ISSN 1004-9037,CODEN SCYCE4
Journal of Data Acquisition and Processing Vol. 41,No. 1,Jan. 2026,pp. 53－65
DOI:10. 16337/j. 1004-9037. 2026. 01. 004

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

面向低空高密度飞行安全的无人机识别信息可信构造与容量分析

孙汉存，白子轩，许　晋，葛　宁

（清华大学电子工程系，北京 100084）

摘　要：随着中国低空经济的高速发展，低空空域呈现超大规模节点接入与超高密度频谱复用的新特征，无人机实时安全监管成为重大挑战。根据中国强制性标准要求及民航局规定，无人机需以广播形式对其运行识别信息进行不间断报送，地面监测节点以此进行身份识别。然而标准广播模式缺乏源可信认证机制，存在较大安全隐患，且现有研究缺乏针对我国标准格式的广播容量理论分析与量化评估。针对以上问题，本文提出使用国密SM2算法的广播式运行识别信息可信构造方法，在标准广播报文基础上附加数字签名，形成抗攻击的强认证能力，规避国际算法后门风险。其次，建立适用于Wi-Fi信标广播体制的低空信道容量理论分析，并通过仿真实验验证表明载波侦听多址接入（Carrier sense multiple access，CSMA）机制相较纯ALOHA协议性能提升约85%。在理想信道环境假设下，使用2.4 GHz单频段、20 MHz带宽、1 s更新周期及18 dBm发射功率，引入国密签名后的可信广播理论容量为82架/km^2，有效满足当下15～22架/km^{2}的高密度容量需求。为降低引入签名带来的容量影响，本文进一步提出可变频次签名策略，在高密度场景下减少容量损失，同时确保身份认证信息的完整性与不可抵赖性。本文提出的签名方法与容量分析模型可为未来低空监管系统部署提供理论依据与设计参考。

关键词：低空经济；广播式运行识别；国密SM2签名算法；Wi-Fi信标；容量分析

中图分类号：V279＋.2；TN929.5　　**文献标志码：**A

引用格式：孙汉存，白子轩，许晋，等.面向低空高密度飞行安全的无人机识别信息可信构造与容量分析[J].数据采集与处理，2026，41(1)：53-65. SUN Hancun，BAI Zixuan，XU Jin，et al. Trustworthy remote identification and capacity analysis for high-density low-altitude UAV safety[J]. Journal of Data Acquisition and Processing，2026，41(1)：53-65.

引　　言

低空经济作为国家战略性新兴产业，正经历从政策驱动向规模商用的关键跃迁。近年来，中央设立低空经济发展专责机构，在“十四五”专项规划[1]基础上形成“十五五”规划建议，同时出台《无人驾驶航空器飞行管理暂行条例》等系列顶层设计，从空域管理、安全标准到产业培育奠定制度基础。地方层面积极响应，截至2025年，全国已有30多个省、市、区将低空经济纳入政府工作报告，在基础设施建设、产业链引育、标准体系制定与安全监管等方面配套财政支持与专项政策，形成央地协同的良性格局。政策与市场的双轮驱动下，全国掀起低空经济热潮，产业规模呈指数级增长。据民航局《民航行业发展统计公报》[2]报道，截至2024年底，全行业注册无人机共217.7万架，较2023年底激增98.5%；预计2030年将突破600万架；市场规模方面，预测到2035年将达3.5万亿元，发展前景广阔。

基金项目：企业创新发展联合基金（U22B2001）。
收稿日期：2025-11-15；**修订日期：**2026-01-13

低空规模扩张必然带来飞行活动的日趋稠密化与复杂化。以深圳为例,《深圳市低空基础设施高质量建设方案(2024—2026)》明确提出,到2026年底将建成低空起降点1 200个以上,开通载人、载货等各类低空商业航线1 000条以上。根据NASA UTM项目定义,目前低空高密度环境可达15~22架/km^{2}的运行负载[3]。可以进一步预见,随着低空产业纵深发展,低空空域将呈现超大规模节点接入、超高密度频谱复用及异构航迹时空交错的新特征。在此环境下,飞行器种类与数量繁多,三维飞行航迹交织复杂,“黑飞”“乱飞”问题频发,传统雷声光电监测手段因无法穿透障碍物且难以识别身份,对低慢小目标易出现漏检、错检,已无法适应低空空域监管需求。为此,美国于2021年率先提出Remote ID制度,强制无人机在飞行过程中主动广播身份、位置等信息,实现透明化监管[4]并完善相关法规体系。

中国低空监管体系建设同样稳步发展,2023年国家强制性标准《民用无人驾驶航空器系统安全要求》(GB 42590—2023)明确要求“轻型和小型无人驾驶航空器实施飞行活动,应通过网络主动向综合监管服务平台报送识别信息”,并规定“广播远程识别应采用Wi-Fi信标或蓝牙广播协议发送报文”。2024年,民航局进一步发布《民用微轻小型无人驾驶航空器运行识别最低性能要求》,规范每种类型的广播式运行识别报文采用固定25字节结构,并规定动态报文更新频率不低于1次/s。相关规范的出台,为低空飞行监管划定了技术基线。

然而,广播式运行识别机制在开放空口环境下存在安全缺陷。由于广播报文缺乏认证机制,极易受到欺骗、干扰或伪造信号攻击[5-6]。攻击者可轻易伪造基本ID报文或位置向量报文,使恶意无人机通过身份仿冒混入合法机群;或篡改位置信息突破电子围栏进入禁飞区;或实施报文重放攻击导致监管系统误判。虽然国内外已有部分研究考虑引入身份验证机制,但主要针对欧美Remote ID体制,采用的国际签名算法存在潜在后门风险[7]。而在已有的可信广播系统的容量分析研究中[8],也尚未针对中国标准格式下的低空广播容量展开探索。当下,针对中国广播式运行识别体制的可信身份构造方法及空口容量边界分析仍属空白。为此,本文研究了符合中国标准的广播式运行识别信息可信构造方法,并通过理论推导与仿真分析对其空口容量边界进行量化分析。主要贡献如下:

(1) 提出一种面向低空广播式运行识别信息的可信构造方法,基于国密SM2算法的可信签名构造方法,在报文基础上附加64字节SM2数字签名,实现低空飞行器源端广播的强身份认证。该方法在保持低通信与低计算开销的同时,具备自主可控特征,规避国际算法潜在后门风险。

(2) 建立Wi-Fi信标体制下的低空广播式身份认证空口容量理论模型,推导在高密度广播冲突信道下的最大并发节点数。实验结果表明,Wi-Fi信标体制采用载波侦听多址接入(Carrier sense multiple access,CSMA),相较纯ALOHA性能提升约85%。在理想信道环境假设下,使用2.4 GHz单频段、20 MHz带宽、1 s更新周期及18 dBm发射功率,引入国密签名后的可信广播理论容量为82架/km^2,较标准广播下降15.5%,但仍远超当下15~22架/km^{2}高密度定义容量,并为未来5~10年的发展留有充分空间。

(3) 提出可变频次签名策略,通过对无人机广播的静态身份信息选择性签名,在高密度场景下可将容量损失控制在5%~10%范围内,同时确保身份认证信息的完整性与抗抵赖性,为未来高密度低空飞行场景提供可扩展的安全认证方案。

1 研究现状

1.1 广播式身份认证机制

当前,针对Remote ID安全增强的研究主要包含基于公钥签名和基于轻量级对称认证两种。欧美Remote ID安全研究主流方案普遍采用数字签名体系,利用数字签名算法(Digital signature algorithm,DSA),椭圆曲线数字签名算法(Elliptic curve digital signature algorithm, ECDSA)及Ed25519算法等方案[9]为广播内容附加签名实现实时身份认证。然而,此类方案在无人机高密度场景中可能存在不同程度的效率问题。部分方案(如DSA)生成的签名长达256位,计算开销大,在无人机硬件平台上将带来

较大的计算时延。而后续的ECDSA等签名方案虽缩短了签名长度,但并没有规避数字签名路线本身带来的报文加长和密钥管理问题。随着对隐私保护需求的提升,研究者提出A^{2}RID[10]协议,通过群签名技术,对无人机广播信息签名避免无人机被长期追踪,但需要更大的通信开销代价。针对上述公钥签名路线的局限性,一些研究尝试利用定时高效流丢失容忍认证机制(Timed-efficient stream loss-tolerant authentication,TESLA)等轻量级对称认证协议[11]规避密钥管理的复杂度。然而,该技术路线能够认证的是拥有相同密钥的成员身份,而非某个特定个体的唯一身份[12],不符合我国对无人机使用"综合监管服务平台"进行统一监管的需求。此外,该路径依赖于SHA-256/密钥哈希信息鉴别码(Hash-based message authentication code,HMAC)系美标算法和跨域无人机服务供应商,对非盟友国存在技术封锁条款,与我国自主可控的要求也直接冲突。因此,当前欧美身份认证机制的发展方向与我国需求仍存在较大的不一致性,直接参照欧美发展路径存在较大风险。

国内研究方面,国密SM2/SM3算法在车联网[13]等场景中已验证技术可行性,而其64字节签名长度和适配于国产硬件的加速潜力为无人机场景提供了较好基础。考虑到数字签名路线的准确个体身份认证能力和实时认证优势,使用国密算法进行无人机广播式身份认证存在较强的可行性。然而,当前研究尚未系统探索国密算法在无人机广播式运行识别中的具体应用方式。

1.2 高密度广播信道容量理论分析

随着无人机密度激增,广播信道容量边界成为了监管系统效能的关键制约。早期无线信道容量分析始于ALOHA与CSMA的对比研究。ALOHA协议作为纯粹的随机访问机制,其最大吞吐量理论极限为18.4%(纯ALOHA)[14]与36.8%(时隙ALOHA)[15],在低节点密度下尚可维持,但节点数超过50时碰撞概率呈指数级上升。CSMA协议通过载波监听将理论容量提升至60%~80%,但仍无法避免隐藏终端问题。IEEE 802.11标准的CSMA/CA机制引入虚拟载波侦测与指数退避,奠定了现代随机接入网络的理论基石。Bianchi[16]提出的二维马尔可夫链模型是分析高密度场景下CSMA/CA容量的里程碑工作。

在Wi-Fi广播模式下,我国规定无人机广播式运行识别采用Wi-Fi信标帧,其与分布式协调功能数据模式存在本质差异。信标广播不接收确认应答,无人机发送端无法感知碰撞,导致传统基于重传退避的Bianchi模型[16]失效。在此条件下,信标广播过程应建模为无重传、单次退避的简化CSMA协议。Ma等[17]、Ni等[18]、Samaras等[19]通过引入空闲状态、排队论模型等方法,将Bianchi模型[16]迁移至非饱和信道、广播通信与隐藏节点等场景下的信道模型分析。当下针对无人机广播运行识别信息的容量分析研究较少,且主要针对欧美Remote ID标准。美国联邦航空管理局通过野外试验数据给出了在多设备场景下的包接收率和探测概率随设备密度的变化[20],但并未给出理论建模与分析。朱奕安等[21]通过实测数据详细分析了Remote ID的传输距离和定位误差等性能,并提出基于深度强化学习的通信协议配置算法,有效降低了高密度低空飞行场景下的通信时延[22],但尚缺乏针对Wi-Fi信标广播中CSMA机制的容量分析,因此目前仍需从理论角度完善对该广播模型的性能研究。另外在广播内容上,现有研究尚未对国密签名在低空场景下的空口容量损耗进行定量评估,在环境建模时也未考虑我国民航局对轻小型无人机在2.4 GHz频段的有效全向辐射功率(≥11 dBm)要求,相关系统性的容量仍有待分析。

2 无人机运行识别广播场景系统建模

本文考虑一个连续的三维空域,其中无人机节点的地理位置服从强度为ρ的均匀泊松点过程(Poisson point process, PPP)分布,无人机的高度服从区间$[h_{\min}, h_{\max}]$上的均匀分布。各无人机节点依照国家标准规定的频次与功率采用Wi-Fi信标协议广播运行识别信息,本文将单一无人机的广播事件建模为一个强度为λ的泊松过程。假设空间中的通信信道是理想的自由空间信道,信号在传播过程中只经历自由空间路径损耗,忽略阴影衰落和多径衰落等干扰,发射端与接收端天线具有单位增益,传播过程

中的路径损耗可以表示为

$$\mathrm{PL(dB)}=10\lg\frac{P_{\mathrm{T}}}{P_{\mathrm{R}}}=-20\lg\frac{c}{4\pi df_{\mathrm{c}}} \tag{1}$$

式中：P_{T}为发射端功率，P_{R}为接收端功率，c为光速，f_{c}为载波频率，d为发射端与接收端之间的距离。各地面监测站位置固定，并具备瞬时信干噪比(Signal to interference plus noise ratio，SINR)检测能力。系统的瞬时信干噪比定义为

$$\mathrm{SINR}_i=\frac{P_{\mathrm{R}i}}{P_{\mathrm{noise}}+\sum\limits_{k\in M,\ k\neq i}P_{\mathrm{R}k}} \tag{2}$$

式中：$P_{\mathrm{R}i}$表示无人机i广播的信号在监测站处接收到的功率强度，P_{noise}为接收机噪声功率，M表示所有同时发送数据的无人机集合。监测站接收来自无人机i的信号时，首先检测接收端的功率强度$P_{\mathrm{R}i}$是否超过接收灵敏度阈值P_{th}。当$P_{\mathrm{R}i}>P_{\mathrm{th}}$时，监测端进一步判定$\mathrm{SINR}_i$的强度，当$\mathrm{SINR}_i$超过预设的解调门限$T_{\mathrm{th}}$时，信号能够成功解码。

本文评估以下两种经典的随机接入协议的网络状态。

(1) 基于ALOHA的无人机运行识别信息广播

在纯ALOHA协议下，每个无人机节点在需要广播运行识别信息时立即发送数据包，无需侦听信道状态。这种机制的优点是协议开销极低，但缺点是当多个无人机在同一时间窗口内发送数据时，数据包会发生碰撞，导致传输失败。因此，纯ALOHA方法在高密度场景下的传输失败率较高。Wi-Fi信标广播本身不使用ALOHA协议，本文将其作为基线方法提供参考。

(2) 基于CSMA的无人机识别信息广播

CSMA引入了信道感知机制。在此模式下，无人机尝试发送数据前，首先侦听信道以确定信道是否被其他用户占用。若其感知信道空闲，则发送数据；否则，将执行退避策略推迟发送数据。CSMA模式能够有效降低数据包碰撞的概率，但在无线通信环境中，无人机无法实现全局信道状态感知，CSMA模式无法避免隐藏节点问题。这一模式下的场景示意图如图1所示。根据802.11协议，目标节点检测信道繁忙包含载波侦听和能量检测两种模式，即检测信号前导码的灵敏度门限，以及在未检测出前导码的能量监测阈值。在20 MHz带宽场景中，802.11协议建议的信号检测灵敏度门限为$P_{\mathrm{cs}}=-82$ dBm，能量检测阈值为-62 dBm。在无人机广播运行信息场景中，所有信息都以802.11协议格式发送，目标节点的侦听范围以CS/CCA门限为准。图1的蓝色虚线范围表示目标节点可以侦听到的广播信息区域。而在侦听范围之外的无人机，即隐藏节点，在广播信息时目标节点无法判定信道繁忙，仍可能出现数据包碰撞的情况。后文将基于这一系统模型进行Wi-Fi信标体制下的可信广播式运行识别信息的空口容量理论分析与仿真实验验证。

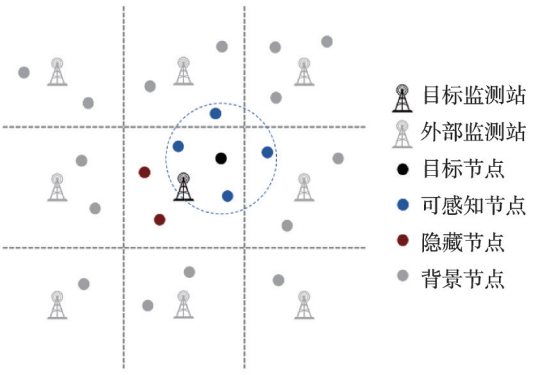

图1 CSMA模式下广播场景示意图

Fig.1 CSMA-based broadcast operation model

3 可信广播式运行识别信息构造与容量分析

3.1 可信广播式运行识别信息构造方法

本节讨论采用Wi-Fi信标广播协议发送报文的广播场景。现行基于《民用无人驾驶航空器系统安

全要求》GB 42590—2023国家标准的信息帧结构在开放空口下存在伪造、篡改等威胁。为填补该安全缺口,本文在标准报文尾部附加数字签名字段,形成可信运行识别信息广播帧,帧结构如表1所示。Wi-Fi信标帧中,各字段的含义或取值如下。(1) Element ID:固定取值为221,代表IEEE 802.11协议规定的厂商专用字段。(2) Len:表示从OUI/CID字段到信标帧结束所有字段总长度。(3) OUI/CID:固定取值为16 387 004,为无人机运行识别信息的专用编码。(4) Vend Type:固定取值为13,为Wi-Fi信标广播场景的专用编码。(5) Message Counter:消息计数器,取值范围为0~255。(6) 运行识别信息:第1字节固定取值为25;第2字节取值为打包报文中的报文数量N,最大为10;第3字节开始,依次为每条报文的报头及其内容,单条报文总长度为25字节。(7) 数字签名:数字签名字段长度为64字节,签名算法选取与生成流程见3.2节。

表1 Wi-Fi信标模式下可信广播式运行识别信息帧结构

Table 1 Frame structure of trustworthy remote ID under Wi-Fi Beacon mode

字段	Element ID	Len	OUI/CID	Vend Type	Message Counter	运行识别信息	数字签名
长度/字节	1	1	3	1	1	$2+N\times25$	64

目前,广播式运行识别报文的必选内容包括基本ID报文、位置向量报文与系统报文,运行描述报文为可选项。因此,以最长报文为例,可信广播式运行识别信息的报文长度约为173字节。在信息更新率方面,广播式运行识别信息的播发频次为静态报文至少3 s一次,动态报文至少1 s一次。

3.2 基于SM2的无人机广播式识别信息签名与验证方法

为了确保无人机广播的运行识别信息具备数据完整性和不可抵赖性,采用SM2算法实现广播式运行识别信息的可信数字签名。SM2算法是我国自主研发的基于椭圆曲线密码的公钥密码算法[23]。本节提出基于SM2算法的无人机广播式运行识别数字签名方法,具体包括系统初始化、密钥生成、数字签名生成和数字签名验证。

(1) 系统初始化

基于大素数q构造有限域F_q,并构造一个椭圆曲线方程$E(F_q)$:$y^2=x^3+ax+b\ (\mathrm{mod}\ q)$。选择椭圆曲线$E(F_q)$上的一个基点$G=(x_G,y_G)$,确定基点$G$的阶为$n$,并确定椭圆曲线$E(F_q)$中$n$的余引子$h$,构成SM2算法的系统参数集$P=\{F_q,\ a,b,G,n,h\}$,其中$n$为256比特。

(2) 密钥生成

无人机随机选取整数$d_A(1\leqslant d_A\leqslant n-2)$作为私钥,并计算$P_A=d_AG=(x_A,\ y_A)$作为公钥对外公开,用于验证签名。此外,签名者与验签者都需要计算用户的杂凑值Z_A以增强安全性。Z_A通过对无人机ID、公钥和系统参数进行哈希运算得到,即$Z_A=H_{256}(\mathrm{ENTL},\ \mathrm{ID},\ a,\ b,x_G,y_G,\ x_A,\ y_A)$。其中,ID为国家标准文件《民用无人驾驶航空器唯一产品识别码(征求意见稿)》规定的,每台无人驾驶航空器应具有的长度为20字符的唯一产品识别码;ENTL是由ID长度转化而来的字节数组。

(3) 数字签名生成

记M为待签名数据,即无人机的广播式运行识别信息,数字签名生成包含以下步骤:

① 拼接杂凑值Z_A与广播式运行识别消息M,并进行哈希计算,得到哈希值$e=H(Z_A\|M)$。

② 选择随机数$1\leqslant k\leqslant n-2$,并计算椭圆曲线点$(x_1,y_1)=[k]G$。

③ 计算签名分量$r=(e+x_1)(\mathrm{mod}\ n)$,如果$r=0$或$r+k=n$,则返回步骤②。

④ 计算签名分量$s=\left((1+d_A)^{-1}\cdot(k-rd_A)\right)(\mathrm{mod}\ n)$,如果$s=0$,则返回步骤②。

⑤ 将(r,s)作为消息的数字签名输出。其中,两个分量的长度各自为32字节,数字签名总长度为64字节。

(4) 数字签名验证

为了验证签名是否由正确的私钥生成,以及消息在传输过程中是否被篡改,接收端利用公钥验证数字签名的过程,包含以下步骤:

① 检查签名分量是否在合法范围内,即$1 \leqslant r, s \leqslant n-2$。若验证失败,则验签不通过。

② 计算待验数据$e' = H(Z_A \| M')$,计算$t = r + s \pmod n$。若$t = 0$,则验签不通过。

③ 计算椭圆曲线点$(x_1', y_1') = [s]G + [t]P_A$,计算$R = (e' + x_1') \pmod n$。若$R = r$,则验签通过。

表2展示了基于SM2算法的签名方法与国际现有无人机广播式运行识别信息认证方法的性能对比。其中,TESLA认证方法[11]采用基于对称密钥认证机制,其认证对象为同一密钥组内的成员,且依赖密钥延迟披露完成验证,无法实现对单条广播消息的实时身份;A^{2}RID[10]通过引入基于双线性映射的群签名机制,实现匿名条件下的认证,但导致通信开销显著增加,在高密度无人机广播场景下面临可扩展性挑战。相比之下,基于ECDSA[9]与本文的SM2签名方法,能够对单一无人机个体实时认证,签名字段长度较低,更适合广播认证场景。进一步,SM2作为国家密码标准算法,在标准化与监管合规性方面具有天然优势。因此,本文方法在保证个体身份可验证的同时,兼顾了实时性、通信效率与签名可靠性,更适用于我国无人机广播式运行识别场景。

表2 典型无人机运行识别认证机制对比

Table 2 Comparison of UAV Remote ID authentication methods

对比项目	TESLA[11]	A^{2}RID[10]	ECDSA[9]	SM2
认证对象	同一密钥组的无人机群	单一无人机	单一无人机	单一无人机
认证实时性	延迟认证	实时认证	实时认证	实时认证
认证机制	对称密钥认证	基于双线性映射的群签名	基于椭圆曲线的数字签名	基于椭圆曲线的数字签名
单条认证字段长度/字节	64	约1 300	64	64

3.3 可信广播式运行识别信息容量分析

在纯ALOHA模式下的空口容量已经有较成熟的研究,本节主要分析CSMA模式下的广播式运行识别信息的空口容量。我国无人机广播式运行识别信息采用Wi-Fi信标帧,在CSMA监听过程中,只进行单次退避,在退避计数器归零时发送数据。信标广播不接收确认应答,因此无人机发送端无法感知碰撞,不存在数据重传。将广播运行识别场景下,单无人机节点的状态建模为一个马尔可夫过程,由于只进行单次退避,状态转移模型得到简化,其状态转移图如图2所示。其中,与Bianchi模型[16]类似,状态$0, 1, \cdots, W_0 - 1$表示节点退避过程的计数状态。为了实现非饱和信道的分析,状态转移图中引入状态-1,表示节点处于空闲状态,没有需要发送的数据包。依据Bianchi模型,马尔可夫过程状态转移的虚拟时间间隔为

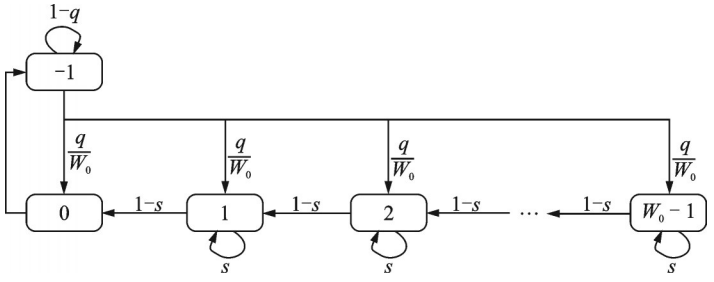

图2 CSMA模式下节点状态转移图

Fig.2 State transition diagram for CSMA-based broadcast

$$T_{\mathrm{v}}=(1-s)t_{\mathrm{Slot}}+sT_{\mathrm{s}} \tag{3}$$

式中:t_{Slot}代表信道中单一时隙的时间,T_{s}代表一次成功的传输所占用信道的时间,s代表信道繁忙的概率,即在节点能够侦听到的范围S_{c}中,没有其他节点正在发送的概率。令每一个虚拟时隙T_{v}中,单一节点发送数据的概率为p_{tran},而S_{c}中节点服从强度为ρ泊松点过程,因此有

$$s=\sum_{n=0}^{+\infty}\frac{\mathrm{e}^{-\rho S_{\mathrm{c}}}(\rho S_{\mathrm{c}})^{n}}{n!}\left(1-(1-p_{\mathrm{tran}})^{n}\right) \tag{4}$$

在状态转移图中,q代表单一虚拟时隙T_{v}中,节点有新的待发送数据包的概率,即

$$q=1-\mathrm{e}^{-\lambda T_{\mathrm{v}}} \tag{5}$$

基于图2,可以得到马尔可夫链的状态转移方程为

$$\begin{cases}P(-1|-1)=1-q\\P(-1|0)=1\\P(i|i)=s\\P(i-1|i)=1-s\\P(0|-1)=P(i|-1)=\dfrac{q}{W_0}\end{cases} \tag{6}$$

式中$i=1,2,\cdots,W_0-1$。根据上述马尔可夫过程的状态转移方程可以求得该过程的稳态分布S为

$$\begin{cases}S_{-1}=\dfrac{2(1-s)}{2(1+q)(1-s)+q(W_0-1)}\\S_0=\dfrac{2q(1-s)}{2(1+q)(1-s)+q(W_0-1)}\\S_i=\dfrac{W_0-i}{W_0}\dfrac{2q}{2(1+q)(1-s)+q(W_0-1)}\end{cases} \tag{7}$$

根据状态转移图的定义,在每一个虚拟时隙中,单一节点发送数据的概率为$p_{\mathrm{tran}}=S_0$。基于以上分析,将CSMA的退避过程对节点的影响等效建模为对数据发送频率的影响。基于式(4~7),可以数值求解其中的未知量T_{v}、s、q、p_{tran}。

基于以上退避流程,目标节点在广播运行识别信息时能够避免与侦听范围内节点的数据包碰撞。但CSMA方法无法避免隐藏节点问题,因此需要考虑隐藏节点对广播事件的影响。利用自由空间路径损耗公式,无人机A的发射功率P_{T},载波侦听门限P_{cs}以及监测站接收灵敏度P_{th},可以得到无人机能够侦听到的区域半径r_{c},以及监测站O能够接收到信号源的最大距离r_{t}。假定无人机与监测站之间的距离为d,图3展示了在广播运行识别信息场景下,因为隐藏节点影响造成影响的区域范围。其中,为了简化分析,将无人机、监测站设置为相同高度只考虑平面上的隐藏节点分布。记C_{Ac}、C_{Ot}分别为无人机侦听区域与监测站可接收区域,图中C_1与C_2所示区域为对无人机A造成干扰的潜在隐藏节点。而由于监测站的SINR检测机制,与监测站距离超过r_i的节点在监测站接收时,由于功率较低不会对无人机A的广播信息造成干扰。当$r_i<r_{\mathrm{t}}$时,实际对无人机A造成干扰的节点为区域C_2中的节点。因此,对节点A造成干扰的节点所在区域面积为

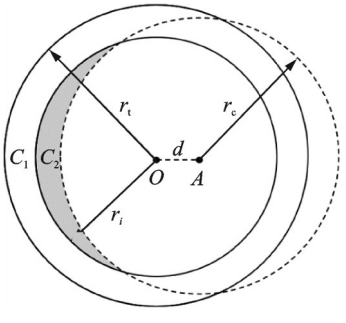

图3 CSMA模式下隐藏节点区域示意图

Fig.3 Hidden node region in CSMA-based broadcast

$$S_{\mathrm{h}}(d)=\begin{cases}S(r_{\mathrm{t}},r_{\mathrm{c}},d)-S(r_i,r_{\mathrm{c}},d) & r_i<r_{\mathrm{t}}\\ S(r_{\mathrm{t}},r_{\mathrm{c}},d) & r_i\geqslant r_{\mathrm{t}}\end{cases} \tag{9}$$

式中$S(r_1,r_2,d)$代表两圆相交时,其中一圆面积减去相交面积的计算公式,为

$$S(r_1,r_2,d)=\pi r_1^2-r_1^2\arccos\frac{d^2+r_1^2-r_2^2}{2dr_1}-r_2^2\arccos\frac{d^2+r_2^2-r_1^2}{2dr_2}+\sqrt{d^2r_1^2-\left(\frac{d^2+r_1^2-r_2^2}{2}\right)^2} \tag{10}$$

为了能够完整地传输广播信息,侦听区域内的节点在同一时隙不能发送广播信息,且隐藏节点在后续的K个虚拟时隙不能发送广播信息,其中K表示一次完整的广播信息占用的虚拟时隙数。由于隐藏节点之间广播事件也存在CSMA的限制,各隐藏节点间的广播事件不完全独立,近似得到监测站能够正确接收广播信息的概率表达式为

$$P_{\mathrm{s}}(d)=\sum_{n_1=0}^{+\infty}\frac{\mathrm{e}^{-\rho\pi r_{\mathrm{c}}^2}(\rho\pi r_{\mathrm{c}}^2)^{n_1}}{n_1!}(1-p_{\mathrm{trans}})^{n_1}\sum_{n_2=0}^{+\infty}\frac{\mathrm{e}^{-\rho S_{\mathrm{h}}(d)}(\rho S_{\mathrm{h}}(d))^{n_2}}{n_2!}(1-p_{\mathrm{trans}})^{n_2K} \tag{11}$$

进一步,将$P_{\mathrm{s}}(d)$在区间$[0,r_{\mathrm{t}}]$上加权积分,可以计算监测站正确接收广播信息概率的理论近似值。

4 仿真结果与分析

4.1 仿真参数设置

本节通过数值分析仿真无人机广播式运行识别信息的空口容量。仿真实验中采用的相关仿真参数如表3所示。为了比较各方法的性能,本节选用以下评价指标:

(1) 数据包接收率(Packet reception ratio, PRR):表示监测站成功接收的广播式运行信息数据包总数占全部飞行器生成的数据包总数的百分比。

(2) 平均广播延时T_{d}:表示成功接收的数据包从生成到地面监测站接收过程的平均时间。

(3) 网络容量密度$\rho(p)$:表示在最小数据包接收率为p时,系统能够承载的最大无人机密度。

表3 仿真参数取值

Table 3 Simulation parameter settings

参数	取值
载波频率f_{c}/MHz	2 437
带宽B/MHz	20
数据速率R/Mbps	6
发射功率P_{T}/dBm	16~20
噪声基底P_{noise}/dBm	−95
接收灵敏度P_{th}/dBm	−82
SINR解调门限T_{th}/dB	10
时隙时间t_{slot}/μs	9
短帧间隔t_{SIFS}/μs	10
分布式帧间隔t_{DIFS}/μs	28
传播延时t_{prop}/μs	2
竞争窗口长度W_0	16

4.2 可信广播式运行识别信息容量仿真

相较于侧重多协议切换机制的部分现有研究,本文实验重点关注在我国标准Wi-Fi信标广播体制下,不同接入机制与系统参数对空口容量的影响。根据3.2节的分析,实验中设置标准无人机广播式运行识别信息数据平均包长为180字节,带有数字签名的可信广播式运行识别信息数据的平均包长为250字节。实验选取MAC帧头224位,物理层帧头192位。因此,可以利用信道的数据速率计算出不同长度数据包对应的发送时间,标准数据包约为361 μs,带有可信签名的数据包约为454 μs。在实验中,首先固定无人机广播信息的发射功率为20 dBm,比较ALOHA与CSMA两种模式下的数据包接收率,并将仿真结果与理论分析比较,结果如图4所示。根据实验结果可以看出,在相同广播状态下,相较于ALOHA模式,CSMA模式能够显著提升数据包接收率,特别是在高密度场景下作用更加明显。对广播数据进行签名在两种模式上都降低了检测率性能,但在CSMA模式下加入可信广播,性能仍好于ALOHA模式下的标准广播场景。此外,图4中两条虚线展示了CSMA模式下广播式运行识别信息空口容量的理论分析值,与实际仿真结果基本吻合。

CSMA模式由于避免了侦听范围内的大部分数据包碰撞,在数据包接收率上表现出较好的性能,但退避机制会导致数据包传输出现广播延迟T_d。依据国家现行规定,轻小型无人驾驶航空器的广播发射功率应不小于11 dBm,实验考虑不同的无人机广播发射功率P_T,选取16、18、20 dBm三个典型值进行分析。在不同功率条件下,广播数据包播发的平均延迟如图5所示。更大的发射功率让无人机能够侦听到更大范围内的信道干扰,因此所需要的平均退避时间相应更长。而采用可信广播方案增加了信道中每一个数据包的发送时间,进而增大了信道被占用的概率,导致广播数据的平均延迟增大,但整体的延迟在高密度场景下仍小于1 ms,远小于对广播数据新鲜度的需求,不会对系统性能造成显著影响。

无人机广播数据的接收率最终将决定信道的空口容量,进而决定空域中可承载无人机的密度。设定空域中允许的最小数据包接收率为$p=90\%$,比较不同场景下空域中的最大无人机密度$\rho(p)$。在不同的发射功率与广播模式的条件下,得到的最大无人机密度如图6所示。由于隐藏节点的存在,CSMA模式的性能无法到达理论最大吞吐量。根据实验结果,CSMA模式能够承载的最大无人机密度约为ALOHA模式的两倍。引入国密数字签名后的空域容量较标准广播模式下降约10%~20%,但仍高于ALOHA模式下的性能。此外,在不同的模式下,除了存在最大空域容量的不同,监测站可监听的最大范围也会影响系统整体的容量与成本。在P_T取值16、18、20 dBm时,监测站可监听的最大范围分别为0.77、0.98、1.23 km。若选择较小的无人机广播功率,能够减少隐藏节点的数目,减少可能的数据包碰撞,但由于信号传播能力有限,需要更密集的监测站部署,反之,选择较大的功率能够实现间隔更远的布站方案,但会造成空域容量的损失。

4.3 签名变频次容量仿真

根据以上分析,加入数字签名的广播式运行识别信息会在一定程度上增加空口负载,进而降

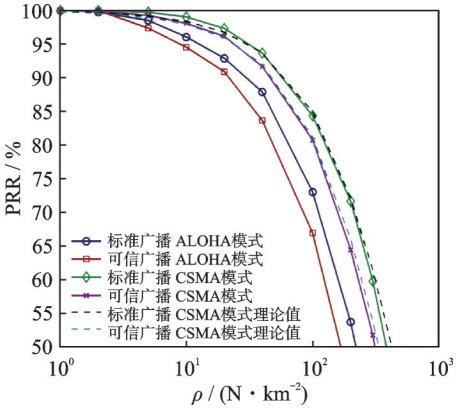

图4 ALOHA与CSMA模式下的PRR性能

Fig.4 PRR performance under ALOHA and CSMA modes

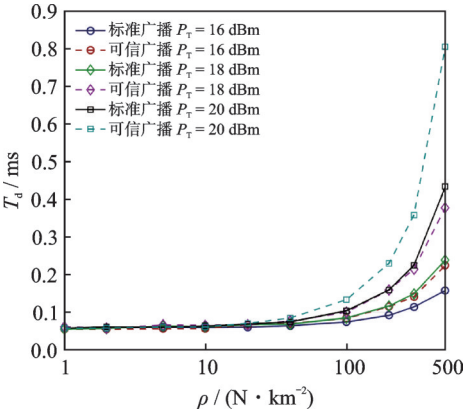

图5 不同广播功率在CSMA模式下的延时性能

Fig.5 Delay performance of CSMA under different transmission powers

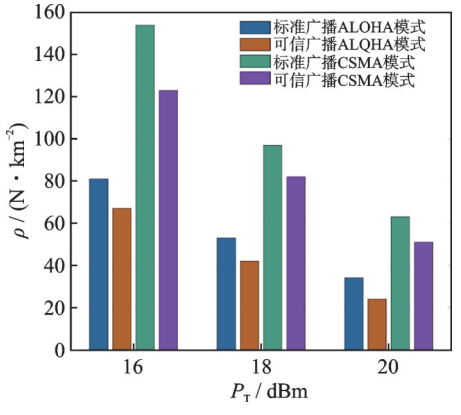

图6 不同广播功率下的空口容量性能

Fig.6 Air interface capacity under different transmission powers

低空口容量。在高密度场景下,本文进一步采用一种基于信息类型的变频次签名策略,以在安全需求与通信性能之间取得平衡。现有无人机的静态信息更新率与播报频次规范为至少3 s一次,而动态状态信息的播报频次为至少1 s一次。为了实现广播源的强身份认证与抗抵赖,本节提出一种签名策略为仅对包含静态身份信息的广播报文附加数字签名。以无人机广播功率20 dBm为例,图7展示了在变频次场景下,数据包接收率与空域无人机密度的变化趋势。在较高密度场景下,变频次签名能够在保障身份认证信息安全的需求下,提升3%~5%的PRR。相应地,在最小数据包接收率的约束下,在高密度空域采用变频次签名能够额外提升约10%的空域容量。因此,在实际场景中,可以根据业务安全需求和空域密度,选择是否使用数字签名以及签名频次,在系统容量与安全需求二者之间取得平衡。

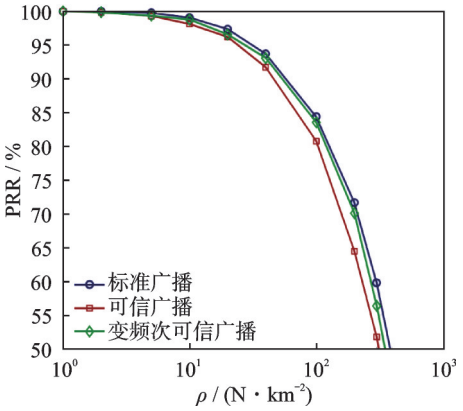

图7 变频次可信广播的PRR性能

Fig.7 PRR performance of variable-frequency trustworthy broadcast

5 未来展望

5.1 双频段协同

本文容量模型基于2.4 GHz单频段20 MHz带宽进行研究。面对低空高密度压力,2.4/5 GHz双频段频谱资源的协同是未来首要的研究方向。针对双频段资源,存在两种主要利用策略:双频段动态切换以及双频段冗余广播。

双频段动态切换指无人机可从2.4/5 GHz双频段中动态选择其一进行身份识别信息广播,实现广播容量的直接扩增。由于两频段在传播特性与电磁环境方面呈现显著差异,可以考虑随空域高度切换、随信道忙闲切换等多种切换方式。例如,在近地超低空区域(100 m以下)可以考虑使用5 GHz频段规避地面设备干扰,而在低空空域(100 m以上)采用2.4 GHz频段提升覆盖能力等。不同切换策略下的广播容量仍需进一步分析。

双频段冗余广播指无人机将相同的身份识别信息同时在2.4/5 GHz双频段上播发,虽不能带来广播容量的提升,但能够防止因某一频段过于拥塞导致信息丢失,从而提升接收端的接收概率。该方案适用于机场周边等对安全监管性能要求更高的重点监管区域,但代价是广播能耗将有所上升。

另外,我国自主研发的星闪短距通信技术[24],同样具有成为下一代低空识别载体的潜力。通过星闪基础接入技术(Sparklink basic,SLB)和星闪低功耗接入技术(Sparklink low energy,SLE)的双模协同,星闪能够实现短距离的全场景覆盖,但其目前在无人机平台的集成尚未完全成熟,且与现有Wi-Fi监测基础设施的协议栈兼容性有待验证。

5.2 编队时隙编排

在各维域资源难以进一步扩充的情况下,优化介质访问控制策略将有助于低空广播逼近理论容量上限。本文模型已说明,尽管有载波侦听作为性能保底,随机接入机制在超高密度下碰撞概率仍面临快速恶化,如果能够从密集竞争转向协同编排,或将更有利于提升超高密度下的广播容量。在物流、巡检等协同作业场景中,无人机群往往按照固定航路及编队飞行,机间的相对位置较为有序、变化幅度较小。此时,无人机群可采用TDMA协议将1 s的广播周期细分,集群成员按预先规划的顺序接入,信道容量将趋近于理论上限。然而,此方案要求无人机平台具备微秒级时钟同步精度(可通过GPS PPS信号或5 G空口同步),并牺牲广播的随机接入特性,更适用于行业级无人机集群。

另外,Wi-Fi联盟基于IEEE 802.11ai提出了Wi-Fi NAN(Neighbor awareness networking)协议[25],提供了轻量级时间窗口同步机制,可视为一种“软TDMA”折中方案。各节点在预先约定的发现窗口(Discovery window,DW)唤醒并广播身份报文,其余时间深度休眠,以极低能耗实现时分广播效果。其核心优势在于能够通过时间同步功能(Timing synchronization function,TSF)实现自组织毫秒级时钟同步,而无需依赖外部授时。但Wi-Fi NAN的各个DW内仍采用CSMA/CA竞争接入,未能消除隐藏终端问题,在无人机拓扑剧烈变化时,DW协商开销可能导致同步失效。故其适用性可能局限于低速场景,在高速混合作业空域的性能仍需进一步评估。

5.3 跨系统干扰共存

本文容量模型假设理想信道条件,然而实际城市环境中,2.4 GHz频段已被802.11n、蓝牙、ZigBee等无线系统广泛占用,跨系统干扰将导致无人机广播接收端基底噪声水平上升,对广播可靠性与系统容量产生进一步影响。针对上述问题,未来研究可在本文模型基础上纳入外部干扰强度、占空比等参数进行修正,以构建更贴近真实环境的理论模型。在无人机侧,可进一步探索基于认知无线电的频谱接入思路,通过对不同子信道干扰状态的短时感知,选择相对空闲的频段进行广播,以缓解干扰分布不均场景下的丢包问题。但该方式可能引入额外的感知时延,与运行识别信息的实时性要求之间存在潜在权衡。

除无人机自主感知外,还可考虑由地面监管平台汇聚区域内的频谱使用信息,并向无人机广播可用频段状态,辅助进行接入决策。然而,该方案将增加系统架构复杂度及部署成本。进一步地,从管理层面推动频谱共享或专用频段机制,亦可能为运行识别信息的可靠广播提供支撑,但相关问题仍涉及技术可行性、频谱资源协调及政策适配等多方面因素,未来仍需在各方案之间寻求最优解。

6 结束语

本文面向低空经济高密度发展背景下的无人机实时监管需求,针对我国广播式运行识别标准的安全与容量挑战,系统研究了基于国密SM2算法的可信构造方法及Wi-Fi信标体制下的空口容量边界。首先,提出了符合我国民航局规定的广播式运行识别信息可信构造方案。该方案在25字节强制报文基础上附加64字节SM2数字签名,满足了自主可控的安全监管需求。其次,建立了Wi-Fi信标广播模式的低空信道容量理论模型。理论分析表明,CSMA机制相较纯ALOHA协议使空口容量方面提升约85%;在理想信道环境假设下,使用2.4 GHz单频段、20 MHz带宽、1 s更新周期及18 dBm发射功率,引入国密签名后的可信广播理论容量为82架/km^2,较标准广播下降15.5%,但仍满足2030年前城市低空场景需求,且可通过动态调整签名间隔,降低引入签名带来的开销。由于本文容量模型较为理想,仍存在未考虑城市环境中异构系统的跨系统干扰、未建模蓝牙容量模型、动态签名频次动态调整等问题,未来工作将进一步探索低空监管系统的安全容量边界。

参考文献:

[1] 中国民用航空局、国家发展改革委、交通运输部.“十四五”民用航空发展规划[R].北京:中国民用航空局,2021.

[2] 中国民用航空局.2024年民航行业发展统计公报[R].北京:中国民用航空局,2025.

[3] National Aeronautics and Space Administration (NASA). Results and analysis from flight testing multiple USS providers in NASA's TCL4 demonstration[R]. Washington, DC, USA: [s.n.], 2020.

[4] BELWAFI K, ALKADI R, ALAMERI S A, et al. Unmanned aerial vehicles' remote identification: A tutorial and survey[J]. IEEE Access, 2022, 10: 87577-87601.

[5] TEDESCHI P, ALI AL NUAIMI F, 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, 2024, 20(2): 1069-1080.

[6] JIA Z, HE S, ZHU Q, et al. Trusted routing for blockchain-empowered UAV networks via multi-agent deep reinforcement learning[J]. IEEE Transactions on Communications, 2025, 73(12): 14227-14242.

[7] BERNSTEIN D J, LANGE T, NIEDERHAGEN R. Dual EC: A standardized back door[M]//The New Codebreakers. Berlin, Heidelberg: Springer, 2016: 256-281.

[8] ZHU Y, JIA Z, ZHANG L, et al. Delay optimization in remote ID-based UAV communication via BLE and Wi-Fi switching [EB/OL]. (2025-06-30). https://arxiv.org/abs/2506.07715.
[9] ALHASHMI A. A system for secure remote identification of drones[D]. Abu Dhabi: Khalifa University of Science and Technology, 2024.
[10] WISSE E, TEDESCHI P, SCIANCALEPORE S, et al. A^{2}RID: Anonymous direct authentication and remote identification of commercial drones[J]. IEEE Internet of Things Journal, 2023, 10(12): 10587-10604.
[11] VEARA J, JAIN M, MOY K, et al. TBRD: TESLA authenticated UAS broadcast remote ID[EB/OL]. (2025-10-30). https://arxiv.org/abs/2510.11343.
[12] PERRIG A, SONG D, CANETTI R, et al. Timed efficient stream loss-tolerant authentication (TESLA): Multicast source authentication transform introduction[R]. USA: RFC, 2005.
[13] 苏彬庭, 方禾, 许力. 基于国密SM2的车联网高效匿名认证协议[J]. 网络与信息安全学报, 2025, 11(3): 98-108.
SU Binting, FANG He, XU Li. Efficient anonymous authentication protocol for internet of vehicles based on Chinese cryptographic SM2[J]. Chinese Journal of Network and Information Security, 2025, 11(3): 98-108.
[14] ABRAMSON N. THE ALOHA SYSTEM: Another alternative for computer communications[C]//Proceedings of the Fall Joint Computer Conference. Houston, Texas: ACM, 1970: 281.
[15] BERTSEKAS D, GALLAGER R. Data networks[M]. Greece: Athena Scientific, 2021.
[16] BIANCHI G. Performance analysis of the IEEE 802.11 distributed coordination function[J]. IEEE Journal on Selected Areas in Communications, 2000, 18(3): 535-547.
[17] MA X, CHEN X. Performance analysis of IEEE 802.11 broadcast scheme in ad hoc wireless LANs[J]. IEEE Transactions on Vehicular Technology, 2008, 57(6): 3757-3768.
[18] NI M, ZHONG Z, PAN J, et al. Non-saturated performance analysis of IEEE 802.11 broadcast in 2-D mobile ad hoc networks [C]// Proceedings of 2012 IEEE Global Communications Conference (GLOBECOM). Anaheim, CA, USA: IEEE, 2013: 427-432.
[19] SAMARAS I K, HASSAPIS G D. A flexible analytical Markov model for the IEEE 802.15.4 unslotted mechanism in single-hop hierarchical wireless networks with hidden nodes[J]. Wireless Personal Communications, 2013, 72(4): 2389-2424.
[20] Federal Aviation Administration. Demonstration and validation of remote ID detect-and-avoid[R]. [S.l.]: ATM, 2025.
[21] 朱奕安, 何佳, 贾子晔, 等. 基于ADS-B与Remote ID的低空智联网无人机监视性能分析[J]. 数据采集与处理, 2025, 40(1): 27-44.
ZHU Yian, HE Jia, JIA Ziye, et al. ADS-B and Remote ID based performance analysis for UAV surveillance in low-altitude intelligent networks[J]. Journal of Data Acquisition and Processing, 2025, 40(1): 27-44.
[22] JIA Z, ZHU Y, WU Q, et al. Remote ID based UAV collision avoidance optimization for low-altitude airspace safety[J]. Chinese Journal of Aeronautics, 2025. DOI: https://doi.org/10.1016/j.cja.2025.103841.
[23] 国家密码管理局. SM2椭圆曲线公钥密码算法: GM/T 0003—2012[S]. 北京:中国标准出版社, 2012.
[24] 国际星闪联盟. 星闪无线通信系统架构V1.0.0 [EB/OL]. (2022-09-22). https://www.sparklink.org.cn/trial.
[25] Wi-Fi ALLIANCE. Wi-Fi aware specification v4.0[EB/OL]. (2022-12-07). https://www.wi-fi.org/file/wi-fi-aware-specification.

作者简介:

孙汉存(2000-),男,博士研究生,研究方向:通信网络安全等,E-mail: shc22@mails.tsinghua.edu.cn。

白子轩(1997-),男,助理研究员,研究方向:智能无线资源管理等。

许晋(1990-),男,助理研究员,研究方向:空间网络安全、低空安全管控、可信身份认证等。

葛宁(1971-),**通信作者**,男,研究员,研究方向:网络通信等,E-mail:gening@tsinghua.edu.cn。

(编辑:张黄群)

Trustworthy Remote Identification and Capacity Analysis for High-Density Low-Altitude UAV Safety

SUN Hancun, BAI Zixuan, XU Jin, GE Ning*

(Department of Electronic Engineering, Tsinghua University, Beijing 100084, China)

Abstract: With the rapid development of the low-altitude economy in China, the low-altitude airspace is characterized by massive device connectivity and intensive spectrum utilization, posing significant challenges to the real-time safety supervision of unmanned aerial vehicles (UAVs). According to China's mandatory standards and civil aviation regulations, UAVs are required to continuously broadcast their Remote identification (Remote ID) information for monitoring and identification. However, the absence of source authentication in standard broadcast protocols introduces security risks. Moreover, existing research lacks theoretical capacity analysis and quantitative evaluation specifically for the Chinese standard broadcast format. To address these issues, this paper proposes a trustworthy construction method for broadcast Remote ID utilizing the national SM2 cryptographic algorithm. By appending digital signatures to standard messages, this method ensures resilient authentication and eliminates potential security vulnerabilities inherent in international algorithms. Furthermore, we formulate a channel capacity model for the Wi-Fi Beacon broadcast system. Simulation results show that the carrier sense multiple access (CSMA) mechanism achieves an 85% performance improvement compared to the pure ALOHA protocol. Under ideal channel assumptions, using 2.4 GHz single-band, 20 MHz bandwidth, 1 s update cycle, and 18 dBm transmission power, the theoretical capacity of the trustworthy broadcast with SM2 signatures is 82 aircraft/km^2, which effectively meets the current high-density capacity demand of approximately 15—22 aircraft/km^2. Additionally, a dynamic signature frequency strategy is developed to balance security and capacity. The proposed signing method and capacity analysis model provide a theoretical foundation and design reference for the future deployment of low-altitude regulatory systems.

Highlights:

1. A trustworthy broadcast Remote ID scheme based on the national SM2 cryptographic algorithm is proposed for Wi-Fi Beacon-based UAV identification.
2. The capacity of trustworthy Remote ID broadcasting in high-density UAV scenarios is theoretically analyzed and evaluated.
3. A variable-frequency signature strategy is designed to balance security and capacity in high-density UAV scenarios.

Key words: low-altitude economy; broadcast remote identification; SM2 cryptographic algorithm; Wi-Fi Beacon; capacity analysis

---

Foundation item: Joint Fund for Enterprise Innovation and Development (No.U22B2001).
Received: 2025-11-15; **Revised:** 2026-01-13
***Corresponding author, E-mail:** gening@tsinghua.edu.cn.