ISSN 1004-9037,CODEN SCYCE4
Journal of Data Acquisition and Processing Vol. 39,No. 1,Jan. 2024,pp. 2－14
DOI:10. 16337/j. 1004-9037. 2024. 01. 002

http://sjcj. nuaa. edu. cn
E-mail:sjcj@nuaa. edu. cn
Tel/Fax:＋86-025-84892742

区块链赋能的低空智联网

金永光[1]，叶方伟[2]，卢晓珍[2]，吴启晖[1]，马凯光[1]

(1. 南京航空航天大学电子信息工程学院,南京 211106;2. 南京航空航天大学计算机科学与技术学院,南京 211106)

摘　要：低空智联网是低空经济发展的重要基础设施,在这种复杂的系统中,无人机的安全控制面临着空域安全、数据安全及频谱安全等多重安全挑战。为了同时解决这3个问题,本文提出了一个基于区块链的三面协同监管架构,同时使用链上和链下信息。链上包含无人机身份和注册等信息,而链下包含广播式自动相关监视(Automatic dependent surveillance-broadcast,ADS-B)和频谱等信息。为解决跨域认证问题,提出了一种基于ADS-B信息和无证书的高效签名算法。由于ADS-B协议中缺乏纠错机制,ADS-B信息在传输过程中容易受到信道噪声和干扰而产生错误,因此哈希验证可能会失败。为了缓解这种签名失败,设计了一种基于纠错码的跨层签名算法进行纠错。经实践验证,基于区块链的三面协同监管平台已成功试用于长江低空示范试验区。

关键词：区块链;低空智联网;广播式自动相关监视

中图分类号：TN92　　**文献标志码**：A

Low-Altitude Intelligent Network Empowered by Blockchain

JIN Yongguang[1], YE Fangwei[2], LU Xiaozhen[2], WU Qihui[1], MA Kaiguang[1]

(1. College of Electronic and Information Engineering, Nanjing University of Aeronautics & Astronautics, Nanjing 211106, China;
2. College of Computer Science and Technology, Nanjing University of Aeronautics & Astronautics, Nanjing 211106, China)

Abstract: Low-altitude intelligent network is an instrumental infrastructure for the outgrowth of low-altitude economy. However, the safety control of the unmanned aerial vehicles (UAVs) presented in such complex system faces multiple security challenges such as airspace security, data security, and spectrum security. To address these three issues simultaneously, a blockchain-based three-sided collaborative regulatory architecture, with the use of both "on-chain" and "off-chain" information, is proposed. The "on-chain" contains identity and registration information of UAVs, while the "off-chain" contains automatic dependent surveillance-broadcast (ADS-B) information and spectrum information. To solve the problem of cross-domain authentication, an effective signature algorithm is developed, which is based on the ADS-B information and certificateless signature. Furthermore, due to the lack of error correction mechanism in the ADS-B protocol, errors are easily incurred by channel noise and interference during the transmission of the ADS-B information. Consequently, the hash verification may fail. In order to alleviate such signature failure, a cross-layer signature algorithm based on error correction code is designed for correcting errors. The proposed blockchain-based three-sided collaborative regulatory platform has been well experimented over the Yangtze River low-altitude demonstration pilot zone and achieved great

基金项目:国家重点研发计划(2020YFB1005900)。
收稿日期:2023-10-10;**修订日期**:2023-12-08

success.

Key words: blockchain; low-altitude intelligent network; automatic dependent surveillance-broadcast (ADS-B)

引　　言

近年来,低空空域已成为国家战略资源,广泛服务于低空运输、公共安全与应急救灾等重要领域[1]。预计到“十四五”末,我国低空经济将产生3万亿元至5万亿元的市场规模,拥有广阔的市场空间和发展前景。低空经济的发展需求使得低空智联网应运而生。低空智联网(Low-altitude aerial intelligent network,LAIN)是在低空空域内运营的实体网络,是实现“人-机-物”三元融合智能互联的重要基础设施[2]。然而,随着作为低空智联网重要组成部分的无人机数量的日益增长,同时由于其移动性和动态性带来了应用范围的多样性[3],造成了巨大的安全隐患,使得低空智联网面临空域安全[4]、频谱安全[5]和数据安全[6]等多维重大安全隐患,制约着我国经济社会的转型发展。因此,需要对低空智联网进行集空域安全、频谱安全和数据安全为一体的综合安全管控。

传统的监管方式以行业内监管为主,不同行业之间的数据和资源隔离,无法得到有效的协同管控,形成数据孤岛阻碍着信息的跨行业应用,无法解决低空智联网面临的空域安全、频谱安全和数据安全等多维重大安全隐患。区块链是一种块链式存储、不可篡改、安全可信的去中心化分布式账本,它结合了分布式存储、共识机制和密码学等技术,确保数据的安全和透明性,已被广泛应用于监测低空无人机实时飞行数据、异常行为查看、管理与共享数据等方面。但是,现有的基于区块链解决方案,虽然打破了传统监管方式所形成的数据壁垒,却没有实现低空智联网链上链下的总体管控,即监管上只针对链上信息,没有与链下物理平台的信息结合。其中,链上信息包含无人机注册信息和密钥信息等,链下信息包含广播式自动相关监视(Automatic dependent surveillance-broadcast,ADS-B)、用于频谱检测时的频谱信息和空域信息等。

为解决传统监管所形成的业务壁垒和目前区块链方式存在链上链下信息割裂的问题,本文首次提出了一种基于区块链的三面协同监管架构体系。在该架构中,监管机构同时利用链上和链下的信息,实现低空智联网的综合安全管控。同时,针对跨空域认证难题,提出了一种基于ADS-B和无证书签名的无人机跨域认证机制,保障无人机群在执行任务时需要进行跨信任域和跨网络环境的无人机身份信息管理。最后,由于该认证机制依赖于有效的签名算法,但ADS-B报文格式和传输协议缺少纠错机制,而签名算法中哈希验证需要保证信息不可错。因此,为解决ADS-B传输过程中因信道噪声造成的误码率导致签名失效的问题,本文设计了一种基于纠错码的跨层签名算法。

1　低空智联网研究现状

1.1　低空智联网

低空经济作为一种综合性的新型经济业态,以低空空域(通常海拔3 km以下)为依托,以民用有人驾驶和无人驾驶航空器为主,以载人、载货及其他作业等多场景低空飞行活动为牵引,辐射带动制造、飞行、保障以及综合服务等相关产业融合发展,已成为新的经济增长点。同时,也是未来经济发展的重要引擎之一。

低空经济的高速发展依赖于低空智能网络的完善。低空智联网作为一种新兴的智能网络,包括由地面移动用户和基础设施组成的地面网络、空中平台组成的近地空间,是实现“人-机-物”三元融合智能互联的重要基础设施和建设空天地一体化网络的重要组成部分,对解决地面基础设施部署困难、减轻

移动网络拥塞负担、增强用户服务覆盖范围以及促进低空经济发展具有重要的意义，可支撑实现第六代通信技术无缝泛在互联，推动智能网络服务由地面向低空空域的发展。低空智联网产业的革新响应国家对低空经济的发展需求，颠覆传统空域静态单一划分方式，促进低空空域快速开放与优化使用，对提升我国低空经济开发水平具有重大意义。

1.2 传统低空智联网监管方法

传统监管方式以完善和制定相关法律法规来管控低空空域飞行行为、划分低空空域的安全责任和明确低空空域相关人员以及设备的要求作为基础。近年来，我国无人机监管制度逐步完善，相继提出了《无人驾驶航空器飞行管理暂行条例》《民用航空空中交通管理规则》和《民用无人机生产制造管理办法（征求意见稿）》等法规，明确了当前无人机分类、申报流程、空中交通管理和企业制造等方面的相关监管标准和规定，形成了包括法律、部门规章和企业制造等在内的无人机监管体系。

无人机远程ID可以帮助政府监管机构对消费类、民用类等低空无人机的识别，全世界许多企业和机构纷纷对其展开了大量研究并取得了丰富成果。美联邦航空管理局（Federal Aviation Administration, FAA）公布无人机Remote ID最终规则[7]，其通过让无人机自行传送给执法部门和安全官员识别信息来帮助识别和发现那些违反规定的无人机。2019年，大疆科技有限公司公开了一套通过WiFi技术直接连接无人机和移动终端设备的远程ID方案，能识别大疆及其他无人机制造商的飞行器，且不需要蜂窝网络或其他外部系统，解决了网络无法覆盖地区的无人机监管需求。皮尔斯航空公司（Pierce Aerospace）开发了远程识别系统Flight Portal ID，具有多方联动使用的普适性，能够解决无人机的身份识别问题，为空中交通管制员和航空当局的空中监管提供用户信息。

同时，一些学者也展开了用无人机远程ID实现监管的研究，并取得了丰富的成果。文献[8]提出一种符合Remote ID标准的无人机匿名远程识别的解决方案ARID，该方案允许无人机使用短暂的假名广播符合Remote ID的消息，只有可信机构才能链接到无人机及其运营商的长期标识符，保护无人机免受冒充和欺骗性报告，实现对无人机的有效监管。文献[9]提出了匿名直接身份验证和远程识别（A^2RID），解决了Remote ID明文广播带来的隐私问题。文献[10]分析当前Remote ID方案，确定需要工业界和学术界共同应对的多重挑战，以此提高无人机的安全性和隐私性。

另外，无人机轨迹的监控对于确保无人机的安全运行、遵守法律法规、管理空域以及建立公众信任至关重要。文献[11]提出一种基于蜂窝移动网的无人机监管系统，通过蜂窝移动网将分散在不同空域的无人机的位置及态势信息收集传输到云数据中心，并将数据实时推送至监管平台，实现对无人机实时监管。文献[12]提出用于无人机整体路径规划和轨迹跟踪的自动飞行技术，提升无人机的自主飞行规划能力。文献[13]提出一种采用基于机器学习的方法预测无人机完成计划路径的飞行时间的方法，将无人机遥测产生的总飞行时间与预测的飞行时间进行了比较，可以有效地预测飞行交叉路径的无人机之间可能发生的碰撞，支持无人驾驶在交通安全上的监管。

由于无人机应用范围日益拓展、飞行任务日益多样和低空场景日益复杂，使得低空智联网跨行业监管的迫切性加剧。但是，传统的监管方式以行业监管为主，而行业之间的数据和资源隔离，却无法得到有效的协同管控，最终形成数据孤岛并阻碍信息的跨行业应用，无法解决低空智联网面临的空域安全、频谱安全和数据安全等多维重大安全隐患。

1.3 基于区块链的低空智联网监管方法

区块链由于其具有不可篡改、透明度、安全性和智能合约等特性，使其成为监管无人机活动的一个强大工具，已被广泛应用于监测无人机实时飞行数据、异常行为查看、管理与共享数据，为监管机构提供无人机的整个生命周期完整的溯源记录，确保无人机数据监测、传输与存储、身份验证和授权的安全

稳定性。

一些学者利用区块链不可篡改性和透明性,将飞行数据记录在区块链上,确保了数据的真实性和可靠性,有助于监管机构跟踪无人机的飞行活动,确保其遵守相关法律法规。文献[14]提出基于区块链的无人机生态系统去中心化可审计安全日志记录,依靠哈希链和默克尔树为存储的日志记录生成证明。文献[15]提出基于异构区块链的无人机数据安全框架,来确保无人机收集的数据的安全性和保密性。文献[16]设计了一个基于网络编码的区块链共识,实现无人机网络高效和安全的通信。文献[17]利用区块链技术在无人机物联网(Internet of drone things, IoDT)中进行恶意节点检测,解决了在IoDT中的服务交付过程中提供商和消费者的不信任问题。文献[18]提出了一套基本分析和关键要求,帮助构建区块链辅助无人机通信的隐私和安全模型,帮助无人机管理和支持去中心化的数据存储系统。

还有一些学者利用区块链来有效地管理无人机操作者的身份验证和授权,确保只有授权的个人或实体才能操作无人机。文献[19]提出一种具有大数据分析功能的基于区块链的安全认证密钥管理框架,解决无人机互联网(Internet of drones, IoD)通信面临的隐私和安全问题。文献[20]提出一种物理安全且隐私保护的区块链认证方法,解决无人机执行任务时的隐私、安全和跨域身份验证问题。文献[21]提出了一种区块链辅助无人机认证和访问控制方案,解决传统无人机认证和访问控制方案无法满足无人机跨域认证和监管要求等弊端。文献[22]提出了一种基于区块链的安全无人机租赁机制,提供了相互身份验证机制,可以抵御中间人、冒充、修改、重放和中继攻击。

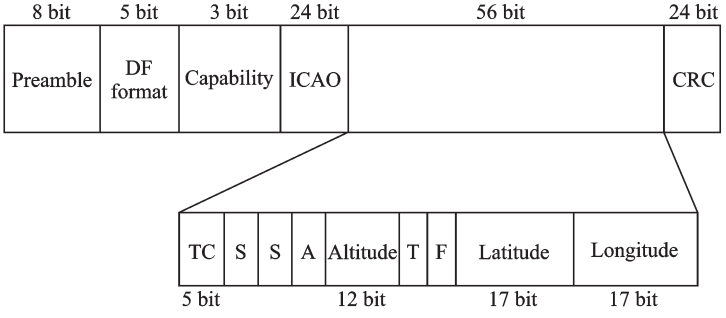
上述基于区块链的解决方案都是利用区块链的不可篡改性,将数据记录在区块链上,帮助监管机构跟踪和追溯无人机的飞行行为,但是并没有打破传统监管方式形成的数据壁垒和实现不同业务信息的跨行业应用。同时,没有实现区块链平台、监管平台和物理平台的三面协同管控,即监管上只针对于链上信息,没有与链下物理平台的信息结合,没有实现低空智联网链上链下的总体管控。单独使用区块链的信息会面临性能瓶颈、隐私泄露及成本较高等问题,难以应对复杂业务场景,无法与现有系统和平台无缝集成,导致数据和业务逻辑的交互存在局限性。同时,链下信息可以实时反应出低空资源(如空域资源、频谱资源等)的使用情况和低空业务的执行情况,可以帮助监管机构实时掌握各区域内低空资源的使用状态,包括使用强度、利用率、数据传输速率、使用范围和使用业务类型等,并根据链下实时信息对低空用户提交的任务需求(用频需求、飞行空域需求和数据访问请求等)进行合理安排,从而更好地管控低空智联网。

因此,为了解决数据壁垒和链上链下信息割裂及不能耦合的问题,本文研究了基于区块链的链上链下三面协同管控框架。在该架构中,监管平台不仅可以利用区块链平台链上无人机注册和身份等信息,同时结合了物理平台链下ADS-B和频谱等信息,实现链上链下数据融合,实现集空域安全、频谱安全和数据安全为一体的综合安全管控,提高低空智联网应对多样化安全管控风险的处置能力。

1.4 广播式自动相关监视

基于区块链的三面协同框架以同时结合链上链下信息为主要特征。其中,在面向低空智联网的场景下,ADS-B信息是实现链下监管的重要依托,可以提供实时、准确的无人机位置信息(包括飞机经度、纬度、高度和时间等信息)来辅助无人机的监管。ADS-B不需要像二次雷达那样手动操作或查询,飞行器自动将其位置、高度、速度、航向和识别号等信息广播给其他飞机或地面站,供管制员和飞行员监控飞行器状态[23],可以明显减少地形对信号覆盖的影响,并且由于精度更高、监视能力更强、使用寿命长和维护费用低等优点,大大降低了民用航空空中交通管制的成本,已经成为民用航空的主要监视方法之一[24],在我国航空领域的应用也越来越广泛。ADS-B系统主要通过1090ES、VDL-Mode4和UAT三种数据链进行消息广播。ADS-B最常见的实现方式是使用S模式扩展Squitter[25],

其中数据被封装在帧中，如图1所示。每个ADS-B帧共120位，由用于同步的前导码、指示所使用协议的下行链路格式(Dont fragment，DF)字段、表示协议子格式的能力字段、唯一标识每架飞机的国际民用航空组织(International Civil Aviation Organizition，ICAO)字段和用于错误检测的循环冗余校验(Cyclic redundancy check，CRC)字段组成。其中，ADS-B数据长56 bit，包括发射飞机的位置、速度或方向。



Preamble：用于同步的前导码　　DF format：指示使用下行链路格式
Capability：协议子格式的能力字段　　ICAO：每架飞机的唯一标识
CRC：循环冗余校验检错　Altitude：高度　TC：指示数据类型　S：监视状态　A：是否单天线
Latitude：纬度　　Longitude：经度　T：时间指示　　F：CPR位置信息是奇数秒/偶数秒

图1　ADS-B数据帧格式

Fig.1　ADS-B data frame format

紧凑位置报告(Compart position reporting，CPR)[26]是1 090 MHz扩展振荡脉冲数据链在传输中为了减少经纬度传输位数而定义的。为了提高ADS-B报文的传输效率，CPR算法忽略位置信息中长时间不变的几个高阶位，同时为了解决只接收到单个位置信息时解码难以确定目标飞机的正确位置信息的问题，CPR编解码技术对目标飞机采用两种不同格式的编码，分别称为偶编码和奇编码，各占发送时间的50%[27]。CPR编码为了确认飞机的准确位置，将地球按经度和纬度分为许多不同编号的区域(Zone)，然后通过对纬度Zone和经度Zone进行编码来确认飞机的大致位置的。CPR全球空中位置编码实现过程如下：首先，根据CPR编码是奇编码还是偶编码确定南北向纬度Zone的尺寸后，将输入的纬度转变为纬度坐标输出(即CPR坐标纬度)；然后，通过确定经度Zone的数目N和东西向经度Zone的尺寸后，将输入的经度转变为XZ_i经度坐标输出(即CPR坐标经度)。最后，将求出CPR坐标经/纬度的转换为17 bit的二进制序列，并按照空中位置信息格式封装为56 bit的短报文。

含有飞机空中位置信息的ADS-B传输过程为：在发送端，目标飞机采用CPR算法将自己的经度和纬度分别编码为17 bit的二进制序列，然后按照图1所示的报文格式先将该序列封装成ME(Message，extended squitter)字段域56 bit的空中位置信息，再对该信息按一定规则加入控制元组装成112 bit的ADS-B报文信息，经过脉冲位置调制(Pulse-phase modulation，PPM)编码后以便于信号的传输，最后通过对1 090 MHz调制向外广播。在接收端，本机先通过PPM解调获得目标飞机的112 bit的报文信息，再由CPR信源解码获得所需的目标飞机位置信息。

2　基于区块链的三面协同系统框架

针对低空智联网实现集空域安全、频谱安全和数据安全为一体的监管需求，本文提出基于联盟链的链上链下三面协同监管体系架构，整个系统的架构如图2所示。该体系架构从空间分布式、层级穿透式及业务全维度监管三方面开展技术攻关，解决了传统监管方式和传统区块链监管方式面临的两方面

难题,即:在传统监管方式中,不同业务间数据和资源隔离,无法得到有效的协同管控,形成数据孤岛阻碍着信息的跨行业应用的难题;传统区块链监管上只针对于链上信息,没有与链下物理平台的信息结合,链上信息和链下信息割裂、不能耦合的难题。

在空间分布式方面,构建了面向监管角色、业务系统和多用户链的空间分布式监管机制,融合角色属性访问控制及秘钥共享等技术实现了对不同监管角色和被监管用户的分布式监管访问控制。其中,链上链下协同可以在保证链上数据的不可篡改和完整性的基础上,将敏感信息和隐私数据存储在链下,通过加密和访问控制等手段保护数据安全,即用户只可获取加密后的数据,想要获取明文数据必须符合权限控制策略,具有机密性、共谋攻击等防护能力,实现了区块链数据的安全共享。

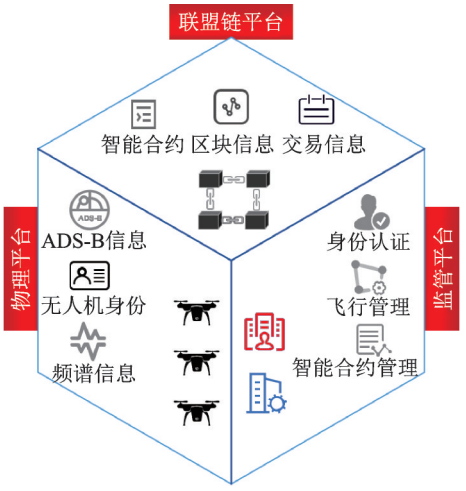


图2 基于联盟链的三面协同监管框架

Fig.2 Three-faced collaborative regulatory framework based on consortium blockchain

在层级穿透式方面,设计了联盟链链上交易行为、链下监管平台业务行为和物理平台实时信息三面结合的层级穿透式监管方法,采用椭圆曲线加密算法,实现了对低空智联网业务事前、事中、事后的全周期的安全监管,破解分布式监管业务链上执行影响范围广、范围控制难度大的难题,实现对链下业务行为的可信监管,实现业务信息在联盟链之间的交流和共享信息,消除不同业务信息之间的壁垒,支撑联盟链对低空智联网业务事前、事中、事后的全周期监管。具体如下:

(1)事前链下业务管理与认证。监管平台将无人机身份信息和飞行业务信息进行登记,包括无人机唯一标识码、无人机型号、无人机设备参数及业务信息等。监管平台验证设备及业务合规性后,通过加密算法为设备生成密钥,完成业务合规性认证准入。

(2)事中链上链下协同监管。监管平台通过获取链下物理平台实时信息,并通过链上监管合约,实现对应无人机业务的审批和监管。如,结合链上注册信息和链下物理平台提供的无人机身份信息,可以帮助监管平台实现无人机安全认证,实现低空数据的安全共享和保障数据安全;结合链上航迹规划的合约信息和链下物理平台提供的ADS-B信息,可以帮助监管平台实时掌握和判定无人机的飞行轨迹和保障空域安全;结合链上交易信息和链下物理平台提供的无人机频谱监测数据,可以帮助监管平台实现低空空域频谱的合理分配和保障频谱安全。

(3)事后跨链全流程追溯与分析。监管平台利用无人机业务信息对链上数据进行跨链追溯,将低空无人机的相关数据溯源链接,并针对数据进行全周期审计。基于跨链数据查询,批量导出联盟链数据,随后对数据检查敏感词,并输出检查结果文件供监管排查之用。通过导出的数据记录,可以实现对低空无人机不同业务中违规行为的追溯和追责。

针对传统监管方案链上交易行为和链下业务行为监管分离问题,本文提出了业务全维度监管方法,实现联盟链链上交易行为、链下监管平台业务行为和物理平台实时信息三面结合。该方法支持低空数据共享、数据隐私交易、低空无人机管控和无人机行为监测评估等低空智联网业务行为监管。具体流程如下:

(1)业务申请:无人机等用户在申请执行任务之前,需要进行身份验证,确保申请者的身份合法有效。联盟链监管平台会要求用户提供真实有效的身份信息,包括个人或组织的身份证明等。用户提交身份验证后,监管平台可以将用户的注册信息录入到区块链中,包括用户的基本信息、联系方式、申请

资格和权限等。同时,监管平台为每个注册用户分配相应的权限,以便用户在申请任务时能够按照其权限进行操作。

(2)业务数据需求规划:监管机构对用户提交的任务需求(用频需求、飞行空域需求和数据访问请求等)进行审核,并将初步的审核结果上链。监管平台进一步审核通过后,可以向用户授权特定的任务使用权限(包括身份有效期、空域范围、频段范围等),并将授权信息记录在区块链上,确保审核过程的透明性和可追溯性以及授权的合法性和可信度。

(3)业务行为监测:各区域内的监测设备将实时监测低空资源(频谱、空域等)的使用情况,包括使用强度、利用率、数据传输速率、使用范围及使用业务类型等,并对这些信息进行分析和处理,生成相应的业务监测报告,包括资源使用情况统计及业务行为分析、资源使用异常报告等内容。各个监测设备将区域内的业务监测报告上传至联盟链中。监管平台从联盟链中获取业务监测报告,对网络中各用户的业务行为进行评估和分析。一旦发现行为异常行为,监管平台将及时采取包括对低空资源的重新分配、对违规用户的使用行为进行限制、对违规使用设备进行定位和追踪等措施。

2.1 基于ADS-B和无证书签名的无人机跨域认证机制

由于无人机群在任务执行时环境的动态变化,需要解决跨信任域和跨网络环境的无人机身份信息认证问题,但是传统认证方式依靠中心节点进行身份认证,存在重复认证、证书管理效率低等问题,而区块链分布式特征与跨域场景更加契合,可以解决无人机飞行区域跨越不同区域控制中心场景下的跨域身份认证问题。同时,ADS-B可以作为无人机在签名阶段哈希验证的消息本体,并提供实时、准确的无人机位置信息(包括飞机经度、纬度、高度和时间等信息),可以帮助监管机构实时掌握无人机的飞行动态。因此,本文提出了一种基于ADS-B和无证书签名的无人机跨域认证机制,如图3所示。首先,通过智能合约充当密钥生成中心,替代了传统密钥分发中的可信第三方,利用智能合约的不可篡改性,解决了密钥分发中需要第三方的可信问题。其次,利用无人机的物理特征(如无人机的生产序列号等出厂信息)和ADS-B提供实时、准确的无人机位置信息(包括飞机经度、纬度、高度和时间等信息)来辅助认证,同时结合联盟链上的密码学信息,可以保证无人机跨域认证(如无人机飞行区域跨越不同区域控

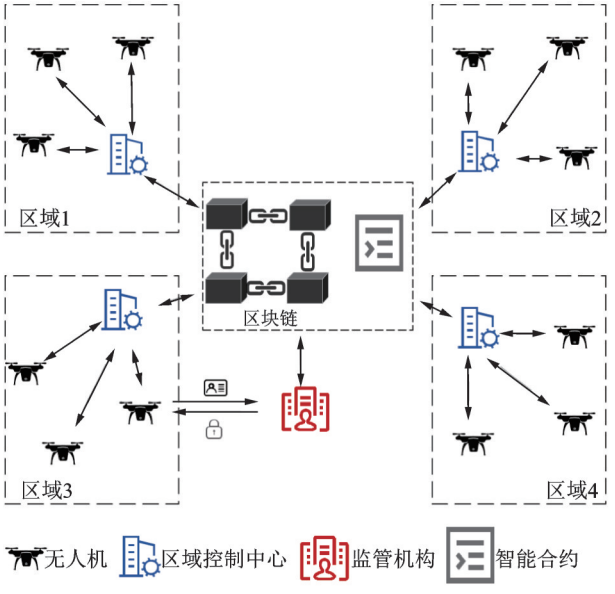


图3 基于ADS-B和无证书签名的无人机跨域认证机制

Fig.3 UAV cross-domain authentication mechanism based on ADS-B and certificateless signature

制中心场景下的身份认证)的安全和可信。最后,本签名算法除了使用传统密钥外还利用了一组虚拟身份ID来实现无人机签名认证的匿名性。该算法实现了真实注册身份信息与链上虚拟ID的解耦,保障除了监管机构可以通过链上虚拟ID监管用户行为外,其他未经授权的实体无法知道无人机的真实身份,以便在验证消息真实性的同时不泄露无人机的长期身份、所有者和制造商的身份,实现了对无人机真实身份信息的隐私保护和基于链下链上信息协同完成无人机跨域身份认证。根据功能划分不同的实体,具体主体划分如下:

(1)监管机构(Regulator,RE):它是受信任的第三方(Trusted third party, TTP),充当飞行管理部门,其作用包括:①存储和注册合法无人机,包括授予无人机合法身份、颁发空域飞行许可证,并管理无人机的真实身份列表;②为合法无人机的认证提供密码材料,在认证系统中,RE被认为是可信实体,根据外部请求协调组织内的其他实体,完成无人机的授权和认证;③监管无人机违法行为,分析区域控制中心提供的有关无人机入侵敏感区域和非法访问的报告,识别所提供证据真实性并追溯无人机长期身份和所有者。

(2)区域控制中心(Area control center,ACC):ACC由监管部门在不同区域部署,验证无人机发来的签名信息,并根据需求为合法无人机提供差异化的接入服务。此外,ACC还可以接收并解码ADS-B信号,以协助RE监控无人机,如果检测到欺诈和恶意行为,将报告RE进行身份披露和实施制裁。最后,ACC可以接入区块链网络,获取各地区存储的身份列表,对跨域飞行的飞机进行身份认证。

(3)智能合约:针对密钥生成中心(Key generation center, KGC)泄密攻击和特权内部攻击,本文用智能合约代替传统的KGC,它负责生成系统参数和无人机的部分私钥。而且,由于区块链不可逆的特性,一旦部署了这个智能合约,任何人都无法伪造数据,甚至合约所有者本身也无法伪造数据。同时,该区块链中的受损节点无法获取该合约的任何私人信息。

(4)联盟链:存储无人机用户生成的伪身份和对应的未撤销的参数。监管机构负责维护联盟链的账本,并允许组织内的实体根据需要访问和更新区块链。

(5)无人机:搭载ADS-B的通用无人机,会周期性地匿名广播签名的ADS-B消息,报告其位置和标识等信息。

在基于ADS-B和无证书签名的无人机跨域认证机制中,相关认证过程主要包括如下步骤:

(1)监管主密钥生成:智能合约根据配置的参数(散列函数、椭圆曲线上的加法群生成元等)随机生成监管机构的私钥,并通过椭圆曲线上的群映射得到监管机构的主密钥。

(2)虚拟数字身份生成:首先,每架无人机在起飞前都需要获得其飞行路径中不同区域的授权,为此无人机向出发地的区域控制中心提交其真实身份信息(低空无人机的生产序列号等出厂信息)和飞行计划,请求获取临时身份证明(仅在执行本次飞行任务期间有效);其次,区域控制中心首先检查该无人机身份是否已经存在,若存在,则直接进行飞行计划审批,否则需要验证身份的合法性。监管部门在审核身份和飞行计划通过后,将无人机的身份信息通过智能合约选择适当的随机数和使用监管机构的公钥生成一组虚拟身份ID,并上链保存,以便在无人机做出违法行为之后,监管机构可以追踪到它的真实身份。无人机在执行任务过程中,随机在假名列表中选择虚拟身份ID进行消息签名,这可以降低真实身份信息泄露的风险和防止被追踪。

(3)无人机密钥生成:无人机的私钥采用基于数字身份无证书签名算法生成,其中私钥一部分是由智能合约通过监管机构的公钥以及用户的虚拟身份ID生成,另一部分由无人机在本地自己生成。对应的无人机完整公钥可以通过私钥在椭圆曲线加法群上的映射生成。

(4)无人机签名生成:完成上述步骤后,无人机将要广播的ADS-B信息使用自己的私钥生成签名,验证者(区域控制中心)收到签名后可以通过联盟链上的虚拟身份ID和系统参数验证签名的有效性,从

而实现有效的身份管理。

(5)无人机签名验证:当需要对用户进行身份验证时,区域控制中心根据接收到带签名的ADS-B消息,先检查时间戳是否满足预定义的最大传输延迟。若满足,可搜索联盟链获得无人机的假名列表和系统参数对无人机的身份信息进行核实,验证无人机身份信息是否存在且在任务有效时间内,避免身份信息被篡改或伪造。如果验证失败,则拒绝接收无人机的消息,同时将情况报告给监管机构进行追责。如果验证成功,则接受无人机发来的签名信息,并根据需求提供差异化的接入服务。

(6)无人机违规追溯:区域控制中心在验证无人机身份合法后,会根据广播的ADS-B信息中无人机的位置信息(包括飞机经度、纬度、高度和时间等信息),实时监管无人机飞行情况是否与申请的飞行计划一致。通过身份和轨迹判定双重判定之后的无人机,区域控制中心会将相关信息上传至联盟链记录,表明双方已达成交易并开始为无人机提供通信服务。否则,区域控制中心将拒绝无人机的接入,并将无人机的信息上报给监管机构。由监管机构通过链上虚拟ID和注册信息追溯到违规无人机的真实身份,撤销其伪身份PID和追究相关负责人的责任。

如图4所示,在基于数字身份的无证书签名算法中,采用有限域椭圆曲线加密算法,通过智能合约充当密钥生成中心,同时利用ADS-B位置信息辅助认证,引入一组虚拟身份ID保证认证匿名性,从而实现无人机在飞行区域跨越不同区域控制中心场景下的身份认证管理。算法具体流程如下:

(1)系统初始化阶段:监管机构给定安全参数k,生成两个大素数p和q,P为椭圆曲线上q阶加法循环群G的生成元,其中$q>2^k$。KGC选择3个抗碰撞的Hash函数:$H_0:\{0,1\}^*\times G\rightarrow Z_q^*$,其中$Z_q^*$为去掉非零元素的加法循环群;$H_1:\{0,1\}^*\times G\times G\rightarrow Z_q^*$;$H_2:\{0,1\}^*\times G\times G\times G\rightarrow Z_q^*$。随机选择$s\in Z_q^*$作为主密钥,并计算系统的公钥$P_{\text{pub}}=sP$。然后KGC在联盟链上公布系统参数$\text{params}=\{G,p,q,P,P_{\text{pub}},H_0,H_1,H_2\}$,而系统主密钥$s$秘密存储。

(2)假名生成阶段:无人机向出发地的区域控制中心提交其真实身份和飞行计划,监管部门在审核身份和飞行计划通过后,将无人机真实身份ID发送给KGC;KGC随机选择一组$j_{\text{ID}}^i\in Z_q^*$,$i=1,2,\cdots,n$,计算$J_{\text{ID}}^i=j_{\text{ID}}^iP$,$h_0^i=H_0(\text{ID},J_{\text{ID}}^i,P_{\text{pub}})$,然后计算$\text{PID}_i=\text{ID}\oplus sh_0^i(\bmod q)$,并将$(\text{PID}_i,J_{\text{ID}}^i)$插入负责存储伪身份的联盟链中。

(3)部分私钥提取:监管机构将无人机的伪身份$\text{PID}=\text{PID}_1\oplus\text{PID}_2\oplus\cdots\oplus\text{PID}_i$发送给KGC,KGC生成一个随机数$r_{\text{ID}}\in Z_q^*$,计算$R_{\text{ID}}=r_{\text{ID}}P$,$h_1=H_1(\text{PID},R_{\text{ID}},P_{\text{pub}})$。然后计算$s_{\text{ID}}=r_{\text{ID}}+sh_1(\bmod q)$,并通过安全通道将$(R_{\text{ID}},s_{\text{ID}})$发送给无人机。

(4)设置公钥和私钥:无人机接收到部分私钥s_{ID},首先检查$s_{\text{ID}}P=R_{\text{ID}}+h_1P_{\text{pub}}$是否成立。如果成立,则部分私钥有效,无人机随机选择$x_{\text{ID}}\in Z_q^*$作为秘密值,计算$X_{\text{ID}}=x_{\text{ID}}P$,$PK_{\text{ID}}=R_{\text{ID}}+h_1X_{\text{ID}}$,$SK_{\text{ID}}=s_{\text{ID}}+h_1x_{\text{ID}}$,然后,无人机将$PK_{\text{ID}}$作为自己的公钥,将$SK_{\text{ID}}$作为私钥。

(5)签名:无人机为了对广播的ADS-B消息m进行签名,随机选择一个假名PID_i和$z_{\text{ID}}\in Z_q^*$,计算$Z_{\text{ID}}=z_{\text{ID}}P$,$h_2=H_2(\text{PID}_i,Z_{\text{ID}},PK_{\text{ID}},m,t_i)$,其中$t_i$为当前时间戳,同时计算:$\tau_{\text{ID}}=z_{\text{ID}}+SK_{\text{ID}}h_2(\bmod q)$,然后无人机将$\sigma=(\tau_{\text{ID}},Z_{\text{ID}})$作为ADS-B消息的签名。签名生成之后,无人机广播$\{m,t_i,\sigma\}$。

(6)验证:区域控制中心在接收到签名和ADS-B消息后,先检查时间戳是否满足$t-t_i<\Delta t$。其中,t为当前时间戳,Δt为预定义的最大传输延迟。若满足,结合联盟链上的假名列表和系统参数来验证无人机的假名PID_i是否合法。若合法,则提取出广播的ADS-B信息m,计算$h_2=H_2(\text{PID}_i,Z_{\text{ID}},PK_{\text{ID}},m,t_i)$,并验证$\tau_{\text{ID}}P=Z_{\text{ID}}+(PK_{\text{ID}}+P_{\text{pub}}h_1)h_2$是否成立。如果成立,则代表无人机的身份合法。在通过身份和位置双重判断之后,区域控制中心会根据无人机需求提供差异化的接入服务,否则则拒绝并上报监管机构。

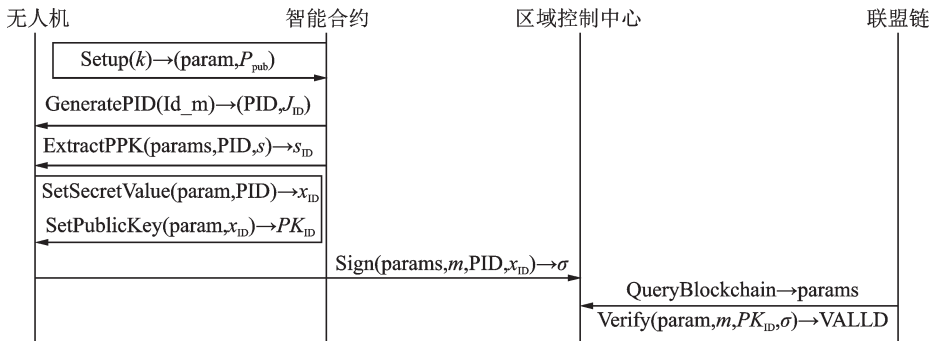


图4 无证书跨域签名流程

Fig.4 Certificateless cross-origin signing process

2.2 跨层签名算法

在上述基于ADS-B和无证书签名的无人机跨域认证机制中,认证过程需要数字签名方案来保证身份认证的正确性和有效性,其中签名阶段的签名方案依赖于消息在收发两端能够正确无误地传输。更确切地说,签名阶段依赖于消息哈希验证的正确性。然而,ADS-B报文格式中缺少纠错机制,且消息在通过广播方式传输时,由于信道噪声的存在使得ADS-B消息并不能无误传输,即使很小的误比特率也会导致哈希之后的输出结果截然不同,使得区域控制中心接收到的ADS-B信息与无人机进行签名时的ADS-B信息不一致,从而导致签名验证阶段无法进行,使得签名算法不可用。因此,本节从消息本体中随机抽取一个短的消息,并通过纠错码编码形成码字来代替签名算法中哈希验证的消息,以保障区域控制中心使用的哈希验证信息与无人机在签名时所使用的哈希验证消息一致,保证签名算法的有效性。

具体而言,ADS-B在S模式通信下,使用CRC错误控制编码。在所有类型的S模式下行链路消息中,最后24位保留用于CRC余数。在ADS-B中,CRC余数直接附加作为消息的最后24位。用于ADS-B(以及其他S模式消息)的生成器$G(x)$的多项式形式为

$$G(x)=x^{24}+x^{23}+x^{22}+x^{21}+x^{20}+x^{19}+x^{18}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{10}+x^{3}+1 \quad (1)$$

该生成器用于每条ADS-B消息。在CRC余数的计算和错误的验证中,设x_i代表消息的每一位,$M(x)$代表ADS-B消息对应的多项式,则CRC余数(奇偶校验)$P(x)$可以计算为

$$\begin{cases} M(x)=\sum_{i=0}^{87} a_i x^i \qquad a_i \in (0,1) \\ P(x)=M(x)\%G(x) \end{cases} \quad (2)$$

式中%表示取余操作。如果最后24个余数位全部为零,则消息正确。CRC能够有效地检测数据中的错误,但是CRC不具备纠错机制,需要引入纠错机制来保障ADS-B在传输过程中即使因为噪声出现错误也可以恢复出签名哈希验证中所使用的信息。

因此,本文提出一种基于纠错码的跨层签名的算法来解决ADS-B传输过程中信道噪声造成的误码率导致签名失效的问题。由于ADS-B的位置信息比特位总共只有46位(12位高度+17位经度+17位维度),传统无线通信中用于信息纠错的长码,如LDPC、Turbo等很难应用。因此,本文采用适用于一类控制信道的短码来作为本文的纠错码用于跨层签名方案中,具体而言,本文采用(16,5)的Reed-Muller(RM)码。RM码被应用于LTE协议的上行通道控制码[28]、美国发射的"水手"号深空探测器就使用RM码来传输火星的黑白照片[29]等,其高可靠性被广泛验证。

RM码是GF(2)域上的线性非系统码,其码长$n=2^m$,维数$k(r,m)=\sum_{i=0}^{r} C_m^i$,最小汉明距离$d_{\min}=2^{m-r}$。采用生成矩阵进行编码的具体流程如下:

当$r=0$时,生成矩阵被定义为

$$\boldsymbol{G}(0,m)=[\underbrace{1\quad 1\quad \cdots\quad 1}_{2^m}] \tag{3}$$

当$r\geqslant 1$时,通过式(4)采用迭代的方式得到生成矩阵为

$$\boldsymbol{G}(r,m+1)=\begin{bmatrix}\boldsymbol{G}(r,m) & \boldsymbol{G}(r,m)\\ \boldsymbol{0} & \boldsymbol{G}(r-1,m)\end{bmatrix},\quad \boldsymbol{G}(m,m)=\begin{bmatrix}1 & 0 & \cdots & 0\\ 0 & 1 & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & 1\end{bmatrix}_{2^m\times 2^m} \tag{4}$$

本文随机提取46位ADS-B位置信息中5位作为原始信息采用(16,5) RM码进行编码,即使用式(5)将选择的原始数据编码为16位数据并作为本文的纠错码用于跨层签名方案中。

$$[b_2(1),b_2(2),\cdots,b_2(16)]=[b_1(1),b_1(2),\cdots,b_1(5)]\times \boldsymbol{G} \tag{5}$$

式中$\boldsymbol{G}$为生成矩阵。本文采用$\boldsymbol{G}(1,4)$,具体结果由式(6,7)所得,$[b_1(1),b_1(2),\cdots,b_1(5)]$为5位原始位置信息,$[b_2(1),b_2(2),\cdots,b_2(16)]$为RM编码之后的16位纠错码。

$$\begin{cases}\boldsymbol{G}(1,4)=\begin{bmatrix}\boldsymbol{G}(1,3) & \boldsymbol{G}(1,3)\\ \boldsymbol{0} & \boldsymbol{G}(0,3)\end{bmatrix}\\ \boldsymbol{G}(1,3)=\begin{bmatrix}\boldsymbol{G}(1,2) & \boldsymbol{G}(1,2)\\ \boldsymbol{0} & \boldsymbol{G}(0,2)\end{bmatrix}\\ \boldsymbol{G}(1,2)=\begin{bmatrix}\boldsymbol{G}(1,1) & \boldsymbol{G}(1,1)\\ \boldsymbol{0} & \boldsymbol{G}(0,1)\end{bmatrix}\end{cases} \tag{6}$$

$$\boldsymbol{G}(1,4)=\begin{bmatrix}1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0\\ 0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1\\ 0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1\\ 0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1\\ 0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1\end{bmatrix} \tag{7}$$

无人机经过编码得到16位纠错码$[b_2(1),b_2(2),\cdots,b_2(16)]$,并将其附加到广播的ADS-B消息之后。区域控制中心在接收到签名后,采用大数逻辑算法[30]进行译码。译码主要基于向量之间的距离(指两个向量对应位上不同元素的个数,即汉明距离)进行,即对于任意接收序列,首先计算该序列与(16,5) RM码字集合中所有码字的距离,然后再将所得距离最小的码字作为译码结果,最后得到选择的5位原始信息$[b_1(1),b_1(2),\cdots,b_1(5)]$,从而保证区域控制中心接收到的ADS-B信息与无人机进行签名时的ADS-B信息一致,确保基于ADS-B和无证书签名的无人机跨域认证机制中数字签名方案的正确性和有效性。若区域控制中心基于纠错码恢复出来的验证信息与在无人机进行签名时哈希验证使用的信息不一致,就丢弃该信息,并将相关记录汇报给监管机构,由监管机构对其违规行为进行相应处理。

3 结束语

本文探讨了区块链赋能低空智联网的协同监管问题,首次提出了一种基于联盟链的链上链下三面协同监管架构体系。在该架构体系中,监管机构不仅利用链上的信息,还结合了链下物理层面的ADS-B信息,实现了集空域安全、频谱安全和数据安全为一体的综合安全管控,提高低空智联网应对多样化安全管控风险的处置能力。同时,本文还解决了传统的监管方式存在行业间数据和资源隔离无法得到有效协同管控的问题,以及现有的基于区块链的解决方案存在链上信息和链下信息割裂的问题。然后,提出了一种基于ADS-B和无证书签名的无人机跨域认证机制,解决了无人机群在执行任务时需要进行跨信任域和跨网络环境的无人机身份信息管理问题,并提出了一种基于纠错码的跨层签名的算法来解决ADS-B传输过程中因信道噪声造成的误码率导致签名失效的问题。基于本文所提的三面协

同架构体系开发的联盟链监管平台已被成功应用于长江低空示范试验区。试验结果表明,通过联盟链监管平台可以整合各类数据资源,实现了对低空经济各参与方数据的集成、分析和应用,构建了综合性的低空管控平台,协同管理低空中的空域资源、频谱资源和数据资源。该平台将促进低空经济带安全有序地发展,为内河低空智联网建设与无人机应用创新地构建了示范作用的体系、标准和规范。

参考文献:

[1] 董超, 经宇骞, 屈毓锛,等. 面向低空智联网频谱认知与决策的云边端融合体系架构[J]. 通信学报, 2023, 44(11): 1-12.
DONG Chao, JING Yuqian, QU Yuben, et al. Cloud-edge-device fusion architecture oriented to spectrum cognition and decision in low altitude intelligence network[J]. Journal on Communications, 2023, 44(11): 1-12.

[2] 吴启晖, 董超, 贾子晔,等. 低空智联网组网与控制理论方法[J/OL]. 航空学报, (2023-05-15)[2024-01-21]. http://kns.cnki.net/kcms/detail/11.1929.V.20230512.1733.042.html.
WU Qihui, DONG Chao, JIA Ziye, et al. Networking and control mechanism for low-altitude intelligent networks[J/OL]. Acta Aeronautica et Astronautica Sinica, (2023-05-15)[2024-01-21]. http://kns.cnki.net/kcms/detail/11.1929.V.20230512.1733.042.html.

[3] 张珉, 董超, 杨朋,等. 无人机自组网路由协议研究综述[J]. 数据采集与处理, 2022, 37(5): 952-970.
ZHANG Min, DONG Chao, YANG Peng, et al. Overview on routing protocols for flying Ad-Hoc networks[J]. Journal of Data Acquisition and Processing, 2022, 37(5): 952-970.

[4] WATKINS L, HAMILTON D, YOUNG T A, et al. The roles of autonomy and assurance in the future of uncrewed aircraft systems in low-altitude airspace operations[J]. Computer, 2023, 56(7): 41-53.

[5] 周福辉, 张子彤, 丁锐,等. 电磁频谱空间射频机器学习及其应用综述[J]. 数据采集与处理, 2022, 37(6): 1179-1197.
ZHOU Fuhui, ZHANG Zitong, DING Rui, et al. Survey on theory and applications of radio frequency machine learning for electromagnetic spectrum space[J]. Journal of Data Acquisition and Processing, 2022, 37(6): 1179-1197.

[6] AGARWAL P, SHARMA S, MATTA P. Security techniques in unmanned air traffic management system[C]//Proceedings of 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT).[S.l.]: IEEE, 2023: 641-646.

[7] PHADKE A, BOYD J, MEDRANO F A, et al. Navigating the skies: Examining the FAA's remote identification rule for unmanned aircraft systems[J]. Drone Systems and Applications, 2023, 11: 1-4.

[8] TEDESCHI P, SCIANCALEPORE S, DI PIETRO R. ARID: Anonymous remote identification of unmanned aerial vehicles [C]//Proceedings of Annual Computer Security Applications Conference. Virtual Event, USA: [s.n.], 2021: 207-218.

[9] WISSE E, TEDESCHI P, SCIANCALEPORE S, et al. A 2RID-anonymous direct authentication and remote identification of commercial drones[J]. IEEE Internet of Things Journal, 2023, 10(12): 10587-10604.

[10] TEDESCHI P, AL NUAIMI F A, AWAD A I, et al. Privacy-aware remote identification for unmanned aerial vehicles: Current solutions, potential threats, and future directions[J]. IEEE Transactions on Industrial Informatics, 2023, 20(2): 1069-1080.

[11] 庄子艾, 程欣, 刘文豪, 等. 基于蜂窝移动网的无人机监管系统设计与实现[J]. 计算机应用与软件, 2019, 36(7): 143-147, 155.
ZHANG Ziyi, CHENG Xin, LIU Wenhao, et al. Design and implementation of UAV supervision system based on cellular mobile network[J]. Computer Applications and Software, 2019, 36(7): 143-147, 155.

[12] GAO M, YAN T, FU W, et al. Automated flight technology for integral path planning and trajectory tracking of the UAV[J]. Drones, 2023, 8(1): 9.

[13] CONTE C, DE ALTERIIS G, MORIELLO R, et al. Drone trajectory segmentation for real-time and adaptive time-of-flight prediction[J]. Drones, 2021, 5(3): 62.

[14] SARENCHE R, AGHILI F, YOSHIZAWA T, et al. DASLog: Decentralized aauditable secure logging for UAV ecosystems [J]. IEEE Internet of Things Journal, 2023, 10(23): 20264-20284.

[15] ALJUMAH A, AHANGER T A, ULLAH I. Heterogeneous blockchain-based secure framework for UAV data[J]. Mathematics, 2023, 11(6): 1348.

[16] LUO H, WU Y, SUN G, et al. ESCM: An efficient and secure communication mechanism for UAV networks[J]. IEEE Transactions on Network and Service Management, 2024. DOI: 10.1109/TNSM.2024.3357824.

[17] AKRAM J, UMAIR M, JHAVERI R H, et al. Chained-drones: Blockchain-based privacy-preserving framework for secure

and intelligent service provisioning in internet of drone things[J]. Computers and Electrical Engineering, 2023, 110: 108772.

[18] HAFEEZ S, KHAN A R, AL-QURAAN M, et al. Blockchain-assisted UAV communication systems: A comprehensive survey[J]. IEEE Open Journal of Vehicular Technology, 2023, 4: 558-580.

[19] MISHRA A K, WAZID M, SINGH D P, et al. Secure blockchain-enabled authentication key management framework with big data analytics for drones in networks beyond 5G applications[J]. Drones, 2023, 7(8): 508.

[20] SUBRAMANI J, MARIA A, RAJASEKARAN A S, et al. Physically secure and privacy-preserving blockchain enabled authentication scheme for internet of drones[J]. Security and Privacy, 2024: e364.

[21] PAN H, CAO P, WANG W, et al. Blockchain-assisted cross-domain authentication and access control for low-altitude UAV [C]//Proceedings of 2023 IEEE/CIC International Conference on Communications in China (ICCC). [S.l.]: IEEE, 2023: 1-6.

[22] LEE S, SHIN J S. A new location verification protocol and blockchain-based drone rental mechanism in smart farming[J]. Computers and Electronics in Agriculture, 2023, 214: 108267.

[23] YANG Z, KANG X, GONG Y, et al. Aircraft trajectory prediction and aviation safety in ADS-B failure conditions based on neural network[J]. Scientific Reports, 2023, 13(1): 19677.

[24] TONG L, GAN X, WU Y, et al. An ADS-B information-based collision avoidance methodology to UAV[J]. Actuators, 2023, 12(4): 165.

[25] KACEM T, WIJESEKERA D, COSTA P, et al. Secure ADS-B design & evaluation[C]//Proceedings of 2015 IEEE International Conference on Vehicular Electronics and Safety (ICVES). [S.l.]: IEEE, 2015: 213-218.

[26] DUTLE A, MOSCATO M, TITOLO L, et al. Formal analysis of the compact position reporting algorithm[J]. Formal Aspects of Computing, 2021, 33: 65-86.

[27] 刘萍, 倪育德, 马宇申. ADS-B IN CPR编解码仿真及同频干扰研究[J]. 现代导航, 2013, 4(5): 342-347.
LIU Ping, NI Yude, MA Yushen. CPR encoding/decoding simulation and co-channel interference research about ADS-B IN [J]. Modern Navigation, 2013, 4(5): 342-347.

[28] 陈发堂, 何坚龙. LTE系统中Reed-Muller码的编译码算法[J]. 重庆邮电大学学报(自然科学版), 2010, 22(4): 395-399, 410.
CHEN Fatang, HE Jianlong. Reed-Muller coding in long term evolution[J]. Journal of Chongqing University of Posts and Telecommunications(Natural Science Edition), 2010, 22(4): 395-399, 410.

[29] 黄俊杰, 徐位凯, 陈启望, 等. 一种改进的Reed-Muller码递归构造方法[J]. 重庆邮电大学学报(自然科学版), 2015, 27(3): 366-371.
HUANG Junjie, XU Weikai, CHEN Qiwang, et al. Improved recursive constructing method of Reed-Muller codes[J]. Journal of Chongqing University of Posts and Telecommunications(Natural Science Edition), 2015, 27(3): 366-371.

[30] YANG T Y, CHEN H. Modified majority logic decoding of Reed-Muller codes using factor graphs[J]. IET Communications, 2018, 12(7): 759-764.

作者简介:

金永光(1999-),男,硕士研究生,研究方向:区块链、无人机认证与监管,E-mail: yongguangjin999@163.com。

叶方伟(1990-),**通信作者**,男,教授,硕士生导师,研究方向:信息安全与隐私、信息论与编码理论、统计与机器学习理论,E-mail: fangweiye@nuaa.edu.cn。

卢晓珍(1994-),女,副教授,硕士生导师,研究方向:无线通信安全、安全强化学习、联邦学习,E-mail: luxiaozhen@nuaa.edu.cn。

吴启晖(1970-),男,教授,博士生导师,研究方向:认知信息论、电磁空间频谱智能管控、天地一体化信息网络和无人机集群智能通信,E-mail: wuqihui2014@sina.com。

马凯光(1955-),男,特聘教授,博士生导师,新加坡工程院院士,研究方向:图像与视频处理、视频压缩、计算机视觉、人工智能,E-mail: kkma23@nuaa.edu.cn。

(编辑:张黄群)