_i \| h(B_i^*))$ 和 $H(ID_i \oplus PW_i^*)$。即使攻击者能获取到 $\{ID_i, PW_i\}$ 这 2 个因素,却得不到生物特征 B_i,因此本文协议满足三因素认证的安全。

(5)智能卡丢失攻击。当用户 U_i 的智能卡 SC_i 丢失或被窃取时,攻击者可以获取其存储的信息 $\{M_i, SR, (PK_i, SK_i)\}$。但是攻击者无法从这些存储的信息中获得其他任何有用的信息值,并且用户 U_i 的生物特征 B_i 具有唯一性,即使攻击者获取到用户的 ID_i,却也没有 PW_i 和 B_i 无法生成有效的登录信息。因此,所提协议可以抵御智能卡丢失攻击。

(6)用户假冒攻击。攻击者想要假冒用户 U_i 来获取服务器的成功认证,就必须要掌握用户 U_i 的密码 PW_i 和生物特征 B_i,才能生成有效的登录请求消息 $H(ID_i \oplus PW_i^*)$ 并发送给服务器。然而攻击者根本就无法获取到正确的三因素,这一设想明显不成立。因此,所提出的协议是安全的,足以抵御用户假冒攻击。

(7)服务器欺骗攻击。服务器欺骗攻击是指攻击者尝试通过模拟一个合法的服务器来欺骗用户的认证。本协议中,若攻击者试图截获用户 U_i 的验证消息 $\{Au, Sig, R_i, T_i\}$ 并伪装成服务器来获取隐私信息,计算生成验证信息发送给用户以通过用户的认证。然而攻击者无法得到用户的私钥 SK_i 和会话密钥 SR,也不能从 Au 中提取 M_i,因此无法生成正确的验证消息 As 来骗取用户 U_i 的合法验证,从而能够抵抗服务器欺骗攻击。

(8)离线密码猜测攻击。假设攻击者获取到智能卡 SC_i 以及用户 U_i 和服务器之间传输的所有会话信息,并且从中提取出密码 PW_i。由于 PW_i 的值被封装在 PW_i^* 中受到单向散列函数的保护,且用户的生物特征不可伪造,攻击者无法发起离线密码猜测攻击,因此该协议能够抵抗离线密码猜测攻击。

(9)重传攻击。认证过程增加了时间戳 T_i 和 T_j,双方需要在规定时间内进行验证,若在时间戳有效时间段攻击者窃取到通信信息并重放以骗取对方的合法验证。然而,每次会话传输的消息 Au 和 As 中都是由随机数 R_i 和 N 计算而成的,每次传输的消息是变化的。并且认证消息受到 ECCDH 密钥协议的保护,即使攻击者试图通过重播消息连接恶意会话,在不知道秘密参数或随机数的情况下,下一步的通信也无法继续。因此,所提出的协议可以抵抗重传攻击。

(10)中间人攻击。本协议具备双向认证的功能,用户 U_i 和服务器收到对方验证消息后需要验证对方身份的合法性。若攻击者截取到双方交互过程中的会话信息,是无法得到用户 U_i 的生物特征 B_i、用户私钥 SK_i 以及会话密钥 SR,并且每轮的验证信息都是由新的随机数构成,这样攻击者就不能计算出正确的验证信息 Au 和 As。因此,所提协议能够

抵抗中间人攻击。

表 4 展示了本协议与 Ali 等学者[1]、Yu 等学者[6]、Kumar 等学者[7]三个协议的安全性对比。协议[1]使用的是对称加密算法，攻击者一旦利用非法手段获取到密钥就能解密，进而计算相对应的会话信息，假冒合法用户和服务器将会话信息发送给对方以通过合法性验证，因此协议[1]不能抵御用户假冒和服务器欺骗攻击。协议[6]中的会话信息包含的随机数没有经过 ECC 椭圆曲线点乘运算，攻击者很容易通过重放窃取到的会话信息来获得对方的合法性验证，因此无法抵御重传攻击。协议[7]不提供用户匿名和不可追溯性，并且不能抵抗离线密码猜测攻击，因为用户密码在输入后没有经过封装，服务器的验证信息在传输过程中没有经过加密，攻击者可以从会话信息中提取出用户正确的身份信息。综上所述，本文提出的协议在安全性能方面优于其他 3 个协议。

表 4　安全性比较

Table 4　Comparison of security

安全性能	Ali′s protocol [1]	Yu′s protocol [6]	Kumar′s protocol [7]	Proposed protocol
三因素认证	√	√	√	√
双向认证	√	√	√	√
前向安全性	√	√	√	√
匿名和不可追溯性	√	√	×	√
智能卡丢失攻击	√	√	√	√
用户假冒攻击	×	√	√	√
服务器欺骗攻击	×	√	√	√
离线密码猜测攻击	√	√	×	√
重传攻击	√	×	√	√
中间人攻击	√	√	√	√

4　性能分析

本节主要分析本文所提三因素双向认证协议的通信成本、计算成本、存储成本三个性能指标，并与 Ali 等学者[1]、Yu 等学者[6]、Kumar 等学者[7]协议进行对比，以此来探讨本协议的性能优势。

本文采用 Intel ® Core i5 处理器、16 GB 内存的 Windows10 台式计算机上的 Ubuntu22.04 虚拟机环境来测试不同运算的计算成本。其中，异或运算和字符串连接运算所消耗的时间很少，可以忽略不计。用 T_e 表示椭圆曲线点乘运算时间，T_{fe} 表示生物模糊提取器运算时间，T_E 表示非对称加密运算时间，T_D 表示非对称解密运算时间，T_{cm} 表示切比雪夫混沌映射运算时间，T_{sig} 和 T_{ver} 分别表示签名和验证时间，上述运算消耗的时间见表 5。

表 5　相关操作的近似运算时间

Table 5　Approximate time cost of related operations　ms

符号	近似运算时间
T_e	12.305
T_E	2.758
T_D	1.635
T_{sig}	0.547
T_{ver}	0.774
T_{fe}	10.261
T_{cm}	14.109

表 6 展示了该协议与其他 3 个协议在计算时间上的比较结果。根据表 6 的结果可知，本文提出的协议的计算时间为 41.359 ms，比其他 3 个协议的计算时间都要少。与协议[6]相比，计算时间减少了 84.3%，因为在协议[6]中，用户和服务器在认证过程中为确保安全性，使用了 20 次的椭圆曲线点乘运算。因此本文协议相比于这 3 个协议在计算成本上具有优势。

表 6　计算成本比较

Table 6　Computation costs comparison　ms

协议	计算时间
Ali′s protocol [1]	$20T_e + 4T_E + 4T_D = 263.672$
Yu′s protocol [6]	$4T_{cm} = 56.436$
Kumar′s protocol [7]	$6T_{cm} = 84.654$
Proposed protocol	$T_{fe} + 2T_e + T_E + T_D + T_{sig} + 2T_{ver} = 41.359$

存储成本是协议性能的另一评价指标，反映了协议的执行效率。为了各协议具备相同的安全级别，假设哈希函数、混沌映射输出、身份 ID、随机数、时间戳和 ECC 密码算法所需位数分别为 160 bits、160 bits、160 bits、128 bits、32 bits 和 320 bits。在本文协议中，用户存储的数据有用户 ID_i、密码 PW_i、生物特征 B_i'、公私钥对 (PK_i, SK_i)、共享密钥 SR 和智能卡 SC_i，所需的存储空间为：160 + 160 + 160 +160 + 160 + 160 + 160 = 1 120 bits。

服务器存储的数据用户的 ID_i、公私钥对 (PK_i, SK_i)、共享密钥 SR，所需的存储空间为：160 + (160 +160 + 160)n = 160 + 480n bits。因此，用户和服务器的总存储成本为 (1 280 + 480n)bits，存储成本比较见表 7。根据表 7 中的结果可知，随着用户数量 n 不断增加，存储成本也在增加，并且本协议 n 的系数低于其他 3 个协议，因此，本协议在存储性能上具有优势。

表 7 存储成本比较

Table 7 Storage cost comparison bits

协议	存储成本
Ali′s protocol [1]	$160 \times 6 + 160 \times 5n + 160 \times 2 = 1\ 280 + 800n$
Yu′s protocol [6]	$160 \times 11 + 160 \times 4n + 160 \times 2 = 2\ 080 + 640n$
Kumar′s protocol [7]	$160 \times 6 + 32 + 160 \times 5n + 160 \times 4 = 1\ 632 + 800n$
Proposed protocol	$1\ 120 + 160 + 480n = 1\ 280 + 480n$

针对通信效率这一性能问题,本文通过计算传输消息的长度来判断协议的通信成本。本协议需要传输的信息有 $\{Sig, R_i, T_i, Au, As, N, T_j\}$,因为椭圆曲线的长度为 160 bits,椭圆曲线上具有 x 和 y 坐标的点为 320 bits,所以本协议的通信成本为:160×3+320+32×3+128=992 bits。通信成本比较见表 8,本协议的通信成本比 Ali 等学者[1]协议、Yu 等学者[6]协议、Kumar 等学者[7]协议都要低。综合计算成本、存储成本、通信成本这 3 个性能的对比与分析,本协议综合性能优于 Ali 等学者[1]协议、Yu 等学者[6]协议、Kumar 等学者[7]协议。

表 8 通信成本比较

Table 8 Communication cost comparison bits

协议	通信成本
Ali′s protocol [1]	320×4+320×4+320=3 520
Yu′s protocol [6]	160×7=1 120
Kumar′s protocol [7]	160×4+32+160×3=1 152
Proposed protocol	160×3+320+32×3+128=992

5 结束语

物联网技术的发展增加了网络开放性,用户隐私信息容易被泄露。本文针对物联网中隐私泄露、非法攻击等安全问题,基于用户密码、生物特征和智能卡,提出一种三因素双向认证协议。协议中的认证双方通过 2 次信息交互,引入数字签名和时间戳检验,实现双向认证的功能,进而提高认证协议的安全性。并设计会话密钥自动更新机制来防止会话密钥泄露引起的服务器欺骗攻击、重传攻击、中间人攻击等安全问题。通过安全性和性能的分析比较,证明本协议能够抵御各种已知攻击。通过实验分析比较,本协议在计算、通信和存储性能上均优于其他认证协议。未来,会进一步优化该三因素双向认证协议,并将其设计成系统,投入实际应用。

参考文献

[1] ALI R, PAL A K. An efficient three-factor-based authentication scheme in multi-server environment using ECC[J]. International Journal of Communication Systems, 2018, 31(4): e3484.

[2] WANG Feifei, XU Guo′ai, WANG Chenyu, et al. A provably secure biometrics-based authentication scheme for multi-server environment[J]. Security and Communication Networks, 2019(4): 1-15.

[3] WANG Feifei, XU Guo′ai, XU Guosheng. A provably secure anonymous biometrics-based authentication scheme for wireless sensor networks using chaotic map[J]. IEEE Access, 2019, 7: 101596-101608.

[4] KUMAR D, SINGH H K, AHLAWAT C. A secure three-factor authentication scheme for wireless sensor networks using ECC[J]. Journal of Discrete Mathematical Sciences and Cryptography, 2020, 23(4): 879-900.

[5] VINOTH R, DEBORAH L J, VIJAYAKUMAR P, et al. Secure multifactor authenticated key agreement scheme for industrial IoT[J]. IEEE Internet of Things Journal, 2020, 8(5): 3801-3811.

[6] YU Yicheng, TAYLOR O, LI Rui, et al. An extended chaotic map-based authentication and key agreement scheme for multi-server environment[J]. Mathematics, 2021, 9(8): 798.

[7] KUMAR A, OM H. An enhanced and provably secure authentication protocol using Chebyshev chaotic maps for multi-server environment[J]. Multimedia Tools and Applications, 2021, 80(9): 14163-14189.

[8] 李懿,田玉玲. 远程医疗信息系统中的三因素匿名认证协议[J]. 计算机工程与应用, 2023,59(10): 280-287.

[9] DHARMINDER D, MISHRA D, LI X. Construction of rsa-based authentication scheme in authorized access to healthcare services[J]. Journal of Medical Systems, 2020, 44(1): 1-9.

[10] SEBÉ F, DOMINGO-FERRER J, MARTINEZ-BALLESTE A, et al. Efficient remote data possession checking in critical information infrastructures[J]. IEEE Transactions on Knowledge and Data Engineering, 2008, 20(8): 1034-1038.

[11] ZHANG L, ZHU S, TANG S. Privacy protection for telecare medicine information systems using a chaotic map-based three-factor authenticated key agreement scheme[J]. IEEE Journal of Biomedical and Health Informatics, 2016, 21(2): 465-475.

[12] KOBLITZ N. Elliptic curve cryptosystems[J]. Mathematics of Computation, 1987, 48(177): 203-209.

[13] DINARVAND N, BARATI H. An efficient and secure RFID authentication protocol using elliptic curve cryptography[J]. Wireless Networks, 2019, 25(1): 415-428.