边缘计算环境下基于区块链的跨域认证与密钥协商协议

张金花, 李晓伟, 曾　新, 赵榆琴, 段　燃, 杨邓奇
大理大学数学与计算机学院 大理 中国 671000

摘要　身份认证与密钥协商是接入物联网首先要考虑的安全问题。传统的物联网身份认证是基于“云中心-终端设备”的认证架构。而随着边缘计算技术的引入, 认证架构转变为“边缘设备-终端设备”的架构, 传统的认证方式不再适用。此外, 物联网中存在多个通信域, 不同域中的设备之间需要进行跨域间认证与密钥协商。针对以上问题, 本文设计了边缘计算环境下基于区块链的跨域认证与密钥协商协议。将终端设备的证书 Hash 值存储在区块链上, 避免了复杂的证书验证过程。基于联盟链的跨域属性使得不同域间的设备可以顺利完成认证和密钥协商。与已有的跨域认证与密钥协商协议相比, 本文所提出的协议具有较高的效率, 更适用于低性能的物联网设备。

关键词　物联网; 区块链; 跨域认证; 边缘计算
中图法分类号　TP309　DOI 号 10.19363/J.cnki.cn10-1380/tn.2021.01.05

Cross domain authentication and key agreement protocol based on blockchain in edge computing environment

ZHANG Jinhua, LI Xiaowei, ZENG Xin, ZHAO Yuqin, DUAN Ran, YANG Dengqi
School of Mathematics and Computer, Dali University, Dali 671000, China

Abstract　Identity authentication and key agreement are the first security issues to be considered when accessing the Internet of Things(IoT). The traditional identity authentication of IoT is based on the “cloud center-terminal device” authentication architecture. With the introduction of edge computing technology, the authentication architecture has been transformed into “edge device-terminal device” architecture, and the traditional authentication method is no longer applicable. In addition, there are multiple communication domains in the IoT, and cross domain authentication and key agreement are needed between devices in different domains. To solve the above problems, this paper designs a cross domain authentication and key agreement protocol based on blockchain in the edge computing environment. The hash value of the certificate of the terminal device is put on the blockchain to avoid the complicated certificate verification process. Based on the cross domain attribute of consortium chain, the devices in different domains can complete authentication and key agreement successfully. Compared with the existing cross domain authentication and key agreement protocols, the proposed protocol has higher efficiency and is more suitable for low performance IoT devices.

Key words　Internet of Things; blockchain; cross-domain authentication; edge computing

1　引言

随着物联网技术的快速发展, 物联网应用也逐渐广泛。大量的终端设备接入网络中将产生海量级的数据, 这为云中心及时有效地处理数据带来了更大的挑战。边缘计算是指在网络边缘执行计算的一种新型计算模型。网络边缘是指从数据源到云计算中心路径之间的任意计算和网络资源[1]。边缘计算技术的引入减轻了云中心的网络负担, 但同时也引起了一些安全问题。边缘计算环境下的终端数量较多, 层次复杂, 多种安全域并存, 安全性要求更高。身份认证是设备接入网络的第一步也是网络安全的第一道屏障。传统的物联网身份认证协议大多数都是基于云中心-终端设备的网络架构, 而边缘计算环境下

通讯作者: 李晓伟, 博士, 讲师, 硕士生导师, Email: lixiaowei_xidian@163.com。
本课题得到国家自然科学基金(No. 31960119, No. 51809026, No. 61902049), 云南省地方高校联合项目(No. 2017FH001-027, No. 2017FH001-062, No. 2017FH001-063)以及大理大学创新团队项目(No. ZKLX2020308)资助。
收稿日期: 2020-09-18; 修改日期: 2020-11-16; 定稿日期: 2020-11-25

网络架构有所改变, 如图 1 所示。在边缘计算环境中设备计算及通信主要在设备边缘完成, 原有的网络认证模式已不再适用。同时, 边缘计算环境中往往涉及多个域, 多个域间设备安全通信需要跨域间身份认证与密钥协商。物联网单域间身份认证与密钥协商方案已经有比较成熟的研究成果[2-6]。但轻量级的边缘计算环境下跨域间认证与密钥协商方案仍有待研究。

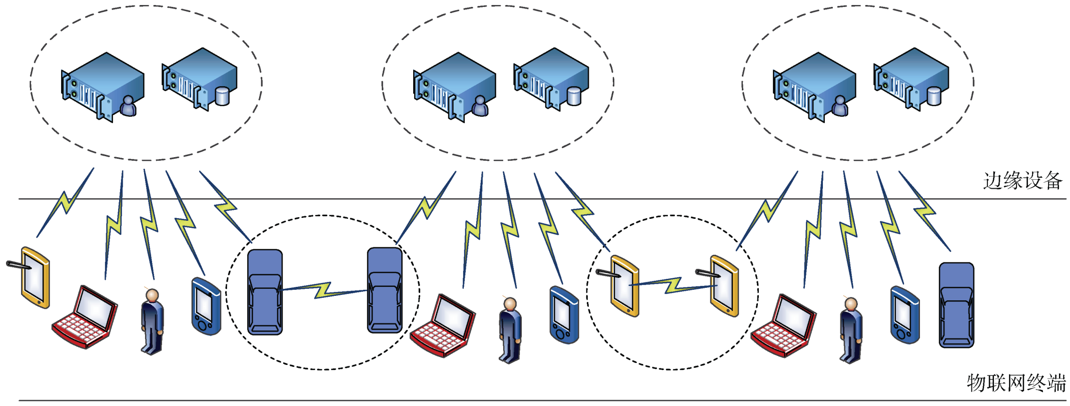

图 1　边缘计算网络-终端网络架构

Figure 1　Edge computing network-terminal network architecture

现有的物联网身份认证主要是基于公钥基础设施(Public Key Infrastructure, PKI)认证技术。PKI 技术依靠数字证书进行身份认证, 依靠加密技术保证信息不被泄漏, 以保证信息的完整性、保密性和抗抵赖性。PKI 解决了互联网络中的公钥分发问题, 是互联网的信任基础, 也是目前保障网络安全较好的认证体系[7]。基于 PKI 体系的物联网跨域认证已有学者做了如下研究: 文献[8]提出一种适用于“云-边-端”一体化物联网认证架构下基于 PKI 和国密 SM9 标识的认证体系。在边缘计算环境中, 物联网终端设备直接在网络边缘进行跨域认证, 实现了高效的跨域认证和位置隐私保护。对于低性能的物联网终端设备, 降低了复杂度并且提高了终端跨域认证的效率。文献[9]结合 PKI 和基于身份的签名(Identity-based signature, IBS)认证体系的优点提出一种基于证书的签名方案, 避免了 PKI 证书管理的复杂性和 IBS 中密钥托管和分发的问题, 实现了安全高效和匿名的物联网移动设备跨域认证。文献[10]提出了基于身份的密码体制和无证书加密体制相结合的认证方法, 并优化了跨域环境下的签密算法, 提出基于不同系统参数的跨域签密方案。该方案能满足临时密钥的安全需求, 可应用在跨域网络中提升计算效率降低成本, 实现了物联网环境下的跨域认证。

基于 PKI 技术的认证方案虽然能实现跨域认证但需要复杂的证书管理体系, 对于物联网终端设备分布广、数量多并且涉及多个通信域等特性, PKI 技术已经不能很好的解决物联网设备身份认证问题。区块链技术的产生推动了数字证书的发展, 区块链与物联网技术的结合也是未来的发展趋势。区块链中的数据区块是以时间顺序为序列、通过链式结构链接形成的数据结构, 每个区块通过存储前一个区块的哈希值来确保区块链的可追溯性[11]。区块链技术具有分布式数据存储、点对点传输、共识机制、加密算法四大特性。区块链解决的就是非安全环境中的可信问题、数据安全问题、身份权限问题和隐私保护问题[12]。区块链的基本结构如图 2 所示。区块标识能对区块进行识别, 区块体中包含某一时间段的所有交易数量, 经过哈希运算最后生成 Merkle 根哈希, 区块之间通过前一区块的哈希值相互连接形成了按时间序列链接的区块链。基于区块链的物联网终端设备跨域认证方案目前研究较少。结合区块链技术的跨域认证方案有如下研究: 文献[13]在不改变 PKI 认证模型的基础上结合区块链技术提出了一种联盟链信任模型, 实现双向实体跨域认证, 并提供快速重认证。通过 Hash 算法验证证书, 减少了公钥签名与验证的次数, 提高了跨域认证的效率。文献[14]提出了一种基于区块链的物联网分布式身份认证架构, 对传统的区块数据结构进行扩充, 引入默克尔帕特里树(Merkle Patricia tree, MPT)存储物联网设备及其数字证书以保证信息的可靠性,提高了认证效率和安全性。文献[15]利用模糊提取技术并结合区块链的智能合约, 提出一种基于生物特征和口令双因子的跨域认证方案。在实现跨域认证的同时, 也避免了生物特征信息泄露保证其安全性。文献[16]设计了一种基于区块链的智能合约去中心化身份管理与认证模型, 利用智能合约实现对

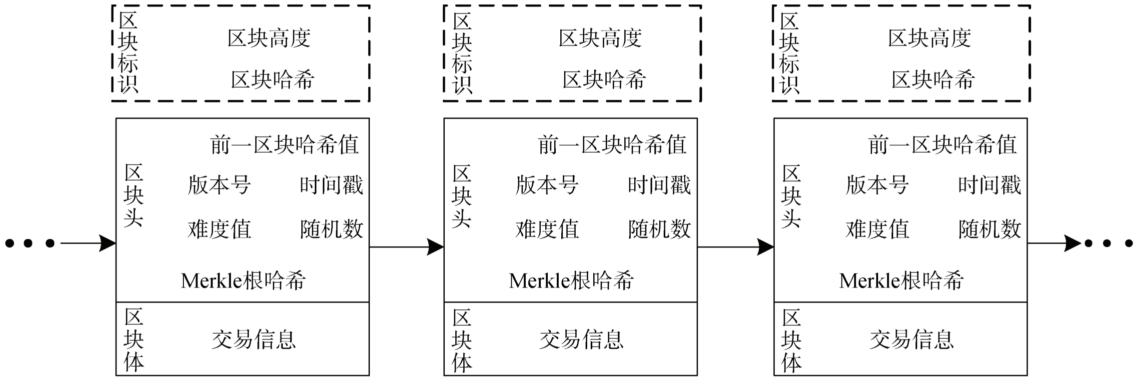

图 2 区块链基本结构
Figure 2 Basic structure of blockchain

用户身份信息的发布、认证和撤销, 实现不同场景中的交叉认证。

以上物联网认证方案中, 跨域认证的方案一类是基于PKI和IBS的认证体制, 主要是中心化的认证方式, 这种认证方式一旦中心服务器受到攻击就会威胁到整个系统安全。另一类是利用区块链技术去中心化和不可篡改的特性设计分布式环境下的物联网认证方案, 这种方案设计相比传统中心化的认证方式实现了更安全和高效的认证效率。由于物联网环境中的异构性以及存在多种不同的安全域, 其中低性能的终端设备计算能力有限, 在一些要求低延迟、实时性的物联网场景中, 基于传统中心化的认证方式难以实现跨域认证和通信。本文主要解决现有物联网环境中存在的低性能终端设备跨域认证问题, 利用区块链技术特点更好地解决跨域认证中存在的安全性问题。在“边缘设备-终端设备”网络架构下设计区块链的联盟链信任模型, 将终端设备的数字证书记录在区块链上减少了认证开销, 并且提高了认证的可靠性。本文基于以上认证方案设计边缘计算环境下物联网终端设备同域和跨域认证与密钥协商协议, 保证终端设备间通信的安全性。

2 基于区块链的物联网认证方案

2.1 系统架构与区块链共识机制

2.1.1 系统架构

基于区块链的物联网终端认证架构如图 3 所示, 主要由物联网终端设备(Devices, *D*)、边缘认证服务器(Edge Servers, *ES*)、区块链认证中心(Blockch-ain Certificate Authority, *BCCA*)构成。根据区块链的共识机制选出每个域内高性能的边缘认证服务器 *ES*, 将 *ES* 和 *BCCA* 作为联盟链内的节点并且相互之间是可信的。*BCCA* 主要负责证书的颁发, 将证书的哈希值和状态信息都存储区块链上。对终端设备拥有的证书哈希值与区块链上的证书哈希值进行比较以实现物联网终端设备身份认证, 减少了数字证书的签名与验证过程。由于区块链不可篡改以及可追溯的特性, 本文提出的方案能够提高物联网终端设备身份认证的效率和安全性。

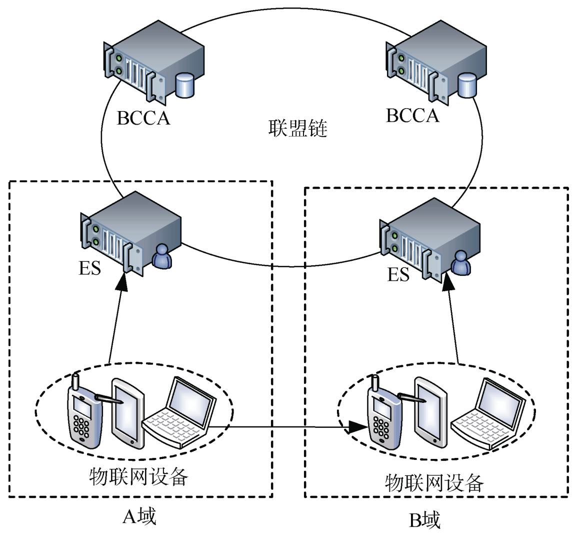

图 3 基于区块链的物联网终端认证架构
Figure 3 Blockchain-based IoT terminal authentication architecture

2.1.2 区块链共识机制

本文基于联盟链的特性设计了物联网设备跨域认证架构, 如何保证联盟链内的节点记账达成一致, 是区块链研究的重点。本文选择适用于联盟链的委托权益证明(Delegated Proof of Stake, DPoS)的共识机制, 根据 DPoS 的工作机制将联盟链内的节点划分为 3 类:

1) 股民: 包括全体节点;
2) 股东代表: 节点投票选出若干名代表记账;
3) 候选人: 竞争股东代表的节点。

在 DPoS 的工作机制中全体节点都可以作为候

选人竞争股东代表，由股民根据占股比例进行投票选举，获得票数最多的若干名候选人成为股东代表，股东代表的人数由系统决定。股东代表负责记账，落选的候选人成为股民，除股东代表外的其余节点同步账本实现联盟链内的共识。

2.2 方案设计

本节基于区块链的物联网认证架构进行方案设计，认证方案分为终端设备身份注册、设计同域和跨域认证与密钥协商协议三个阶段，同域和跨域认证的终端设备身份注册阶段相同。物联网终端设备认证与密钥协商协议的符号说明如表 1 所示。

表 1 物联网跨域认证协议符号说明

Table 1 Symbol description of IoT cross-domain authentication protocol

符号	含义
$BCCA$	区块链认证中心
ES_i	第 i 域的边缘认证服务器
D_i	第 i 域终端设备
p	素数
g	素数 p 的本原根
P_{ES_i}, S_{ES_i}	边缘认证服务器公私钥对
P_i, S_i	终端设备公私钥对
E_{P_i}, D_{S_i}	公钥加解密算法
Sig_{S_i}, V_{P_i}	数字签名验证算法
H	安全的哈希函数
N_i	随机数
a, b	私有随机数

2.2.1 终端设备身份注册

本方案的身份注册是指终端设备 D_i 通过边缘认证服务器 ES 进行注册，身份注册流程图如图 4 所示。具体步骤如下:

1) 设备 D_i 向 ES 发送注册请求。

$$Regr_i = E_{P_{ES}}\left(IC_i\right)$$

2) ES 接收到 D_i 的注册请求，用私钥解密验证是否为合法用户，若验证通过，则注册成功; 反之，返回注册失败。

3) ES 向 $BCCA$ 发送申请证书请求。

$$RCert = (ID_i, P_i, Sig_{S_{ES}}(N_1), N_1)$$

4) $BCCA$ 通过验证随机数及签名的有效性，若验证通过则生成数字证书，T 表示证书的有效期，并将数字证书的哈希值 $h_I = H\left(Cert_i\right)$ 写入区块链。

$$Cert_i = (ID_i, P_i, T)$$

5) $BCCA$ 将生成的证书哈希值返回给 D_i。

2.2.2 同域认证与密钥协商

随着物联网设备的增加，云中心的网络负担也随之增加。边缘计算技术的出现为终端设备的身份认证提供了更方便和高效的认证方式，终端不再需要向云中心申请认证，而是在网络边缘进行本地化的认证。以 A 域为例设计同域认证与密钥协商协议。同域认证与密钥协商流程图如图 5 所示，具体步骤如下:

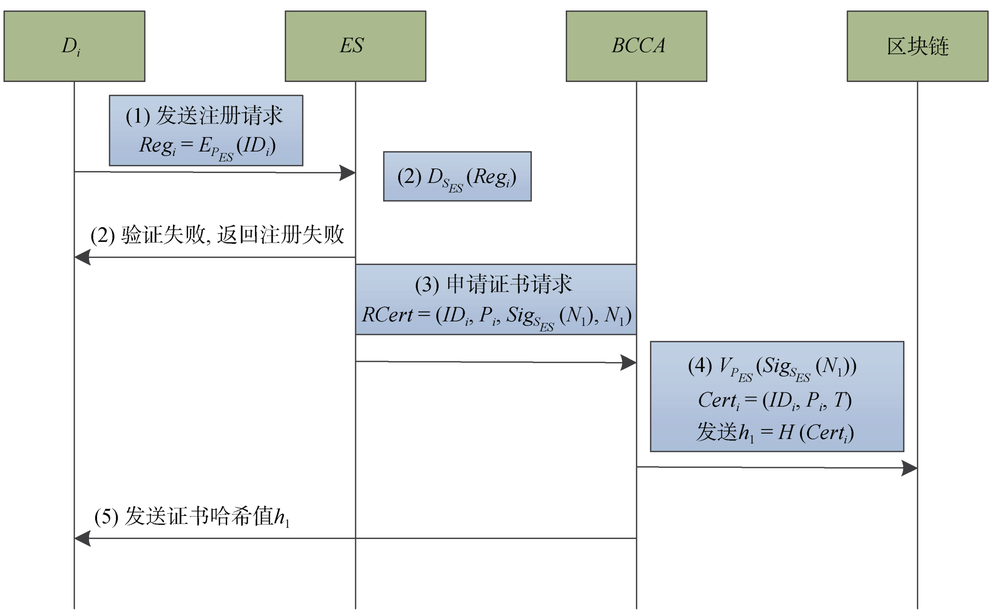

图 4 身份注册流程图

Figure 4 Flow chart of identity registration

1) 设备 D_A 向本域边缘认证服务器 ES_A 发送认证请求，h_1' 为终端设备存储的数字证书哈希值。

$$Req = E_{P_{ES_A}}(ID_A, h_1')$$

2) ES_A 收到请求消息后用私钥解密，验证身份信息。若验证通过则为已经注册过的设备，继续执行下一步；反之，重新发送接入认证请求。

3) ES_A 向区块链发送请求 D_A 数字证书哈希值的消息。

$$Rep = (ID_A, P_A, N_2)$$

4) 区块链节点收到消息后查看 N_2 是否有效，若有效将 D_A 的证书哈希值 h_1 发送给 ES_A。

5) ES_A 收到消息后将区块链上存储的数字证书哈希值与终端设备发送的数字证书哈希值比较是否一致，若结果相同则认证成功；反之，认证失败。

6) ES_A 向 D_A 发送认证成功的消息。

$$Suc = E_{P_A}(N_3)$$

7) D_A 收到消息后用私钥解密得到随机数 N_3, D_A 向 ES_A 发送密钥协商的消息，$KS_1 = H(ID_A, N_3, N_4)$ 即会话密钥。

$$Repk = E_{P_{ES_A}}(KS_1)$$

8) ES_A 收到消息后用私钥解密得到回话密钥 KS_1。

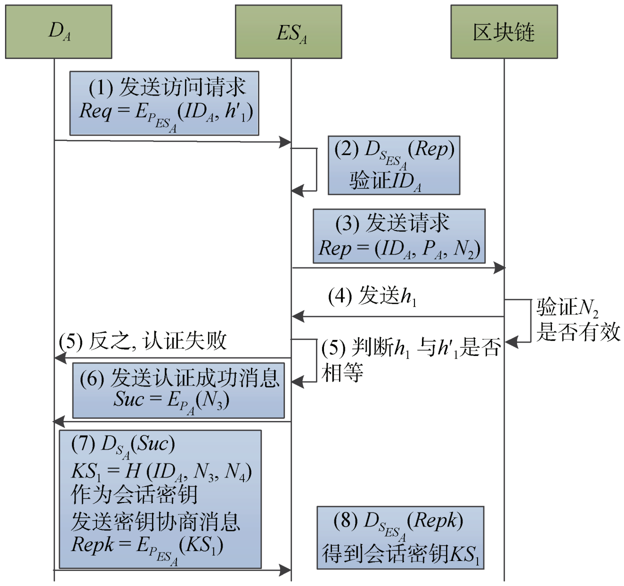

图 5 同域认证与密钥协商流程图

Figure 5 Flow chart of same domain authentication and key agreement

2.2.3 跨域认证与密钥协商

以 A、B 两个域为例进行终端设备的跨域间通信，假设 A 域设备 D_A 漫游到 B 域，通过 ES_B 对 ES_A 的认证间接实现 ES_B 对 D_A 的认证，从而实现 D_A 的跨域认证。跨域认证与密钥协商流程图如图 6 所示，具体步骤如下:

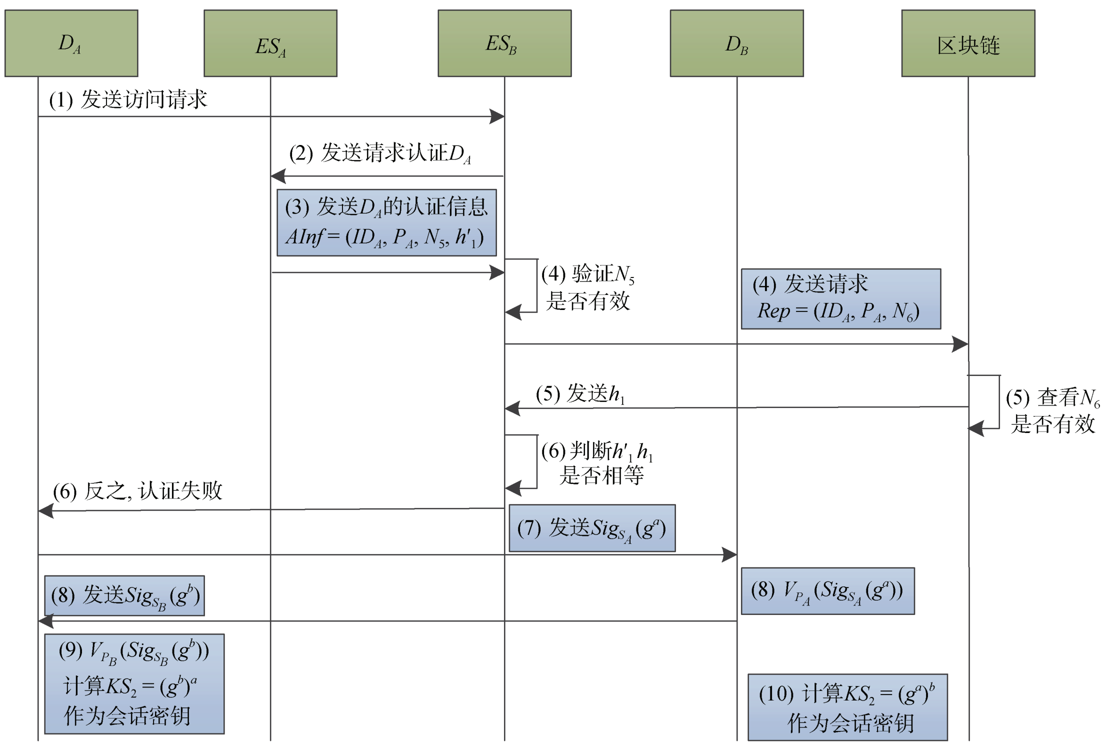

图 6 跨域认证与密钥协商流程图

Figure 6 Flow chart of cross domain authentication and key agreement

1) 终端设备 D_A 向边缘认证服务器 ES_B 发送访问请求。

2) ES_B 收到访问请求后向 A 域边缘认证服务器 ES_A 发送请求认证 D_A 的消息。

3) ES_A 收到请求消息后向 ES_B 发送关于 D_A 的认证信息。

$$AInf = (ID_A, P_A, N_5, h_1')$$

4) ES_B 收到消息后通过查看 N_5 是否有效, 若有效则 ES_B 向区块链发送请求 D_A 数字证书哈希值的消息。

$$Rep = (ID_A, P_A, N_6)$$

5) 区块链节点收到消息后查看 N_6 是否有效, 若有效将 D_A 的数字证书哈希值 h_1 发送给 ES_B。

6) ES_B 收到消息后将区块链上存储的数字证书哈希值与终端设备发送的数字证书哈希值比较是否一致, 若结果相同则认证成功; 反之, 认证失败。

7) 设备 D_A 通过了认证服务器 ES_B 的认证后, 可以进行跨域通信。D_A 若要与 B 域终端设备 D_B 之间安全通信需要进行密钥协商。D_A 产生一个私有的随机数 a, 计算 g^a 并将 $Sig_{S_A}\left(g^a\right)$ 发送给 D_B。

8) D_B 收到消息后验证签名并得到 g^a, 同时 D_B 产生一个私有的随机数 b, 计算 g^b 并将 $Sig_{S_B}\left(g^b\right)$ 发送给 D_A。

9) D_A 收到消息后验证签名并得到 g^b, D_A 通过计算 $KS_2 = \left(g^b\right)^a$ 得到会话密钥为 KS_2。

10) D_B 通过计算 $KS_2 = \left(g^a\right)^b$ 得到的会话密钥与 D_B 的相同。

3 安全性分析

3.1 认证安全性

本文提出的物联网终端设备认证与密钥协商协议是基于 PKI 的认证体系并结合区块链技术实现, 区块链认证中心 $BCCA$ 将生成的数字证书哈希值 $H(Cert_i)$ 存储在区块链上作为认证凭证。由哈希函数的单向性可知, 假如有攻击者获取了哈希值也无法解密得到数字证书, 保证了数字证书的安全性。由于区块链不易篡改的特性, 实现了物联网终端设备同域与跨域认证凭证的安全性。在同域认证过程中, 基于公钥加密算法互相发送消息, 只有拥有私钥的设备才能解密, 保护了设备的身份信息不被泄露, 实现了安全的认证与密钥协商协议过程。在跨域认证过程中, D_A 向 B 域请求跨域认证是通过 ES_A 向 ES_B 发送终端设备 D_A 的相关认证信息, 再由 ES_B 通过区块链验证 D_A 的认证凭证。ES_A 和 ES_B 都是联盟链内的节点, 通过联盟链的 DPoS 共识机制选取节点, 只有通过共识机制验证的节点才能加入到联盟链内, 因此联盟链内节点是可信的。从而保证了终端设备信息的安全性, 减少了使用公钥加解密算法的运算次数, 实现了终端设备更高效和安全的跨域认证。

3.2 会话密钥安全性

本文在跨域认证过程中建立了安全通信的会话密钥, 分别为同域认证的物联网终端设备 D_i 和边缘认证服务器 ES_i 以及跨域认证中两个终端设备 D_A 与 D_B 之间的密钥协商。在同域认证密钥协商过程中 D_i 和 ES_i 分别选取随机数通过公钥加密算法发送给对方, 再进行 Hash 处理 $H(ID_A, N_3, N_4)$, 其他设备没有对应的私钥无法解密获取会话密钥, 假如有攻击者能监听到会话密钥也无法解密。在跨域认证密钥协商过程中两个终端设备的会话密钥设计基于 DH 密钥协商协议。Canetti 和 Krawczyk 提出了基于签名的认证器[17], 本文中的密钥协商过程为 A, B 双方分别发送数字签名 $Sig_{S_A}\left(g^a\right)$ 及 $Sig_{S_B}\left(g^b\right)$, 该过程可以视为将原始的 DH 密钥协商协议经过认证器对消息认证, 由文献[17]的证明可以得出该密钥协商过程是安全的。

3.3 抵抗重放攻击

在整个认证的过程中, 发送请求消息时会加入随机数, 接收方通过查看随机数的有效性来确认消息的准确性。在认证过程中, 边缘认证服务器 ES_i 向区块链节点请求数字证书哈希值时加入随机数 $Rep = (ID_A, P_A, N_2)$, 区块链节点通过验证随机数的有效性来判断消息的真实性。假如有攻击者截取了消息再重新发送, 但由于随机数的时效性将会导致失败, 所以能够抵抗重放攻击。

3.4 前向安全性

本文在两个跨域的终端设备密钥协商过程中考虑到会话密钥的前向安全性, 利用DH密钥协商协议进行会话密钥协商。假如攻击者获取了当前的会话密钥 $KS = \left(g^b\right)^a$, 其中 a 和 b 是通信双方随机选取的秘密值, 均为通信双方私有。攻击者在不知道 a 和 b 的情况下, 由离散对数困难问题可知很难求出会话密钥 KS, 在此之前双方通信的会话密钥也很难得到。基于以上会话密钥协商过程, 能够保证终端设备跨域通信的安全性。

4 性能分析

本文提出一种边缘计算环境下基于区块链的物联网终端设备认证与密钥协商协议，本节对比文献[9]和文献[14]的计算开销进行性能分析。不同方案的计算开销对比如表 2 所示，表中数字的单位为每种算法的运算次数。

表 2 计算开销对比
Table 2 Calculation cost comparison

方案	数字签名与验证	哈希运算	公钥加解密	双线性对	指数运算
文献[9]	2	3	2	0	8
文献[14]	6	2	4	4	0
本文方案	3	2	4	0	4

与文献[9]对比本文方案使用较少的指数运算，文献[9]中物联网设备的跨域认证是基于传统的中心化认证方式，一旦中心受到攻击，会对整个认证过程造成威胁。与文献[14]对比本文方案使用较少的数字签名与验证算法，而且没有复杂的双线性对运算，在一定程度上减少了计算开销。相比文献[14]本文方案更适合低性能的物联网终端设备跨域认证。对比以上两种方案，本文方案有较少的计算开销。为了进一步分析算法的计算开销，本文对密码学算法的运行时间进行测试。实验环境为：英特尔 i7 处理器，3GHz 主频，8GB 内存。其中 T_S 表示一次数字签名与验证的运行时间，T_{PK} 表示一次公钥加解密的运行时间，T_h 表示一次哈希算法的运行时间，T_i 表示一次指数运算的运行时间，T_E 表示一次双线性对运算的运行时间。经过多次运行取平均值得到结果如下：T_S、T_{PK}、T_h、T_i 和 T_E 的运行时间分别为 2.005ms、3.830ms、0.001ms、6.324ms 和 11.450ms。为方便对比，本文选择的数字签名算法为 ElGamal 数字签名算法，加密算法选择的是 ElGamal 加密算法。本文方案与文献[9]和[14]计算耗时对比如图 7 所示。从图 7 中可以看出本文总的计算消耗仅为 46.633ms，少于其他两种方案，更适用于低性能的物联网设备。

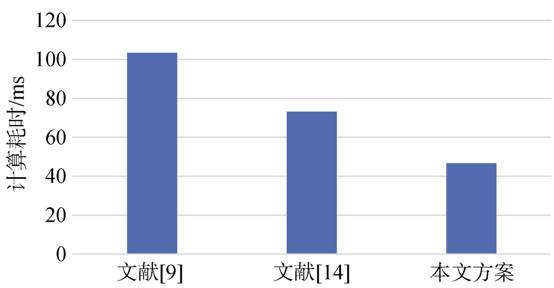

图 7 计算耗时对比
Figure 7 Comparison of calculation time

5 结束语

针对目前存在的物联网终端设备认证复杂和低效率的问题，本文利用边缘计算技术设计了基于区块链的跨域间物联网终端设备认证架构。通过边缘设备而非云中心对终端设备进行认证，将终端设备的认证进行本地化处理，减轻了云中心的网络负担，同时也提高了认证效率。并且对认证与密钥协商协议应有的安全属性进行了分析。同已有的物联网终端设备认证方案相比，在满足认证与密钥协商安全性的基础上，本文方案具有较少的计算开销，更适合低性能的物联网终端设备认证与密钥协商。

参考文献

[1] Shi W S, Sun H, Cao J, et al. Edge Computing—an Emerging Computing Model for the Internet of everything Era[J]. *Journal of Computer Research and Development*, 2017, 54(5): 907-924.
(施巍松, 孙辉, 曹杰, 等. 边缘计算:万物互联时代新型计算模型[J]. *计算机研究与发展*, 2017, 54(5): 907-924.)

[2] Yu S, Park K, Park Y. A Secure Lightweight Three-Factor Authentication Scheme for IoT in Cloud Computing Environment[J]. *Sensors*, 2019, 19(16): 3598.

[3] Gupta B B, Tewari A. A Novel ECC-based Lightweight Authentication Protocol for Internet of Things Devices[J]. *International Journal of High Performance Computing and Networking*, 2019, 15(1/2): 106.

[4] Santos M L B A, Carneiro J C, Franco A M R, et al. FLAT: Federated Lightweight Authentication for the Internet of Things[J]. *Ad Hoc Networks*, 2020, 107: 102253.

[5] Wu H L, Chang C C, Chen L S. Secure and Anonymous Authentication Scheme for the Internet of Things with Pairing[J]. *Pervasive and Mobile Computing*, 2020, 67: 101177.

[6] Huang J C, Shu M H, Hsu B M, et al. Service Architecture of IoT Terminal Connection Based on Blockchain Identity Authentication System[J]. *Computer Communications*, 2020, 160: 411-422.

[7] Kang J P, Wang S M, Du Z Q. Application of PKI Technology in the Information Safety[J]. *Process Automation Instrumentation*, 2020, 41(4): 107-110.
(康剑萍, 王沈敏, 杜竹青. PKI 技术在信息安全中的应用[J]. *自动化仪表*, 2020, 41(4): 107-110.)

[8] Wu W. Research on Internet of Things Identity Authentication and Privacy Protection Technology in Edge Computing Environment[D]. Xidian University, 2019.
(吴卫. 边缘计算环境下物联网身份认证与隐私保护技术研究[D]. 西安电子科技大学, 2019.)

[9] Ding Y S, Li L X, Li Z H. Certificate-based Cross-domain Authentication Scheme with Anonymity[J]. *Chinese Journal of Network*

and Information Security, 2018, 4(5): 32-38.
(丁永善, 李立新, 李作辉. 基于证书的匿名跨域认证方案[J]. *网络与信息安全学报*, 2018, 4(5): 32-38.)

[10] Wan Y W. Research on cross-domain authentication mechanism under the environment of Internet of Things[D]. Nanchang University, 2018.
(万雨薇. 物联网环境下的跨域认证机制研究[D]. 南昌大学, 2018.)

[11] Li Y, Men J B, Yu H, et al. Overview of Blockchain Capacity Expansion Technology[J]. *Electric Power Information and Communication Technology*, 2020, 18(6): 1-9.
(李洋, 门进宝, 余晗, 等. 区块链扩容技术研究综述[J]. *电力信息与通信技术*, 2020, 18(6): 1-9.)

[12] Huang Z Y. The Application of Blockchain in Edge Computing and IoT[J]. *Cyberspace Security*, 2018, 9(8): 25-30.
(黄忠义. 区块链在边缘计算与物联网安全领域应用[J]. *网络空间安全*, 2018, 9(8): 25-30.)

[13] Zhou Z C, Li L X, Li Z H. Efficient Cross-domain Authentication Scheme Based on Blockchain Technology[J]. *Journal of Computer Applications*, 2018, 38(2): 316-320, 326.
(周致成, 李立新, 李作辉. 基于区块链技术的高效跨域认证方案[J]. *计算机应用*, 2018, 38(2): 316-320, 326.)

[14] Tan C, Chen M J, Amuah E. Research on Distributed Identity Authentication Mechanism of IoT Device Based on Blockchain[J]. *Chinese Journal on Internet of Things*, 2020, 4(2): 70-77.
(谭琛, 陈美娟, Amuah Ebenezer Ackah. 基于区块链的分布式物联网设备身份认证机制研究[J]. *物联网学报*, 2020, 4(2): 70-77.)

[15] Zhang H D, Liu G R, Wang L F, et al. Research on cross domain identity authentication mechanism based on blockchain technology[J]. *Guangdong Communication Technology*, 2018, 38(7): 23-31.
(张昊迪, 刘国荣, 汪来富, 等. 基于区块链技术的跨域身份认证机制研究[J]. *广东通信技术*, 2018, 38(7): 23-31.)

[16] Pan W, Huang X F. Identity Management and Authentication Model Based on Smart Contract[J]. *Computer Engineering and Design*, 2020, 41(4): 915-919.
(潘维, 黄晓芳. 基于智能合约的身份管理及认证模型[J]. *计算机工程与设计*, 2020, 41(4): 915-919.)

[17] Canetti R, Krawczyk H. Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels[M]. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001: 453-474.

张金花 于2018年在郑州轻工业大学网络工程专业获得学士学位。现在大理大学计算机技术专业攻读硕士学位。研究领域为区块链技术及物联网安全。Email: jinh_zhang007@163.com

李晓伟 于2013年在西安电子科技大学信息安全专业获得博士学位。现任大理大学数学与计算机学院讲师。研究兴趣包括: 网络安全协议、云计算安全、区块链技术。Email: lixiaowei_xidian@163.com

曾新 于2013年在云南大学信息学院获得硕士学位, 现任大理大学数学与计算机学院讲师。研究兴趣包括: 空间并置模式挖掘、关联规则挖掘。Email: hbzengxin@163.com

赵榆琴 于2008年在云南师范大学计算机软件与理论专业获得硕士学位。现任大理大学数学与计算机学院讲师。研究兴趣包括: 大数据分析、人工智能。Email: mygod569@163.com

段燃 于2019年于中国科学院大学信息安全专业获得硕士学位。现任大理大学数学与计算机学院信息安全专业教师, 主要研究方向: 安全漏洞。Email: drnipc@126.com

杨邓奇 于2012年在四川大学计算机科学与技术专业获得博士学位。现任大理大学数学与计算机学院副教授。研究兴趣包括: 数字签名、身份认证、人工智能。Email: dengqiyang@163.com