文章编号:1671-4598(2023)10-0153-07 DOI:10.16526/j.cnki.11—4762/tp.2023.10.024 中图分类号:TP391 文献标识码:A

基于区块链的分布式无人机数据安全模型

何 勇[1,2], 张航宇[1], 郭智鸿[1], 苏桐桐[1], 李 虎[1], 王凯乐[1]
(1. 中国电建集团西北勘测设计研究院有限公司 数字与智慧工程院, 西安 710065;
2. 西安市清洁能源数字化技术重点实验室, 西安 710065)

摘要: 针对无人机协同作业信息安全和数据通信问题, 提出一种基于区块链的分布式无人机数据安全模型; 首先, 利用轻量化加密技术重构无人机区块链结构, 设计适用于物联网边缘计算场景的分布式区块链网络模型; 然后, 调用智能合约实现区块链数据的安全共享, 并结合信誉评估方案和代理权益证明思想, 提出融合共识协议的工作量证明方法完成数据交易; 实验结果表明: 作为数据安全共享实例, 所提方法可使受攻击的无人机信誉值降至不可信任状态, 并在不同攻击模式下的能够有效抑制恶意攻击, 执行自适应工作量证明的共识算法的正常节点交易率可提升 3～4 倍, 为无人机数据共享提供了安全保障。

关键词: 区块链; 无人机; 数据安全; 自适应工作量证明

Data Security Model for Distributed UAV Based on Blockchain

HE Yong[1,2], ZHANG Hangyu[1], GUO Zhihong[1], SU Tongtong[1], LI Hu[1], WANG Kaile[1]
(1. Degital and Smart Engineering Div, NorthWest Engineering Corporation Ltd, Xi'an 710065, China;
2. Xi'an Key Laboratory of Clean Energy Digital Technology, Xi'an 710065, China)

Abstract: Focusing on the information security and data communication of UAVs cooperative operation, a data security model for distributed UAV based on blockchain is proposed. A blockchain structure of UAV is reconstructed by using lightweight encryption, and a distributed blockchain network model is designed that suitable for the edge computing scenario of the Internet of things. The smart contract to complete the secure sharing of blockchain data is deployed, and a consensus protocol of work proof is proposed to complete the data transaction that combining with the reputation evaluation scheme and the idea of proxy rights and interests proof. Experimental results show that as an example of data security sharing, the BC _ UAV can reduce the reputation value of the attacked UAV to an untrusted and effectively suppress malicious attacks under different attack modes, while the normal node transaction rate of the consensus algorithm with adaptive workload proof can be increased by 3～4 times, so that the model provides a security guarantee for UAV data sharing.

Keywords: blockchain; UAV; data security; consensus protocol of work proof (CP-WP)

0 引言

无人机通过与地面基站实时通信, 可为物联网提供一体化的智能服务, 已广泛应用于货运调度、应急救援、精准农业、电网巡检等领域[1]。与云计算场景不同, 分布在高空的移动无人机不依赖于集中式架构模式, 无需将终端请求汇集至云服务中心进行统一处理, 而是使用了大量边缘计算方法进行数据处理和分析[2-3], 保证了网络数据传输的稳定性。然而, 无人机作为物联网边缘层连接的终端设备[4], 命令和数据往往通过不受信任的信道进行传输[5-6], 在将数据通过低时延传输边缘层节点的同时带来了安全性差、防篡改性弱的问题, 容易受到 Sybil、DoS/DDoS、GPS 欺骗等网络攻击[7], 使无人机偏离计划航行或数据窃取。

为增强高空移动无人机的数据通信的安全性。近年来, 研究者开始尝试利用区块链技术解决无人机协同作业的信息安全问题[8]。区块链是一项起源于比特币的新兴技术[9], 它将数据区块按照时间顺序相连, 形成一个不可篡改的和去中心化的分布式账本。文献 [10] 在无人机群和传感器云之间设计了一个分布式支付系统, 将区块链用作分布式公共账本, 以确保数据的完整性、可追溯性和不可伪造性。但该方法占有空间较大, 终端设备产生的数据规模不断增长, 且忽略了无人机有限的计算荷载; 文献 [11] 提出了一种基于区块链的无人机数据采集方法, 使用一个内存高效的数据结构 π-哈希 bloom 过滤器来验证用户的身份验证, 并用集中记账方式记录区块之间的交易信息, 从而过滤恶意设备, 但该方法需要频繁地查找区块内容, 不可避免地使数据传输的延迟性有所提高; 文献 [12] 提出了一种基于区块链共识算法的无人机网络自主运行架构, 并采用图一致性进行有效性验证。但该方法不太适用于动态通信拓扑变化较大的物联网情景。为解决这些问题, 本文提出了

收稿日期:2022-12-16; **修回日期**:2023-02-01。
基金项目:中国电建集团西北勘测设计研究院有限公司信息化项目(NWE2021-020)。
作者简介:何 勇(1986-),男,在读硕士生,工程师。
张航宇(1996-),男,在读硕士生,助理工程师。
引用格式:何 勇,张航宇,郭智鸿,等. 基于区块链的分布式无人机数据安全模型[J]. 计算机测量与控制,2023,31(10):153-159.

一种基于区块链的分布式无人机数据安全模型 BC _ UAV，主要功能如下：

1）设计一种分布式区块链网络模型，该模型在边缘层节点和终端层无人机节点分别设置边缘层区块链和无人机区块链[13-14]，利用轻量加密技术重构区块链结构，以减轻无人机的数据计算荷载。

2）提出一种区块链数据安全传输方法。调用智能合约完成区块数据的安全传输，边缘层节点定期将无人机区块链中的交易数据以默克尔帕特里夏数树[15]（MPT，Merkle Patricia tree）的结构打包成区块发布到边缘层区块链上，利用时间戳信息并通过指针在无人机区块链上找到相应的数据交易位置。

3）提出一种融合共识协议的工作量证明算法[16]（CP-WP，consensus protocol of work proof）。结合信誉评估方案[17]，并利用代理权益证明[18]（DPoS，delegated proof of stake）思想，完成交易一致性协议，共同维护无人机之间账本数据的一致性和准确性。

1 系统架构

1.1 分布式区块链网络模型

为实现无人机与边缘层网关设备的安全通信，设计一种分布式区块链网络模型，主要由终端层、边缘层和控制层组成。如图 1 所示，层与层之间通过数据信息传输相互协作。其中：1）终端层由无人机组成，采用私有链技术形成无人机区块链网络，无人机通过与边缘层设备进行通信访问并交易数据，发布至无人机重构区块链上；2）边缘层由物联网中的网关节点组成，采用联盟链技术形成边缘层区块链，负责接收来自无人机的数据请求，并对无人机区块链中交易的合法性进行验证，使用私钥对验证结果进行签名，将验证结果打包交易发布至无人机区块链上，形成终端层无人机重构区块链的快照信息，以防止恶意终端无人机对区块链网络破坏，减少边缘节点存储空间；3）控制层由地面控制站和云服务器组成，定期对边缘层区块链数据进行备份、注册、授权等，无人机运用 5G 通信技术接入物联网边缘层设备中。

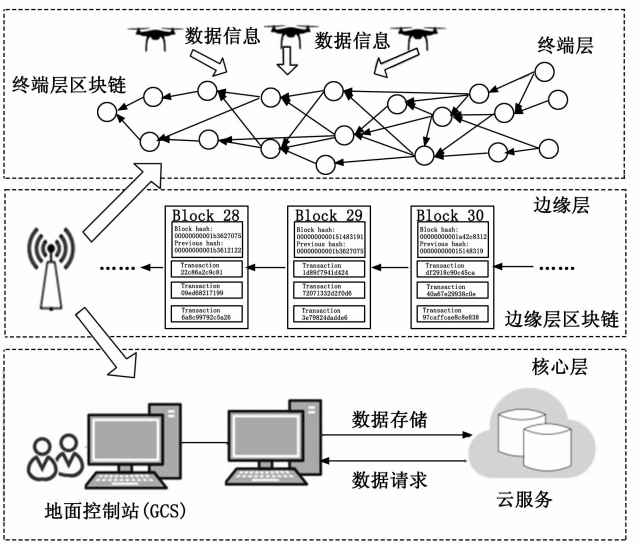

图 1 分布式区块链网络模型

1.2 重构无人机区块链结构

考虑无人机分布式区块链网络由轻量级和低能耗的物联网设备组成，要求这些设备拥有与比特币网络中的矿工同等的计算能力是不合理的，其不适用于大量数据交互场景，因此提出一个重构区块链架构，以减少无人机的存储空间和计算压力。

1）区块链结构。类似于比特币，共分为区头和区体两个部分。与传统的区块组合不同，重构区块链结构是针对轻量级物联网设备以及无人机之间的通信而定制的，利用轻量级密码技术 Keccak[19-20]重新定义所有交易数据，并保存于分布式账本中。如图 2 所示，重构区块链的块头包括当前块头哈希、前一块头哈希、信誉树根、策略列表、时间戳和事务树根等索引信息，主要依赖于共识协议算法指定节点以生成新的区块，每个节点都引用最新的策略来处理事务，一旦无人机存在诸如区块中列出的查询访问隐私数据，或者创建转发无效区块和交易的可疑行为，则重新计算每个无人机的信誉值。

2）工作方式。将整个系统的边缘层节点、终端层无人机和控制层服务器之间的通信格式化为事务，采用图 2 所示的事务信息结构，（1）无人机使用哈希函数对收集的数据进行计算并获得字长固定的索引信息，索引信息打包成交易事务后上传至无人机区块链上；（2）无人机区块链采用不可逆的交易单元组成，边缘层区块链主要是在每一个区块中存储无人机区块链的交易快照，其区块头存储指向前置区块的哈希指针和时间戳，块体包含以 MPT 结构存储于分布式账本的交易信息，用于快速检索和安全存储。

3）事务处理。边缘层区块链每隔一定时间戳会向无人机分发一对公钥和私钥，以允许其签署交易，表示上一个时间戳的所有交易被确认。这样，在分布式区块链网络模型中，向区块链系统添加新的无人机由系统自动创建，每台无人机的信誉值初始化为 $r=60$，信誉值会根据无人机实施的行为而变化。当命令事务启动时，要求无人机提供包括状态数据和图像数据数据，或向无人机设备发送控制命令并执行。否则，系统将修改策略列表以禁止与其通信，或将信誉值设置得更低以通知网络中的其他无人机取消该无人机的资格。在合法查询的前提下，一旦没有收到响应将启动报告交易，广播特定无人机的可疑活动。

与传统分布式区块链结构相比，利用轻量级密码技术 Keccak 减轻无人机的数据计算荷载，并在事务处理上自动创建新的无人机用户，将所有计算集中于边缘层节点上，提高了数据交易速度和检索速度。

2 数据安全共享

在分布式区块链网络模型的基础上，所有数据以重构区块的形式保存于分布式账本中，当无人机数据通过交易到达边缘层区块链时，需提供数据安全传输服务。

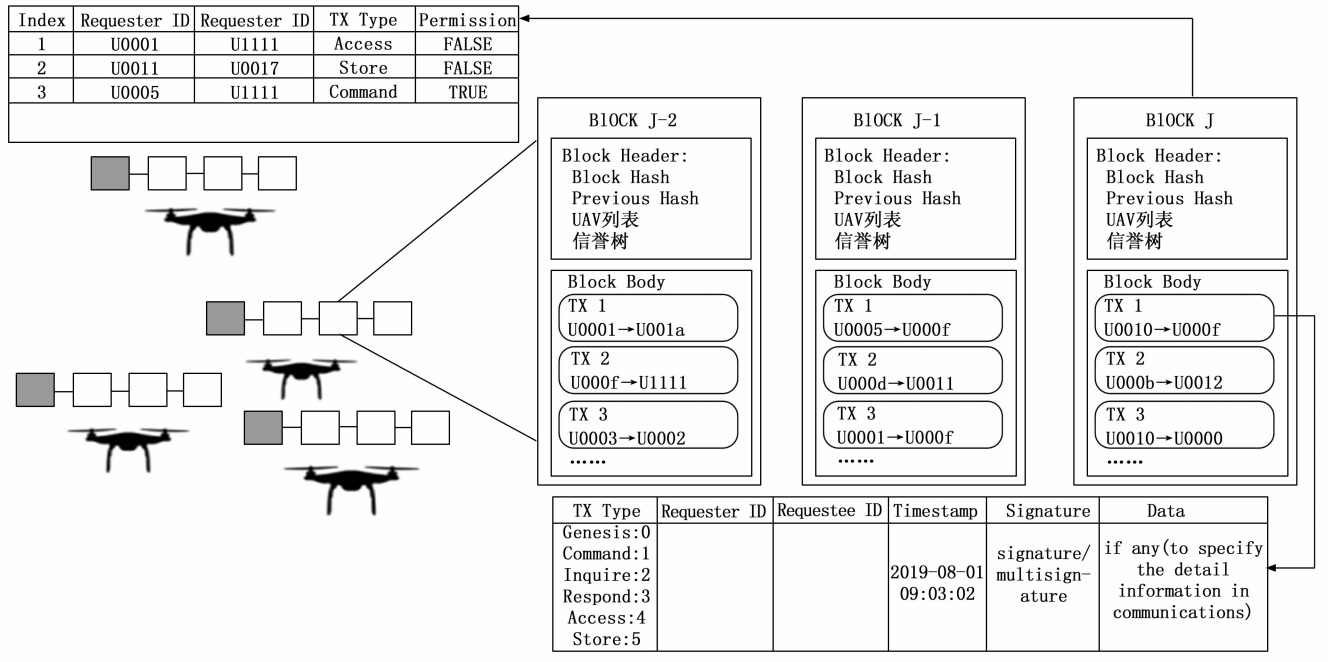

图 2　重构区块链结构和事务信息

2.1　智能合约过程

数据智能合约部署于重构无人机区块链上，无人机在当前物联网中设置的边缘节点上进行网络注册后，就可以调用该智能合约完成索引信息的安全传输，智能合约过程如图 3 所示。

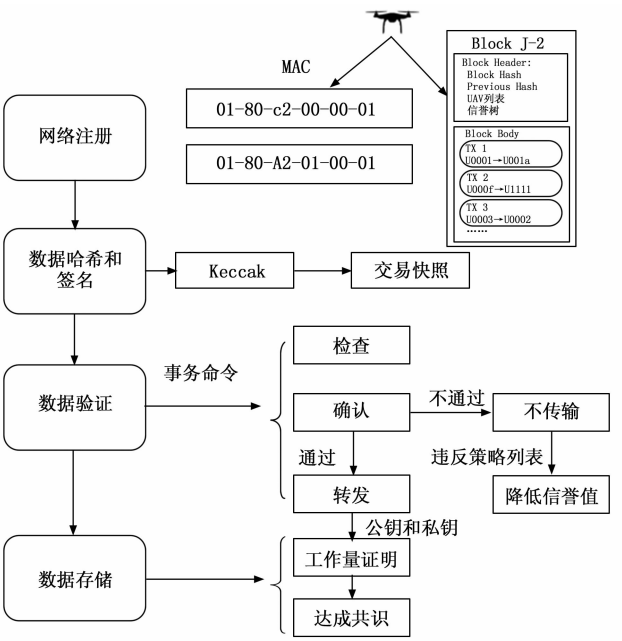

图 3　智能合约过程

1）网络注册。每个无人机都会根据其 MAC 地址创建一个私钥 ∂_m、最新时间戳 T_c 和随机散列值 $hbar$，通过注册加入无人机区块链网络，并预先加载一个策略指示数据传输操作。

2）数据哈希。每个无人机在发送消息之前都需要执行 Keccak 哈希函数，用于生成 JSON 格式序列化存储的交易快照。然后，无人机针对交易快照实施签名并打包形成交易，将交易内容作为输入参数，用于调用智能合约。

3）数据验证。由于调整无人机挖矿难度的贡献值是由边缘层节点对某一时间戳的交易进行数据验证，显式地在无人机区块链中输出。当边缘层节点在对等网络中接收到一个命令事务时，智能合约对交易内容实施检查，以此确认签名节点是否在边缘层中注册通过。然后，智能合约将确认后的消息反馈给无人机形成信誉值。如果验证通过，则将事务转发给邻居；否则，如果接收到的事务缺乏数据完整性，则将其视为错误且不传输，而如果接收到的事务违反策略列表，则接收方生成报告事务以通知网络中的其他无人机，并且将特定无人机的信誉值降低。类似地，成功报告恶意行为的接收者将获得声誉价值的增加。

4）数据存储。数据验证通过后，边缘层区块链会向无人机发送一对公钥和私钥，证明该交易的签名凭证，启动智能合约。智能合约将确认当前的数据存储是否与接收的交易存储地址匹配，如果匹配则表示数据存储完成。在智能合约中通知终端层节点执行共识协议，达成共识后则将该交易发布于重构无人机区块链中。

2.2　数据检索

在智能合约过程中，边缘层区块链节点将验证到的交易信息打包发布至边缘层上，其由多条单向链不可逆的形式进行存储，链上的每个区块代表该无人机在某一时间内发布的交易快照，并以 MPT 形式存储于块头，每个交易映射为 MPT 的叶子节点，其内容包括交易数据标签信息、信誉值以及交易哈希指针，该指针主要是指向终端层的交易。

MPT 中的两个子节点计算出一个父节点哈希值，将根节点的哈希值保存于区块头，最终形成一个哈希关联的二叉树。MPT 的模型结构如图 4 所示。

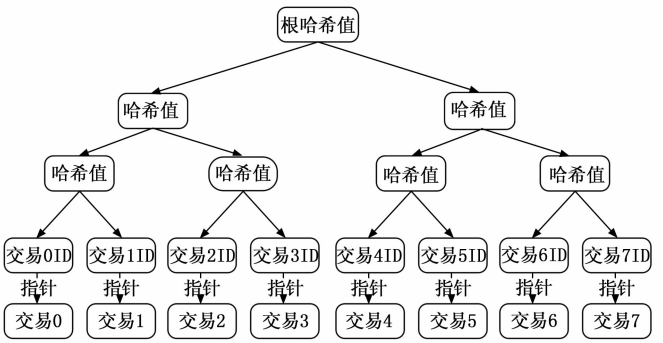

图 4 MPT 模型结构

分布式区块链网络模型中的数据检索主要是通过区块中的标签信息判断数据并发出请求，边缘层节点首先向前检查区块头中的时间戳并确认位置，然后从该区块头开始逐个遍历 MPT 子节点以及对应的信誉值，最后按照哈希指针找到对应的信誉值较高的交易，完成检索任务。通过这种检索方式，边缘层节点仅需对区块头进行验证，且边缘节点将无人机区块链中的交易以信誉值和时间顺序形成单向区块链，可以有效地降低遍历时间，减少计算荷载。

2.3 数据传输

不同区块链之间通过哈希指针完成区块验证，分布式区块链网络模型中的数据传输主要是边缘节点与无人机节点之间的数据交互行为，本文以联盟链 Hyperledger Fabri[21]为基础，该联盟链解决了传统方法中需要昂贵的挖矿计算来提交交易，可以在最短延迟时间内构建或扩展区块链，帮助无人机建立联盟许可的区块链网络，且多个无人机可以共享控制和操作边缘层网络节点的权限。同时，利用 gossip[21]数据传播服务将账本和通道数据传播给对等无人机节点，使授权的无人机以最快的时间连接到无人机区块链中，设一个边缘层节点 N_R 和一个终端层无人机节点 N_U。

1）N_U 作出一个区块传输请求，N_R 按照 Hyperledger Fabri 同步 N_U 管理的区块链，即 N_U 将当前区块请求以哈希指针方式指向自身区块链和 N_R 区块链。

2）N_U 通知 N_R 数据传输请求发生，N_R 响应后主动对应 N_U 的区块链，同步到该区块链后，N_R 取出快照信息并检索数据。若 N_R 为该快照数据的所属者，则输出 N_{Direct} 数据直接进行共享。若 N_R 为该快照数据的所属者，则 N_R 咨询 N_U 是否传输该数据快照给其他边缘层节点，经同意后采用公钥对传输数据加密。

3）N_R 通知边缘层区块链上节点，同步传输 N_U 的快照信息。

3 共识协议

3.1 信誉评估方案

使用信誉评估方案确保边缘层节点接收到无人机数据区块的有效性，减少区块验证的开销。信誉值表示无人机在其最近的生命周期中对区块链网络的贡献度，影响信誉值的因素主要是恶意操作、传播错误消息以及信息攻击等不合法交易。边缘层链上区块的交易快照中，无人机节点的信誉值以 MPT 的结构存储于块头，因此边缘层节点会定期对无人机区块链的交易进行数据验证，无人机需要根据验证交易中的内容自适应调整工作量证明算法难度，共同维护数据。以概率 P 选择接受请求或转发交易，概率 P 计算方式如下：

$$P_i=\begin{cases}1 & r\geqslant 10\\ \dfrac{\rho_1\cdot r}{\sum_{j=1}^{N} r_j\cdot C_i} & r\geqslant 60\\ \dfrac{\rho_2\cdot r}{\sum_{j=1}^{N} r_j\cdot C_i} & r\geqslant 60\end{cases}\tag{1}$$

式中，P_i 表示接受无人机 U_i 请求的概率，r_i 表示 U_i 的信誉值，C_i 表示 U_i 执行可疑操作的数量，ρ_1 和 ρ_2 表示无人机的协同系数分别为 $r\geqslant 60$ 和 $r<60$，初始化设置每个无人机节点的信誉值为 60，如果执行恶意操作，则该节点信誉值可能会降低，如果成功报告可疑无人机或恶意入侵信息，则信誉值可能会增加。因此，高信誉值有利于信息被接受和信任，但是一旦请求者的信誉值低于 20，相邻无人机将拒绝转发其发起的几乎所有交易。

3.2 共识协议实现过程

为增强边缘层节点数据交易，完成交易一致性协议，共同维护无人机之间账本数据的一致性和准确性，提出 CP-WP 方法。该方法主要是利用 DPoS 思想对工作量证明方法进行优化调整的过程，其核心是根据权益的多少随机选举一个委员，将边缘层节点视为矿工节点，具体实现过程如下：

1）根据边缘层节点获取的区块链结构，将数据交易中已签名的交易打包进入该区块以生成完整的区块体，形成 MPT。判断距上次难度的时间是否已产生 2 016 个区块，以获得新的难度位，从而获得新的数据区块并提高信誉值。

2）将时间划分为间隔相同的时间戳，利用信誉证明选举委员（参照 DPoS 思想），每个委员对应一个时间戳进行投票。

3）每个时间戳产生一个区块，处理一个请求交易事务，如果生成的区块未得到大多数边缘层节点的确认，则该时间戳内不会产生区块。

4）多个连续的时间戳形成一个窗口，如图 5 所示，设有 n 个窗口，边缘层节点生成区块头，该区块中编码了与无人机身份相关的一对公钥（pub_i）、权益 s_i 和随机数种子 ρ_i，后续每个窗口均会基于前一个窗口的基本数据运行，以区块头中的每个候选人所持有权益的概率，选择每个时间戳对应的委员 $U_k=F(S_n,\rho_n,r_k)$，其中 S_n 为窗口 n 中由所有候选人组成的集合 $(U_1,U_2,\cdots,U_n)$，ρ_n 为窗口 n 中使用的随机数种子，ρ_n 与当前窗口中每位候选人持有的权益 $(s_1,s_2,$

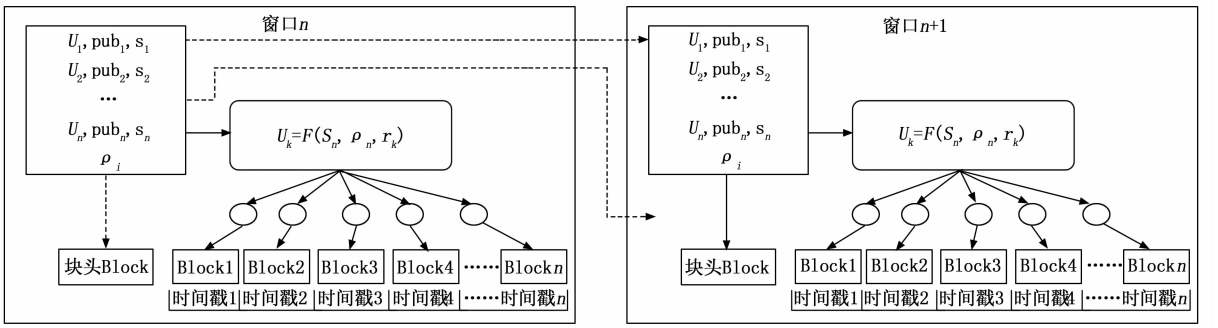

图 5　共识协议执行

…，s_n）有关，r_k 为为第 k 个时间戳对应的索引信息。根据随机数种子 ρ_n，函数 $F()$ 从候选人集合 S_n 中随机选出第 k 个时间戳对应的委员 U_k。

5）对于委员候选人，当刚好被选为该时间戳上的委员，则执行交易和广播工作，否则在边缘层节点上进行数据验证。当被选择的区块处于信誉值较低状态时，则不生成区块。这样，在不同时间戳内，不断地进行委员会选举并验收数据的过程，直到窗口结束后会生成相应的委员，从而实现每个时间戳内选举的随机性，确保委员的选择不会被攻击者操纵。例如，当网络中一个无人机突然发现自己在没有预期的情况下进入或接近禁飞区时，它有理由怀疑受到攻击，并立即生成选举事务，将攻击情况与其他节点进行比较，一旦它们彼此不匹配，则无人机就极有可能受到攻击，此时无人机就启动警报事务，通知邻居无人机节点采取预防措施来降低风险。

6）边缘层节点对接收的新区块进行验证，如果验证通过则将新区块添加到主区块链上，并继续挖矿直到符合要求的区块产生。最终，在边缘层节点的区块中写入交易信息，形成关于边缘层的分布式一致性账本。

4　实验分析

针对 BC _ UAV 模型，本文采用 10 个无人机高空数据采集作为实验数据进行分析，无人机初始状态为随机分布，整个系统形成一个全网状或半网状拓扑局域网，通过自组网可以相互通信，从而可以进行信息资源共享与交换。这些无人机节点通过连接和继承不同边缘层节点的接口实现操作，以此维护分布式无人机数据安全。

利用 UB-ANC 仿真器[22]在不同攻击模式下说明其有效性，UB-ANC 仿真器是一种基于 ns-3 技术的多智能体无人机网络模拟器，每个无人机的数据传输率为 1 Mbps。实验环境为 3.1 GHz Intel Core i7 CPU，内存 16 G，操作系统 Windows 10，地面控制站工具为 Q Ground Control。

4.1　效率评估

4.1.1　无人机节点信誉评估

模拟了一个不需要数字签名、哈希和区块链技术的场景作为基本方案，与本文所提方法进行比较，由于 UB-ANC 仿真器的限制，实验忽略了通信的平均延迟。

实验结果如图 6 所示，无人机节点的信誉值随时间变化的情况，在没有信誉评估方案的基本方案中，受攻击的无人机节点信誉值随时间的增加而增加，因为其它无人机节点无法检测到任何恶意活动；而在 BC _ UAV 中，由于增加了信誉值评估方案，并使用 CP-WP 算法进行一致性验证，受攻击无人机节点的信誉值迅速降低到阈值（$r=60$）以下，当节点的信誉低于阈值时，其他节点将不信任该节点，从而保证了无人机群分布式决策的安全性。

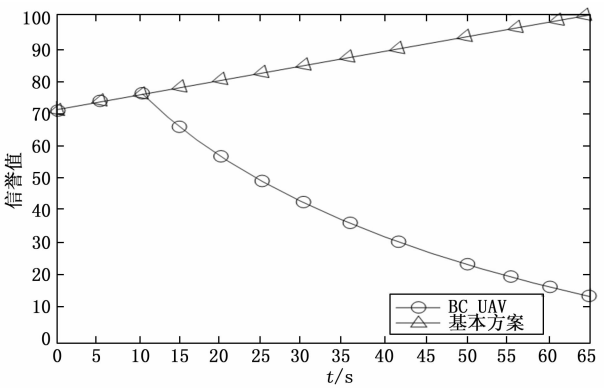

图 6　受攻击无人机节点的信誉值变化

4.1.2　平均吞吐量

表 1 在边缘层节点中从无人机到地面站、从无人机到无人机、从地面站到云端、从无人机到云端等 4 种包流，比较基本场景和 BC _ UAV 的流量大小，说明本文模型利用数字签名、加密和哈希函数在内的加密技术增加了传输的有效载荷的大小。

表 1　包流的评估

包流	基本方案/bytes	BC_UAV/bytes
从无人机到地面站	20	35
从无人机到无人机	15	25
从地面站到云端	60	62
从无人机到云端	20	35

如图 7 所示，随着网络中无人机数量的增加（最高到 10 个无人机），BC _ UAV 的平均吞吐量增加，总体逐渐趋

向于稳定状态，且高于基本方案，说明系统延迟时间小，能够快速趋于收敛。这是由于 BC _ UAV 设计了一个轻量级的重构无人机区块链，在 CP-WP 算法中引入 DPoS 思想进行难度调整与优化，同时利用快照形式将交易存储于边缘层节点中，减轻了无人机计算荷载。

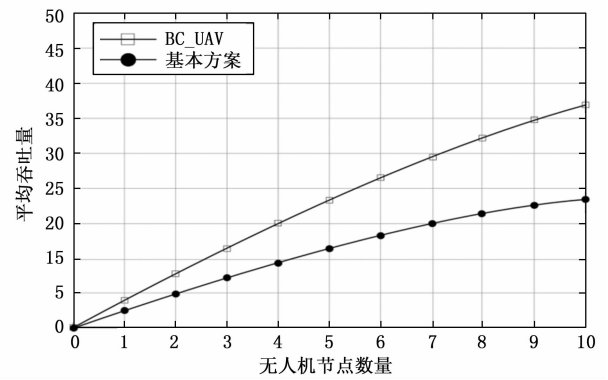

图 7 BC _ UAV 平均吞吐量比较

4.2 同攻击模式下无人机节点的信誉变化

一个理想的安全数据交易应对攻击行为是比较敏感的，边缘层节点每次对网络中交易检查得出的是无人机节点行为的信誉值。假设单个无人机节点的交易上限为 20，实验模拟了 3 种攻击模式分别布置于 3 个边缘层节点上，并设置 5 个检查点分析无人机区块链网络的信誉值变化。

节点 1：模拟合法行为。在检查区间发布 20 笔正常交易。

节点 2：模拟 GPS 欺骗。生成或伪造原始 GPS 信号，使投票交易事务无法声明 GPS 信息本身，在每个检查区间发送 20 笔交易，其中混入一笔伪造交易，造成无法检测该 GPS 信息本身。

节点 3：模拟女巫攻击。在每个检查区间发送 20 笔交易，其中混入一笔虚假交易限制网络中其它无人机访问。

节点 4：模拟 DoS/DDoS 攻击。向无人机网络或单个无人机节点发送多余或高频次的请求，在检查点 3 发送 25 笔交易。

如图 8 所示，关于节点 2，信誉值线性增长较合法行为节点 1 慢，这是由于节点 2 在每个检查周期混入一笔伪造交易行为，无人机在发布交易时必须验证已确认的交易，一旦无人机发现自己处于或接近禁飞区，它将发送一个投票事务来声明交易信息，这将调用共识协议，允许每个无人机向请求者发送一条错误/错误消息，而边缘层节点在计算信誉值时不考虑无人机节点的伪造行为。关于节点 3，由于交易内容为虚假信息，数据包丢弃和数据包选择性转发，使无人机节点的得不到认可，从而信誉值逐步降低。关于节点 4，其交易数量超过了上限的 10%，其荣誉值在检查点 3 处突然下降，并在检查点 4 和检查点 5 处开始增长缓慢，因为防止 DoS/DDoS 攻击是通过策略表实体限制网络中每个无人机的访问权限，当交易数量超过上限时荣誉值开始下降。该实验证明了数据智能合约对攻击行为作出了比较良好的反应，同时还说明了边缘层区块链和无人机区块链共同维护交易账本的过程。从实验中还看出，一个安全可靠的节点，通过 5 次检查就能达到信誉值上限 60。

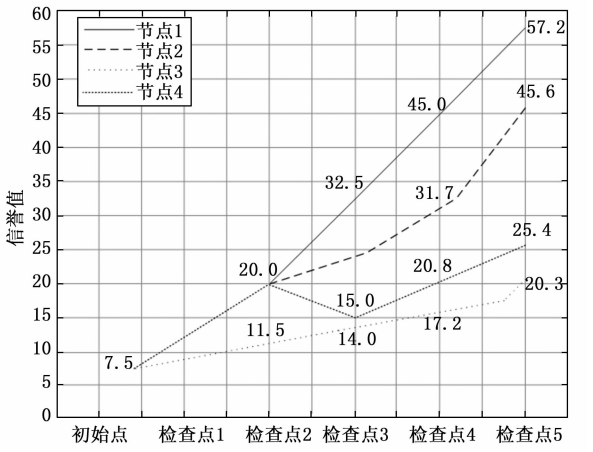

图 8 节点信誉值随攻击行为变化情况

4.3 共识协议在不同难度的执行时间

边缘层节点通过不断调整和优化无人机节点的信誉值，描述对本文所提 CP-WP 方法的有效性，从而降低可靠节点的开销。

如图 9 所示，共识算法在不同难度的执行时间，正常节点交易率可提升 3～4 倍，首先计算重构区块链信息的哈希值，然后设共识算法的最小难度为 1 个点，即在每个时间戳产生一个区块，处理一个请求交易事务，使难度每增加 1 个点，对应哈希结果时间增加 1 倍，将 17 作为算法的基准难度值，当难度小于 16 时，执行时间较低，当难度大于 18 时，执行时间增长较快。这是由于 BC _ UAV 的共识协议算法主要根据权益的概率随投票选举委员，在多个连续的时间戳形成连续窗口，从而验证交易信息，形成分布式一致性账本。表 2 描述了信誉值与 CP-WP 难度的映射关系，实验进行 30 次数据处理，区块链信息在每次实验中均随机变化，取平均值作为最终结果。

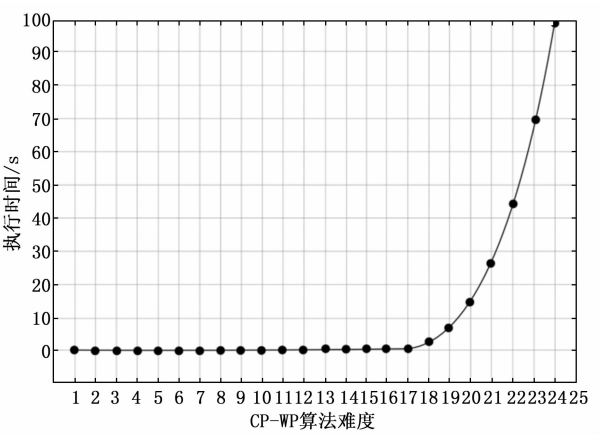

图 9 共识算法在不同难度的执行时间

表 2　信誉值与 CP-WP 难度的映射关系

信誉值	难度	时间/s
(−∞,10)	25	120.00
[10,0)	24	60.80
[0,1)	23	26.90
[1,2)	22	17.026
[2,3)	21	8.215
[3,4)	20	3.660
[4,5)	19	1.770
[5,10)	18	0.190
[10,15)	17	0.110
[15,20)	16	0.015
[20,25)	15	0.069
[25,30)	14	0.025
…	…	…

5　结束语

本文提出了一种基于区块链的分布式无人机数据安全模型 BC_UAV，主要是设计了适用于物联网边缘计算场景的分布式区块链网络模型，调用智能合约完成区块数据的安全传输，提出自适应工作量证明的共识算法完成交易数据的一致性协议，通过实验证明方法的有效性。后续工作将引入知识学习方法，将智能合约过程、共识协议过程扩展为可解释过程，有效刻画区块链在无人机数据安全传输的关系。

参考文献：

[1] PAKROOH R, BOHLOOLI A. A survey on unmanned aerial vehicles-assisted internet of things: a service-oriented classification [J]. Wireless Pers Commun., 2021, 119: 1541 - 1575.

[2] GAO J, LI M, ZHUANG W. UAV-assisted edge computing: rural IoT applications [J]. Connectivity and Edge Computing in IoT: Customized Designs and AI-based Solutions, Wireless Networks, Springer, 2021: 63 - 92.

[3] FOTOHI R, NAZEMI E, ALIEE F S. An agent-based self-protective method to secure communication between UAVs in unmanned aerial vehicle networks [J]. Vehicular Communications, 2020, 26 (100): 267 - 287.

[4] APOSTOLOPOULOS P A, FRAGKOS G, TSIROPOULOU E E, et al. Data of floading in UAV-assisted multi-access edge computing systems under resource uncertainty [J]. IEEE Transactions on Mobile Computing, 2021 (99): 1.

[5] GE C P, MA X S, LIU Z. A semi-autonomous distributed blockchain-based framework for UAVs system [J]. Journal of Systems Architecture, 2020, 107 (10): 17 - 28.

[6] 牛玉坤. 移动环境中区块链的隐私保护和可扩展技术研究 [D]. 合肥：中国科学技术大学，2022.

[7] 刘汉卿，阮　娜. 区块链中攻击方式的研究 [J]. 计算机学报，2021，44 (4)：786 - 805.

[8] CH R, SRIVASTAVA G, GADEKALLU T R, et al. Security and privacy of UAV data using blockchain technology [J]. Journal of Information Security and Applications, 2020, 55 (10): 26 - 70.

[9] LI X Q, JIANG P, CHEN T, et al. A survey on the security of blockchain systems [J]. Future Generation Computer Systems, 2020, 107: 841 - 853.

[10] YOUSSEF S B H, REKHIS S, BOUDRIGA N. A blockchain based secure IoT solution for the dam surveillance [C] //2019 IEEE Wireless Communications and Networking Conference (WCNC), 2019: 1 - 6.

[11] ISLAM A, SHIN S Y. Bus: A blockchain-enabled data acquisition scheme with the assistance of UAV swarm in internet of things [J]. IEEE Access, 2019, 7 (103): 231 - 249.

[12] KUZMIN A, ZNAK E. Blockchain-base structures for a secure and operate network of semi-autonomous unmanned aerial vehicles [C] // 2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), 2018: 32 - 37.

[13] 李晓伟，陈本辉，杨邓奇，等. 边缘计算环境下安全协议综述 [J]. 计算机研究与发展，2022，59 (4)：765 - 780.

[14] 殷昱煜，叶炳跃，梁婷婷，等. 边缘计算场景下的多层区块链网络模型研究 [J]. 计算机学报，2022，45 (1)：115 - 134.

[15] YU M, SAHRAEI S, LI S, et al. Coded Merkle tree: solving data availability attacks in blockchains [J]. IACR Cryptology ePrint Archive, 2019.

[16] 夏　清，窦文生，郭凯文，等. 区块链共识协议综述 [J]. 软件学报，2021，32 (2)：277 - 299.

[17] 苗　升，刘小雄，黄剑雄，等. 无人机视觉 SLAM 环境感知发展研究 [J]. 计算机测量与控制，2021，29 (8)：1 - 6，41.

[18] 马兆丰. 区块链技术开收指南 [M]. 北京：清华大学出版社，2021.

[19] ASHERALIEVA A, NIYATO D. Reputation-based coalition formation for secure self-organized and scalable sharding in IoT blockchains with mobile edge computing [J]. IEEE Internet of Things Journal, 2020 (99): 1.

[20] ALI I, KHAN R, NOSHAD Z, et al. Secure service provisioning scheme for lightweight clients with incentive mechanism based on blockchain [C] // IEEE Access, 2020, 8: 1048 - 1061.

[21] ANDROULAKI E, BARGER A, BORTNIKOV V, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains [C] //Proceedings of the 13th EuroSys Conference, 2018: 1 - 15.

[22] MODARES J, MASTRONARDE N, DANTU K. Ub-anc emulator: An emulation framework for multi-agent drone networks [C] //2016 IEEE International Conference on Simulation, Modeling, and Programming for Autonomous Robots (SIMPAR), 2016: 252 - 258.