DOI:10.15991/j.cnki.411100.2025.01.008

# 基于高效历史工作证明区块链的无人机身份认证方案

杜晓玉[1,2,3],张俊杰[1],李 辉[4*],党兰学[2],韩志杰[1]

(1.河南大学 软件学院,河南 开封 475004;2.河南大学 计算机与信息工程学院,河南 开封 475004;
3.河南省工业互联网工程技术研究中心,郑州 450046;4.开封科技传媒学院,河南 开封 475000)

**摘 要**:当前,无人机身份认证网络存在着密钥泄露、冒充攻击和单点故障等问题.因此,有关研究人员提出将区块链技术与无人机身份认证网络结合起来.但现有基于区块链的无人机身份认证方案中存在着资源消耗大、交易费用高、吞吐量低和交易确认延迟大等问题.为此提出了一种新型的无人机身份认证方案——基于高效历史工作证明区块链的无人机身份认证方案(EPOH).为提升通讯效率,EPOH 方案采用了联盟链作为数据存储中心,并通过统计一段时间内各节点转发交易数量的方法来优化节点选举过程.此外还设置了冷却期来避免单个节点连续多次成为领导者,从而保障了系统的去中心化特性.EPOH 方案还通过连续哈希证明技术,通过生成区块内的事件次序证明,消除了时钟同步的需要,从而大幅提高共识达成速度.安全分析部分显示出 EPOH 方案能够抵御恶意分叉的能力.实验分析部分验证了 EPOH 方案能够有效提高系统吞吐量,降低交易确认延迟,显著降低资源消耗和交易成本.

**关键词**:无人机身份认证方案;区块链;共识算法;历史工作证明

**中图分类号**:TP393.0 **文献标志码**:A **文章编号**:1003-4978(2025)01-0021-11

# A Drone Authentication Scheme Based on An Efficient Historical Proof-of-History Blockchain

DU Xiaoyu[1,2,3], ZHANG Junjie[1], LI Hui[4*], DANG Lanxue[2], HAN Zhijie[1]

(1. *School of Software, Henan University, Henan Kaifeng* 475004, *China*;
2. *School of Computer and Information Engineering, Henan University, Henan Kaifeng* 475004, *China*;
3. *Henan Province Engineering Technology Research Center of Industrial Internet, Zhengzhou* 450046, *China*;
4. *Technology and Media University of Henan Kaifeng, Henan Kaifeng* 475000, *China*)

**Abstract**: Currently, there are problems such as key leakage, impersonation attack and single point of failure in UAV authentication network. Therefore, relevant researchers have proposed a scheme that combines blockchain technology with UAV authentication network. However, there are problems such as high resource consumption, high transaction cost, low throughput and high transaction confirmation delay in the existing blockchain-based UAV authentication schemes. For this reason, a novel UAV authentication scheme, the Efficient Proof-of-History of Work blockchain-based UAV authentication scheme (EPOH), is proposed. To improve the communication efficiency, the EPOH scheme adopts a federation chain as the data storage center and optimizes the node election process by counting the number of transactions forwarded by each node over a period of time. A cooling-off period is also set to avoid a single node from becoming the leader multiple times in a row, thus safeguarding the decentralized nature of the system. The EPOH scheme also dramatically improves the speed of consensus attainment by eliminating the need for clock synchronization through the successive hash proof technique by generating proofs of the order of events within a block. The security analysis section shows the ability of the EPOH scheme to withstand

**收稿日期**:2024-11-16

**基金项目**:河南省重点研发与推广专项(232102211009,242102210196,242102210202);开封市科技计划发展项目(2201010)

**作者简介**:杜晓玉(1979-),女,河南濮阳人,博士,教授.研究方向:物联网安全、数据中心网络结构及性能研究、无线传感器网络及车联网抗毁性研究.

* 通信作者, E-mail: HumcLihui@outlook.com

malicious forks. The experimental analysis section verifies that the EPOH scheme can effectively improve system throughput, reduce transaction confirmation delay, and significantly reduce resource consumption and transaction cost.

**Key words**: UAV authentication scheme; blockchain; consensus algorithm; proof of history

## 0 引言

无人机身份认证方案是确保无人机在执行任务时能够安全、可靠地进行通信和数据交换的关键技术.到目前为止,大多数无人机身份认证方案机制为建立在无线传感器网络下的认证机制,即结构分为用户节点和服务器节点的非分布式机制[1].这些方法虽然在一定程度上能够提供身份验证和数据保护,但在无人机这一特殊应用场景下,它们的局限性逐渐显现.例如,无人机移动速度快,导致网络的拓扑结构频繁变化,节点间的信任关系复杂[2].对于采用公钥基础设施的系统通常需要一个可信的第三方证书颁发机构(CA)来管理密钥和证书,这在无人机大规模部署时不仅增加了系统的复杂性,还可能导致单点故障.

区块链是一种分布式账本技术[3],其核心特点在于去中心化、不可篡改性和透明性[4].这些特性使得区块链能够在没有中央控制节点的情况下,通过网络中的多个节点共同维护一份连续的、按时间顺序排列的数据记录[5].共识机制是区块链技术的核心[6],但由于其效率低下,会在应用于物联网系统时造成一些严重的瓶颈[7].

本文设计了一种基于高效历史工作证明区块链的无人机身份认证方案,在解决中心化认证方案单点故障的基础之上,改进区块链的共识算法,加快节点间共识达成效率,提高共识机制的交易处理效率以及区块链网络的吞吐量,从而更适用于无人机身份认证场景.

## 1 相关工作

针对以往无人机身份认证方案面临的一系列问题,近年来一些研究人员提出了各种解决方案.2022 年,Gao 等[8]基于非分布式网络面临的单点故障问题,提出了一种基于区块链的非对称认证和密钥协商协议(BC-AKA),相较于传统认证方案提升了安全性和可靠性.但区块链网络仍面临着效率低下的问题,首先要改进主流的工作量证明(PoW)共识机制[9-10].PoW 最初是由比特币[11]引入作为区块链的共识算法[12],但 PoW 要求节点通过解决复杂的数学问题来争夺区块链上的区块添加权.这种方法虽然安全,但效率低下,能耗高.

作为 PoW 机制的代替方案,King 等[13]在 2012 年提出权益证明(PoS)机制.在 PoS 中,节点根据持有的币龄或权益来争夺区块添加权,减少了能源消耗并提高了速度,但仍存在 Gas 费用高的问题.

2021 年,Kim 等[14]通过调整 PoW 出块间隔的方式,提出了一种在保证安全性的前提下提高 PoW 区块链网络性能的方法.其实验结果显示该方法可以使区块链每秒能处理的交易数量(TPS)提升至 66～120.2022 年,Ren 等[15]提出了一种新型双模式共识协议.在大多数活跃节点处于网络通信状况良好时,系统可以通过快速模式操作加快共识.在非理想条件下,备份协议会接管快速模式的协议,而不需要重新开始已挂起的轮次,其实验结果显示该方法可以使区块链 TPS 性能提升至 2 500 以上.

2023 年,Zhou 等[16]提出了一种基于区块链时空大数据的组认证方案.利用区块链的去中心化解决单点故障,将单点认证与组认证相结合,通过组认证提高认证效率,利用单点认证准确识别非法节点.其仿真结果显示该网络的 TPS 可进一步提高至 300～350.

2018 年,Solana 的创始人 Anatoly Yakovenko 发布了 Solana 区块链项目白皮书[17].Solana 旨在提高与其他区块链相比的可扩展性,同时不损害去中心化和安全性[18],其区块链网络的 TPS 可达 50 000[19].CoinGecko 于 2024 年 5 月 17 日发布的《Fastest Chains》报告中显示,Solana 是大型区块链中速度最快的,最高日均真实 TPS 达到 1 054.这使得 Solana 采用的 PoH 算法成为投入公开网络环境下速度最快的共识算法,Solana 及其采用的 PoH 算法也逐渐被更多人所关注.

通过以上方案,使得区块链网络可以达到较高的交易处理效率.但由于以上算法均设计为面向公有区块链的共识算法,需要利用区块链内虚拟货币来达成共识.虚拟货币的引入会降低共识达成速度且不适用于无

人机身份认证的网络环境.EPOH 方案将采用联盟链，并通过流量统计选举机制来替代上述方案所采用的权益证明选举机制，从而摆脱区块链对虚拟货币的依赖，同时利用连续哈希证明技术来加快共识达成速度.

## 2 系统模型

EPOH 的认证模型如图 1 所示，系统主要由无人机群和边缘节点两部分主体组成.

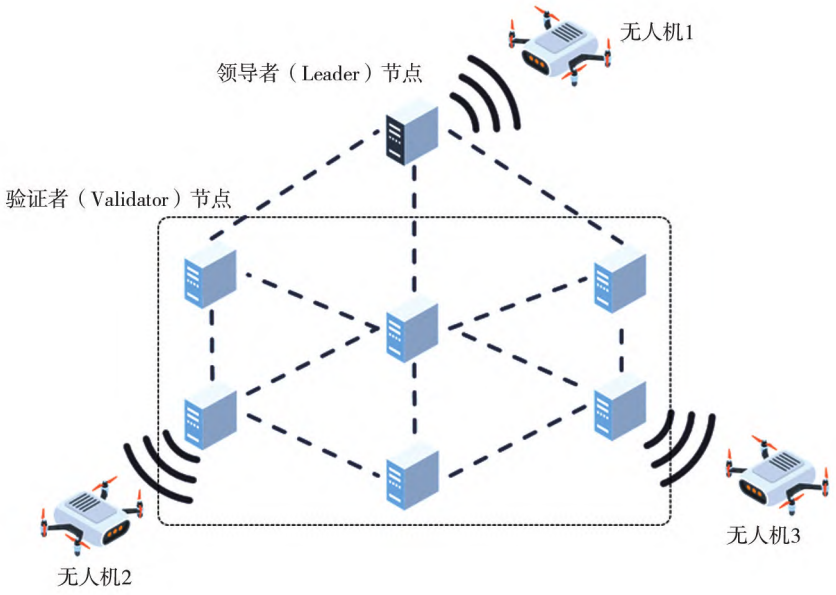


**图 1 EPOH 系统模型图**

Fig.1 EPOH system model diagram

无人机群：作为 EPOH 中的用户设备.当无人机与认证方案通信时，会有一个相应的区块链节点（即边缘节点）接受并处理无人机的通讯内容.每个无人机需要存储区块链节点的公钥（*PKNode*）、订阅者身份（*SUPI*），以完成身份验证和密钥协议过程.

边缘/认证节点：认证节点作为负责使 EPOH 维持运行的群体，负责存储链上数据，并与其他节点一起构建出完整的认证方案.

从节点功能的角度上来说，每个边缘节点会接收到自己信号范围内无人机的讯息，处理无人机在注册阶段、密钥生成、身份认证等阶段的用户请求.不同的边缘节点设备在硬件设备层面是平等的.但在具体认证过程中，边缘节点会涉及到领导者节点（Leader）和验证者节点（Validator）的分化和选举.其中，领导者节点负责创建新的区块，并确保这些事务按照正确的顺序被添加到历史记录中，并将这些区块广播给网络中的其他节点.验证者节点是网络中的普通节点，它们负责验证领导者节点创建的区块和事务.验证者节点首先会检查区块中的事务是否符合网络的规则和协议，之后验证者节点会通过自己的历史记录来验证区块的完整性和一致性.

从数据存储的角度上来说，每个认证节点都会在本地存储一份完整的历史区块链链上数据，并通过协作，不断地同步新的用户交易数据到区块链，完成认证方案的运转.

## 3 历史工作证明（PoH）

大部分共识算法中会涉及到时钟同步机制，不同设备需要通过时钟同步来确定交易记录的顺序，但这会导致交易过程中的巨大时延.而 Solana 所采用的历史工作证明（PoH）算法提供了一种可以直接确定两个事件之间发生次序的方法，以此来取消时钟同步环节，从而大大提高共识达成速度.

PoH 核心为构造事件次序证明，工作原理如下，从某个随机起始值运行哈希函数并获取对应的输出并将其作为输入再次传递给哈希函数，从而进行连续哈希运算.记录该函数被调用的次数以及每次调用的输出.选择的起始随机值可以是任何字符串，如表 1 所示.

**表 1 节点构造时间流逝证明**

Tab.1 Node construction of proof of time elapsed

| 计数 | 哈希运算 | 结果 |
|---|---|---|
| 1 | *Sha*256(“任意值”) | 哈希 1 |
| 2 | *Sha*256(“哈希 1”) | 哈希 2 |
| 3 | *Sha*256(“哈希 2”) | 哈希 3 |
| 4 | *Sha*256(“哈希 3”) | 哈希 4 |
| 5 | *Sha*256(“哈希 4”) | 哈希 5 |
| … | … | … |

由于哈希函数的抗冲突性,哈希值只能由单个计算机线程按顺序计算.比如计数 5 处的哈希值无法预测,只能从起始值实际运行算法 5 次之后推算出计数 5.因此可以从数据结构推断出计数 5 在时间次序上一定发生在计数 1 之后,即计数 1 和计数 5 之间有真实时间的传递.

该哈希序列还可用于记录在生成特定哈希计数之前创建的某些数据.使用“组合”函数将数据片段与当前计数处的当前散列组合起来.下一个生成的哈希值在插入特定数据后才能生成,因此可以表示为数据的时间戳,作为事件发生的证明,如表 2 所示.

**表 2 事件发生记录**

Tab.2 Event occurrence record

| 计数 | 哈希运算 | 结果 |
|---|---|---|
| 1 | *Sha*256(“任意值”) | 哈希 1 |
| 200 | *Sha*256(“哈希 199”) | 哈希 200 |
| 300 | *Sha*256(“哈希 299”) | 哈希 300 |
| 316 | *Sha*256(“哈希 315”,数据 1 哈希) | 哈希 316 |
| 400 | *Sha*256(“哈希 399”) | 哈希 400 |
| 500 | *Sha*256(“哈希 499”) | 哈希 500 |
| 600 | *Sha*256(“哈希 599”,数据 2 哈希) | 哈希 600 |
| 700 | *Sha*256(“哈希 699”) | 哈希 700 |
| … | … | … |

在表 2 表示的序列中,事件 1 携带的数据(数据 1)是在哈希 316 之前创建的,事件 2 携带的数据(数据 2)是在哈希 600 之前创建的.此时,数据的哈希结果会和前一计数的哈希结果一同构建出当下计数的哈希结果.因为初始过程仍然是连续的,所以可以推出输入序列的事物一定是在计算未来的哈希值之前的某个时间发生的,即事件 1 一定发生在计数 315 到计数 316 之间的计算过程中,事件 2 一定发生在计数 599 到计数 600 之间的计算过程中.通过观察该序列的记录便可以确定所有事件插入的顺序.

## 4 基于高效历史工作证明区块链的无人机身份认证方案

### 4.1 高效历史工作证明算法(EPOH)

在 PoH 中,节点的身份选举需要依赖虚拟货币来完成,不适用于无人机身份认证等物联网络环境下.故本文基于 PoH 算法,提出一种新的共识算法——高效历史工作证明算法(Efficient Proof of Historical Work, EPOH).

EPOH 共识算法包括两个部分,领导节点选举环节和节点达成共识环节.

#### 4.1.1 领导节点选举环节

每一台节点设备都将不间断地进行 PoH 算法中的连续哈希运算.如图 2 所示,1 600 次哈希为一个 Slot,4 个 Slot 为一次领导者节点的工作时间轮次(Round).在 EPOH 中,节点无需竞争记账权,而是在一轮次的时间段内,区块链网络通过统计上一轮次时间段内不同节点转发的交易数来选出领导者节点.在轮次即将结束时,由向领导者节点提交转发量最多交易的节点(或领导者自身)来担任下一轮次的领导者节点,以此来最大限度地提升通讯效率.

考虑到区块链的去中心化特性,如果一个节点连续 6 轮担任领导者节点,那么它将进入一段冷却期,在未来 2 轮次内,交易数量统计将会忽略该节点.

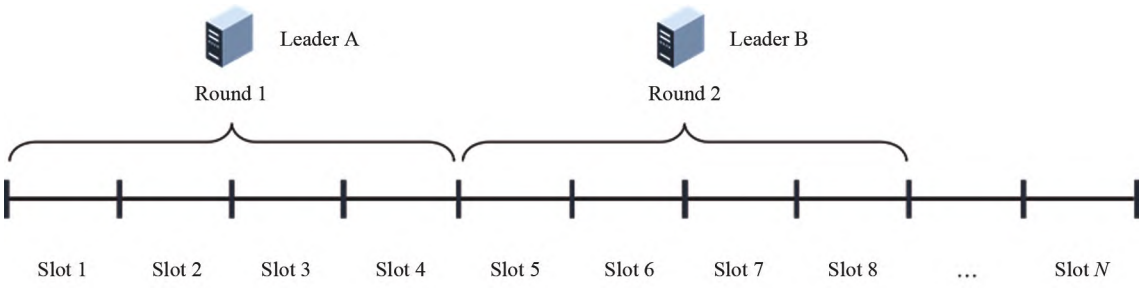


**图 2　领导者节点工作轮次示意图**

Fig.2　Diagram of the working rounds of leader nodes

4.1.2　达成共识环节

首先，Leader 节点在进行连续哈希运算的同时，时刻负责收集网络内任意节点接受到的无人机数据.以 Leader 节点在其工作轮次内共接受到 2 次用户数据为例，如图 3 所示.

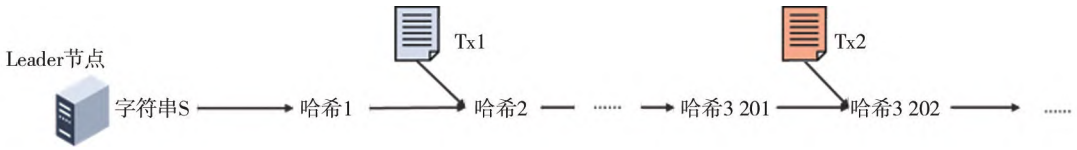


**图 3　领导者节点生成事件证明哈希序列示意图**

Fig.3　Schematic diagram of the leader node generating a hash sequence of event proofs

Leader 节点分别在哈希 1 到哈希 2，以及哈希 3 201 到哈希 3 202 过程中接收到了无人机的传输数据事件，分别为 Tx1 和 Tx2.从发生次序上来说，哈希 3 202 一定发生在哈希 2 之后，故 Tx2 在区块链中的记录一定位于 Tx1 之后，而整条哈希结果链就是 Leader 节点的记录事件的证明.且这一过程无法被并行加速，即顺序地从哈希 1 执行到哈希 6 400 仅可在单个处理器的单核内顺序执行.这是因为，即使强行将这一过程并行处理，由于其他核心需要等待自己工作计数的前一次计数的哈希值才能开始工作，故这一单核连续哈希过程无法并行加速处理.

接下来，Leader 节点将发布生成的哈希序列交由 Validator 节点验证.对于 Validator 节点来说，可以使用多核处理器并行验证该序列是否正确，所用的时间比生成该序列所需的时间要少得多，如图 4 所示.

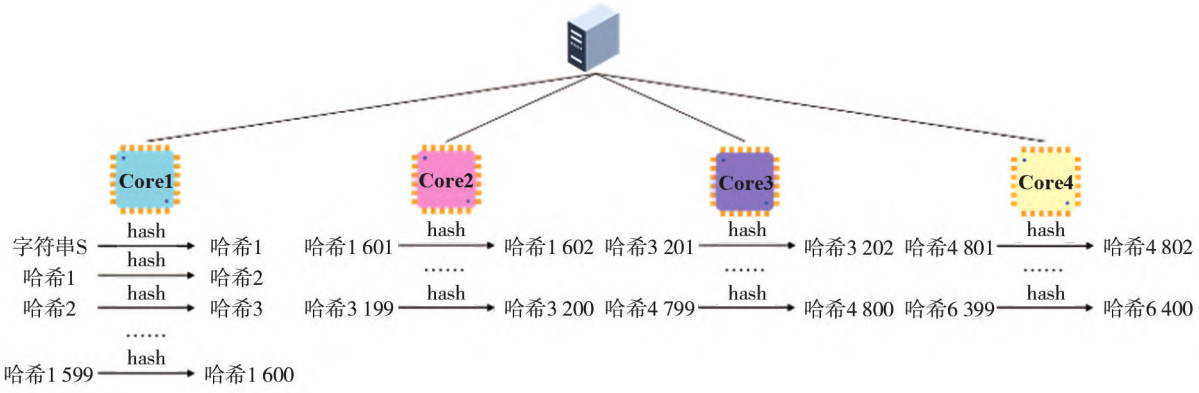


**图 4　区块生成与区块验证对比**

Fig.4　Comparison of block generation and block verification

在图 4 中，以 4 核心的 CPU 为例.作为验证者，可以将已经存在的待验证序列根据自身 CPU 核心数将结果分成 4 个切片，并可以并行执行，只需确保每个切片从起始哈希到最后一个哈希都是正确的切片，即可完成验证.且核心数越多的 CPU 在进行验证时，越能大大缩短验证速度.二者的用时分别为：

生成哈希序列的预期时间 $t_c$ 为：

$$t_c = \frac{N}{n_p}. \tag{1}$$

式中，$N$ 为所需的哈希总数，$n_p$ 是一个核心每秒能进行的哈希次数.验证序列是否正确的预期时间 $t_v$ 为：

$$t_v = \frac{N}{n_p \times n}. \tag{2}$$

式中,$n$ 为用于计算的 CPU 拥有的核心数量.由公式(1)和公式(2)可知,验证者的验证用时 $t_v$ 要大大小于生成序列 $t_c$,其缩减倍数便为验证者节点的核心数量 $n$.

### 4.2 认证流程

EPOH 为联盟链网络来代替传统的中心化认证机构.从数据存储的层面讲,中心化认证机构存储的用户数据将保存至分布的认证节点上,同时各认证节点在 EPOH 中将作为区块链网络中的节点,即面向无人机的边缘节点.

系统包括初始化阶段、认证和密钥协商阶段.

#### 4.2.1 系统初始化阶段

该阶段无人机需要预先注册的信息为身份 $SUPI$ 和长期对称密钥 $K$.但接收注册信息的服务模块均在区块链节点上,为分布式结构.节点在收到无人机的预注册信息后,会将注册信息打包在区块内,和其他节点一起同步在链上,用于后续身份验证.

同时,认证节点需要生成一对非对称密钥,用于和用户设备协商会话密钥,生成后无人机将保存节点公钥 $PKNode$.具体方法如下:

(1) 私钥生成:节点选择一个椭圆曲线 $E(Fp)$和基点 $G$,设私钥 $SKNode$,满足 $1<SKNode<order(G)$.

(2) 公钥生成:公钥 $PKNode$ 为基点 $G$ 的 $d$ 倍,即 $Q=dG$.

加解密示例为:

关于加密,设要加密的消息为 $M$,接收公钥为 $PK$.加密过程包括一个临时随机数 $k$,然后计算 $k$ 倍的基点 $G$ 以及 $k$ 倍的接受者公钥 $PK$,然后将 $M$ 与 $kQ$ 进行点的加法运算.加密的表达式为:

$$C=(kG, M+kQ). \tag{3}$$

关于解密,接收者使用自己的私钥 $SK$ 来解密消息,接收到密文 $C$ 后,使用私钥 $SK$ 将密文中的 $kQ$ 取消,然后得到原始消息 $M$.解密的表达式为:

$$M=M+kQ-d(kG). \tag{4}$$

式中,加密中的 $kG$ 是椭圆曲线上的点的倍乘,而解密中的 $d(kG)$是私钥与 $kG$ 的点乘运算.

#### 4.2.2 认证和密钥协商阶段

系统认证过程如图 5 所示,部分符号说明如表 3 所示.

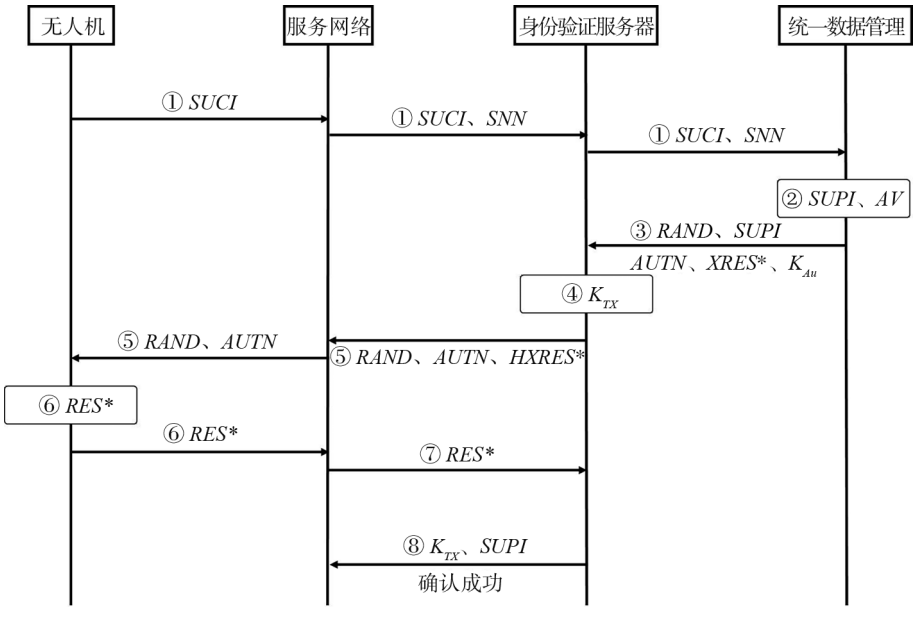


**图 5 无人机身份认证流程图**

Fig.5 Drone identity authentication flowchart

**表 3 部分符号说明表**

Tab.3 Partial symbol description table

| 符号 | 解释 |
|---|---|
| $SNN$ | 服务网络名称(服务代码 ‖ $SNId$) |
| $AMF$ | 16 位认证管理字段 |
| $RAND$ | 128 位随机挑战 |
| $SQN$ | 48 位序列号,根序列号 $sqn$ 在用户初始化时生成 |
| $K$ | 共享长期密钥 |
| $f1—f5$ | 单向函数 |
| $XRES$ | 预期响应 |
| $CK$ | 保密性密钥 |
| $IK$ | 完整性密钥 |
| $AK$ | 匿名密钥,用于隐藏序列号 $SQN$ 值 |
| $AUTN$ | 认证令牌 |
| $MAC$ | 验证消息的正确性,以实现用户对网络的认证 |

(1) 首先无人机通过以下公式将 $SUPI$ 加密得到其临时身份 $SUCI$:

$$SUCI = enc((SUPI, \sim R), PKNode). \tag{5}$$

式中,~为取反运算,然后无人机将带有 $SUCI$ 的注册请求发送到服务网络模块.服务网络模块将 $SUCI$ 与 $SNN$ 传输到身份验证服务器.身份验证服务器认证通过检查服务网络列表来获取 $SN$.成功后,身份验证服务器向智能合约发送认证请求.

(2) 智能合约使用注册身份解密功能($SIDF$)解密 $SUCI$ 以检索 $SUPI$.然后,智能合约根据以下公式生成认证向量 $AV$ 发送到身份验证服务器(其中,$KDF$ 是 TS 33.220[20] 中规定的密钥导出函数):

$$AV = RAND \| K_{Au} \| AUTN \| XRES^*, \tag{6}$$

$$RES^* / XRES^* = KDF((CK, IK), (SNN, RAND, RES/XRES)), \tag{7}$$

$$XRES = f2(K, RAND), \tag{8}$$

$$CK = f3(K, RAND), \tag{9}$$

$$IK = f4(K, RAND), \tag{10}$$

$$MAC = f1(K, SQN \| RAND), \tag{11}$$

$$AUTN = SQN \oplus AK \| AMF \| MAC, \tag{12}$$

$$K_{Au} = KDF((CK, IK), (SNN, SQN \oplus AK)). \tag{13}$$

然后 $AV$ 和 $SUPI$ 将被发送到身份验证服务器作为认证数据响应.

(3) 身份验证服务器存储 $XRES^*$、$SUPI$ 和 $K_{Au}$,由公式(7)生成 $XRES^*$($HXRES^*$),并由以下公式计算 $K_{Tx}$(会话密钥):

$$K_{Tx} = KDF(K_{Au}, SNN). \tag{14}$$

(4) 身份验证服务器暂存 $K_{Tx}$,然后将 $RAND$、$AUTN$ 和 $HXRES^*$ 作为认证消息发送到服务网络模块,服务网络模块存储 $HXRES^*$ 并向无人机发送 $RAND$ 和 $AUTN$.

(5) 无人机将从 $AUTN$ 获得的 $MAC$ 进行比较.一旦验证成功,无人机计算 $RES^*$ 和 $K_{Tx}$,并将 $RES^*$ 发送给服务网络模块以隐式证明 $K_{Tx}$ 的所有权.

(6) 服务网络模块由公式(7)计算 $RES^*$($HRES^*$)并检查它是否与存储的 $HXRES^*$ 匹配.当 $HRES^*$ 等于 $HXRES^*$ 时,$RES^*$ 被发送到身份验证服务器进行验证.

(7) 身份验证服务器比较 $RES^*$ 和 $XRES^*$,如果当 $RES^*$ 等于 $XRES^*$ 时,将认证结果 $SUPI$ 和 $K_{Tx}$ 发送至服务网络模块.

(8) 无人机在接收到认证成功的消息后,根据相同的步骤计算 $K_{Tx}$.

## 5 安全分析

### 5.1 会话安全

本方案引入了椭圆曲线密码学来实现会话密钥 $K_{Tx}$ 的构建.攻击者若想破解出密钥,需要达成以下目标:

$$t < M_t. \tag{15}$$

式中,$t$ 为解密 $kQ=P$ 所需的时间,$M_t$ 为可接受的最长破解时间.由于在给定椭圆曲线上的两个点 $P$ 和 $Q$ 的情况下,寻找一个整数 $k$ 使得 $kQ=P$ 是非常困难的,通过遍历所有可能性来找到正确的密钥 $k$ 需要不切实际的时间.并且攻击者尝试通过遍历猜测密钥 $k$ 的概率可以表示为:

$$P(guessingk)=\frac{1}{order(G)}. \tag{16}$$

式中,$order(G)$是曲线的阶,这个数值通常非常大,且随着 $order(G)$的增加,攻击者的时间开销将会呈指数上升,我们将会在实验分析中验证这一点.

### 5.2 共识机制安全

对于分布式的区块链网络来说,攻击者如果想胁持整个网络并随意篡改全网数据,就需要以一己之力挑战全网节点.对于 PoW 算法来说,攻击者需要拥有超过全网 51%的算力;对于 PoS 算法来说,攻击者需要有超过全网 51%的虚拟代币;对于 EPOH 来说,攻击者需要从分叉节点开始,以更快的哈希速度生成相较主链更长的侧链.

具体的攻击过程为:攻击者想要篡改已经记录上链的某段历史数据,但篡改此处的数据后,由于后续数据的哈希值是由原数据生成的,这势必会导致验证者节点检查不通过.故攻击者需要有单核性能超过全网任何一台节点设备的 CPU 来重新生成后续哈希,否则将永远无法生成更长的侧链.同时,正是由于 EPOH 的哈希结果只能由单个计算机线程按顺序计算,故无法做到并联多台强大的多核 CPU 或 GPU 设备来加速这一过程,并且这一特性不会随着摩尔定律而发生改变.

如攻击者确实企图使用相较于任何一个网络节点都更强大的处理器来进行分叉攻击,这一点 EPOH 将采用类似 PoS 中防御长程攻击的策略,即全网节点会周期性地检查最新的区块,将当下的工作中心聚焦于最近 4 *round* 区块内,并拒收那些重组了过分久远的记录的区块.

## 6 实验分析

实验分析将从 EPOH 的性能和安全两个方面展开.性能方面,实验将对区块链的交易吞吐量(TPS)、交易延迟和引入椭圆曲线加密对时间开销的影响进行分析;安全方面,实验将对无人机通讯密钥的安全性进行测试,同时对共识机制的安全性进行分析.

### 6.1 性能测试

#### 6.1.1 TPS 性能和交易延迟

为了对系统的 TPS 性能进行测试,本文使用 go 语言搭建了一条本地区块链,其运行环境为一台搭载了 R7-5800H CPU 的计算机,RAM 为 16 GB,操作系统为 Windows 11 23H2.实验将选取主流 CPU 频率范围(2.0~3.2 GHz),来模拟在不同节点设备环境下,EPOH 的 TPS 性能和交易延迟性能的表现.测试内容为:模拟无人机消息发送、领导者节点接收并打包消息(生成包含 6 400 条数据验证信息的区块),以及验证者节点验证新区块的三个过程,测试的结果如图 6 所示.

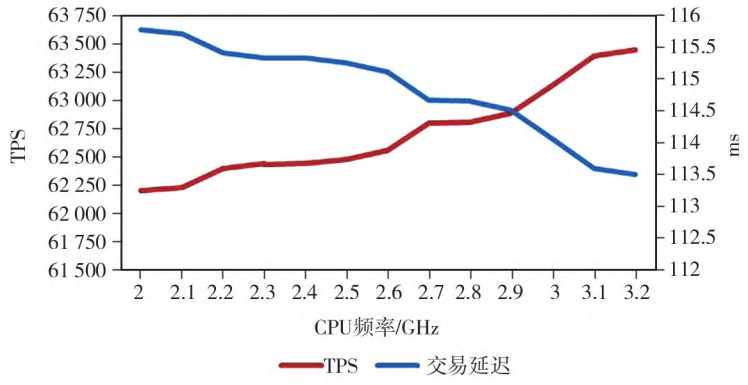


**图 6 CPU 频率和 TPS、交易延迟关系图**

Fig.6 Relationship between CPU frequency, TPS, and transaction latency

根据结果显示，在不同 CPU 频率下，TPS 性能范围为 62 197～78 797 TPS.交易延迟受到的影响较小，不会出现较大偏差，交易延迟范围为 113.5～115.8 ms.接下来将不同性质网络的信息处理效率和交易延迟情况进行对比，结果如表 4 所示.

**表 4　各交易网络 TPS 对比**

Tab.4　Comparison of TPS for various transaction networks

| 交易网络 | 共识算法 | 每秒能处理的交易数量/TPS | 交易延迟/ms |
|---|---|---|---|
| 比特币网络 | PoW | 7 | 600 000 |
| 以太坊网络 | PoS | 15 | 15 000 |
| 文献[12] | 改进的 PoW | 66～120 | 5 000～9 000 |
| 文献[13] | Flexico | 1 000～2 500 | 11 000～15 000 |
| Solana | PoS+PoH | 50 000 | 500 |
| EPOH | EPOH | 62 197～78 797 | 114～116 |

其中，比特币网络和以太坊网络的 TPS 分别为 7 和 15[21]，交易延迟分别为 10 min[22]和 15 s[23].由此可见，虽然采用了 PoS 算法的以太坊网络相对于比特币网络有了巨大的提升，但仍不适用于搭建无人机等需要即时通信的网络.文献[14]针对 PoW 算法的出块间隔进行了调整，同时会对打包陈旧区块的矿工进行额外奖励.通过以上手段，PoW 区块链性能提升到了 66～120 TPS 的水平，交易延迟也有所缩短，为 5～9 s.但会进一步依赖虚拟货币来达成节点共识，且对于即时通信网络来说，其 TPS 性能需要进一步提高，交易延迟需要进一步缩短.文献[15]设计了一种双模式共识协议，其中双模式的含义为网络良好环境和网络延迟环境.当网络条件良好时，Flexico 会使用快速模式.在这个模式下，只有活跃节点参与共识过程，以此来减少参与共识的节点数量，从而降低通信复杂度，提高共识效率.该算法通过对双模式的引入，使区块链网络通信性能提升至 2 000～2 500 TPS，且可以在不涉及虚拟货币的情况下达成节点共识.但与高 TPS 相对应的是高延迟，随着交易数量的增加，网络的交易延迟也会随之增高，为 11～15 s.

Solana 区块链采用了结合 PoS 的 PoH 算法.PoS 算法用于选举出 Leader 节点.之后，由于 PoH 设计为无需精确的时钟同步，只求确保交易顺序的正确，故领导者节点可以快速出块，验证者节点可以快速验证.其 TPS 可达 50 000[19]，交易延迟也大为缩短，为 500 ms 左右.但其中的 PoS 算法涉及到虚拟货币的使用，PoH 中提高并发性的扩容设计不适用于无人机身份认证场景.EPOH 方案通过测试，证明了其在满足更加适用于无人机身份认证和密钥协商环境的情况下，实现了区块链网络的高性能.实测性能可达 62 197～78 797 TPS.同时，EPOH 的交易延迟也达到了极低的水平，为 114～116 ms.

#### 6.1.2　椭圆曲线加密时间开销

EPOH 方案在无人机密钥协商环节引入了椭圆曲线加密技术，因此，实验接下来将测试椭圆曲线的引入是否会对时间开销产生较大的影响.首先，为了计算不同椭圆曲线阶数($p$)下的加密时间成本开销，实验将对 EPOH 分多组进行实验，每组采用不同的 $p$ 值，以得出不同阶数对应的椭圆曲线对加解密时间开销的影响曲线，结果如图 7 所示.

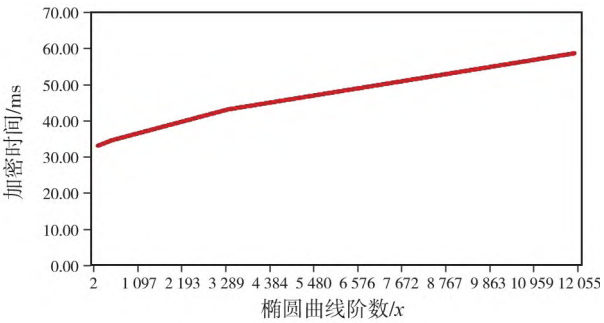


**图 7　椭圆曲线阶数和加解密时间开销关系图**

Fig.7　Relationship between elliptic curve order and encryption/decryption time overhead

从图中可知，随着椭圆曲线阶数 $x$ 的增加，所需的加密时间开销 $y$ 会有所上升，但整体维持在小于 0.1 s的水平.因此，椭圆曲线加密技术的引入虽然会对整体通讯效率产生一定的影响，但系统仍然可以保持在可用的范围内.

### 6.2　安全测试

#### 6.2.1　会话安全

EPOH 系统采用椭圆曲线加密技术来构建会话密钥 $K_{Tx}$.为了证明在时间上，攻击者通过遍历方法破解会话密钥 $K_{Tx}$ 是不可行的，我们进行了会话密钥安全性分析实验.实验测试了在不同阶数($p$)的椭圆曲线下，通过遍历破解的方法来测试所需的时间成本.为了直观地对比正常使用秘钥解密和暴力破解所需时间的差

距,本文做了二者在椭圆曲线不同阶数的情况下所需的时间对比图(图 8).

由实验结果可知,随着所选的椭圆曲线阶数的增加,对正常解密所需时间开销的影响极小(从 0.038 3 s增至 0.048 8 s).但通过遍历的方法来破解密钥的难度则会呈指数增加(所需时间从 0.000 3 s 增至2 050.87 s).即随着椭圆曲线阶数的增加,正常无人机和节点的通信效率受到的影响极小,但攻击者采用暴力破解的方式遍历会话密钥 $K_{Tx}$ 在时间层面则会越来越不现实.

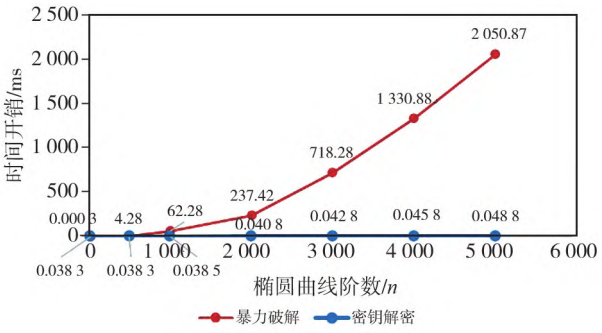


**图 8 暴力破解和密钥解密时间开销对比图**

Fig.8 Comparison chart of time overhead for brute force cracking and key decryption

6.2.2 共识机制安全

在共识机制安全的章节中,本文讨论了攻击者会企图使用相较于任何一个网络节点都更强大的处理器来进行分叉攻击的情况.为了验证共识机制的安全性,我们模拟了这一场景.

实验首先通过在不同 CPU 频率环境下运行 EPOH 哈希,得出不同 CPU 频率对应的哈希速度折线图,结果如图 9 所示.

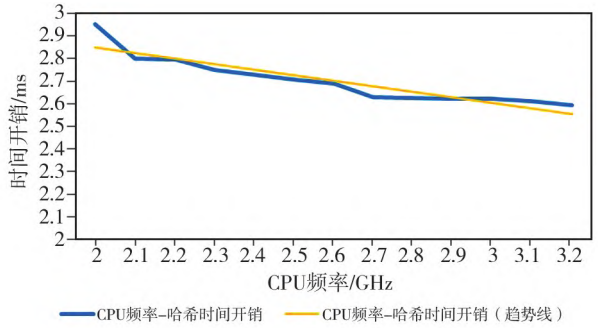


**图 9 CPU 频率和 CPU 哈希运算时间开销关系图**

Fig.9 Relationship between CPU frequency and CPU Hash operation time overhead

由图像可得,随着 CPU 频率的增加,所需的哈希时间也会相应减少,但总体处于 2.7 ms 的水平.通过计算得出 CPU 频率 $x$ 和哈希时间开销 $y$ 的趋势线为:

$$y = -0.244\ 8x + 3.338\ 2. \tag{17}$$

接下来将模拟攻击者选取了超出网络节点平均处理器性能来进行分叉攻击的实例.以 3.2 GHz 的 R7-5800H 处理器作为攻击者,2.3 GHz 的 i5-8300H 处理器作为正常节点平均 CPU 频率的参考,攻击者链长度落后主链 1 *round* 为例.二者哈希速度分别为 2.594 3 和 2.751 1 ms,则作为攻击者的 R7-5800H 至少需要经历 14 *round* 才可以产生超出主链的支链.

目前 CPU 单核最高频率可达 4.2 GHz,若攻击者设备的 CPU 性能可达 4.2 GHz,而 2.0 GHz 为节点设备的平均 CPU 频率.根据 CPU 频率和哈希时间开销的拟合曲线可得,即便如此攻击者也至少需要 5 *round* 才可以产出超出主链的支链.对此,EPON 仅接受 4 *round* 范围内的待认证区块,超出该范围的待认证交易将会被验证节点拒绝;且攻击者在实际情况中的起始区块高度会远大于 1 *round*,故攻击者几乎没有分叉链条的可能.

## 7 结论

本文提出了一种新型的基于高效历史工作证明算法(EPOH)的无人机身份认证方案——EPOH,为区块链技术在无人机网络中的应用提供了新的视角和解决方案.

实验结果表明,EPOH 不仅提高了交易处理速度,而且保证了网络的去中心化特性和安全性,可适用于需要高效率和高安全性的多种区块链应用场景.EPOH 针对现有区块链技术的局限性,特别是在资源消耗、交易费用、吞吐量和确认延迟方面进行了显著改进.然而,EPOH 在某些方面,如数据隐私保护,仍需探索新的安全机制以应对不断变化的安全威胁.

**参考文献:**

[1] ZHANG L, XU J, OBAIDAT M S, et al. A PUF-based lightweight authentication and key agreement protocol for smart UAV networks[J]. IET Communications, 2022, 16(10): 1142-1159.

[2] 朱辉,张业平,于攀,等.面向无人机网络的密钥管理和认证协议[J].工程科学与技术,2019,51(3):158-166.
ZHU H, ZHANG Y P, YU P, et al. Key management and authentication protocol for UAV network[J]. Aduanced Engineering Sciences, 2019, 51(3): 158-166.
[3] 张歌,苏路明.区块链技术多场景应用述评[J].河南大学学报(自然科学版),2022,52(3):320-328.
ZHANG G, SU L M. Review on multi-scenario applications of blockchain technology[J]. Journal of Henan University (Natural Science), 2022, 52(3): 320-328.
[4] TRIPATHI G, AHAD M A, CASALINO G. A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges[J]. Decision Analytics Journal, 2023: 100344.
[5] ANDREW J, ISRAVEL D P, SAGAYAM K M, et al. Blockchain for healthcare systems: Architecture, security challenges, trends and future directions[J]. Journal of Network and Computer Applications, 2023, 215: 103633.
[6] NASIR N M, HASSAN S, ZAINI K M. Securing permissioned blockchain-based systems: An analysis on the significance of consensus mechanisms[J]. IEEE Access, 2024.
[7] TANG F, XU T, PENG J, et al. TP-PBFT: A scalable PBFT based on threshold proxy signature for IoT-blockchain applications[J]. IEEE Internet of Things Journal, 2023.
[8] GAO Z, ZHANG D, ZHANG J, et al. Bc-aka: Blockchain based asymmetric authentication and key agreement protocol for distributed 5G core network[J]. China Communications, 2022, 19(6): 66-76.
[9] IRRESBERGER F, JOHN K, MUELLER P, et al. The public blockchain ecosystem: An empirical analysis[J]. NYU Stern School of Business, 2023.
[10] KARAME G. On the security and scalability of bitcoin's blockchain[C] //Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. 2016: 1861-1862.
[11] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system[J]. Decentralized Business Review, 2008.
[12] BAJRA U Q, ROGOVA E, AVDIAJ S. Cryptocurrency blockchain and its carbon footprint: Anticipating future challenges[J]. Technology in Society, 2024, 77: 102571.
[13] KING S, NADAL S. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake[J]. Self-published paper, August, 2012, 19(1).
[14] KIM H, KIM D. Adjusting the block interval in PoW consensus by block interval process improvement[J]. Electronics, 2021, 10(17): 2135.
[15] REN S, LEE C, KIM E, et al. Flexico: An efficient dual-mode consensus protocol for blockchain networks[J]. PLoS One, 2022, 17(11): e0277092.
[16] ZHOU B, ZHAO J, CHEN G, et al. Security authentication mechanism of spatio-temporal big data based on blockchain [J]. Applied Sciences, 2023, 13(11): 6641.
[17] YAKOVENKO A. Solana: A new architecture for a high performance blockchain v0. 8.13[J]. Whitepaper, 2018.
[18] IVANOV M, JOHNSON E. A comprehensive review of decentralization technologies in bitcoin, ethereum, and solana [J]. Advances in Computer Sciences, 2024, 7(1): 1-8.
[19] MARTIN S. Decentralized frontiers: A comparative study of bitcoin, ethereum, and solana technologies and challenges [J]. Journal of Innovative Technologies, 2024, 7(1): 1-5.
[20] 3GPP TS 33.220 v.14.0.0, 17, 12, 2016, Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)[S].
[21] ZHAO C, ZHANG S, WANG T, et al. Bodyless block propagation: Tps fully scalable blockchain with pre-validation[J]. Future Generation Computer Systems, 2024: 107516.
[22] ZHAO X, ZHANG G, SI Y W. An efficient dynamic transaction storage mechanism for sustainable high-throughput Bitcoin[J]. The Journal of Supercomputing, 2023, 79(13): 14388-14426.
[23] ALDYAFLAH I M, ZHAO W, UPADHYAY H, et al. The design and implementation of a secure datastore based on ethereum smart contract[J]. Applied Sciences, 2023, 13(9): 5282.

责任编辑:李园园