计算机科学
COMPUTER SCIENCE

基于区块链的物联网可追踪匿名跨域认证方案

汪秋丽, 任志宇, 吴翔宇, 管秋国, 王海超

引用本文

汪秋丽, 任志宇, 吴翔宇, 管秋国, 王海超. 基于区块链的物联网可追踪匿名跨域认证方案[J]. 计算机科学, 2025, 52(5): 337-344.

WANG Qiuli, REN Zhiyu, WU Xiangyu, GUAN Qiuguo, WANG Haichao. Blockchain-based Internet of Things Traceable and Anonymous Cross-domain AuthenticationScheme [J]. Computer Science, 2025, 52(5): 337-344.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.240100190

基于区块链的物联网可追踪匿名跨域认证方案

汪秋丽[1]　任志宇[1]　吴翔宇[1]　管秋国[1]　王海超[2]
1 信息工程大学密码工程学院　郑州 450001
2 国家计算机网络应急技术处理协调中心江苏分中心　南京 210000
(1941124532@qq.com)

摘　要　随着物联网技术的广泛应用,跨域信息共享需求日益迫切,跨域身份认证方案是确保跨域安全协作的基础。基于设备真实身份实现跨域认证存在隐私泄露的风险,而匿名认证方案又存在难以追踪恶意设备的隐患。针对上述问题,基于区块链技术提出了可追踪匿名跨域认证方案。结合单向哈希链和无证书密码,为设备生成多个无关联的假名身份及对应的公私钥对,利用动态累加器计算变更后的域信息,每次跨域认证使用不同的假名,依据域信息与密钥生成中心颁发的跨域凭证进行身份认证,既保护了设备隐私,又可以恢复恶意设备的真实身份,对其追责。BAN逻辑正确性分析和形式化安全证明表明,所提方案具有较高的安全性;与其他方案相比,认证过程中的计算开销和通信开销较低。

关键词:跨域认证;可追踪性和匿名性;单向哈希链;动态累加器
中图分类号　TP309

Blockchain-based Internet of Things Traceable and Anonymous Cross-domain Authentication Scheme

WANG Qiuli[1],REN Zhiyu[1],WU Xiangyu[1],GUAN Qiuguo[1] and WANG Haichao[2]
1 School of Cryptography Engineering,Information Engineering University,Zhengzhou 450001,China
2 National Computer Network Emergency Response Technical Team/Coordination Center of Jiangsu,Nanjing 210000,China

Abstract　With the wide application of Internet of things technology,there is an increasing demand for cross-domain information sharing,and cross-domain authentication scheme is the foundation for ensuring cross-domain secure collaboration. Realizing cross-domain authentication based on the real identity of the device has the risk of privacy leakage,while the anonymous authentication scheme has the hidden danger of making it difficult to track malicious devices. To address the above problems,a traceable and anonymous cross-domain authentication scheme based on blockchain technology is proposed. Combining one-way hash chain and certificateless cryptography,multiple unrelated pseudonym identities and corresponding public-private key pairs are generated for the device. Dynamic accumulator is used to calculate the changed domain information. Different pseudonyms are used for each cross-domain authentication,and identity authentication is performed based on the domain information and the cross-domain credentials issued by the key generation center,which not only protects the privacy of the device,but also recovers the real identity of the malicious device and holds them accountable. BAN Logic Correctness analysis and formal security proofs show that the proposed scheme has high security. Compared with other schemes,the calculation cost and communication cost in authentication process are lower.

Keywords　Cross-domain authentication,Traceability and anonymity,One-way hash chain,Dynamic accumulator

1　引言

物联网[1](Internet of Things,IoT)将各种传感器、处理器等智能设备连接起来,形成一个巨大的网络。这些设备实时产生数据,与周围其他设备交换数据并建立联系。IoT广泛应用于智能家居、智能电网、智能医疗系统、工业物联网和车联网等领域,提高了人们的生活质量和生产效率。预计2025年,物联网终端设备将激增到750亿台[2]。然而,物联网技术的应用也带来了层出不穷的安全隐患。例如,可穿戴设备采集大量用户的身体健康信息,如果对身份不加保护,将带来用户隐私泄露的风险;车联网包含大量的车载传感器设备,如果攻击者将设备的多次认证交互消息关联起来,则攻击者将分析出用户的行驶轨迹,甚至能够得出用户的住址、常去场所等信息[3]。因此,物联网环境下,研究

到稿日期:2024-01-29　返修日期:2024-06-19
基金项目:中原科技创新领军人才项目(224200510003)
This work was supported by the Zhongyuan Science and Technology Innovation Leading Talent Project(224200510003).
通信作者:任志宇(ren_ktzy@163.com)

设备身份隐私的保护机制至关重要。

在海量、多维、异构的物联网环境下，各个组织为保护自身资源不受非法访问，会建立独立于其他组织的身份认证体系，形成相互隔离的信任域。然而，随着物联网应用的不断丰富，单个域内完成工作变得困难，通常需要多域合作[4]。但是面对复杂的网络环境，一些组织出于对外域设备接入带来的安全顾虑，不愿和其他域进行数据共享与跨域合作。身份认证作为安全防护的第一步，亟需设计一个安全跨域认证协议来满足跨域协作需求。

在跨域过程中，各域相互独立，彼此互不信任，建立离散域之间的信任是一个很大的挑战。近年来迅速发展的区块链技术为此提供了新的解决思路，它基于底层去中心化网络、共识算法、智能合约和密码算法等技术建立去信任网络，具有去中心化、不可篡改性和可追溯性的特点，且联盟链节点只有经过授权才可以加入，符合多域合作的场景，借助区块链平台可以建立去中心化信任[5-7]。

在跨域认证过程中，保护设备身份隐私和追踪恶意设备身份尤为重要。屡见不鲜的安全事件和潜在的安全隐患说明了身份泄露将带来严重的后果，然而，对设备身份信息的保护，也为攻击者发起恶意行为时隐藏自己的身份提供了机会。因此，在保护设备身份隐私的同时，能够追踪恶意设备身份也是十分必要的。

在认证方案中，通过匿名认证实现身份隐私保护是一种常用的方式。文献[8-11]使用假名机制实现匿名，这些方案中，假名在其有效期内将被多次使用，使得攻击者可以将该假名发送的多次会话消息链接起来，造成隐私泄露。为进一步保护假名的安全性，Cui 等[12]为物联网设备生成多个假名身份，每次通信可以选择不同的假名来保护隐私；Zhang 等[13]在设备完成认证后会更新设备的假名。虽然以上两个方案加强了隐私保护，但这些方案都无法对恶意设备进行追踪。为了实现监管功能，Xue 等[14]根据恶意设备的假名查询注册列表，以追踪设备的真实身份，并分别在主链与从链上发布撤销交易，更新设备状态信息；Liu 等[15]和 Feng 等[16]通过可信权威机构，结合自身私钥、设备真实身份、身份有效期等信息，为设备生成多个假名，只有拥有私钥的权威机构才能根据假名恢复出真实身份。但以上方案依然存在假名在其有效期内被多次使用的问题。

综上所述，现有跨域认证方案不能很好地解决匿名认证和设备监管这一看似矛盾的需求。本文提出了一种物联网场景下基于区块链的可追踪匿名跨域认证方案，在保护设备隐私的同时，实现了双向认证以及可监管功能。安全性证明和实验分析表明，本方案具有很好的安全性和较低的计算与通信开销。本文的具体贡献如下：

1）基于区块链平台，提出一种设备与设备之间安全高效的跨域认证方案，实现了跨域双向认证与密钥协商。考虑到链上存储限制，用动态累加器来减小存储开销。

2）基于单向哈希链和无证书密码，为设备分配多个无关联的假名身份和与之对应的公私钥对，既保护了设备的隐私，又可以根据假名恢复出真实身份进行追责。

3）BAN 逻辑正确性分析和形式化安全证明表明，本方案满足安全需求，能够抵制常见攻击；性能分析表明，认证时设备端的计算开销和通信开销较小。

本文第 2 章介绍数学假设、系统框架、安全需求和安全模型；第 3 章描述跨域认证流程；第 4 章对协议正确性与安全性进行分析，结合安全需求对协议的安全属性进行讨论；第 4 章进行了性能评估；最后总结本文。

2 可追踪匿名认证框架

本章阐述相关数学假设，概述系统框架，归纳总结跨域认证安全需求，并介绍安全模型。

2.1 数学假设

椭圆曲线离散对数问题（ECDLP）：给定椭圆曲线上两点 P 和 $Q=xP(x\in Z_q^*)$，其中 q 为大素数，由 Q 求解整数 x 是困难的。

计算性的椭圆曲线 Diffie-Hellman 假设（ECDHP）：给定椭圆曲线上的点 $P, Q_1=aP, Q_2=bP$，其中 $a, b\in Z_q^*$，计算 abP 是困难的。

强 Diffie-Hellman（q-SDH）假设：设 G 是 p 阶循环群，p 为素数，g 是 G 的一个生成元，$a\in Z_q^*$。给定一个 $q+1$ 元组 $(g, g^a, \cdots, g^{a^q})$，计算 $(x, g^{1/(x+a)})\in Z_p^*\times G$ 是困难的。

2.2 系统框架

本文的系统框架如图 1 所示，包含 3 个部分：物联网设备 DE、密钥生成中心 PKG 和认证服务器 AS。

1）物联网设备 DE：物联网设备拥有少量的计算和存储资源，不能进行复杂的操作，但是可以存储假名身份并进行简单的密码学运算。

2）密钥生成中心 PKG：假设 PKG 可信，拥有强大的计算能力和存储资源。PKG 负责域内 DE 和 AS 的注册，为 DE 生成假名身份和颁发跨域凭证，对恶意设备进行追踪。作为联盟链节点，PKG 会将域信息发布在链上。

3）认证服务器 AS：AS 作为链上节点，负责查询发布的域信息，辅助 PKG 完成设备认证，减轻 PKG 的负载。

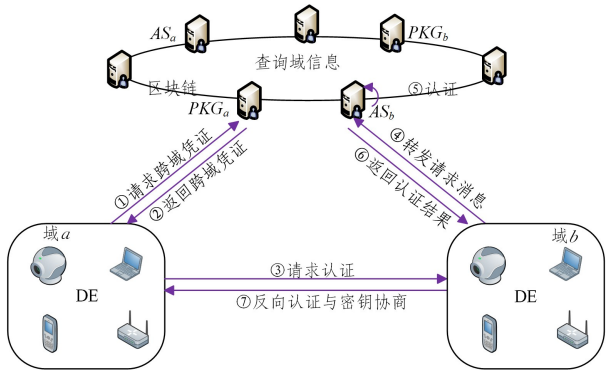

图 1 系统框架图

Fig. 1 System architecture

2.3 安全需求

安全性和隐私性是物联网最重要的因素，而它的开放性、异构性、动态性、终端设备计算和存储资源有限性等特点[17]，使物联网容易受到各种网络攻击[1]。根据物联网结构，基于先前的研究工作[11-14]，对物联网场景下跨域认证与密钥协商

协议所需满足的安全需求进行归纳。

1)双向认证：通信双方在传输数据之前进行身份互认证，以建立信任关系。

2)匿名性：为了保护设备的隐私，其他实体不能通过截获的消息得出设备的真实身份。

3)不可链接性：攻击者不能将同一设备的多次会话消息链接起来。

4)可追踪性：当设备发生恶意行为时，可以实施监管功能，揭露它的真实身份。

5)抵制各种攻击：跨域认证与密钥协商协议应能够抵制常见的攻击，如重放攻击、假冒攻击和中间人攻击。

2.4 安全模型

本节基于文献[18-20]，提出了适合本方案的安全模型。模型包含 PKG，AS 和 DE 3 类参与者，分别用符号 Π_{PKG}^{i}，Π_{AS}^{j}，Π_{DE}^{k}来表示它们的第 i,j,k 个实例。攻击者 $\mathcal{A}$向参与者发起查询，参与者被动地回答 $\mathcal{A}$的各种查询，通过与参与者交互，试图破坏协议的安全性，这一交互过程称为对参与者的问询。攻击者 $\mathcal{A}$的能力由以下对参与者的问询进行定义。

$Execute(\Pi_{\mathrm{PKG}}^{i},\Pi_{\mathrm{AS}}^{j},\Pi_{\mathrm{DE}}^{k})$：本问询模拟了被动攻击。攻击者通过此问询，可以获得参与者之间传输的消息。

$Send(\Pi_{\mathrm{PKG}}^{i},\Pi_{\mathrm{AS}}^{j},\Pi_{\mathrm{DE}}^{k},m)$：本问询模拟攻击者对 3 类参与者的主动攻击。例如，$\mathcal{A}$可以伪装成 Π_{DE}^{k}发送消息 m 给 Π_{PKG}^{i}或者 Π_{AS}^{j}，如果验证通过，那么 $\mathcal{A}$就会接收到相应的响应消息。

$Hash(x,h(x))$：Hash 预言机维护一个哈希列表$(x,h(x))$，记录所有的查询和应答。在这个问询中，$\mathcal{A}$发送一个消息 x，若 x 在列表中，则返回对应的 $h(x)$值给攻击者；否则，随机生成一个字符串 $k\in Z_q^*$ 返回给攻击者，并将其记录在列表中。

$Reveal(\Pi_{\mathrm{DE}}^{k})$：该问询模拟已知密钥安全。当 $\mathcal{A}$进行 Reveal 问询时，返回设备之间建立的会话密钥。

$Test(\Pi_{\mathrm{DE}}^{k})$：此问询模拟会话密钥的语义安全。当 $\mathcal{A}$进行 Test 问询时，Π_{DE}^{k}首先随机选取一比特 $b\in\{0,1\}$，并对 b 的值保密。若 $b=1$，则 Π_{DE}^{k}返回真实的会话密钥给 $\mathcal{A}$；否则，返回一个与会话密钥长度相同的随机值给 $\mathcal{A}$。

$\mathcal{A}$必须判断 Π_{DE}^{k}返回的密钥是否真实。$\mathcal{A}$执行完 Test 问询后，将输出对 b 的猜测值 b'，如果 $b'=b$，则 $\mathcal{A}$赢得游戏，破坏了本协议 $\mathcal{P}$的安全性。我们用 Succ 表示事件“敌手 $\mathcal{A}$赢得游戏”，则 $\mathcal{A}$破坏本协议 $\mathcal{P}$安全性的优势为 $Adv_{\mathcal{A}}^{\mathcal{P}}(AKA)=|2Pr[Succ]-1|=|2Pr[b'=b]-1|$。

定义 1(语义安全，AKA-secure) 协议 $\mathcal{P}$是 AKA-secure 的，如果对于任意多项式时间计算能力的攻击者 $\mathcal{A}$，$Adv_{\mathcal{A}}^{\mathcal{P}}(AKA)$都可以忽略。

3 跨域认证方案流程

3.1 方案概述

本文设计了基于区块链的可追踪匿名跨域认证方案。采用 Hyperledger Fabric v1.4 区块链平台的拜占庭容错算法(PBFT)达成共识。方案包含 4 个阶段，分别为系统初始化阶段、注册阶段、身份撤销与更新阶段、跨域认证与密钥协商阶段。系统初始化阶段，各域中的 PKG 生成各自域的系统参数，并将包含系统参数的交易信息广播到区块链上，为后续跨域认证做准备。注册阶段分为 AS 注册和 DE 注册，为了实现可追踪匿名认证，为设备生成了多个无关联的假名，进行跨域认证时，设备使用假名身份，并且 PKG 能够根据假名身份追踪到恶意设备的真实身份。此外，为了更好地保护设备隐私，本文采取无证书密码方式为设备生成公私钥对，摆脱了 PKG 对设备的密钥托管导致的设备私钥泄露的问题。由于将所有假名身份的公钥信息上传到区块链上将会带来很大的通信与链上存储开销，故本文采用了动态累加器技术，只在链上保存各域的累加值，既不影响认证，又减小了开销。在身份撤销与更新阶段，对每个使用过的假名进行撤销，确保会话消息的不可链接性。跨域认证与密钥协商阶段，在跨域前，设备 DE_{U1}^{a}预先向本域 PKG_a 申请跨域凭证。在跨域认证时，向外域设备 DE_{U2}^{b}提供跨域凭证，由于物联网设备存储资源小，无法存储链上信息，所以 DE_{U2}^{b}需要将跨域凭证转发给 AS_b，请求对凭证进行验证，AS_b 根据凭证和区块链上存储的域信息对设备 DE_{U1}^{a}进行认证，并将认证结果返回给 DE_{U2}^{b}。为便于阅读，表 1 对关键符号进行了说明。

表 1 符号说明

Table 1 Symbols and their notations

符号	含义说明
D_a/D_b	域 a/域 b
DID_i	域标识符
$PID_{Ui,j}$	DE_{Ui}^{a}设备的第 j 个假名
msk_i	PKG_i 的私钥
P_{pub_i}	PKG_i 的公钥
sk_{AS}^{i}	AS_i 的私钥
U_{AS}^{i}	AS_i 的公钥
SD_{U1}/SD_{U2}	随机选取的种子
$(x_{1j},z_{U1_j}^{a})$	假名 $PID_{U1,j}$的私钥
$P_{U1_j}^{a}$	假名 $PID_{U1,j}$的公钥

3.2 系统初始化

以域 D_a 为例，PKG_a 选定安全参数 l，输出系统公开参数 $(p_a,q,G_a,G_T,G,e_a,g_a,pk_{\mathrm{acc}},P,P_{pub_a},H_1,H_2,H_3)$，其中 e_a：$G_a\times G_a\rightarrow G_T$ 为双线性映射，g_a 和 P 分别为群 G_a 和 G 的生成元，大素数 p_a 是群 G_a 和 G_T 的阶，动态累加器的公私钥对 $sk_{\mathrm{acc}}=\lambda_a\in_R Z_{p_a}^*$，$pk_{\mathrm{acc}}=(g,g^{\lambda_a},\cdots,g^{\lambda_a^{v}},u)$，系统主密钥 $msk_a=s_a\in Z_q^*$ (q 为大素数)，$P_{pub_a}=s_aP$，3 个哈希函数 H_1：$\{0,1\}^*\rightarrow Z_q^*$，$H_2$：$\{0,1\}^*\rightarrow Z_q^*$，$H_3$：$\{0,1\}^*\times G\rightarrow Z_q^*$。$PKG_a$ 发布累加值交易 $ATX=(DID_a,v,p_a,q,G_a,G_T,G,e_a,g_a,P,U_{\mathrm{AS}}^{a},pk_{\mathrm{acc}},\Delta,sig_{s_a})$，其中 DID_a 为域标识符，公钥信息 U_{AS}^{a}和初始累加值 Δ 为空，v 为域信息版本号，sig_{s_a} 为 PKG_a 对累加值交易的签名。此过程中，区块链作为分布式账本，存储身份认证过程中所需的关键数据，如各域的累加值和版本号。由于区块链具有去中心化和不可篡改性等特点，因此其为跨域时验证设备身份提供认证信息。

3.3 注册阶段

3.3.1 AS 注册

以 AS_a 注册为例，AS_a 通过安全信道将真实身份 ID_{AS}^{a}发送给 PKG_a，PKG_a 随机选取 $r_{\mathrm{AS}}^{a}\in Z_q^*$，计算 $R_{\mathrm{AS}}^{a}=r_{\mathrm{AS}}^{a}P$，私钥 $sk_{\mathrm{AS}}^{a}=r_{\mathrm{AS}}^{a}+s_a\cdot H_1(ID_{\mathrm{AS}}^{a}\parallel R_{\mathrm{AS}}^{a})$，公钥 $U_{\mathrm{AS}}^{a}=sk_{\mathrm{AS}}^{a}\cdot P$。$PKG_a$

发送$\{R_{AS}^a, sk_{AS}^a, U_{AS}^a\}$给$AS_a$，更新累加值交易$ATX$。$AS_a$验证$R_{AS}^a + H_1(ID_{AS}^a \| R_{AS}^a) P_{pub_a} = U_{AS}^a$是否成立，若成立，则保存公私钥对；否则重新申请。

3.3.2 *DE* 注册

以DE_{U1}^a注册为例，介绍注册流程。

第1步 DE_{U1}^a的真实身份记为ID_{U1}^a，它随机选取$m+1$个随机数$x_{1k} \in Z_q^*$（$k=0,1,\cdots,m$）作为生成长期私钥和m个临时私钥的秘密值，计算$X_{1k} = x_{1k} P$。通过安全通道向PKG_a发送注册请求$\{ID_{U1}^a, X_{10}, X_{11}, \cdots, X_{1m}\}$。

第2步 PKG_a选取两个随机种子SD_{U1}和SD_{U2}，由式(1)中的两个单向哈希链生成m个假名$PID_{U1,j} = (pid_{1,j,1}, pid_{1,j,2})$，$j \in [1,m]$。

$$\begin{cases} H_{1,j} = H_2^j(SD_{U1}) \\ H_{1,m-j+1} = H_2^{m-j+1}(SD_{U2}) \\ pid_{1,j,1} = H_2(H_{1,j} \oplus H_{1,m-j+1}) \\ pid_{1,j,2} = ID_{U1}^a \oplus H_3(s_a pid_{1,j,1}, P_{pub_a}) \end{cases} \tag{1}$$

第3步 PKG_a为设备真实身份生成长期公私钥对：选取随机数$y_0 \in Z_q^*$，计算$P_{U1}^a = X_{10} + y_0 P$，$h_{1,0} = H_1(ID_{U1}^a \| P_{U1}^a)$，$h_{2,0} = H_2(ID_{U1}^a \| P_{U1}^a)$，$z_{U1}^a = h_{1,0} y_0 + h_{2,0} \cdot s_a$。然后为$m$个假名生成公私钥对：随机选取$y_1, \cdots, y_m \in Z_q^*$，计算$P_{U1_j}^a = X_{1j} + y_j P$，$h_{i,j} = H_i(pid_{1,j,1} \| pid_{1,j,2} \| P_{U1_j}^a)$，其中$i \in [1,2]$，$j \in [1,m]$，$z_{U1_j}^a = h_{1,j} y_j + h_{2,j} \cdot s_a$，$\beta_{U1} = H_1(ID_{U1}^a \| SD_{U1} \| SD_{U2})$，$\beta_{U1}$为设备的累加元素。$PKG_a$将$\{PID_{U1,j}, P_{U1}^a, P_{U1_j}^a, z_{U1}^a, z_{U1_j}^a, \beta_{U1}\}$通过安全通道发送给$DE_{U1}^a$，将$(ID_{U1}^a, P_{U1}^a, SD_{U1}, SD_{U2})$保存在本地数据库中。$DE_{U1}^a$验证$(h_{1,0} x_0 + z_{U1}^a) P = h_{1,0} P_{U1}^a + h_{2,0} \cdot P_{pub_a}$和$(h_{1,j} x_j + z_{U1_j}^a) P = h_{1,j} P_{U1_j}^a + h_{2,j} P_{pub_a}$是否成立，若成立，则本地保存长期私钥$(x_{10}, z_{U1}^a)$和公钥$P_{U1}^a$，以及$m$个假名身份$PID_{U1,j}$和对应的完整私钥$(x_{1j}, z_{U1_j}^a)$与公钥$P_{U1_j}^a$；否则重新申请。

第4步 PKG_a计算累加值$\Delta' = \Delta^{\beta_{U1} + sk_{acc}}$，发布新的累加值交易$ATX' = (DID_a, v', \Delta', sig_{s_a})$到链上，其中$v'$为更新后的域信息版本号，$sig_{s_a}$为$PKG_a$对累加值交易的签名。

3.4 身份撤销与更新

以PKG_a撤销假名身份$PID_{U1,j}$为例，当PKG_a为$PID_{U1,j}$颁发跨域凭证后（具体见3.5节），将$pid_{1,j,1}$保存在本地撤销列表。每个假名身份只使用一次，保证了不可链接性。

当设备DE_{U1}^a所剩假名身份个数不超过L（L为预先规定的阈值）个时，可以重新向PKG_a申请假名，流程与DE_{U1}^a注册时类似，但发送注册请求时用PKG_a的公钥加密，PKG_a收到消息后解密，基于椭圆曲线密码用X_{10}将生成的假名加密，并发送给DE_{U1}^a。

3.5 跨域认证与密钥协商

首先，设备请求PKG为其颁发跨域凭证，这一步骤可以在设备空闲时预先完成。之后，来自不同域的两个设备进行认证，并协商会话密钥。如图2所示，以域D_a内的设备DE_{U1}^a和域D_b内的设备DE_{U2}^b为例，描述认证流程。

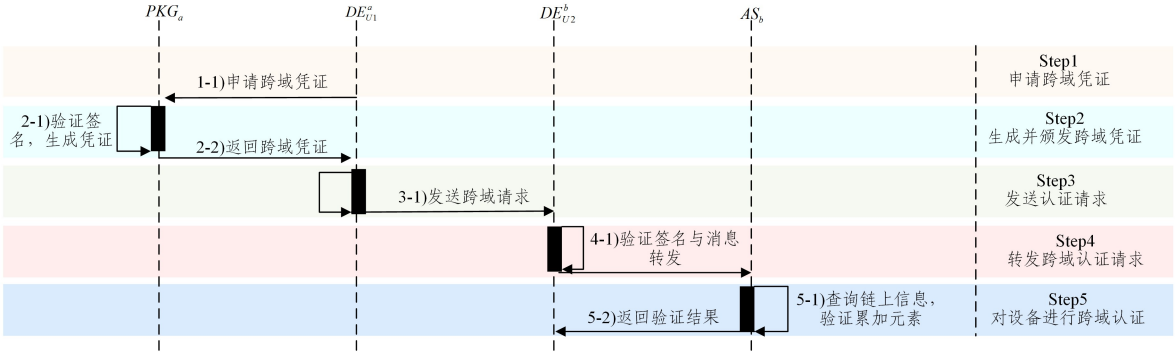

图2 跨域单向认证流程图

Fig. 2 Cross-domain one-way authentication process

Step1 申请跨域凭证

$DE_{U1}^a \rightarrow PKG_a: M_1 = \{PID_{U1,j}, DID_b, N_1, sig_{x_{10}}\}$

DE_{U1}^a以假名身份$PID_{U1,j}$向PKG_a申请跨域授权，DID_b为目的域标识符，N_1为随机数，$sig_{x_{10}}$为设备利用长期私钥(x_{10}, z_{U1}^a)得到的签名（计算方法见Step3）。

Step2 生成并颁发跨域凭证

1）PKG_a收到跨域授权请求后，检查身份$PID_{U1,j}$是否在撤销列表，若不在撤销列表中，则计算$ID_{U1}^a = pid_{1,j,2} \oplus H_3(s_a pid_{1,j,1}, P_{pub_a})$，根据$ID_{U1}^a$在本地数据库中检索设备的公钥$P_{U1}^a$，对签名进行验证（验证方法见Step4）。若验证不通过，则拒绝请求；否则，计算累加元素β_{U1}，生成见证$w_{U1} = \Delta^{1/(\beta_{U1} + sk_{acc})}$。根据$DID_b$在链上检索域$D_b$的公钥，生成跨域凭证$\mu = En_{U_{AS}^a}(PID_{U1,j}, \beta_{U1}, w_{U1}, v)$，其中$v$为域信息版本号。

2）PKG_a返回跨域凭证μ给DE_{U1}^a。

$PKG_a \rightarrow DE_{U1}^a: M_2 = \{\mu, N_1, sig_{msk_a}\}$

Step3 发送认证请求

$DE_{U1}^a \rightarrow DE_{U2}^b: M_3 = \{PID_{U1,j}, P_{U1_j}^a, DID_a, \mu, N_2, sig_{x_{1j}}\}$

DE_{U1}^a根据PKG_a的公钥验证消息的完整性，并检查M_2中随机数与N_1是否一致，防止重放攻击。若验证不通过，则重新申请；否则，DE_{U1}^a以假名身份$PID_{U1,j}$与DE_{U2}^b进行交互，发送跨域请求M_3。其中，$sig_{x_{1j}}$的计算基于椭圆曲线Schnorr签名算法：DE_{U1}^a随机选取$w_1 \in Z_q^*$，计算$\beta_1 = w_1 P$，$\gamma = H_1(\beta_1 \| M_3)$，$\eta_1 = w_1 + \gamma(h_{1,j} x_{1j} + z_{U1_j}^a)$，$sig_{x_{1j}} = (\beta_1, \eta_1)$。

Step4 转发跨域认证请求

$DE_{U2}^b \rightarrow AS_b: M_4 = \{PID_{U2,j}, P_{U2_j}^b, DID_a, PID_{U1,j}, \mu, N_3, sig_{x_{2j}}\}$

DE_{U2}^b收到消息后，验证签名。验证过程如下：计算$h'_{1,j} =$

$H_1(pid_{1,j,1} \parallel pid_{1,j,2} \parallel P^a_{U1_j})$，$h'_{2,j}=H_2(pid_{1,j,1} \parallel pid_{1,j,2} \parallel P^a_{U1_j})$，$\gamma'=H_1(\beta_1 \parallel M_3)$，$\delta=h'_{1,j} \cdot P^a_{U1_j}+h'_{2,j}P_{pub_a}$，验证 $\eta_1 P=\beta_1+\gamma'\delta$ 是否成立，若不成立，则拒绝请求；否则保存随机数 N_2，添加随机数 N_3，发送 M_4 给 AS_b。

Step5　对设备进行跨域认证

1）AS_b 收到消息后验证签名，若不成立，则请求重新转发；否则，用私钥解密 μ 获取假名身份 $PID_{U1,j}$，β_{U1}，w_{U1} 以及版本号 v。检查 $PID_{U1,j}$ 与 M_4 中包含的身份是否一致，若不一致，则认证失败；否则，根据 DID_a 在链上查询域 D_a 的累加值及其他参数。验证 $e(w_{U1}, g_a^{\beta_{U1}} g_a^{\lambda_a})=e(\Delta, g_a)$ 是否成立，若成立，则说明 DE^a_{U1} 的累加元素在累加集合中，认证成功；否则认证失败。

2）返回验证结果

$AS_b \rightarrow DE^b_{U2}: M_5=\{N_3, \text{success}, sig_{sk^a_{AS}}\}$

Step6　反向认证

DE^b_{U2} 收到 M_5 后，检查随机数和签名，若没有验证通过，则重新请求认证；否则根据返回结果判定是否接受 DE^a_{U1} 的认证请求。可以通过类似的方式实现 DE^a_{U1} 对 DE^b_{U2} 的认证，但 DE^b_{U2} 在发送反向认证请求时，除了生成一个随机数 N_4 外，还需要将保存的 N_2 包含在请求消息中，DE^b_{U1} 检查随机数是否与发送的一致。

Step7　会话密钥协商

完成跨域认证流程后，DE^a_{U2} 收到 DE^a_{U1} 的签名 $sig_{x_{1j}}=(\beta_1, \eta_1)$，$DE^a_{U1}$ 收到 DE^a_{U2} 的签名 $sig_{x_{2j}}=(\beta_2, \eta_2)$，其中 $\beta_1=w_1 P$，$\beta_2=w_2 P$，w_1 和 w_2 分别由 DE^a_{U1} 和 DE^a_{U2} 随机选取，它们的会话密钥 $SE=w_1\beta_2=w_2\beta_1=w_1 w_2 P$。

Step8　完成挑战应答，认证及密钥协商结束

$DE^a_{U1} \rightarrow DE^b_{U2}: M_6=\{N_2, N_4, HMAC_{SE}\}$

在完成反向认证，建立了会话密钥后，DE^a_{U1} 将 N_2，N_4 以及利用密钥 SE 生成的消息认证码发送给 DE^b_{U2}。DE^b_{U2} 验证完成后，双方完成了挑战应答流程，删除此次使用的假名身份，认证与密钥协商结束。

4　安全性分析

4.1　协议正确性分析

本节利用 BAN 逻辑对跨域认证协议的正确性进行形式化分析。

1）推理规则

（R1）消息新鲜性规则：如果 P 相信消息 X 是新鲜的，那么 P 相信 (X,Y) 是新鲜的。

$$\frac{P \models \#(X)}{P \models \#(X,Y)}$$

（R2）随机数验证规则：如果 P 相信消息 X 是新鲜的，且 P 相信 Q 发送过 X，则 P 相信 Q 相信 X。

$$\frac{P \models \#(X), P \models Q|\sim X}{P \models Q \models X}$$

（R3）累加器规则：如果 Q 相信累加值为 Δ，累加元素 x_i 的见证为 W_i，且 Q 收到包含 P 累加元素 x_i 的消息 M，则 Q 相信 P 发送过消息 M。

$$\frac{Q \models \xrightarrow{\Delta, W_i} P, Q \triangleleft \langle M \rangle_{x_i}}{Q \models P|\sim M}$$

（R4）信仰规则：如果 P 相信 Q 相信 (X,Y)，那么 P 相信 Q 相信 X。

$$\frac{P \models Q \models (X,Y)}{P \models Q \models X}$$

（R5）仲裁规则：如果 P 相信 Q 对 X 有仲裁权，且 P 相信 Q 相信 X，那么 P 相信 X。

$$\frac{P \models Q \Rightarrow X, P \models Q \models X}{P \models X}$$

2）协议目标

本文跨域认证协议应满足目标 G1 和 G2，其中 P 代表 DE^a_{U1}，Q 代表 DE^b_{U2}。考虑到 DE^b_{U2} 对收到的跨域认证请求转发给 AS_b 进行验证，为了更好地理解，在证明过程中，用 AS_b 代替 DE^b_{U2}。

G1：$Q \models (P \xleftrightarrow{\beta_1} Q)$

G2：$P \models (P \xleftrightarrow{\beta_2} Q)$

跨域认证目标是 P 和 Q 互认证，接受对方的随机数 β_1 和 β_2，基于 ECDHE 密钥协商算法，利用收到的随机数生成会话密钥 $SE=w_1\beta_2=w_2\beta_1$。

3）消息的形式化描述

P 与 Q 之间的消息可以形式化描述为：

$$M_3=(PID_{U1,j}, P^a_{U1_j}, DID_a, \{PID_{U1,j}, \beta_{U1}, w_{U1}, v\}_{U^a_{AS}}, N_2, \langle \beta_1, \eta_1 \rangle_{x_{1j}})$$

4）协议假设

（A1）$Q \models \#(N_2)$

（A2）$Q \models P \Rightarrow \beta_1$

（A3）$Q \models \xrightarrow{\Delta} P$，这个假设模拟了 AS_b 可以查询区块链来得到每个域的累加值 Δ。

5）证明过程

Q 收到消息 M_3 后验证签名，确保消息的完整性，并解密得到 P 的累加元素 β_{U1} 和见证 w_{U1}。通过计算 $e(w_{U1}, g_a^{\beta_{U1}} g_a^{\lambda_a})=e(\Delta, g_a)$ 是否成立，来验证 β_{U1} 是否包含在累加值 Δ 中，如果包含，则由（A3）和（R3）可以推出：

$$\frac{Q \models \xrightarrow{\Delta, w_{U1}} P, Q \triangleleft \langle M_3 \rangle_{\beta_{U1}}}{Q \models P|\sim M_3} \tag{2}$$

根据（A1）和（R1）可得：

$$\frac{Q \models \#(N_2)}{Q \models \#(M_3)} \tag{3}$$

根据式（2）、式（3）和（R2）可以推导出：

$$\frac{Q \models \#(M_3), Q \models P|\sim M_3}{Q \models P \models M_3} \tag{4}$$

由式（4）和（R4）可得：

$$\frac{Q \models P \models M_3}{Q \models P \models P \xrightarrow{\beta_1} Q)} \tag{5}$$

根据式（5），（A2）和（R5）可以推出：

$$\frac{Q \models P \Rightarrow \beta_1, Q \models P \models (P \xrightarrow{\beta_1} Q)}{Q \models (P \xrightarrow{\beta_1} Q)}$$

故协议可以实现 G1。同理，通过反向认证可以得到 $P \models P \xrightarrow{\beta_2} Q)$，实现目标 G2。

综上，不同域的设备 DE^a_{U1} 和 DE^b_{U2} 可以相互认证，基于

随机数 β_1 和 β_2 协商会话密钥 $SE=w_1\beta_2=w_2\beta_1$。

4.2 协议安全性分析

定理 1 敌手 $\mathcal{A}$ 破坏协议 $\mathcal{P}$ 语义安全的优势如式(6)所示，其中 q_{exe}，q_{send} 和 q_{hash} 分别表示执行 Execute 问询、Send 问询和 Hash 问询的次数，$|Hash|$ 表示哈希函数的值域空间大小，$Adv_{\mathcal{A}}^{\text{ECDHP}}$ 表示 $\mathcal{A}$ 解决 ECDHP 的优势。

$$Adv_{\mathcal{A}}^{\mathcal{P}}(AKA)\leqslant\frac{q_{\text{hash}}^2+(q_{\text{exe}}+q_{\text{send}})^2}{|Hash|}+2Adv_{\mathcal{A}}^{\text{ECDHP}} \tag{6}$$

为了证明式(6)，定义 4 个游戏，记为 $Game_r$($r=0,1,2,3$)。在每个游戏中，$\mathcal{A}$ 会猜测 b 值，定义 $Succ_r$ 表示事件“$\mathcal{A}$ 通过猜测 b 值赢得游戏 $Game_r$”。

$Game_0$：这个游戏表示初始攻击，$\mathcal{A}$ 进行 Test 问询，当 $b=1$ 时，$\mathcal{A}$ 获得真实的会话密钥。故有：

$$Adv_{\mathcal{A}}^{\mathcal{P}}(AKA)=|2Pr[Succ_0]-1| \tag{7}$$

$Game_1$：这个游戏表示经过 Execute 和 Reveal 问询之后，$\mathcal{A}$ 执行 Test 问询判定返回值是否为真实的密钥。敌手即使窃听了参与者之间所有的通信消息和之前的会话密钥，也不能根据这些信息获取计算密钥所需的参数 w_1 和 w_2。因此，与 $Game_0$ 相比，$\mathcal{A}$ 通过 $Game_1$ 获胜的优势并没有增加，故：

$$Pr[Succ_1]=Pr[Succ_0] \tag{8}$$

$Game_2$：该游戏通过执行 Send 问询和 Hash 查询来模拟主动攻击。敌手拦截消息后，试图通过修改它们中的任意一条，来伪造一个可以通过认证的合法消息。根据生日悖论[21]，有：

$$|Pr[Succ_2]-Pr[Succ_1]|\leqslant\frac{q_{\text{hash}}^2+(q_{\text{exe}}+q_{\text{send}})^2}{2|Hash|} \tag{9}$$

$Game_3$：在这个游戏中，$\mathcal{A}$ 试图通过截获的消息计算 $\Pi_{\text{DE}}^{k_1}$ 和 $\mathcal{A}_{\text{DE}}^{k_2}$ 之间的会话密钥。通过 w_1P 和 w_2P 计算 $SE=w_1w_2P$，这需要 $\mathcal{A}$ 在多项式时间内解决 ECDHP 数学假设，因此：

$$|Pr[Succ_3]-Pr[Succ_2]|\leqslant Adv_{\mathcal{A}}^{\text{ECDHP}} \tag{10}$$

在 $Game_3$ 结束后，没有任何与输出 b 相关的信息泄露，故有：

$$Pr[Succ_3]=\frac{1}{2} \tag{11}$$

结合式(7)－式(11)，可以得出：

$$\begin{aligned}&\frac{1}{2}Adv_{\mathcal{A}}^{\mathcal{P}}(AKA)\\&=\left|Pr[Succ_0]-\frac{1}{2}\right|\\&=|Pr[Succ_0]-Pr[Succ_3]|\\&\leqslant|Pr[Succ_0]-Pr[Succ_1]|+|Pr[Succ_1]-\\&\quad Pr[Succ_2]|+|Pr[Succ_2]-Pr[Succ_3]|\\&\leqslant\frac{q_{\text{hash}}^2+(q_{\text{exe}}+q_{\text{send}})^2}{2|Hash|}+Adv_{\mathcal{A}}^{\text{ECDHP}}\end{aligned} \tag{12}$$

即 $Adv_{\mathcal{A}}^{\mathcal{P}}(AKA)\leqslant\frac{q_{\text{hash}}^2+(q_{\text{exe}}+q_{\text{send}})^2}{|Hash|}+2Adv_{\mathcal{A}}^{\text{ECDHP}}$。

故定理 1 成立。

4.3 安全属性分析

本节通过非形式化分析，进一步分析协议的安全属性和可以抵抗的常见攻击，并与文献[11]、文献[13]、文献[14]进行对比。分析表明，所提方案是安全的，满足 2.3 节的安全需求。

1)双向认证：通过对设备的签名和累加元素/见证的验证，完成设备的认证。在跨域过程中，每条消息带有签名，在没有私钥的情况下，攻击者不能伪造出合法的签名。跨域凭证包含了设备的累加元素及见证，其中见证由 PKG 利用动态累加器私钥生成，若要伪造可以通过验证的累加元素和对应的见证，则需要解决 q-SDH 数学假设。

2)匿名性：与其他设备通信时，使用假名身份 $PID_{U1,j}=(pid_{1,j,1},pid_{1,j,2})$，其中 $pid_{1,j,2}=ID_{U1}^a\oplus H_3(s_apid_{1,j,1},P_{pub_a})$，可以计算设备的真实身份 $ID_{U1}^a=pid_{1,j,2}\oplus H_3(s_apid_{1,j,1},P_{pub_a})$，但攻击者不知道 PKG 的私钥，不能得出匿名设备的真实身份。

3)不可链接性：设备每次会话都使用不同的假名身份，这些假名由 PKG 随机选取的种子经过多次哈希后生成，假名之间无关联，且不会暴露真实身份。

4)可追踪性：当假名身份为 $PID_{U1,j}=(pid_{1,j,1},pid_{1,j,2})$ 的设备发生恶意行为时，PKG_a 可以根据私钥恢复出匿名设备的真实身份 $ID_{U1}^a=pid_{1,j,2}\oplus H_3(s_apid_{1,j,1},P_{pub_a})$。

5)已知密钥安全：会话密钥 $SE=w_1\beta_2=w_2\beta_1=w_1w_2P$，其中 w_1 和 w_2 是随机数，取值与之前会话无关。攻击者即使知道了之前的会话密钥，依然不会增加得知当前会话密钥的优势。

6)重放攻击：发送的消息都带有随机数，通过随机数检查与挑战应答模式，可以有效避免消息重放攻击。

7)假冒攻击：基于 Schnorr 签名算法的安全性[22]，在没有私钥的情况下，无法生成合法的签名，故攻击者无法假冒合法的设备或服务器。

8)中间人攻击：在这类攻击中，攻击者作为通信双方之间的中介传输消息。根据前面的分析，攻击者不能修改或伪造拦截的消息，所以可以抵抗中间人攻击。

将本方案与文献[11]方案、文献[13]方案、文献[14]方案进行对比，结果如表 2 所列。可以看出，文献[11]方案不能抵抗常见的攻击，且文献[11]和文献[14]方案隐私保护不足，可以将设备的多次会话链接起来；而文献[13]方案不能对设备进行追踪，只有本方案可以同时满足这些安全属性，抵抗常见攻击。

表 2 安全属性对比

Table 2 Comparison of security attributes

安全属性	文献[11]方案	文献[13]方案	文献[14]方案	本文方案
双向认证	√	√	√	√
匿名性	√	√	√	√
不可链接性	×	√	×	√
可追踪性	×	×	√	√
已知密钥安全	√	√	√	√
抵抗重放攻击	×	√	√	√
抵抗假冒攻击	×	√	√	√
抵抗中间人攻击	×	√	√	√

5 性能分析

本章对所提方案进行实验，从计算开销、通信开销两个方面进行分析。实验使用 Ubuntu20.04 操作系统；在 32.0 GB RAM、Intel(R) Core(TM) i7-11800H@2.30 GHz 硬件平台上进行。

5.1 计算开销

为评估本方案的计算开销，对跨域认证过程中涉及实体的计算量进行统计，对设备的计算开销进行模拟，并与其他方案进行对比。为便于表示，对符号作以下规定：CSM/CPA 表示椭圆曲线群上的标量乘法/点加；$GFMul/GFAdd$ 表示有限域 Z_q^* 上的乘法/加法；$GSM/GEXP$ 表示循环群 G 的乘法/幂运算；$H/En/De/BP$ 表示哈希运算/公钥加密/解密/双线性对运算。

5.1.1 理论分析

表 3 列出了所有实体在单向认证与密钥协商过程中的计算量。在 DE_{U2}^b 对 DE_{U1}^a 的认证过程中，DE_{U2}^b 将消息转发给 AS_b，由 AS_b 进行认证，DE_{U1}^a 和 DE_{U2}^b 都没有运行复杂的双线性运算和幂运算。

表 3 跨域认证与密钥协商过程中各实体的密码操作统计

Table 3 Stats on cryptography operations of each entity during cross-domain authentication and key negotiation

实体	计算量
DE_{U1}^a	$2CSM+2GFMul+2GFAdd+H$
DE_{U2}^b	$9CSM+4CPA+2GFMul+2GFAdd+7H$
AS_b	$5CSM+2CPA+3GFMul+2GFAdd+4H+GEXP+2BP+De$

5.1.2 模拟实验

将本方案中物联网设备跨域认证与密钥协商过程中的计算开销与文献[11]方案、文献[13]方案、文献[14]方案进行对比。由于我们假设服务器端拥有强大的计算能力，因此不再对比服务器端的计算开销。在前面所述的实验环境下，使用 SHA-256 及 secp256r1 椭圆曲线作为参数进行模拟，CSM，CPA，GFMul，GFAdd，H 和 GEXP 的运行时间分别是 0.049 9 ms，0.005 ms，0.000 8 ms，0.000 1 ms，0.000 3 ms，0.031 1 ms。

表 4 列出了各个方案中设备端跨域认证与密钥协商过程中的计算开销。现有基于区块链的跨域认证方案可分为设备与设备之间的认证、设备与服务器之间的认证[7]。本文与文献[11]方案、文献[13]方案均属于前者，文献[14]方案属于后者。这两类方案适用场景不同，前者主要解决不同域设备之间的端到端安全认证与密钥协商，后者则主要关注设备与服务器之间的安全交互。在进行设备之间的认证时，对于存储资源小的设备来说，无法保存链上的所有信息，只能借助服务器完成认证，因此相较于设备与服务器的认证方案，增加了两设备交互时的签名与验签工作，导致前者的开销均高于文献[14]方案。但本方案的计算开销低于其他两个方案。从图 3 可以看出，当设备数量为 100 时，本方案的计算开销相较于文献[11]方案和文献[13]方案分别减少了约 40.65% 和 27.23%。

表 4 设备端跨域认证与密钥协商过程计算开销对比

Table4 Comparison of computation overhead on devices during cross-domain authentication and key negotiation

文献	计算量	计算开销/ms
[11]	$18CSM+6CPA+6GFMul+7GFAdd+13H+GEXP$	0.968 7
[13]	$14CSM+4CPA+5GFMul+4GFAdd+16H+2GEXP$	0.790 0
[14]	$8CSM+3CPA+2GFMul+2GFAdd+5H$	0.417 5
Ours	$11CSM+4CPA+4GFMul+4GFAdd+8H$	0.574 9

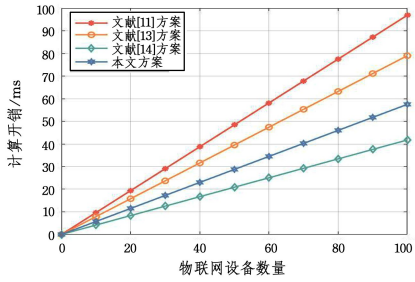

图 3 设备端跨域认证与密钥协商计算开销模拟结果

Fig. 3 Simulation results of computation overhead on devices during cross-domain authentication and key negotiation

5.2 通信开销

本节将跨域认证与密钥协商过程中的通信开销与其他方案进行对比。根据前面的参数设置，假设域标识符、版本号为 4 bytes，随机数、种子长度为 32 bytes，哈希函数的输出为 32 bytes，设备的真实身份为 32 bytes，设备的假名身份为 64 bytes；$G_{a1}/G_{a2}/Z_q^*$ 中元素的长度为 32 bytes，G 中元素的长度为 64 bytes。

跨域认证与密钥协商过程中，设备 DE_{U1}^a 首先向 DE_{U2}^b 发送跨域请求 M_3，需 392 bytes；DE_{U2}^b 将包含跨域凭证的消息 M_4 发送给 AS_b，通信开销为 392 bytes；最后，DE_{U2}^b 收到 128 bytes 认证成功的消息，以及 96 bytes 的挑战应答消息。重复以上过程，可以完成双向认证与密钥协商，总通信开销为 1 920 bytes。

同理，文献[11]方案、文献[13]方案、文献[14]方案在跨域认证与密钥协商过程中的通信开销分别为 3 144 bytes，2 612 bytes，748 bytes。图 4 展示了各方案的通信开销，虽然文献[14]方案的通信开销最小，但该方案单一的假名身份容易造成身份的链接攻击。即使文献[14]方案为每个设备生成一个假名，利用假名机制来实现匿名性，但根据会话消息中的签名和链上存储信息，可以将同一设备的多次会话消息关联起来，收集并分析这些会话消息，将有助于攻击者识别假名设备的真实身份，从而打破了匿名性特征，这将严重危害设备的隐私，与方案设计基于隐私保护的初衷背道而驰。

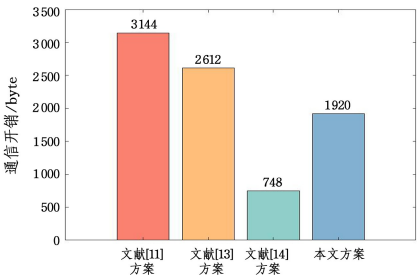

图 4 跨域认证与密钥协商过程通信开销对比

Fig. 4 Comparison of communication overhead during cross domain authentication and key negotiation

为了实现设备间跨域认证时的匿名性和不可链接性，需要为设备生成多个假名，并将设备认证信息上传到由各域中服务器维护的联盟链上，以便跨域认证。然而，物联网设备的存储资源有限，不能作为链上节点保存链上的所有认证数据，导致设备间的跨域认证需要依靠服务器完成，从而设备必须

将认证信息转发给服务器，不可避免地增加了跨域认证时的通信开销。与文献[11]方案和文献[13]方案这些设备间跨域认证方案相比，本方案通信开销最低，说明本方案通信开销适中，是可接受的。

结束语 针对跨域认证容易泄露设备身份隐私和匿名认证难以对恶意设备追踪的问题，本文提出了一种基于区块链的可追踪匿名跨域认证方案。将单向哈希链和无证书密码相结合，为设备生成多个无关联的假名，在保护设备隐私的同时，密钥生成中心还可以根据私钥恢复出恶意设备的真实身份，对设备追责。BAN 逻辑正确性分析和形式化安全证明表明，本文方案具有良好的安全性，满足安全需求；计算开销和通信开销分析说明了，本方案跨域认证时计算开销小，通信开销低。本文方案在识别出恶意设备的基础上，实现了对恶意设备的追踪与监管，未来计划设计信誉评估机制，以自动对恶意设备进行准确高效的识别，最终构建发现、追踪与惩治恶意设备一体化的系统。

参 考 文 献

[1] NANDY T, IDRIS M Y I B, NOOR R M, et al. Review on security of internet of things authentication mechanism[J]. IEEE Access, 2019, 7(99): 1-36.

[2] CHOUHAN P K, MCCLEAN S, SHACKLETON M. Situation asses-sment to secure IoT applications[C]// 2018 Fifth International Conference on Internet of Things: Systems, Management and Security. IEEE, 2018: 70-77.

[3] KANG J, YU R, HUANG X, et al. Privacy-preserved pseudonym scheme for fog computing supported internet of vehicles [J]. IEEE Transactions on Intelligent Transportation Systems, 2017, 19(8): 2627-2637.

[4] SINGH P, MASUD M, HOSSAIN M S, et al. Cross-domain secure data sharing using blockchain for industrial IoT[J]. Journal of Parallel and Distributed Computing, 2021, 156(10): 176-184.

[5] ZHANG S E, TIAN C W, LI B G. Review of identity authentication research based on blockchain technology[J]. Computer Science, 2023, 50(5): 329-347.

[6] CHENG G J, DENG S G, WEN Y Y, et al. Survey on blockchain based Internet of Things authentication mechanisms[J]. Journal of Software, 2023, 34(3): 1470-1490.

[7] YANG T, ZHANG G H, LIU L, et al. A survey on authentication protocols for Internet of Things[J]. Journal of Cryptologic Research, 2020, 7(1): 87-101.

[8] WEI S, WU X, ZHANG Z. Blockchain-based Cross-domain Trust Authentication Mechanism in Industrial Internet of Things[J]. Journal of Chinese Computer Systems, 2024, 45(4): 975-983.

[9] CHEN Y B, ZHONG C R, ZHOU C R, et al. Design of cross-domain authentication scheme based on medical consortium chain [J]. Computer Science, 2022, 49(S1): 537-543.

[10] ZHU H Y, ZHANG X Y, XING H L, et al. Lightweight terminal cross-domain authentication protocol in edge computing environment[J]. Chinese Journal of Network and Information Security, 2023, 9(4): 74-89.

[11] SHEN M, LIU H, ZHU L, et al. Blockchain-assisted secure device authentication for cross-domain industrial IoT[J]. IEEE Journal on Selected Areas in Communications, 2020, 38(5): 942-954.

[12] CUI J, LIU N, ZHANG Q, et al. Efficient andanonymous cross-domain authentication for IIoT based on blockchain[J]. IEEE Transactions on Network Science and Engineering, 2022, 10(2): 899-910.

[13] ZHANG Y, LI B, WU J, et al. Efficient andprivacy-preserving blockchain-based multifactor device authentication protocol for Cross-domain IIoT[J]. IEEE Internet of Things Journal, 2022, 9(22): 22501-22515.

[14] XUE L, HUANG H, XIAO F, et al. A cross-domain authentication scheme based on cooperative blockchains functioning with revocation for medical consortiums[J]. IEEE Transactions on Network and Service Management, 2022, 19(3): 2409-2420.

[15] LIU X J, ZHONG Q, XIA Y J. Efficient authentication scheme for cross-trust domain of IoV based on double-layer shard blockchain[J]. Journal on Communications, 2023, 44(5): 213-223.

[16] FENG X, CUI K P, XIE Q Q, et al. Distributed Anonymous Authentication Scheme Based on the Blockchain in VANET[J]. Journal on Communications, 2022, 43(9): 134-147.

[17] LIU Y, WANG J, YAN Z, et al. A survey on blockchain-based trust management for Internet of Things[J]. IEEE Internet of Things Journal, 2023, 10(7): 5898-5922.

[18] YING B, NAYAK A. Anonymous and lightweight authentication for secure vehicular networks[J]. IEEE Transactions on Vehicular Technology, 2017, 66(12): 10626-10636.

[19] XU Z, LIANG W, LI K C, et al. A Blockchain-based Roadside Unit-assisted Authentication and Key Agreement Protocol for Internet of Vehicles[J]. Journal of Parallel and Distributed Computing, 2021, 149(3): 29-39.

[20] XIE Q, WONG D S, WANG G, et al. Provably secure dynamic ID-based anonymous two-factor authenticated key exchange protocol with extended security model[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(6): 1382-1392.

[21] FLAJOLET P, GARDY D, THIMONIER L. Birthday paradox, coupon collectors, caching algorithmsand self-organizing search [J]. Discrete Applied Mathematics, 1992, 39(3): 207-229.

[22] SEURIN Y. On the exact security of Schnorr-type signatures in the random oracle model[C]// Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2012: 554-571.

WANG Qiuli, born in 2000, postgraduate. Her main research interests include blockchain and identity authentication.

REN Zhiyu, born in 1974, Ph. D, associate professor. Her main research interests include network and information security and so on.

（责任编辑：何杨）