基于区块链的分布式物联网设备身份认证机制研究

谭琛，陈美娟，Amuah Ebenezer Ackah
（南京邮电大学通信与信息工程学院，江苏 南京 210003）

摘 要：为了解决物联网集中式平台在设备身份认证过程中兼容性低、抗攻击能力弱等问题，提出了一种基于区块链的分布式物联网设备身份认证架构。将数字身份等信息存入新型区块数据结构中，并根据密码学相关知识提出了分布式物联网设备身份认证机制，设计了设备数字证书颁发和身份认证的详细流程。从各实体间的权力约束、设备隐私性保护、抵御攻击能力等方面对所提机制进行了安全性分析，并对比分析了安全属性、计算开销和存储开销 3 个方面的性能。结果表明，所提出的身份认证机制可以抵御多种恶意攻击，能够实现高度安全的分布式物联网身份认证，并且在性能方面具有一定优势。

关键词：区块链；物联网；分布式；身份认证；密码学
中图分类号：TP309
文献标识码：A
doi: 10.11959/j.issn.2096−3750.2020.00167

Research on distributed identity authentication mechanism of IoT device based on blockchain

TAN Chen, CHEN Meijuan, Amuah Ebenezer ACKAH
College of Telecommunications and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China

Abstract: Aiming to solve problems of the low compatibility and weak anti-attack ability of the Internet of things (IoT) centralized platform in the device identity authentication process, a blockchain-based distributed IoT device identity authentication architecture was proposed. The digital identity and related information were stored in the new block data structure, and a distributed IoT device identity authentication mechanism was proposed based on the cryptography related knowledge. At the same time, a device digital certificate issuance process and a detailed process of the identity authentication were designed. The security analysis of the proposed mechanism were carried out from the aspects of power constraints, device privacy protection, and ability to resist attacks among various entities. The performance of three aspects, which were security attributes, computational overhead and storage overhead, were compared and analyzed. The results show that the proposed identity authentication mechanism can resist a variety of malicious attacks, achieve highly secure distributed IoT identity authentication, and has certain advantages in the performance.

Key words: blockchain, Internet of things, distributed, identity authentication, cryptography

1 引言

近年来，物联网技术[1]的普及和迅速发展使得物联网应用[2]在日常生活中随处可见，并在各个领域发挥着重要作用。但是，物联网设备的局限性、复杂的网络环境以及当前基于集中式和层次化结构的接入控制系统，给物联网领域带来了新的挑战。首先，由于设备分布广、应用环境复杂、计算能力有限等问题，将会给中心化网络模式带来巨大的数据基础设施建设和成本投入。其次，目前的物

收稿日期：2020−04−08；**修回日期**：2020−05−09
通信作者：陈美娟，chenmj@njupt.edu.cn
基金项目：国家自然科学基金资助项目（No.61871237）；江苏省重点研发计划（No.BE2019017）
Foundation Items: The National Natural Science Foundation of China (No.61871237), The Key R&D Plan of Jiangsu Province (No.BE2019017)

联网集中式平台互不兼容，这使得不同平台下的物联网设备之间协同工作及信息共享难以实现。另外，集中式平台抵抗恶意攻击的能力差，隐私数据容易被泄露。物联网设备的数量未来将会快速增长，应用规模更庞大，安全性要求也更高，所以迫切需要实现物联网设备的分布式身份认证及可信接入。

目前，物联网身份认证的常用方案主要有以下 3 种：1) 在基于公钥基础设施（PKI, public key infrastructure）身份认证方案[3]中，证书授权中心为每个设备分配数字证书[4]，该数字证书中包含设备的公钥和证书授权中心的数字签名[5-6]。设备方利用自身私钥生成消息签名，公钥被接收方用于验证签名，此方案在验证过程中不会泄露设备的真实身份。2) 在基于身份的签名（IBS, identity-based signature）方案[7]中，通过设置私钥生成器（PKG, private key generator）实现设备私钥的分发，通过这种方式可以解决设备公钥传送问题。另外，可以利用双线性映射[8-9]实现强指定验证签名，即使在传输过程中消息被泄露，仍可以实现安全、唯一的身份验证。3) 在基于无证书签名（CLS, the certificateless signature）的认证方案[10]中，密钥生成中心（KGC, the key generation center）根据物联网设备身份标识号（ID, identity document）为其生成对应的部分私钥，设备使用秘密值和部分私钥生成实际的私钥。

现阶段，将区块链和物联网结合[11-12]是一种发展趋势，区块链的分布式特性可以满足物联网设备在运动场景下的网络接入需求。另外，区块链数据存储的高度安全性为物联网设备接入后的数据共享和协同工作提供了良好保障。文献[13]提出了一种基于数字证书的认证方案，通过树状存储结构默克尔帕特里树（MPT, Merkle Patricia tree）来扩展区块链数据结构。将物联网设备及其数字证书以键值对形式存储在 MPT 叶子节点中，MPT 随着节点的增加而更新，所有交易及对应更新的 MPT 根都按时间顺序存储在时序默克尔树（CMT, chronological Merkle tree）中，最终被打包上链。在物联网设备身份认证时，可通过数字证书在 MPT 中的存储路径查询其有效性。文献[14]将区块链与边缘计算结合，利用边缘计算来支持区块链系统中的边缘认证服务。建立了分布可信的接入机制，实现了双向认证，提高了认证效率。文献[15]结合区块链及雾计算服务，提出了一种区块链辅助的轻量级匿名认证方案，可以实现灵活的跨数据中心认证并保护设备的隐私，通过区块链及密码学技术减少了通信损耗，认证双方在认证过程中只需发送一次消息，大幅度提高了认证效率。

本文在已有认证方案的基础上，针对目前集中式场景下物联网设备身份认证面临的兼容性及安全问题展开研究，主要贡献包括如下两方面。

1) 引入区块链技术，提出一种分布式物联网设备身份认证架构。通过设置两个半权威机构实现权力分散，从而相互制约，并结合公共数据库（PD, public database），使架构中实体的操作公开、透明、可查，防止权力滥用。

2) 结合密码学技术，制定了物联网分布式身份认证方案。通过数字证书技术保证密钥传输的安全性，引入新型区块数据结构，接收方可以验证发送方的数字证书是否可靠，从而节省了证书查询时间，降低了对存储空间的要求。在物联网设备接入区块链网络前，先验证接入节点的可靠性，然后节点验证设备身份，实现了设备及节点的双向身份认证。另外，通过预签名机制保证了签名伪造破解难度及接入过程的高度安全性。

2　基于区块链的物联网分布式身份认证方案

2.1　系统架构

基于区块链的物联网分布式身份认证架构如图 1 所示，该架构由 5 部分构成，包括执法机构（EA, enforcement agency）、证书授权中心（CA, certificate authority）、区块链边缘网络、物联网设备和 PD。

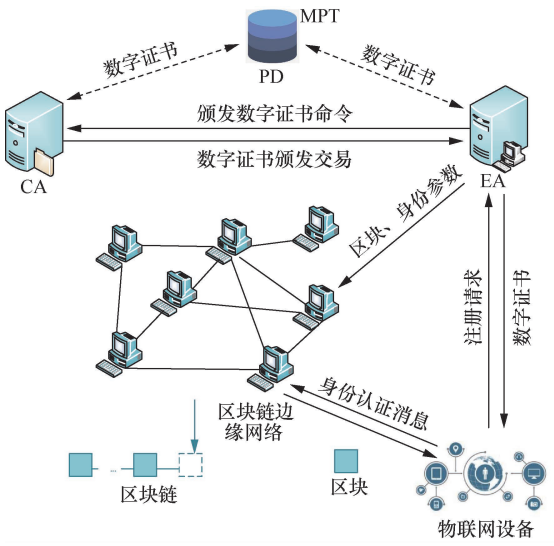

图 1　基于区块链的物联网分布式身份认证架构

2.1.1　EA

EA 的主要职责包括设备登记注册，并为其生

成身份参数、授权 CA 颁发数字证书以及向设备返回数字证书。EA 收集 CA 传来的交易后生成一个区块，并将该区块传递给所有边缘节点进行验证。使用 EA 的密钥加密设备证书与其真实身份之间的可链接性，并将其存储在区块链中。在有争议的情况下，EA 能够显示真实身份。本文假设 EA 是半可信机构，不会恶意跟踪或揭示设备的公钥与其真实身份之间的关联性。

2.1.2 CA

CA 在接收 EA 的颁发数字证书命令后，负责区块链边缘网络节点及物联网设备的数字证书生成，生成数字证书颁发交易并回传给 EA。将数字证书存入 PD，与 EA 共同维护 PD。

2.1.3 物联网设备

物联网设备随机生成 256 bit 的比特串作为私钥，利用椭圆曲线密钥生成算法得到公钥。通过使用椭圆曲线数字签名算法，用 EA 公钥加密注册请求并发送给 EA。接收 EA 回传的数字证书，同时接收节点传来的可靠性证明消息并进行验证。

2.1.4 区块链边缘网络

区块链边缘网络负责存储系统内的所有交易，将打包好的区块共识上链，并将最新区块信息在系统内广播。在 EA 注册身份并接收数字证书，对 EA 传来的设备身份参数进行处理，生成预签名。在区域内的设备请求接入时，将预签名作为节点可靠性证明的一部分。接收设备接入请求消息，并验证身份。制定智能合约，为接入设备划分访问权限。

2.1.5 PD

PD 由 CA 和 EA 共同维护，架构中的其他实体可以访问自身相关信息以及两个半权威机构的每一步操作。数字证书以 MPT 的结构形式存储，MPT 根节点的值作为证书根，最终和 CMT 的交易根共同存储在区块头中。

2.2 分布式物联网设备身份认证

2.2.1 系统初始化

设置系统参数 $\{G_1,G_2,q,G,s,\mathrm{PK},H_1,H_2\}$，并在系统内全网广播。其中，$G_1$ 和 G_2 为椭圆曲线循环群，q 为循环群阶数，G 为循环群生成元。$s\in Z_q^*$ 为系统私钥，PK 为系统公钥。H_1 和 H_2 为哈希函数，分别定义为：$H_1:\{0,1\}^*\times G_1\to Z_q^*$、$H_2:\{0,1\}^*\times G_1\times G_1\to Z_q^*$。EA 和 CA 基于椭圆曲线加密，分别生成其密钥对 $(\mathrm{Pu}_{\mathrm{EA}},\mathrm{Se}_{\mathrm{EA}})$ 和 $(\mathrm{Pu}_{\mathrm{CA}},\mathrm{Se}_{\mathrm{CA}})$，并将公钥 $\mathrm{Pu}_{\mathrm{EA}}$ 和 $\mathrm{Pu}_{\mathrm{CA}}$ 在系统内广播，以便其他实体向其发送加密消息。区块链边缘节点生成密钥对 $(\mathrm{Pu}_n,\mathrm{Se}_n)$，EA 为边缘节点注册并命令 CA 颁发数字证书，再由 EA 将数字证书发送给各节点，此步骤与设备证书颁发流程类似。在认证流程中所涉及的物联网设备用 D_i 表示，区块链边缘节点用 B_n 表示。

2.2.2 数字证书颁发

认证方案通过数字签名验明设备和节点身份，数字签名采用非对称加密，由发送方私钥加密生成，接收方需持有发送方公钥验证签名。使用数字证书对公钥进行加密，以保证其安全传输，设计一种数字证书颁发机制，数字证书颁发流程如图 2 所示，具体步骤如下所述。

步骤 1 设备端 D_i 生成密钥对 $(\mathrm{Pu}_i,\mathrm{Se}_i)$，前者为公钥，后者为私钥。设备向 EA 发出注册请求消息 reg_i 为

$$\mathrm{reg}_i=E_{\mathrm{Pu}_{\mathrm{EA}}}(\mathrm{Pu}_i,\mathrm{ID}_i,t,\mathrm{sig}_{\mathrm{Se}_i}) \tag{1}$$

其中，$E_{\mathrm{Pu}_{\mathrm{EA}}}$ 表示以 EA 公钥进行加密的椭圆曲线加密算法，ID_i 表示设备编号，t 表示请求消息发出时的时间戳，$\mathrm{sig}_{\mathrm{Se}_i}$ 表示以设备 D_i 私钥加密的椭圆曲线数字签名。

步骤 2 EA 接收 D_i 注册请求，并验证消息来源是否可靠，然后通过哈希函数将设备 ID_i 加密为 $h_{i1}=H_1(\mathrm{ID}_i)$。EA 创建设备 D_i 的身份链接 Link_i 为

$$\mathrm{Link}_i=E_{\mathrm{Pu}_{\mathrm{EA}}}(\mathrm{ID}_i\,\|\,r_{\mathrm{EA}}) \tag{2}$$

其中，r_{EA} 表示与设备身份链接相关的随机数。创建身份链接可实现设备匿名，在有争议的情况下，EA 能够揭示设备的真实身份。

步骤 3 EA 向 CA 发送颁发数字证书命令 auth 为

$$\mathrm{auth}=(\mathrm{Pu}_i,T,t,\mathrm{Link}_i,\mathrm{sig}_{\mathrm{Se}_{\mathrm{EA}}}) \tag{3}$$

其中，参数 T 表示数字证书的有效时间，CA 生成数字证书 C_i 为

$$\mathrm{C}_i=(\mathrm{Pu}_i,T,t,\mathrm{Link}_i) \tag{4}$$

步骤 4 CA 将式(4)生成的设备数字证书 C_i 作为 MPT 新的叶子节点并添加到 PD 中，CA 向 EA 发送数字证书颁发交易 tx 为

$$\mathrm{tx}=(\mathrm{Pu}_i,t,\mathrm{auth},\mathrm{sig}_{\mathrm{Se}_{\mathrm{CA}}}) \tag{5}$$

步骤 5 EA 接收交易 tx，并将其打包成新区块 Block_i 广播至区块链边缘网络，边缘节点通过共识算法选出记账节点并将区块上链。式(5)中生成的交

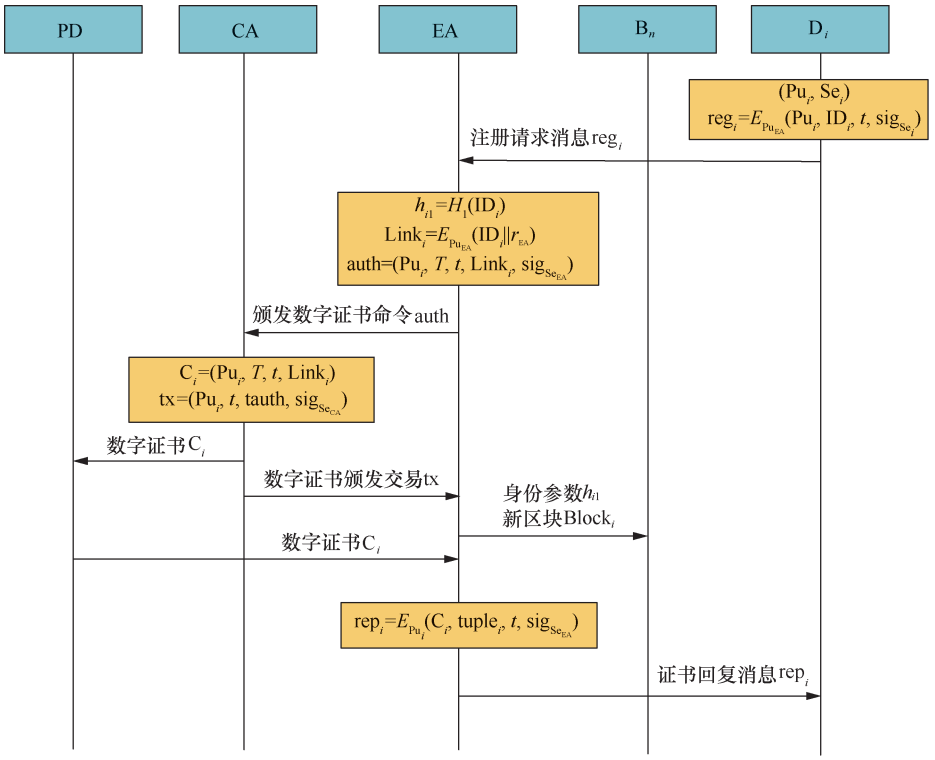

图 2　数字证书颁发流程

易包含 EA 的颁发数字证书命令和 CA 的签名，证书签发过程经过两个半权威机构认证，若发生证书纠纷，则可以查询证书交易内容进行裁定。EA 向区块链边缘网络广播发送物联网设备 D_i 的身份参数 h_{i1}，边缘节点 B_n 接收并保存 h_{i1}，将其作为用于 D_i 身份认证的参数。

步骤 6　EA 从 PD 中取出 CA 为设备 D_i 颁发的数字证书 C_i，并生成证书回复消息 rep_i 为

$$rep_i = E_{Pu_i}(C_i, tuple_i, t, sig_{Se_{EA}}) \tag{6}$$

在式(6)中，$tuple_i$ 为数字证书 C_i 在 MPT 中的查询路径，包含从 MPT 根节点到数字证书 C_i 所在叶子节点路径上的所有节点。

2.2.3　身份认证

由于区块链中可能存在恶意节点，在物联网设备发送身份信息前要验明接入节点是否可靠。本方案通过预签名机制实现了对区块链边缘节点的可靠性验证，再通过主签名对设备进行认证，实现了双向高度安全的身份认证，身份认证流程如图 3 所示，具体步骤如下所述。

步骤 1　设备 D_i 处于节点 B_n 覆盖范围内，并向其发出接入请求消息 req_i 为

$$req_i = E_{PK}(loca_i, t_1, B_L, t_2) \tag{7}$$

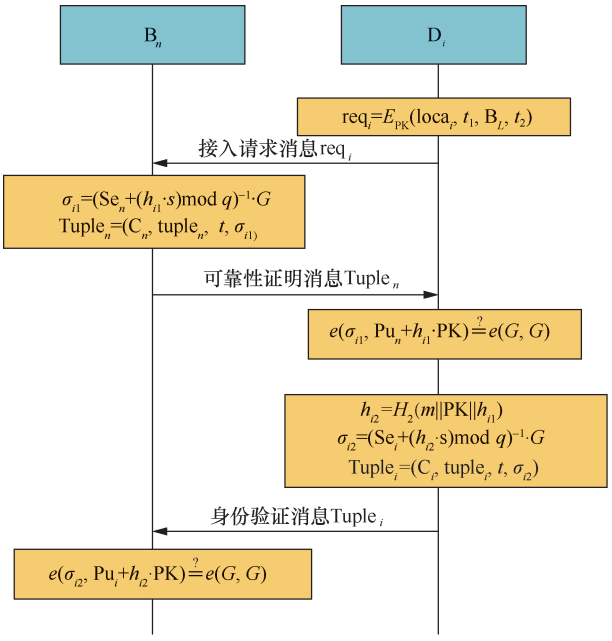

图 3　身份认证流程

在式(7)中，$loca_i$ 表示设备 D_i 的地理位置，t_1 代表消息 req_i 的发送时间，B_L 表示设备上一个接入的节点，t_2 表示设备 D_i 接入上个节点 B_L 的时刻。

步骤 2　在节点接收请求后，首先向节点 B_L 求证设备 D_i 是否曾在此接入。B_L 若有 D_i 在 t_2 时刻的接入记录，则表明接入请求消息 req_i 的可信度较高，

此时节点 B_n 生成可靠性证明消息 Tuple_n 并发送给设备 D_i。

$$\sigma_{i1}=(\text{Se}_n+(h_{i1}\cdot s)\bmod q)^{-1}\cdot G \tag{8}$$

$$\text{Tuple}_n=(\text{C}_n,\text{tuple}_n,t,\sigma_{i1}) \tag{9}$$

在式(8)中，σ_{i1} 表示节点 B_n 生成的预签名；当 C_n 为系统初始化时，证书授权中心为节点 B_n 颁发的数字证书。在式(9)中，tuple_n 为数字证书 C_n 在 MPT 中的查询路径，在系统初始化时，CA 为边缘节点颁发数字证书并将其存入 PD 后，由 EA 将数字证书发送至 B_n，tuple_n 包含从 MPT 根节点到数字证书 C_n 所在叶子节点路径上的所有节点信息。

步骤 3 设备端对边缘节点进行可靠性验证，D_i 首先取出节点数字证书 C_n 中的公钥，计算 tuple_n 路径构成的键值能否和节点公钥哈希值对应，然后根据路径节点哈希值计算 MPT 根值。随着新证书的发布，MPT 根值也随之更新，所以需要将计算得到的根植与最新发布的区块所包含的 MPT 根值进行比较，若一致则表明节点证书有效。最后利用双线性映射的双线性，验证节点签名。

$$\begin{aligned}&e(\sigma_{i1},\text{Pu}_n+h_{i1}\cdot\text{PK})=\\&e((\text{Se}_n+h_{i1}\cdot s)^{-1}\cdot G,(\text{Se}_n+h_{i1}\cdot s)\cdot G)=\\&e(G,G)^{(\text{Se}_n+h_{i1}\cdot s)^{-1}\cdot(\text{Se}_n+h_{i1}\cdot s)}=\\&e(G,G)\end{aligned} \tag{10}$$

若式(10)的等式成立，则证明边缘节点的身份可靠。

步骤 4 在设备 D_i 验证节点 B_n 身份可靠后，D_i 生成身份验证消息 Tuple_i 并发送给节点 B_n。

$$h_{i2}=H_2(m\,\|\,\text{PK}\,\|\,h_{i1}) \tag{11}$$

$$\sigma_{i2}=(\text{Se}_i+(h_{i2}\cdot s)\bmod q)^{-1}\cdot G \tag{12}$$

$$\text{Tuple}_i=(\text{C}_i,\text{tuple}_i,t,\sigma_{i2}) \tag{13}$$

在式(11)中，h_{i2} 表示设备消息摘要；m 为设备身份认证消息明文，在明文中备注已验证节点的可靠性。在式(12)中，σ_{i2} 表示设备生成的主签名。在式(13)中，tuple_i 为数字证书 C_i 在 MPT 中的查询路径。

步骤 5 边缘节点对设备进行身份验证，边缘节点首先取出设备数字证书 C_i 中的公钥，计算 tuple_i 路径构成的键值和设备公钥哈希值能否对应。然后根据路径节点哈希值计算 MPT 根值并与最新区块信息中包含的 MPT 根进行比较，若一致则表明设备证书有效。最后，节点验证设备签名。

$$\begin{aligned}&e(\sigma_{i2},\text{Pu}_i+h_{i2}\cdot\text{PK})=\\&e((\text{Se}_i+h_{i2}\cdot s)^{-1}\cdot G,(\text{Se}_i+h_{i2}\cdot s)\cdot G)=\\&e(G,G)(\text{Se}_i+h_{i2}\cdot s)^{-1}\cdot(\text{Se}_i+h_{i2}\cdot s)=\\&e(G,G)\end{aligned} \tag{14}$$

若式(14)的等式成立，则设备通过身份认证并接入区块链边缘网络。

3 安全性分析

本节将从如下 3 个方面对所提方案的安全性进行分析。

3.1 避免滥用权力

由 CA 广播的所有交易以及证书根都公开且不可变地记录在区块链中，若每个交易都包含 CA 和 EA 的签名，则相当于每个交易都通过 EA 和 CA 授权。若未经 EA 授权，则 CA 不能任意签发或撤销证书。另外，由于 CMT 和 MPT 是用哈希值层叠构建的，在 MPT 根确定的情况下，证书节点数据无法被篡改。由于 CA 新数字证书颁发而更改的 MPT 根附于相应的交易中，该交易按时间顺序记录在 CMT 中。为了验证 MPT 的有效性，可以执行逆操作，并将 MPT 的更改根与附加到前一个交易的根进行比较，若一致则证明 MPT 根有效且未被修改。

3.2 保护设备隐私

除了 EA 之外，系统中没有任何实体能够从 PD 和广播消息中揭示目标设备的真实身份。设备证书与其真实身份之间的链接性被加密，以防止对手跟踪目标设备。如果没有 EA 的私钥，则攻击者无法破解目标设备的身份。另外，加入随机数使每个数字证书中的链接完全不同，这使得对手无法获得 C_i 之前的数字证书间的链接性。对于架构中的每个实体，CA 和 EA 的所有活动都是透明、可验证的，可以防止其故意泄露设备真实身份。

3.3 抵御多种攻击

对于伪造攻击而言，攻击者若要伪造设备身份向节点发送消息 Tuple_i，首先需要计算数字证书 C_i 的路径 tuple_i，根据路径计算的根哈希值必须和当前的 MPT 根相等。由于所提方案中使用的哈希算法 SHA（secure Hash algorithm）具有抗碰撞特性，已知 MPT 根值求节点哈希值是不可行的，数字证书无法伪造。此外，攻击者若想伪造设备生成的主签名 σ_{i2}，需持有设备私钥。然而在非对称加密中，私钥由发送方持有并且高度保密，无法被窃取。因

此，设备身份无法被伪造。同理，为了伪造区块链边缘节点的可靠性来证明消息 Tuple_n，则攻击者必须计算其 tuple_n 及私钥，这也是不可行的，所以节点身份无法被伪造。综上所述，本方案可以抵御伪造攻击。

对于中间人攻击而言，攻击者必须伪造边缘节点或终端的身份，而身份伪造是不可能实现的，因此，说明本方案可抵御中间人攻击。

对于重放攻击而言，身份认证流程中的每条消息都包含时间戳 t，时间戳可以保证消息的唯一性。若攻击者想在设备认证阶段发起重放攻击，则需要修改 Tuple_i 的时间戳。然而，修改时间戳的同时需要修改主签名 σ_{i2}，若节点接收到的消息的主签名与已经接收到的 Tuple_i 认证消息的主签名相同，则将其丢弃，并且设备对节点进行验证时的操作也一样。攻击者无法获得由发送方私钥生成的有效签名，因此，本方案可以抵御重放攻击。

4　性能分析

本节对所提出的分布式身份认证机制在安全属性和计算开销方面进行对比分析，对比方案包括 KPSD[16]、IBCCPA[17]、EAAP[18]和 EPAW[19]。另外，对存储开销也进行了对比分析。

4.1　安全属性比较

将本文所提出的分布式身份认证方案记为 DA（distributed authentication），安全属性比较如表 1 所示。

表 1　　安全属性比较

对比项	KPSD	IBCCPA	EAAP	EPAW	DA
双向认证	×	√	√	√	√
隐私保护	√	√	√	√	√
可追溯	×	√	√	×	√
抗伪造攻击	√	√	√	√	√
抗权力滥用	×	×	×	×	√
抗重放攻击	×	√	×	√	√

主要对比了 6 个关键安全属性，包括：双向认证、隐私保护、可追溯、抗伪造攻击、抗权力滥用和抗重放攻击。其中，√表示所考虑的方案满足特定的安全属性，×表示所考虑的方案不满足特定的安全属性。由上文的分析可知，本文提出的 DA 方案满足以上安全属性。KPSD 方案没有考虑双向认证；KPSD 及 EPAW 方案没有涉及架构内实体身份的揭示，所以不满足可追溯属性；KPSD 及 EAAP 方案内的消息没有加入时间戳机制，所以无法抵御重放攻击；以上方案都没有考虑权威机构的权力制约，所以不满足抗权力滥用。由比较结果可以看出，与其他方案相比，本文方案满足的安全属性更多，安全性更高。

4.2　计算开销比较

认证计算开销是指接收方验证发送方签名和证书花费的时间，不同方案认证计算开销如表 2 所示，表 2 中列出了各种方案所花费的计算开销。其中，T_{bp} 表示 1 次双线性对生成时间，T_{epl} 表示循环群 G_1 的 1 次指数运算时间；T_{ep2} 表示循环群 G_2 的 1 次指数运算时间，T_{m} 表示 1 次椭圆曲线点乘的时间，T_{a} 表示 1 次椭圆曲线点加的时间，T_{h} 表示 1 次哈希运算时间。

表 2　　不同方案认证计算开销

认证方案	验证 1 次证书和签名	验证 n 次证书和签名
KPSD	$4T_{\text{bp}}+5T_{\text{epl}}+5T_{\text{ep2}}$	$(3+n)T_{\text{bp}}+(4+n)T_{\text{epl}}+5nT_{\text{ep2}}$
IBCCPA	$3T_{\text{bp}}+2T_{\text{epl}}+2T_{\text{h}}$	$(2+n)T_{\text{bp}}+2nT_{\text{epl}}+2nT_{\text{h}}$
EAAP	$2T_{\text{bp}}+4T_{\text{epl}}+T_{\text{ep2}}$	$(1+n)T_{\text{bp}}+4T_{\text{epl}}+nT_{\text{ep2}}$
EPAW	$2T_{\text{bp}}+2T_{\text{m}}+T_{\text{h}}$	$(1+n)T_{\text{bp}}+2nT_{\text{m}}+nT_{\text{h}}$
DA	$2T_{\text{bp}}+T_{\text{m}}+T_{\text{a}}+8T_{\text{h}}$	$(1+n)T_{\text{bp}}+nT_{\text{m}}+nT_{\text{a}}+8nT_{\text{h}}$

为了确定分布式身份认证算法的精确计算时间，利用 JPBC[20]密码库对方案中所涉及的密码学运算进行运行时间测试（电脑配置为 2.5 GHz 英特尔 i5 处理器、8 GB 内存），多次运行取平均值，结果显示：T_{bp}、T_{epl} 和 T_{ep2} 运行时间较长，分别为 12.261 ms、7.584 ms 和 5.828 ms。T_{m}、T_{a} 和 T_{h} 运行时间较短，分别为 0.216 ms、0.005 ms、0.001 ms。经计算，在单次认证过程中，本文所提方案的性能明显优于 KPSD（运行时间为 116.104 ms）、IBCCPA（运行时间为 51.593 ms）和 EAAP（运行时间为 60.686 ms）3 种方案的性能。与 EPAW（运行时间为 24.955 ms）方案相比，本文方案省去了 1 次点乘运算、添加了 1 次点加运算及 7 次哈希运算，由于后两种运算的运行时间要少于点乘运算，因此，本文方案的认证开销为 24.751 ms，比 EPAW 少约 0.204 ms。随着证书和签名数量的增加，不同方案计算开销的差距会越来越大，其中，IBCCPA 方案很快超过 EAAP 方案，本文方案的计算开销仍保持最低。

在本文方案中，总计算开销定义为 $T_{\text{total}} = T_{\text{generate}} + T_{\text{verify}}$，即发送方生成验证消息的计算开销 T_{generate} 和接收方认证计算开销 T_{verify} 的总和。接下来，比较 DA 与 EPAW、EAAP 方案的 1 次总计算开销，由于本文方案为双向认证，因此，在计算总开销时分别考虑了设备端 D_i 和节点端 B_n 的情况，不同方案总计算开销如表 3 所示。

表 3 不同方案总计算开销

认证方案	生成 1 次身份信息	1 次完整认证
EAAP	$5T_{\text{ep1}} + T_{\text{ep2}} + T_{\text{h}}$	$2T_{\text{bp}} + 9T_{\text{ep1}} + 2T_{\text{ep2}} + T_{\text{h}}$
EPAW	$4T_{\text{ep1}} + T_{\text{ep2}} + T_{\text{h}}$	$2T_{\text{bp}} + 4T_{\text{ep1}} + T_{\text{ep2}} + 2T_{\text{m}} + 2T_{\text{h}}$
DA(B_n)	T_{m}	$2T_{\text{bp}} + 2T_{\text{m}} + T_{\text{a}} + 8T_{\text{h}}$
DA(D_i)	$T_{\text{m}} + T_{\text{h}}$	$2T_{\text{bp}} + 2T_{\text{m}} + T_{\text{a}} + 9T_{\text{h}}$

经计算，EAAP 方案的计算开销最大，约为 104.435 ms，EPAW 方案次之，约为 61.120 ms。本文方案的节点端总计算开销约为 24.967 ms，设备端由于单次认证与节点端的计算开销只相差 0.001 ms，计算开销极其相近，则差距可以忽略不计，但均远小于 EPAW 和 EAAP 方案的计算开销。

4.3 存储开销分析

针对物联网设备存储容量受限问题，将对本文方案中的存储开销进行分析。物联网设备需要存储的信息包括数字证书 C_i、自身私钥 Se_i 和证书存储路径 tuple_i。物联网设备存储开销如表 4 所示。

表 4 物联网设备存储开销

存储信息	设备 D_i 的存储开销
C_i	100 bit
Se_i	32 bit
tuple_i	228 bit
共计	360 bit

数字证书采取自发行证书，数字证书内存储序列号、公钥以及发行日期等必要信息，约占用 100 bit。椭圆曲线私钥占用 32 bit。tuple_i 内数字证书存储路径节点信息约占用 228 bit，经计算可得，设备端存储开销约为 360 bit，以目前物联网设备的存储容量来看，完全可以接受。节点端需要存储的数据类型和设备端基本一致，区块链节点存储开销如表 5 所示。

与设备端相比，节点端多存储一个身份参数信息 h_{i1}，则多占用 32 bit，所以节点端的存储开销约为 392 bit。为了节省认证时间，本文方案节点端数据存储于节点本地数据库中，而不是上传到区块链，从而避免了区块链数据查询的烦琐过程。

表 5 区块链节点存储开销

存储信息	节点 B_n 的存储开销
C_n	100 bit
h_{i1}	32 bit
Se_n	32 bit
tuple_n	228 bit
共计	392 bit

5 结束语

针对目前物联网集中式管理平台的弊端，本文提出了一种基于区块链的物联网分布式身份认证架构，包括 EA、CA、物联网设备、区块链边缘节点以及 PD 共 5 个部分。另外，对传统的区块数据结构进行扩充，引入了 MPT 数据结构以保证数字证书的可靠性。接下来，分析了物联网设备从数字证书颁发到身份认证的全过程，并对整个系统的安全性做了详细分析。最后将本文所提的物联网身份认证方案和其他方案进行性能对比分析。结果表明，本文方案具有去中心化、权力分散和保护隐私的特性，并且在安全属性、计算开销及存储开销等性能方面具有一定优势。

参考文献：

[1] 邬贺铨. 物联网技术与应用的新进展[J]. 物联网学报, 2017, 1(1): 1-6.
WU H Q. Technology and application progress on Internet of things[J]. Chinese Journal on Internet of Things, 2017, 1(1): 1-6.

[2] YAQOOB I, HASHEM I A T, AHMED A, et al. Internet of things forensics: recent advances, taxonomy, requirements, and open challenges[J]. Future Generation Computer Systems, 2019, 92: 265-275.

[3] FENG T, CHEN W Y, ZHANG D, et al. One-stop efficient PKI authentication service model based on blockchain[C]//CCF China Blockchain Conference. Springer, 2019: 31-47.

[4] 毕宇. 基于区块链智能合约的 PKI-CA 体系设计[J]. 金融科技时代, 2018, 275(7): 44-46.
BI Y. PKI-CA system design based on blockchain smart contract[J]. Financial Technology Time, 2018, 275(7): 44-46.

[5] FAROOQ S M, HUSSAIN S M S, USTUN T S. Elliptic curve digital signature algorithm (ECDSA) certificate based authentication scheme for advanced metering infrastructure[C]//2019 Innovations in Power and Advanced Computing Technologies (i-PACT). IEEE, 2019, 1: 1-6.

[6] 刘巧平, 周斌, 王文涛. 基于椭圆曲线的信息加密及网络身份认证算法的研究[J]. 自动化与仪器仪表, 2016(8): 159-160.

LIU Q P, ZHOU B, WANG W T. Research on information encryption and network identity authentication algorithm based on elliptic curve[J]. Automation & Instrumentation, 2016(8): 159-160.

[7] BEHESHTI-ATASHGAH M, AREF M R, BAYAT M, et al. ID-based strong designated verifier signature scheme andits applications in Internet of things[C]//2019 27th Iranian Conference on Electrical Engineering (ICEE). IEEE, 2019: 1486-1491.

[8] SAHANA S C, BHUYAN B. A provable secure short signature scheme based on bilinear pairing over elliptic curve[J]. IJ Network Security, 2019, 21(1): 145-152.

[9] GUO S Y, HU X, ZHOU Z Q, et al. Trust access authentication in vehicular network based on blockchain[J]. China Communications, 2019, 16(6): 18-30.

[10] HAN S, XIE M D, YANG B L, et al. A certificateless verifiable strong designated verifier signature scheme[J]. IEEE Access, 2019, 7: 126391-126408.

[11] ALI M S, VECCHIO M, PINCHEIRA M, et al. Applications of blockchains in the Internet of things: a comprehensive survey[J]. IEEE Communications Surveys & Tutorials, 2019, 21(2): 1676-1717.

[12] 陈美娟, 朱晓荣. 基于区块链的物联网设备标识研究[J]. 物联网学报, 2018, 2(2): 18-26.
CHEN M J, ZHU X R. Research on IoT device identification based on blockchain[J]. Chinese Journal on Internet of Things, 2018, 2(2): 18-26.

[13] LU Z J, WANG Q, QU G, et al. A blockchain-based privacy-preserving authentication scheme for VANETs[J]. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2019, 27(12): 2792-2801.

[14] GUO S Y, HU X, GUO S, et al. Blockchain meets edge computing: a distributed and trusted authentication system[J]. IEEE Transactions on Industrial Informatics, 2019, 16(3): 1-11.

[15] YAO Y Y, CHANG X L, MIŠIĆ J, et al. BLA: blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services[J]. IEEE Internet of Things Journal, 2019, 6(2): 3775-3784.

[16] LU R X, LI X D, LUAN T H, et al. Pseudonym changing at social spots: an effective strategy for location privacy in VANETs[J]. IEEE Transactions on Vehicular Technology, 2012, 61(1): 86-96.

[17] SHAO J, LIN X D, LU R X, et al. A threshold anonymous authentication protocol for VANETs[J]. IEEE Transactions on Vehicular Technology, 2016, 65(3): 1711-1720.

[18] AZEES M, VIJAYAKUMAR P, DEBOARH L J. EAAP: efficient anonymous authentication with conditional privacy-preserving scheme for vehicular Ad Hoc networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2017, 18(9): 2467-2476.

[19] JEGADEESAN S, AZEES M, BABU N R, et al. EP-AW: efficient privacy preserving anonymous mutual authentication scheme for wireless bodyarea networks (WBANs)[J]. IEEE Access, 2020, 8: 48576-48586.

[20] CARO D A, IOVINO V. jPBC: java pairing based cryptography[J]. International Symposium on Computers and Communications, 2011, 22(3): 850-855.

[作者简介]

谭琛（1995– ），男，江苏徐州人，南京邮电大学硕士生，主要研究方向为区块链技术和物联网等。

陈美娟（1971– ），女，陕西咸阳人，博士，南京邮电大学副教授，主要研究方向为异构无线网络资源管理、区块链技术以及 SDN/NFV 技术等。

Amuah Ebenezer Ackah（1987– ），男，加纳人，南京邮电大学博士生，主要研究方向为物联网、区块链以及 MIMO 等。