IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 27 July 2022, accepted 14 August 2022, date of publication 18 August 2022, date of current version 25 August 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3199909

TOPICAL REVIEW

Unmanned Aerial Vehicles' Remote Identification: A Tutorial and Survey

KAIS BELWAFI, (Member, IEEE), RUBA ALKADI, SULTAN A. ALAMERI, (Member, IEEE), HUSSAM AL HAMADI, (Senior Member, IEEE), AND ABDULHADI SHOUFAN

Electrical and Computer Sciences Department, Khalifa University, Abu Dhabi, United Arab Emirates

Corresponding author: Kais Belwafi (kais.belwafi@ku.ac.ae)

This work was supported by the Khalifa University of Science and Technology from the External Fund under Grant 8434000388.

ABSTRACT UAV remote identification is an emerging technology that allows ground observers to identify a drone in the airspace and obtain information about it and its operator. The goal is to enhance safe operation over people and at night and protect public privacy. Two modes are known for remote identification: broadcast-based and network-based. Although both modes' technical implementation seems straightforward, remote identification is challenging because it includes multiple agents that follow different interests, such as safety, security, privacy, and businesses. Currently, enormous efforts for regulation, standardization, design, implementation, and testing are being made to put this technology forward. This paper aims to outline the landscape of these activities as a survey and tutorial to inform regulators, standardization organizations, industry, and researchers about the state of the art in this technology and to highlight its opportunities and challenges.

INDEX TERMS Remote identification, UAV, UTM, RID regulations, RID standards.

I. LIST OF ABBREVIATIONS

- **ACI:** Airports Council International
- **ADS-B:** Automatic Dependent Surveillance-Broadcast
- **ARC:** Aviation Rulemaking Committee
- **ASTM:** American Society for Testing and Materials
- **ATC:** Air Traffic Control
- **ATM:** Air Traffic Management
- **ATS:** Air Traffic services
- **BVLOS:** Beyond Visual Line of Sight
- **CAA:** Civil Aviation Administration
- **CTA:** Consumer Technology Association
- **DAE:** Drone Alliance Europe
- **DRIP:** Drone Remote Identification Protocol
- **EASA:** European Union Aviation Safety Agency
- **EIRP:** effective isotropic radiation pattern
- **ESN:** Electronic Serial Number
- **FAA:** Federal Aviation Administration
- **FIS-B:** Flight Information Service-Broadcast
- **FRIA:** FAA-Recognized Identification Areas
- **GCS:** Ground Control Station
- **GNSS:** Global Navigation Satellite System
- **GTA:** Government Telecommunication Authority
- **GUTMA:** Global UTM Association
- **IETF:** Internet Engineering Task Force
- **IMSI:** international mobile station identity
- **ISM:** Industrial Scientific and Medical
- **LPWAN:** Low-power Wide-Area Network
- **MCS:** Mobile Crowdsensing
- **MNO:** mobile network operator
- **NAN:** Neighbor Awareness Networking
- **NAS:** National Airspace
- **NASA:** National Airspace Agency
- **NPRM:** Notice of Proposed Rulemaking
- **PSN:** Physical Serial Number
- **ReDroId:** Remote Drone Identification
- **RFID:** Radio Frequency IDentification
- **SIAM:** Secure Integrated Airspace Management
- **TIS-B:** Traffic Information Service-Broadcast
- **UACES:** Unmanned Aircraft Cloud Exchange System
- **UACS:** Unmanned Aircraft Cloud System
- **UAS:** Unmanned Aircraft System

The associate editor coordinating the review of this manuscript and approving it for publication was Halil Ersin Soken.

- **UAV:** Unmanned Aerial Vehicle
- **UTM:** Unmanned Traffic Management
- **USS:** UAV service providers
- **USSP:** U-Space Service Provider
- **VLOS:** Visual Line of Sight

II. INTRODUCTION

The number of Unmanned aerial vehicles (UAVs) is growing and will exceed five million this year and the sales of UAVs will sur-pass 12$ billion, and the potential economic benefit of integrated unmanned airborne systems will generate an estimated $82 billion by 2025 [1]. UAVs, known as drones, are becoming popular due to multiple features such as usage flexibility and relatively low operating costs. Logistic services [2], traffic monitoring [3], agriculture [4], military espionage [5], and law enforcement surveillance [6] are examples of applications that drive the research in this field. Managing the expected large volume of air traffic is the biggest challenge for the wide adoption of this technology. Different threats limit the public acceptance of drone technology, like spying, physical collisions, and carrying explosives [7]. In addition, traditional air traffic management (ATM) systems are not suitable to meet the autonomy and mobility required by unmanned air traffic [8]. Therefore, governments through the world are striving to maintain a secure ATM system. This system seeks to ensure a sufficient level of autonomy and mobility of UAVs and simultaneously boost public acceptance of low-altitude urban air traffic [9].

The enforcement of regulations in low-altitude airspace has been slightly addressed in the literature. Yet, the proposed solutions suffer from serious shortcomings. For example, using wireless networks, Rahman *et al.* [10] proposed a policy enforcement system for UAVs in low-altitude airspace. The proposed method relies on logging the coordinates of the UAV to a cloud server, where the logged path is compared with the approved route of the mission. By this means, the system determines whether the UAV is flying in its allocated corridors or not. This solution is not only power demanding, but also malicious UAV operators can easily manipulate the coordinates to avoid tracking and penalties. Yazdinejad *et al.* [11] employed a set of servers allocated over a geographical area to address the issue of policy enforcement. The servers are used to authenticate drones when entering a specific corridor. The implementation of this solution is costly and lacks scalability as it needs to install numerous servers in each area to enforce the identification and authorization rules. [12] highlighted multiple issues related to the capabilities of law enforcement and national security agencies in detecting, locating, and identifying unlawful drones. So, today's main obstacle to adopting UAV applications is the absence of an efficient monitoring system that enforces the introduced rules and regulations in the urban vicinity.

To overcome some of these challenges, civil aviation agencies in many countries are mandating the deployment of remote identification. In basic terms, remote identification can be described as a digital license plate for UAVs. The ultimate goal of RID is to provide real-time identification and location information that can be used by the public and authorities to monitor airspace and penalize unlawful activities. The European Union Aviation Safety Agency (EASA) published amended regulations for remote identification in April 2020 ((EU) 2020/1058). These regulations mandate that all unmanned aircraft should be equipped with a remote identification system [13]. The FAA in the USA published a final rule for remote identification in January 2021 [14]. Remote ID regulations defined by aviation authorities are typically performance-based without exact specifications of supporting technologies. Instead, these regulations frequently refer to technical standards as possible ways of compliance. One of the standards is the American Society for Testing and Materials (ASTM) Standard Specification for Remote ID and Tracking [15]. ASTM defines two technologies for drones' remote identification: network-based and broadcast-based. The network-based method helps make remote identification information available globally on dedicated servers via the Internet. In the broadcast mode, the drone transmits its identification locally using one-way communication over Bluetooth or Wi-Fi without using the Internet protocol. A local observer can receive the remote ID in real-time using any handheld device that supports the proposed communication links. This remote identification mechanism is presented as a reliable way to detect, identify, track, and manage drones within urban airspace.

Zihe and Tian described the architecture of broadcast and network-based remote identification and reviewed the regulation status in the USA, Europe, Switzerland, Japan, and China [16]. We are also unaware of any survey work about this new technology. The literature lacks a comprehensive review highlighting remote identification's scope, opportunities, and challenges. This paper closes this gap by presenting an in-depth survey of the emerging remote identification technology. Although its technical realization appears straightforward, the RID technology is highly sophisticated and involves multiple stakeholders with different interests. Related activities in this field can be classified into four main categories as depicted in Fig. 1. As a public asset, the safety of airspace is the responsibility of governments in the first place. Therefore, civil aviation authorities worldwide are leading remote identification activities by issuing related regulations. These regulations go hand in hand with standardization efforts by multiple organizations. Regulations and standards seem to affect each other to a considerable extent. On the other hand, the technical capabilities have influenced regulations and standardization activities. For example, the capability of mobile devices and the lack of Internet connectivity have affected the mandated mode of remote identification by civil aviation authorities. The research on remote identification is emerging, and there are just a few contributions in the literature that we will review and discuss.

The paper is organized according to these categories of activities. The following four sections will review

related regulations, standards, technologies, and research.[1] Section VII discusses the RID technology, outlines its opportunities and challenges, and provides some future directions.

III. REGULATIONS

The UAS industry is a diverse and innovative field with enormous potential to enrich the job market. It was, thus, vital for industrialized countries to introduce a set of policies and regulations that paves the way for integrating UAVs into their national airspace while maintaining high levels of safety, privacy, and security for other airspace users as well as the public. In most cases, governments of such countries have already set general rules for commercial and recreational UAS operators, such as obligatory drone registration, avoiding operation in Beyond Visual Line of Sight (BVLOS) mode, flying over no-fly zones, or at night. Some countries have further developed a framework to manage the operation of UAS in the airspace, such as the USA [17], the European Union [18], Russia [19], and China [20]. A detailed review of these frameworks and policies is provided in [21].

Despite these efforts, only few governments have recently realized the significance of real-time UAS identification for allowing security agencies and law enforcement to: i) identify potential threats, ii) respond in real-time, and iii) gather enough information for investigation and forensics. This section, thus, surveys the current regulations related to the RID technology highlighting technical and legal aspects. Table 1 provides a brief overview of our survey.

A. USA

To keep up with the proliferation of recreational and commercial drones, the FAA strives to ensure the safe and secure operation of the airspace ecosystem by introducing standards and regulations. Several rulemakings have been released since the initiation of the UTM project in 2016, which presented a collaboration between the National Airspace Agency (NASA) and the FAA [29]. The four-year-long project comprised several tests in multiple states to demonstrate the required technology for realizing a safe and secure UTM.

In June 2016, the FAA published the final rule for Operation and Certification of Small Unmanned Aircraft systems [30]. Since then, the FAA anticipated a need for another rulemaking that fosters a safe and secure low-altitude operation. According to the FAA, remote identification is a crucial prerequisite for fully integrating UAS in the national airspace [22]. In the same year, the FAA established the Aviation Rulemaking Committee (ARC) to prepare a federal regulatory framework for the UAS operation over people, which also provided recommendations regarding available RID technologies [31].

In December 2019, the FAA released a Notice of Proposed Rulemaking (NPRM) for Remote Identification [32], seeking comments from the public to finalize the RID rules. Over 53k comments were received and reviewed by the FAA prior to announcing the final rule in January 2021 [22]. This rule defined the RID as a digital license plate that should be broadcast by drones weighing more than 0.55 pounds while airborne. Nonetheless, drones weighing less than 0.55 pounds are also required to broadcast a RID if flown over people or at night [33]. Moreover, the final rule identified the basic information that comprises the RID: a unique identifier for the drone, its location, the operator's location, the drone's velocity, a timestamp, and an emergency flag. However, this information may be received by any wireless devices within the broadcast range. The final rule states that correlating the drone's ID with the operator's personal information may only be done by the FAA [34]. It ensures that the privacy of airspace users is preserved.

Originally in the NPRM, the FAA proposed a networking-based RID solution for existing (legacy) drones (this solution will be detailed in Section VI). However, in response to the public comments, this solution was eliminated and replaced by a RID broadcast module that can be embedded into or attached to existing drones [22]. As such, all eligible drones flying under Part 107 [33] are required to broadcast their RID via radio frequency that is receivable by existing personal wireless devices. The operating frequency of the broadcasting module is limited to the unlicensed spectrum, which means 900MHz, 2.4GHz, or 5.8GHz. The broadcasting module shall be built into newly manufactured drones, while an add-on module is permitted for legacy drones. Moreover, the final rule emphasizes the importance of maximizing the broadcast range of the RID. It further states that drones should be manufactured to prevent the operator from disabling the RID function.

In summary, the FAA's final rule on RID requires operators to register their drones and broadcast the defined RID either by a built-in RID module or a stand-alone external module that can be attached to the drone. The latter category does not allow the operation beyond visual line-of-sight. A third category allows operators to fly without broadcasting RID within FAA-Recognized Identification Areas (FRIA) available to community-based organizations and educational institutions [34]. The operation within FRIAs is limited to visual line-of-sight. Finally, the FAA prohibited using ADS-B out and ATC transponders by UAS to limit possible interference with manned aviation communication. These RID final rules are set to be effective from September 2023 onward [22].

B. EUROPE

In Europe, multiple agencies and organizations have called for establishing a common framework that paves the way for drones' safe and secure integration into the airspace. As a result, several initiatives have been introduced. Perhaps, the European Commission was the first to highlight the necessity of remotely identifying drone pilots in the Riga Declaration in March 2015. They envisioned this remote identification framework as an ''electronic identity chip'' and

[1]These sections are relatively independent. Readers interested in specific topics can jump directly to the corresponding section.

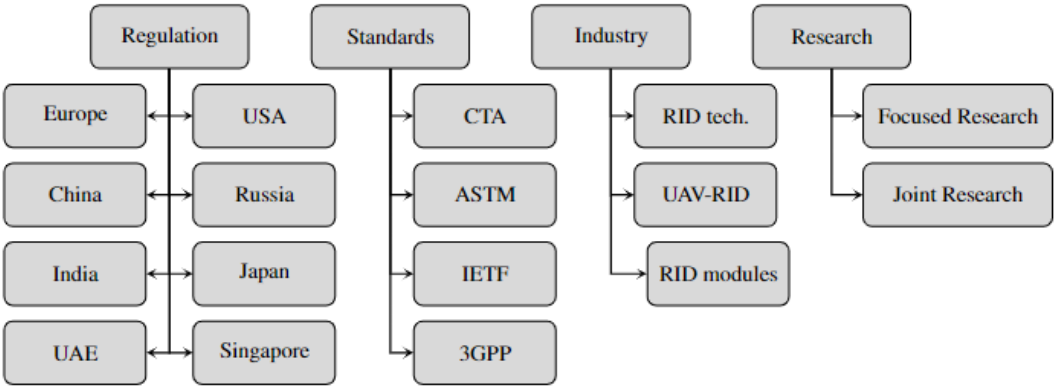


FIGURE 1. Activities related to remote identification.

TABLE 1. Regulations of UAV remote identification in selected countries.

Country	Regulation documents	Agency responsible for regulating UAS	Effective date	Possible means of compliance	Transmission technology	Data to be transmitted	Compliance and enforcement
USA	[22]	Federal Aviation Administration	Sep-2023	Standard RID drone / RID broadcast module add-on	Radio frequency (e.g. Wifi or Bluetooth)	Drone ID, location, altitude, velocity, takeoff location, elevation, time, ad emergency flag	Civil penalty up to $20000 for individuals and up to $33333 for companies.
Europe	[23]	European Union Aviation Safety Agency	Jan-2023	Direct RID / Network RID	Not specified	Operator registration number and verification code, UAS serial number, time, position and height of the UAS, route course, speed, pilot's position, and an emergency flag	
Russia	[19]	Ministry of Transport of the Russian Federation	NA	NA	ADS-B 1090 ES	NA	NA
China	[24]	Civil Aviation Administration of China	NA	Cloud-based surveillance, Direct RID broadcast	ADS-B, radar, cloud, wifi, bluetooth, etc.	operational details	NA
Japan	[25]	Ministry of Land, Infrastructure, Transport and Tourism	Jun-2022	Direct RID broadcast	Bluetooth 5.x, Bluetooth LE Long Range, Wi-Fi Neighbor Awareness Networking, and WiFi Beacon	registration ID, the UAS serial number, location, vector information of the UAS, and authentication information	A fine of up to 500,000 yen
India	[26]	Indian Civi Aviation	6 months from the date of notification	Direct RID	real-time tracking beacon	UAV location, speed, altitude, unified identification number	penalty up to $1332.39
Singapore	[27]	Director-General of Civil Aviation	2-Jan-2020	NA	visual or audio indicator	warnings	NA
UAE	[28]	General Civil Aviation Authority	NA	NA	Warning lights, visual display	registration number or code, or any other identification information, warnings	Up to 100,000 AED penalty.

referred to it as *IDrones*. The Single European Sky ATM Research (SESAR) Joint Undertaking (SJU) has also formalized the UAS integration process into the European airspace. They published multiple versions of the U-Space Concept of Operation (ConOps) [18].

In December 2015, the EASA released a Technical Opinion [35] on the ''Introduction of a regulatory framework for the operation of unmanned aircraft'' Advanced Notice of Proposed Amendment [36]. The document highlighted the role of registration and identification in improving the enforcement of airspace rules and regulations. The Technical Opinion further envisioned the technical implementation of the UAS identification system using existing technologies such as the cellular network or the radio frequency identification (RFID) technology.

Other organizations and committees have also realized the necessity of registration and identification as a centripetal requirement for safe and secure UAS integration into urban airspace. Examples of these organizations are the Drone Alliance Europe (DAE), the Airports Council International

(ACI), and the Global UTM Association (GUTMA). The DAE advocates that the UTM system shall be accompanied by a reliable registration and identification system [37]. Besides UAS identification, the ACI recommends using a *drone mission identification number* to facilitate a risk assessment procedure [38]. On the other hand, several publications [39], [40] by the GUTMA emphasized the role of remote identification in enabling a safe and secure UTM ecosystem.

In August 2016, EASA released a prototype ''Commission Regulation on Unmanned Aircraft Operations'' [41] which defined *electronic identification* as ''the capability to identify an unmanned aircraft in flight without direct physical access to that aircraft.'' It further detailed that ''the system shall transmit the following data as applicable according to standards acceptable by EASA: The registration of the operator; the class of the UAS; the type of UAS operation; the status of its geofencing; its position and height.'' Later, a series of rules [23], [42] have been published by EASA detailing the requirements and specifications of the UAS electronic identification. These eRules defined two main categories of UAS, namely: the *open* category and the *specific* category. The latter category is characterized by special features such as the UAS's ability to transport people and dangerous goods and operate over crowds. Drones operating under this category require special authorization from the National Airspace Agency. On the other hand, the *open* category is further divided into five classes depending on the UAS weight and specifications. Additional two classes were added in the latest eRule [23] published on September 2021. Operating in the open category involves avoiding direct operation over people, maintaining VLOS operation or using a UAS observer, flying at a height of fewer than 120 meters, and carrying only non-dangerous payloads. According to this rule, the remote pilot must ensure that the remote identification system is active and up-to-date.

The rule also lays down the requirements for designing and manufacturing remote identification add-ons. Mainly, it requires manufacturers of remote identification add-on modules to assign a type and a serial number to the remote identification module such that it complies with the requirements of the RID. A UAS operating in the *specific* category at a height below 120 m is required to periodically transmit a *direct remote identification (DRID)* using an open and documented transmission protocol during flight. The SESAR Joint Undertaking defined the DRID [18] as an emitted ''signal that can be received by a handheld device directly giving identification, or using the data carried by that signal to request further information from the U-space e-Identification service.'' The transmitted RID shall at least constitute the UAS operator registration number and a 3-digit verification code provided at the time of registration, the UAS unique physical serial number compliant with standard ANSI/CTA-2063-A-2019, a timestamp, the position and height of the UAS, the route course, the ground speed, the remote pilot position, and an emergency flag.

Further, a UAS operating in the *open* category and weighing less than 250 grams (class C0) is exempted from transmitting a RID. On the other hand, a UAS operating in the open category under classes C1-C3 are subject to the same DRID requirements of the specific category. However, operating in the *open* category allows another form of remote identification: the network remote identification system (NRID). Both schemes, the NRID and the DRID, require sharing the same information as detailed above. The NRID involves sharing this information through a network rather than through direct transmission or broadcasting. Information about the applicability of remote identification for classes C5 and C6 is not provided in [23].

Like the FAA rules, EASA also recommends providing tamper-resistant remote identification systems. EASA also requires manufacturers to provide information in the instruction manual about the transmission protocol used for the DRID emission. UAS operators in Europe are required to abide by these rules by January 2023.

C. RUSSIA

The Ministry of Transport of the Russian Federation has realized the inevitable gains of integrating UAS into urban airspace. The Russian UTM (RUTM) operation concept has been developed by Aeronet National Technological Initiative [19]. However, the standards and technology for UAS remote identification are yet to be finalized [43]. At the initial stage, remote identification is expected to be based on available technical solutions such as ADS-B 1090 ES. Other means of identification, such as mobile data transmission networks, will be considered in future phases.

D. CHINA

As a giant industrialized country, China has shown limitless interest in commercial UAV applications [16]. As a result, the Civil Aviation Administration of China (CAAC) released four rulemakings to regulate UAVs in the urban environment. The first rulemaking (AC-91-FS-2015-31) [44] was released in 2015 and is still in effect despite the release of three other rulemakings concerning the same subject. According to this document, all UAVs expect micro (<1.5 kg) UAVs are required to keep connected to the Unmanned Aircraft Cloud Exchange System (UACES) in order to report their current position and status during flight. It is, essentially, similar to the NRID scheme. As of 2020, eleven certified Unmanned Aircraft Cloud Systems (UACS) were listed in [45]. On the other hand, two standards released by industrial partners [24], [46] specified the information exchange requirements between the UACS and the UAVs. Further, various cybersecurity technologies, including digital signatures and blockchain, were specified.

A recent rulemaking [24] which was released on the 8th of March 2021, focused on the implementation of Remote ID in a way that is more consistent with the FAA framework, including requirements on RID message elements and transmission technologies, namely: NRID and BRID.

Finally, according to [47], the CAAC may require that operational details be ''periodically reported passively by ADS-B, radar, without the need for pilot involvement to UAS cloud systems.''

E. JAPAN

The Japanese Civil Aeronautics Act was amended in June 2020 to make UAS registration mandatory in June 2022. According to [25], the government is also planning to introduce the DRID as a mandatory requirement to allow the real-time identification of drones. In principle, four DRID transmission technologies are proposed: Bluetooth 5.x, Bluetooth LE Long Range, Wi-Fi Neighbor Awareness Networking, and Wi-Fi Beacon. Regardless of the transmission technology, the proposed frequency of RID broadcast is at least once per second. Further, the Minister of Land, Infrastructure, Transport, and Tourism specifies that the RID signal must conform with the ASTM International F3411-19 standards and include information about the registration ID, the UAS serial number, location, vector information of the UAS, and authentication information.

F. INDIA

In August 2021, the Indian Civil Aviation announced a set of rules to regulate drone operation in the urban airspace [26]. Under the mandatory safety features that are required for the certification of UAS, the document states that the central government may, in the future, require the operators to install some safety features such as a ''No Permission – No Takeoff hardware and firmware'' and a ''Real-time tracking beacon that communicates the unmanned aircraft system's location, altitude, speed, and unique identification number.''

G. SINGAPORE

According to a recent document released by the Director-General of Civil Aviation (DGCA) [27], UAS operating in BVLOS must have visual or audio warning indicators to alert nearby personnel when approaching landing zones. To our knowledge, no further requirements for UAS identification are found in the country's official regulatory documents.

H. UAE

The UAE is adopting a national strategy that promotes the country as a hub for cutting-edge technologies. In this context, the General Civil Aviation Authority (GCAA) has developed a framework to regulate the use of UAVs in controlled airspace [48]. Generally, the rules require UAV operators to register their drones before flying, obtain a piloting certificate, avoid Beyond Visual-Line-Of-Sight BVLOS operation, and avoid flying over no-fly zones. However, the requirement for identifying the UAV while flying is not explicitly stated. Rather, Article 70 of the same document defines a maximum penalty of 100,000 AED for flying a drone ''without bearing the nationality and registration marks or displaying incorrect or ineligible marks.'' Another recent rulemaking concerning the same topic was released in June 2020 by the Dubai Civil Aviation Authority DCAA [28]. It provides a more detailed framework for the operation of UAVs in controlled airspace. Nonetheless, it lacks a clear description of the identification required by drones during flight time. Particularly, the rulemaking barely touches the remote identification issue in Article 15 as follows: ''No Person may use an Unmanned Aircraft, or conduct Operation Tests thereof, unless its registration number or code, or any other identifying information prescribed by the DCAA, is displayed thereon.'' Moreover, Raj *et al.* [49] reported that the fine for non-inclusion of warning lights in UAV is around 5000 AED. On the other hand, a Civil Aviation Regulation (CAR) document [50] did not highlight any in-flight identification requirements for UAVs. Despite these limited identification guidelines, the current UAV regulation in the UAE suffers from the absence of a fully regulated remote identification framework that aligns with the best international practices.

IV. STANDARDS

As with any other field, setting an ensemble of rules to be respected while developing and implementing new technologies is crucial. Ideologically, the standardization paradigm involves multiple aspects such as product manufacturing and maintenance, operations and procedures, traffic management, and subsystems. This section highlights the up-to-date standards that address the remote identification problem, such as ASTM, 3GPP DRIP, and CTA. It is quite noteworthy that many standards specific to remote identification are still under development until writing this paper (e.g. ISO/DIS 23629-8).

A. CONSUMER TECHNOLOGY ASSOCIATION

The Consumer Technology Association (CTA) introduced a standard related to remote ID, ANSI/CTA-2063, Small Unmanned Aerial Systems Serial Numbers [51]. The In-Vehicle Electronics Committee WG 23 Unmanned Aerial Systems (UAS) and CTA R6 Portable Handheld developed the standard. According to the CTA-2063 standard, two types of serial numbers can be used to identify the UASs: physical and electronic. The Physical Serial Number (PSN) is assigned to all UASs by the stakeholders that hold the manufacturer and UAS identities. On the other hand, the Electronic Serial Number (ESN) indicates the identity of the international mobile station equipped with the software version and the performance characteristics [52]. In the following subsections, we explain the PSN and ESN components according to the CTA-2063 standard.

1) PHYSICAL SERIAL NUMBER

PSN consists of three essential components as depicted in figure 2: the Manufacturer's Code (MFC), the Length Code (LC), and a Unique Serial Number (USN) allocated by the manufacturer. The CTA, with its stakeholders, is responsible for developing and defining regulations for MFC. The MFC's length is four characters, including any combination of digits and uppercase letters, except the letters 'O' and 'I.' The LC

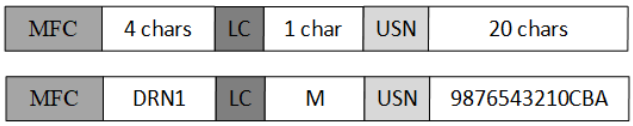


FIGURE 2. The format of the PSN with an example.

is a single alphabetical character that reflects the number of characters in the PSN's serial number. Finally, the manufacturer is responsible for generating and assigning the USN to each UAS product. The USN length ranges from 1 to 20 characters that can be conveyed through a single character of LC using letters A to T, where A = 1 and T = 20. The USN is an alphanumeric code that shall include any combination of digits and uppercase letters except the letters 'O' and 'I.' The bottom rectangle in figure 2 represents an example of a PSN = "DRN1M9876543210CBA", where MFC = "DRN1", LC = "M" to represent a 13 USN characters, and USN = "9876543210CBA".

2) ELECTRONIC SERIAL NUMBER

Figure 3 demonstrates the Electronic Serial Number (ESN) format, which consists of four fields. The first two fields, inherited from the PSN, are the MFC and USN. The other two are the international mobile station identity (IMSI), followed by the software version, and performative characteristics (PC). Unlike the PSN, the ESN has a predefined length of 47 ASCII code characters. According to the standard, if the length of USN is less than 20 characters, the manufacturer must append zeros at the beginning of the USN.

At the bottom of figure 3, we present the same example addressed in subsection IV-A1. The LC is not included in the ESN format. The IMSI with the software version is represented in 16 characters decimal digital code, defined by 3GPP TS 23.003 [53]. If the information on mobile station equipment and software version is not used, the field shall be filled with 16 bytes of 0 × 00 value. Finally, the PC field is composed of seven characters reserved for performative characteristics of the UAS. The first character indicates the standards body where the CTA manages its assignment to define the performative characteristics. If any of the seven performative characteristics characters are not used, they shall be padded with zeros.

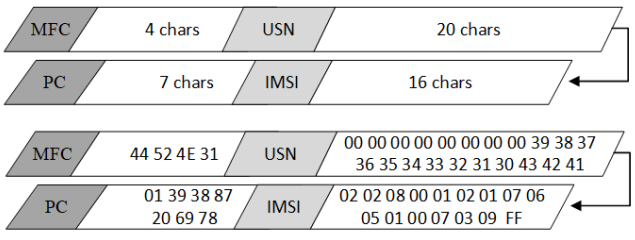


FIGURE 3. The format of the ESN with an example.

B. AMERICAN SOCIETY FOR TESTING AND MATERIALS

American Society for Testing and Materials (ASTM) standard specification covers the performance requirement for RID of the UAVs that operate at very low-altitude airspace over diverse environments. It ensures the accountability of the UAS operators by removing the anonymity factor while conserving the operational privacy of their businesses and customers. Furthermore, it defines the message format, transmission methods, minimum performance standards, and test requirements for the two broadcasting models [15].

1) CONCEPTUAL OVERVIEW

Figure 4 presents the general concept of the RID according to the ASTM standard. The scope of the ASTM standard is limited to the interface between the drone and the user application and does not consider the broadcast receiver hardware. In particular, the specification focuses on using the Bluetooth and Wi-Fi transmission protocols and covers the transmission protocol provided by the available technology. No specific technologies are used for the network RID since it requires cellular network coverage for both UAVs and end-users.

2) PERFORMANCE REQUIREMENT

This subsection emphasizes the minimum performance requirements and transport mechanisms for communicating the RID messages. We summarized the critical information that should be considered during the implementation of the ASTM standard, and we highly recommend referring to the ASTM standard for any details.

Two types of broadcasting messages exist according to the ASTM standard, namely static and dynamic. The static data, like the UAV's identification number, is unchangeable during flight. In contrast, the dynamic data changes, such as its longitude and latitude. The dynamic messages shall be sent at least every second, whereas the static message shall be sent every three seconds. The maximum potential time elapsed since the time of applicability of the dynamic fields in the Location/Vector Message shall be no older than one second.

The RID transceivers should provide sufficient power emitted in an omnidirectional pattern. The Minimum transmission effective isotropic radiation pattern (EIRP) is defined as the minimum EIRP around all 360 degrees of the far-field in the horizontal plane of the transmission pattern. The Minimum EIRP over this entire plane shall not be less than a predefined threshold determined by the national wave law in each country. For example, the Wi-Fi transceiver's EIRP in the USA should be at least 15 dBm.

The ASTM standard describes the transport mechanism by focusing mainly on the Wi-Fi and Bluetooth media because they are widely deployed in commonly handled devices. Mainly, the implementation method utilizes the advertising beacon messages used to declare a device available for pairing. Bluetooth uses channels (37, 38, and 39) to broadcast messages to non-specific endpoints (connectionless), whereas Wi-Fi reserves channel 6 for that purpose. ASTM standard describes the usability of the Wi-Fi technology as a connectionless broadcast mechanism to encapsulate the Open Drone messages using the Wi-Fi management frames. Messages shall be encoded within the Service Discovery Frame,

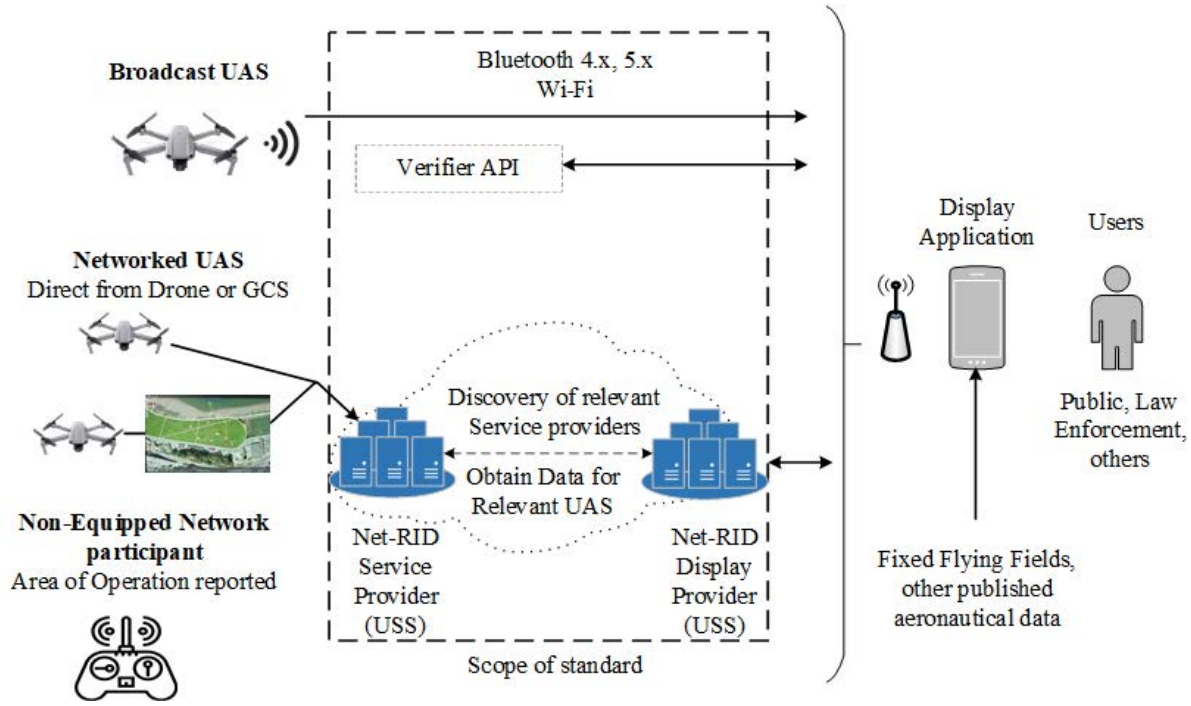


FIGURE 4. RID conceptual overview.

based on the Neighbor Awareness Networking (NAN), to make data available for display without any necessity for a wireless connection. NAN Discovery is operational only in channels 6 and 149 when using 2.4 GHz and 5.745 GHz bands, respectively. Furthermore, NAN is the underlying specification used by Wi-Fi Aware and incorporates capabilities for enhancing peer-to-peer communication by enabling devices to exchange services and information without network infrastructure or setup process. Messages can be sent together in a single pack or dynamic by dividing the message into different packets.

3) MESSAGE FORMAT

Figure 5 illustrates the format and the values of packets used during the broadcast by the BLE 4.x and BEL 5.x. The NAN service discovery frame is the same at the low level, and the main difference per rapport in the BLE packet is at the high header level. Each broadcast message has a header coded in one byte, where the four MSB bits are reserved for defining the message type and the four LSB bits for determining the protocol version. The message header is followed by 24 bytes of data which should be encoded according to a predefined format and using a standard data dictionary. Hence, the size of each broadcast message is 25 bytes padded with nulls when the broadcast data is less than 24 bytes.

The Bluetooth technology supports a broadcast frame to transmit via the beacon channels with a custom message size of 31 bytes, providing 25 bytes available for the broadcast messaging protocol (Open Drone ID) and the other bytes for extra header data. Bluetooth 5.x is an enhanced version of BLE 4.x as it integrates new features, allowing long-range communication and advertising extensions. The ''preamble byte'' of the packet should be tuned to increase the advertisement range by a factor of four. The extended advertisement feature allows up to 255 bytes on non-beacon channels by implementing a pointer in the primary beacons, directing the receiver to read from the secondary channels.

C. INTERNET ENGINEERING TASK FORCE (IETF)

The Internet Engineering Task Force (IETF) has identified a fundamental gap in current regulations and technical standards for remote identification. In particular, most of these regulations and standards consider drone identification as an end rather than a means to support other applications such as air traffic control or drone-to-drone communication. For instance, the current standards and regulations provide little information about enabling an observer to communicate with the pilot to obtain more information on the UAS operation or request an exit from an airspace area in the case of an emergency. The IETF asserts that remote identification should not be used merely for identification, and its function should be expanded to support relevant applications. To achieve this, the IETF aims to leverage available Internet standards and infrastructure and business models for domain name registration to develop necessary protocols that preserve operator privacy, enable strong authentication, and enable authorized parties' immediate use of information.

Towards this goal, the IETF has established a working group to specify an open standard for Drone Remote Identification Protocol (DRIP) in February 2020. The IETF working

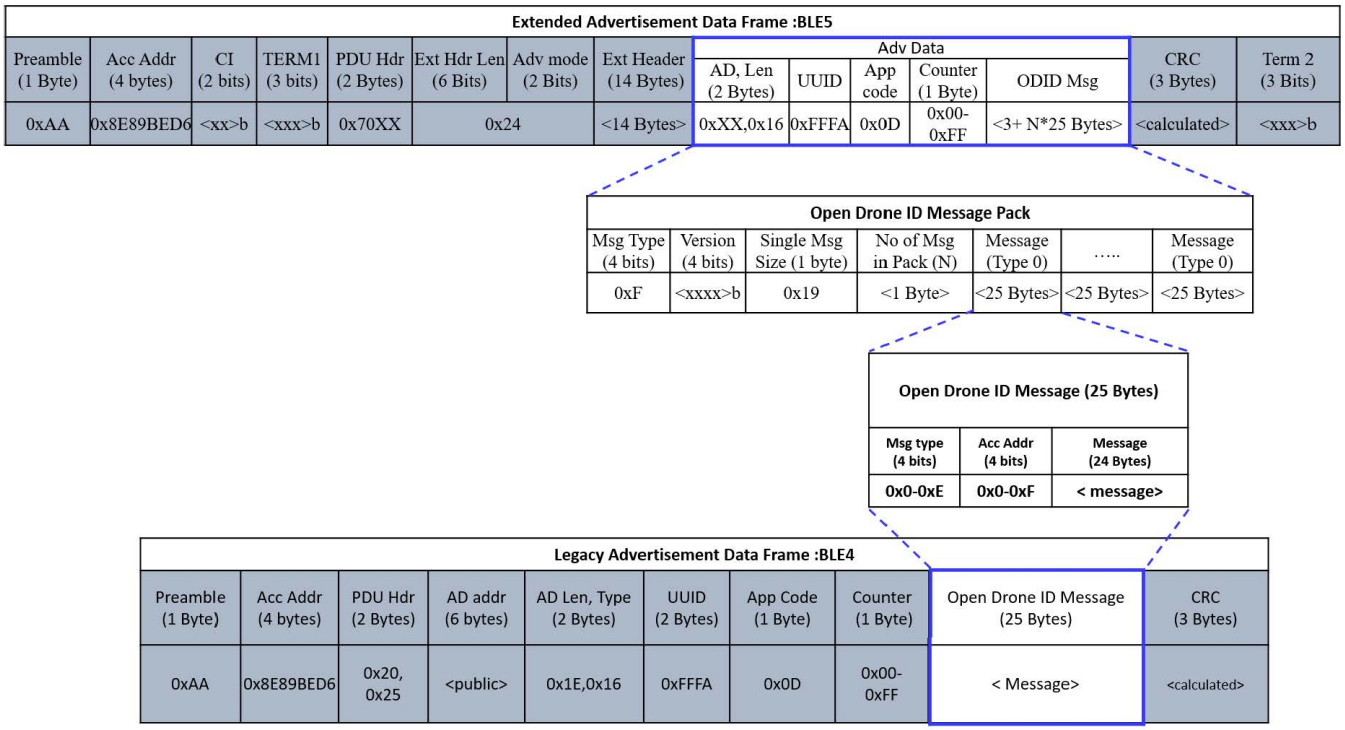


FIGURE 5. BLE frames diagram.

group aims to align the DRIP specifications with national and international regulatory requirements, e.g., those published by the International Civil Aviation Organization, the European Union Aviation Safety Agency, and the US Federal Aviation Administration. Also, DRIP builds upon the link layers specified in the ASTM F3411-19 and enhances its support for applications.

1) DRIP REQUIREMENT SPECIFICATION

The IETF has recently published a request-for-comment document (RFC 9135) that defines terminology and requirements for solutions produced by the DRIP working group [54]. This document highlights that when the drone identifier is appropriately chosen, various Internet protocols and services can be used to support different applications beyond the basic security function of RID. Most Internet protocols require some identifier, such as Network Access Identifier (NAI), Digital Object Identifier (DOI), Uniform Resource Identifier (URI), the domain name, or the public key. For this, DRIP focuses on making information obtained via UAS RID immediately usable by meeting the following objectives:

1) Assure the trustworthiness of the RID
2) Enable verifying that a UAS is registered for RID and registry to classify trusted operators based on known registry vetting.
3) Facilitate independent reports of drone flight data such as location and velocity to confirm or refute the operator self-reports used for UTM tracking
4) Allow authorized parties to establish secure communications with the Remote Pilot.

The RFC document classifies the DRIP requirements into four groups: general requirements, identifier requirements, registry requirements, and privacy requirements. For brevity, Table 2 shows the labels of these requirements. For describing these requirements and their rationales, the reader is referred to [54].

2) DRIP ARCHITECTURE

Starting from the requirements specified in [54] the DRIP working group is developing an architecture for remote identification [55]. The reference scenario shown in Fig. 6 is used. This scenario shows multiple observers. Some of them are members of the general public, and others are government officers with public safety and security responsibilities. Multiple drones are in flight within the observation range, each controlled by its operator through a command and control link (C2). The drones use their IDs to communicate through a vehicle-to-vehicle link (V2) and to ground services through a vehicle-to-infrastructure connection (V2I). The scenario assumes using at least one registry for the lookup of public information and one for private details related to drones and their operators. Finally, the domain name service (DNS) resolves various identifiers and locators of the entities involved.

The core architectural aspect of DRIP is using the Hierarchical Host Identity Tags (HHITs) as self-asserting IPv6 addresses that work as trustworthy remote identifiers for

TABLE 2. DRIP requirements according to RFC 9153.

Requirement Group	Code	Requirement Name
General Requirements	GEN-1	Provable Ownership
	GEN-2	Provable Binding
	GEN-3	Provable Registration
	GEN-4	Readability
	GEN-5	Gateway
	GEN-6	Contact
	GEN-7	QoS
	GEN-8	Mobility
	GEN-9	Multihoming
	GEN-10	Multicast
	GEN-11	Management
Identifier Requirements	ID-1	Length
	ID-2	Registry ID
	ID-3	Entity ID
	ID-4	Uniqueness
	ID-5	Non-spoofability
	ID-6	Unlinkability
Privacy Requirements	PRIV-1	Confidential Handling
	PRIV-2	Encrypted Transport
	PRIV-3	Encrypted Storage
	PRIV-4	Public/Private Designation
	PRIV-5	Pseudonymous Rendezvous
Registries Requirements	REG-1	Public Lookup
	REG-2	Private Lookup
	REG-3	Provisioning
	REG-4	AAA Policy

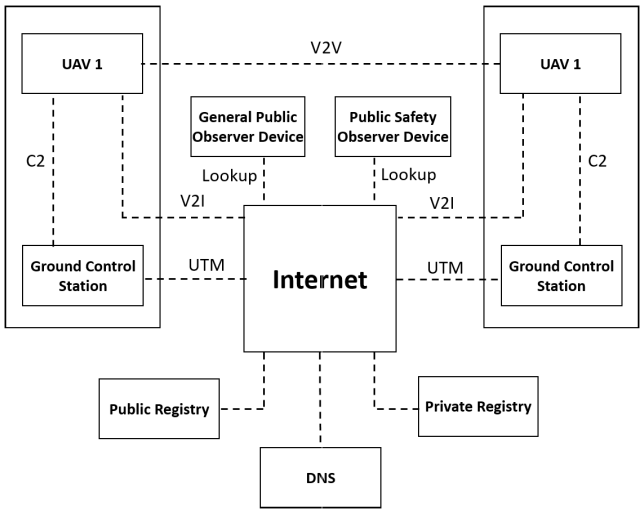


FIGURE 6. DRIP reference scenario.

drones [56]. Self-asserting means that, given the Host Identity (HI), the HHIT Overlay Routable Cryptographic Hash Identifier (ORCHID) construction, and a registry signature on the HHIT, the HHIT can be verified by the receiver. The DRIP builds the remote ID from an asymmetric key pair. The proof of ID ownership is guaranteed by signing this ID with the associated private key. In particular, drone ID is generated cryptographically from hashing the HI public key. The hash value thereof, which makes the drone ID, is called the Host Identity Tag (HIT). The HIT is unique through the second-preimage resistance property of the cryptographic hash function [55].

A drone should be equipped with the HHIT, the public key from which the HHIT was derived, and the corresponding private key to enable message signature. An observer device should contain either the public keys of the DRIP identifier root registries or certificates for subordinate registries. A self-attestation of an HHIT used as a drone ID can be done in as little as 84 bytes when the Edwards-Curve Digital Signature Algorithm (EdDSA) is used [57]. This attestation consists of the HHIT, a timestamp, and the EdDSA signature [55].

A DRIP identifier can be assigned to a drone as a static HHIT by its manufacturer, such as a single HI and derived HHIT encoded as a hardware serial number per CTA2063 [51], [55]. Such a static HHIT should only be used to bind one-time use DRIP identifiers to the unique drone. Depending upon the implementation, this may leave a HI private key in possession of the manufacturer. In general, observers may need Internet access to validate attestations or certificates. The need for connectivity can be avoided by reserving small caches on observer devices with registry public keys and a chain of attestations or certificates, assuming that all parties on the trust path use HHITs for their identities [55].

D. 3rd GENERATION PARTNERSHIP PROJECT (3GPP)

3GPP has started several activities to address the connectivity needs of unmanned aerial systems through mobile networks, including the 5G system. Figure 7 shows a reference model for UAS developed by the 3GPP working groups [58]. Accordingly, UAVs are connected over the cellular network. A UAV operator can control one or more UAVs, and the UAS exchanges application data traffic with a UTM system. A command and control link (C2) that does not use the 3GPP network is in the 3GPP scope.

1) 3GPP GENERAL REQUIREMENTS FOR UAS REMOTE IDENTIFICATION

The Technical Specification TS 22.125 lists 17 general requirements for the remote identification of UAS. Accordingly, the 3GPP system should provide for the following [58]:

1) Enable UTM to associate the drone and its controller and identify them as a UAS.
2) Provide UTM with the identities of the drone and its controller.
3) Enable a UAS to send UTM data about the drone, such as a unique identity, model, vendor, take-off weight, position, owner identity, mission type, route data, and operating status.
4) Enable a UAS to send UTM data about the drone controller, such as the unique identity, position, owner contact details, operator license, and flight plan.
5) Support different levels of authentication and authorization for the data exchange between UAS and UTM.
6) Provide extendible data exchange to meet future applications of UTM.
7) Support different identifiers, including International Mobile Equipment Identity (IMEI), Mobile

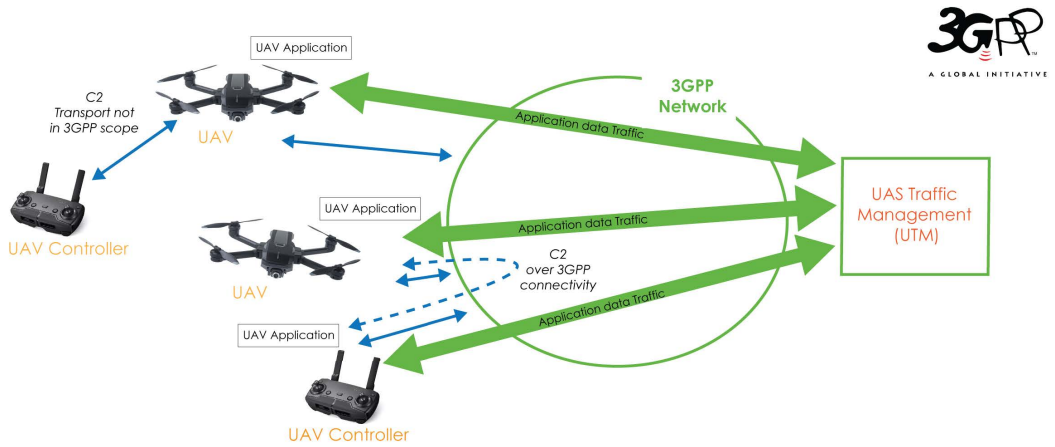


FIGURE 7. UAS reference model by 3GPP [58].

Station International Subscriber Directory Number (MSISDN), International Mobile Subscriber Identity (IMSI), or IP address.

8) Enable user equipment in a UAS to send any of these identifiers to a UTM.
9) Enable a mobile network operator (MNO) to augment the data sent to a UTM with the network-based positioning information of the drone and its controller.
10) Enable UTM to inform an MNO of the outcome of an authorization to operate.
11) Enable an MNO to allow a UAS authorization request only if appropriate subscription information is present.
12) Enable a UAS to update a UTM with the live location information of a UAV and its UAV controller.
13) Provide supplement location information of UAV and its controller to a UTM.
14) Support simultaneously connects a drone and its controller to different public land mobile networks (PLMNs).
15) Enable an MNO to obtain information about the drone's support of 3GPP communication capabilities.
16) Support the differentiation between drones with UAS-capable user equipment and those with the non-UAS-capable user equipment.
17) Support the UTM in detecting drones operating without authorization.

2) 3GPP REFERENCE ARCHITECTURE FOR UAV REMOTE IDENTIFICATION

3GPP published a technical report containing a new 3GPP UAS Network Function standard for UAV identification and tracking to support Remote Identification [59]. This study highlights seven key issues starting with drone identification that raises the following questions:

1) What identities are assigned to a UAV and/or UAV controller in the 3GPP system?
2) How are identities used by a drone or a controller in the 3GPP system?
3) What identities are exchanged with parties outside the 3GPP system?
4) How does the 3GPP system interact with the UTM to enable UAV identification?

The study explores the different solutions to address the reported key issues. One of the optimal solutions includes mapping the network entities and interfaces in the UAV reference architecture to the 3GPP reference architecture. Figure 8 presents an overview of the 3GGP reference architecture for UAV remote identification and more details about the internal architecture can be found in [59]. In summary, the drone should have two identities:

a: CIVIL AVIATION ADMINISTRATION (CAA) LEVEL ID (CAA-ID)

It is assigned to the drone during registration by an unmanned service supplier (USS), and it includes information such as the serial number of the UUID. CAA-ID is used to identify the drone by UTM actors and for remote identification in the network and broadcast mode. The architecture supports mechanisms available to entities outside the 3GPP system (e.g., law enforcement) to resolve a CAA identification and discover the USS for the respective drone. The 3GPP system is provided the CAA-ID by the drone, and it may optionally give this identity to the UTM/USS when providing mobile network operator (MNO) services to the UTM/USS.

b: 3GPP ID

It is provided to the UAV by the MNO or to the UAS by the Access and Mobility Management Function (AMF) or the Session Management Function (SMF). It is used to identify the drone by the 3GPP system. The 3GPP ID includes information about the subscription identity used, e.g., Generic Public Subscription Identifier (GPSI) and Mobile Station Integrated Services Digital Network (MSISDN), the IP address allocated to the Protocol Data Unit (PDU) session, or a 3GPP equipment identifier such as the Permanent Equipment Identifier (PEI) and the International Mobile station

Equipment Identity (IMEI). The USS uses the 3GPP ID to invoke MNO services (e.g., exposure function or location services) or during authorization. The 3GPP ID is in the format of a GPSI, and at least the External Identifier is supported. The 3GPP network allocates the External Identifier without interaction with the USS/UTM and must be unique within the geography (e.g., at least country) of the 3GPP network.

V. TECHNOLOGY AND INDUSTRY

A. OVERVIEW OF THE RID-TECHNOLOGY

This section reviews the prior RID technology to help communities select the optimal technology for UAV-RID and formulate requirements for the devices that perform UAV remote identification. As defined by the ASTM, RID-technology can be categorized into two main groups, as depicted in Figure 9. First, the direct broadcast technology transmits radio signals from the UAV to the nearest ground receiver, as depicted in Figure 9a. The other one, as presented in Figure 9b, is based on the connection of the UAV with the Air Traffic Services (ATS) system via the Internet, like 4G/5G. The future Remote ID systems will undoubtedly be based on both methods instead of just one because the two methods are complementary [16], [60]. For example, ScaleFlyt Remote ID offers direct broadcast and network channels (compliant with ASTM and ASD - STAN) and provides secure communication channels based on cryptography in tamper-proof embedded eSIM [61].

1) BROADCAST TECHNOLOGY

Broadcast Remote ID consists of data transmission in one direction only, with no specific destination or recipient. Anyone within the broadcast range can receive data. The broadcast remote I.D. technology is helpful in areas where network coverage is limited, disrupted, or unavailable. Maintaining a signal between broadcaster and receiver over long distances might not be possible, or there might be too many receivers required to be a feasible solution [62].

a: AUTOMATIC DEPENDENT SURVEILLANCE-BROADCAST (ADSB)

The significant avionics companies created the ADS-B in 1990, one of the most optimal and promising surveillance tracking systems. It provides commercial and military aircraft with an updated communication scheme, extending the communication range to support a radius of up to 370 Km [63]. The ADS-B allows broadcasting autonomously messages containing the location obtained from the Global Navigation Satellite System (GNSS) and other information provided by on-board systems to other UAVs and ground base stations with minimum latency [63], [64]. ADS-B is an element of the U.S. Next Generation Air Transportation System and the UAV can use to detect other aircraft in the national airspace [65]. There are two operation modes of the ADS-B known as ADS-B In and ADS-B Out, as illustrated in Figure 10. The UAV's position, identification, and speed are sent periodically to the ground station in the first mode without requiring any external action. In the second mode, the UAV exchanges such information between each other, mainly related to Flight Information Service - Broadcast (FIS-B), Traffic Information Service Broadcast (TIS-B) data, and other ADS-B messages [63].

The existing ADS-B modules broadcast the message into two main frequencies, which are 1090 MHz and 978 MHz [66]. The 978 MHz is used only in the U.S. for testing purposes and is known as the Universal Access Transceiver (UAT). Many companies have developed low-power and low-cost ADS-B modules, such as ping2020, developed by UAvionics, TT-MC1, designed by Aerobits, and DDA by Sagetech. Other companies like DJI integrate the ADS-B module in all drones released after 2020, allowing notification of any nearby UAV. Unfortunately, today there is no commercial drone equipped with such a module because this might cause unnecessary signal traffic, especially with the growing number of drones. The FAA reported that the ADS-B Out would generate undue signal saturation and create an overall safety hazard for crewed aircraft due to the exponential increase of UAVs in the airspace. Furthermore, ADS-B does not provide information regarding the location of a UAV control station. Although the FAA hints that ADS-B is an inappropriate solution to identify UAVs, many companies and research labs still focus on developing and enhancing ADS-B systems. The enhancement focuses mainly on optimizing the power consumption, which is considered too high for a small battery-powered UAV since the power consumption can go up 20W [67]. A low-power ADS-B is proposed in [68]. The power transmission of the proposed module is less than 1.3W instead of 20W, and the throughput drops to one message every three seconds, which is not enough for safe conflict management. Moreover, due to the enormous transmission power, the ADS-B receivers may suffer channel congestion in high traffic conditions or be blinded by close transmitters ($\leq$ 50 km). Finally, the UAV's ADS-B transceivers are much more expensive than a small UAV [69].

b: RADIO FREQUENCY

Radio-frequency-based systems are overgrowing and represent a promising alternative that drones can use to broadcast their ID. UAVs must integrate transceivers utilizing the right and unlicensed radio frequencies to avoid harmful interference to vital radio systems like emergency services, cellular phones, and satellites. The most commonly used frequencies for broadcasting are 433MHz/2.4GHz for remote control and 5.8 GHz for audio and video links [70]. The used frequencies should primarily respect each country's national and international regulations, such as the power levels, duty-cycles modulation, and sub-channels. Radio-frequency transmitters broadcast continuous messages to advertise their presence for the associated devices. These advertisements usually carry a payload and contain the broadcast Remote ID data. A handheld device does not need to establish a connection to receive Remote ID data; instead, it needs only to receive and process

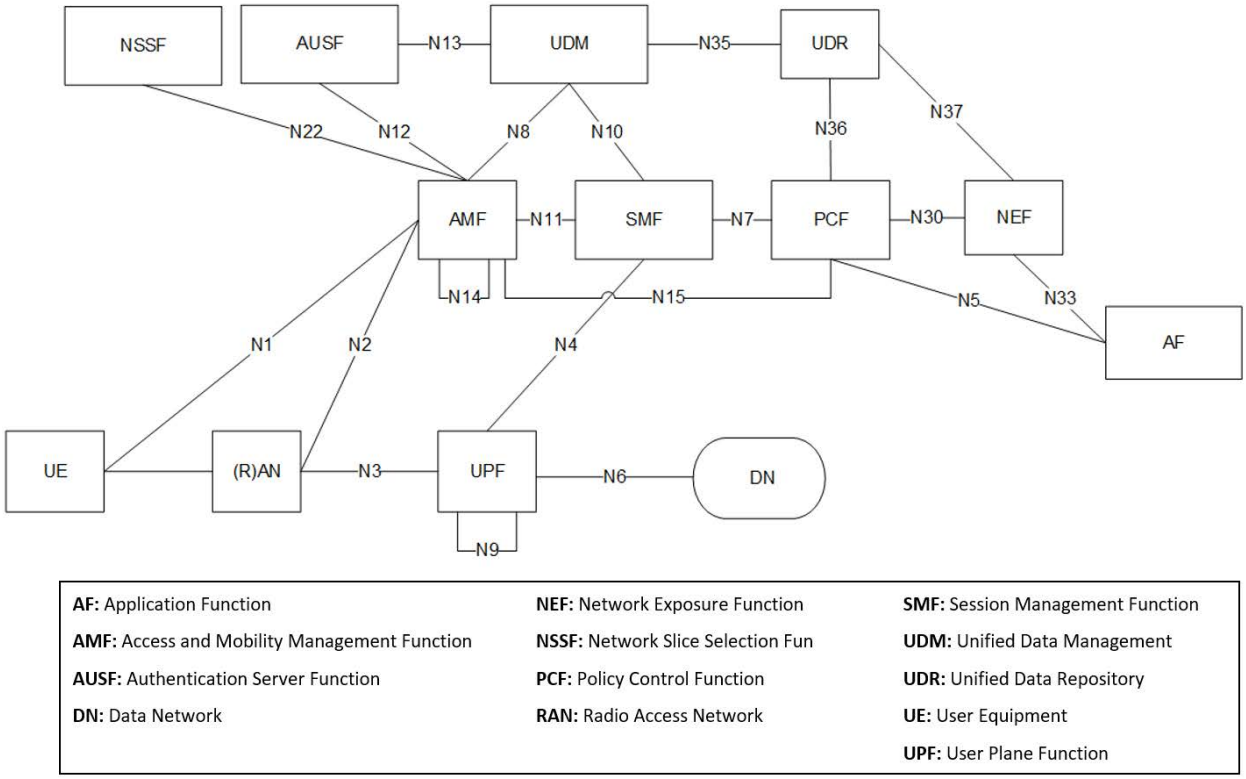


FIGURE 8. 3GPP reference architecture UAV remote identification [59].

the advertisements [15]. The best radio frequency alternatives to broadcast RID are Wi-Fi, Bluetooth, and low-power Wide-Area Network (LPWAN) [71]. We briefly describe these technologies in the remainder of this section.

- Wi-Fi: is a wireless Ethernet standard designed to support local area networks and is known as 802.11b. This standard allows devices to share information using radio frequencies in the gigahertz range [71]. The Wi-Fi modules are available off-the-shelf and inexpensive. No license is needed to operate a Wi-Fi access point or Wi-Fi devices, unlike 5G/6G modules. The cover range of some Wi-Fi modules does not exceed 300m, whereas others can reach 2Km like the Wi-Fi Neighbor Awareness Networking NAN) and Wi-Fi beacon [72], [73]. The power consumption of Wi-Fi NAN and Wi-Fi beacon is 100 mW. To the best of our knowledge, no existing research work uses the Wi-Fi module in the context of broadcasting RID. Some industrial companies have demonstrated the feasibility of broadcasting the RID using Wi-Fi to allow users to monitor nearby drones like the DJI company. Information is transceived directly from drones to off-the-shelf mobile phones, using an existing Wi-Fi protocol, without completing a two-way connection. The prototype is tested on smartphones in areas without any telephone coverage because it does not need to connect to a Wi-Fi base station or cellular network. Furthermore, the smartphone receives Wi-Fi signals from a distance of more than one kilometer away from the transmitting drone.
- Bluetooth: is an excellent wireless standard for wireless communication because it provides a secure connection while maintaining relatively low power consumption. The Bluetooth modules are available off-the-shelf and inexpensive, and there is no need for a license to operate them. The adequate bandwidth of the BLE is 270 kbps and can reach 650 kbps in the new modules. This technology is unsuitable for transmitting a large amount of data, which is not the case with RID. There are two Bluetooth versions: Bluetooth Legacy Advertising (Bluetooth 4.x) and Bluetooth Long Range with Extended Advertising (Bluetooth 5.x). The expected range of the first version is 250m, whereas the range of the second one can reach 1 Km in ideal conditions [73]. The maximum transmission power of the two modules is about ten mW. For example, Unifly Company developed a BLIP system that integrates a BLE module to broadcast the flying and the operator information. The data is accessible online to authorities via a secured application. It can be captured within a distance of up to 200 m of the observer. The consumed energy during the broadcasting is less than ten mW.
- Low-power Wide-Area Network (LPWAN): is another alternative that can address RID broadcasting. The LPWAN communication technology is designed to

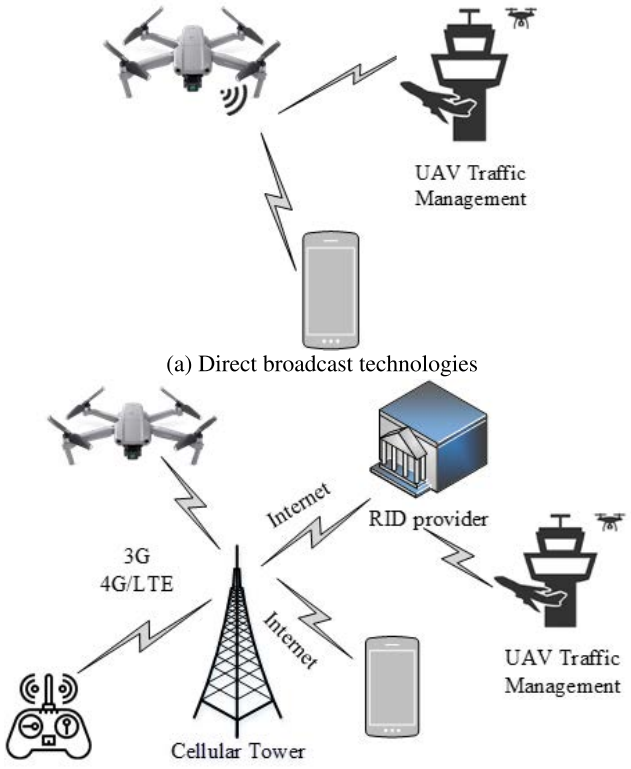


FIGURE 9. Remote ID technologies.

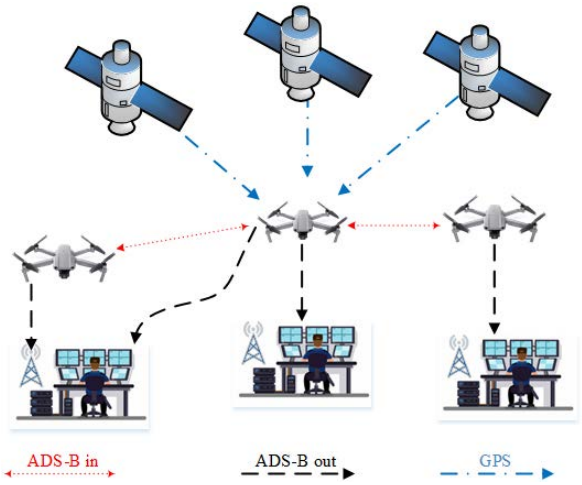


FIGURE 10. Scenario of the ADS-B communication technology [63].

provide long-range at the expense of a low data rate and a high latency, and it operates in the unlicensed Industrial Scientific and Medical (ISM) band. Furthermore, it can operate at a lower cost and power than legacy wireless technologies [74], [75]. The most known unlicensed LPWAN communication technologies are LoRa and sigfox. Sigfox technology is the first IoT network to listen to unlimited objects broadcasting data without network connections. Sigfox is a program-based communications system where all the network and computing complexity is overseen within the cloud instead of the devices. It transmits data within the unlicensed sub-GHz ISM groups (e.g., 868 MHz in Europe, 915 MHz in North America, and 433 MHz in Asia). The maximum data rate of Sigfox is 100 bps, which makes this technology inappropriate for broadcasting the RID. Contrariwise, the LoRa technology has attracted significant attention from industries and academics in recent years because it can reach a data rate of more than 270 kbps and offers long-distance connectivity. For example, in [76], Omkar *et al.* show the feasibility of the LoRa technology in broadcasting RID by studying the reliability and coverage by considering various SNRs, interference conditions, spreading factors, coding rates, and deployment settings. The research group evaluates the amount of degradation due to the LoRa multi-user interference for different scenarios and quantifies the performance gains obtained with different coding rates and spreading factors. Table 3 summarizes the specification of LoRa modules that can be used to broadcast RID.

TABLE 3. Examples of LoRa modules and their specification.

LoRa device	Bit rate (kbps)	Power (mW)	Range (Km)
F8L10S	5.5	3-1000	2-11.5
iM880B	115	25	12
SX1278	3.5	100	10
ES920LR	0.293	20	3

Figure 11 presents a comparison between the previous RID technologies. For example, the LPWAN represents the optimal choice to broadcast the RID due to its low power consumption for long-range distances. The disadvantage of such technology is the low data rate and latency, which makes it inappropriate to transfer big data.

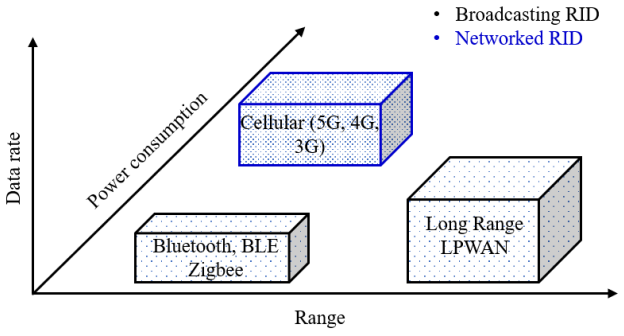


FIGURE 11. Comparison of RID technologies.

2) NETWORKED ID

Network broadcasting consists of data transmission to the internet or a federation of services. Clients can access distributed data to obtain UAV ID and tracking information [62]. The most known networked broadcasting technologies are

the cellular and satellite network (SATCOM). Cellular technology can serve UAV RID by providing wide-area, cost-effective, and reliable wireless connectivity [77]. SATCOM is an attractive alternative to be used in the future to broadcast the UAV RID, and it is expected to be an integral part of the future communication infrastructure [78]. Satellite communication provides a significant latency and coverage area, whereas the cellular network offers a medium latency and coverage area. Satellite communications technology is exclusive for emergencies when land-based communication services are down and during natural disasters.

Furthermore, the current SATCOM technology has the technical disadvantage of the inherent delay in transmission. To our best knowledge, until today, there is no implementation of the UAV RID using satellite communications. Contrariwise, academia and industry have given particular attention to the next generation of the cellular network to support flying UAVs and provide limitless connectivity because the existing cellular infrastructure is optimized to serve user equipment located on or close to the ground.

The network broadcasting model requires subscribing the drone into the network of mobile service operators as it relies mainly on the cellular network [79]. Figure 12 summarizes the different steps to register the UAV in a cellular network. The user must register to an embedded Subscriber Identification Module (eSIM) service by sending a request to the mobile network operator (MNO) to provide information about the UAV. Once the information is verified, the MNO communicates with the Government Telecommunication Authority (GTA), requesting the PIN and the activation code shared with the user to complete the registration. The user should install an application provided by the GTA to manage the UAV connection. The user activates the eSIM in the mobile application and installs the profile in the vehicle using the activation code and the PIN. The application securely sends the PIN and the activation code to the GTA to store the user and the vehicle information in the database and push the PIN code into the vehicle. The UAV confirms its readiness to receive other information from the user, which enters the vehicle's activation code and PIN code. At this stage, the drone and the operator share the secret PIN and the activation code, allowing them to identify each other.

We briefly describe the last industrial networked RID technologies in the remainder of this section.

a: ScaleFlyt REMOTE ID

Is an intelligent solution introduced by Thales Group to secure drone operation on the ground and in the air [61]. Figure 13a present a picture of the ScaleFlyt RID connected to a drone. It comprises an add-on onboard devices, a web server (cloud-based solution), and a back-end application implemented on a mobile application. ScaleFlyt allows the authorities to detect and identify the drone identification number, the operator ID, and the flight authorization. Third parties, such as UTM providers, UAV pilots, and ground receivers, can receive such information via secure networked

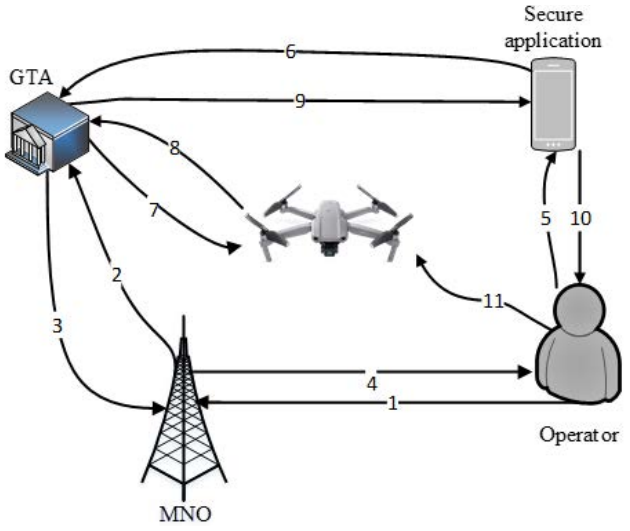


FIGURE 12. UAV registration.

data communication (LTE). ScaleFlyt provides secure communication channels based on cryptography in tamper-proof embedded eSIM. The ScaleFlyt is easy to use, and its cellular connectivity is global and compatible with any airspace manager (UTM/USSP). The UAV operator has to register using his registration number and QR code, configure the tracker, and attach the remote ID device to the drone.

b: NETWORK REMOTE IDENTIFICATION (NET-RID)

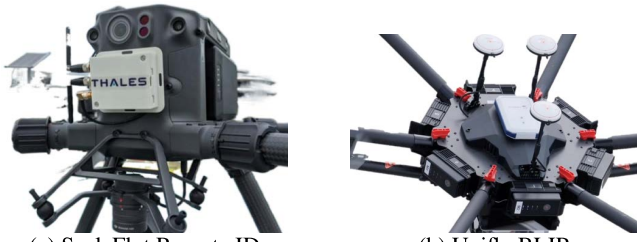
Swiss U-Space Implementation (SUSI) members developed NET-RID, which complies with the U-Space Regulation (EU) 2021/664 adopted by the European Commission [80]. NET-RID provides information about those operations via the internet and allows drone operators to easily share information about their flights with airspace authorities, law enforcement, other operators, and the general public. The necessary information related to the operator and flight is shared using a cellular network via an open-source platform that ensures a U-Space Service Provider (USSP) has obtained all relevant data from other USSPs. The NET-RID service complies with the ASTM F3411 standard, which protects the operator's privacy.

c: BROADCAST LOCATION & IDENTIFICATION PLATFORM (BLIP)

Unfily company designed and developed BLIP as an electronic plate, and UAV tracker [81]. Figure 13b presents a picture of the BLIP mounted on a drone. BLIP system provides maximum tracking accuracy while minimizing latency and securely stores the operator and flight information to Unifly's and other cloud services. It allows authorities and users to access the details of drones flying within a distance of up to 200 meters using Bluetooth low-energy technology. Data are transferred regularly, in compliance with the European legal requirements, through LTE wireless broadband network to the UTM backbone.

d: SECURE INTEGRATED AIRSPACE MANAGEMENT (SIAM)

RelmaTech company recently launched SIAM solution as a robust remote identification and traffic management application to address the critical issues for ensuring the safety of UAVs [82]. The operator and UAV are registered in a public database to track the manned and unmanned vehicles, and each has a digital identification. Besides the remote identification of drones, SIAM allows monitoring of no-fly zone and live feeds to the appropriate third parties and has been operating as a live UTM system for the active drones.



(a) ScaleFlyt Remote ID (b) Unifly BLIP

FIGURE 13. Examples of RID modules.

B. UAV INTEGRATING RID

With the introduction of Remote ID regulations for drones' safe and secure operation, industrial drone manufacturers are expected to comply with such guidelines as per deadlines set by most aviation regulators worldwide. Otherwise, non-complying drones will be prohibited in the long run, resulting in business losses for such an industry. Several major drone companies are trying to cope with the newly proposed regulation by implementing multiple strategies. Minimal invasive modifications for current running production lines of existing models are proposed to mitigate such evolving risks. Current platforms may require firmware updates and add-on hardware deployment to enable the RID feature. To redesign those platforms for a complete built-in RID, suspending current production lines will emerge a more extended cycle design that drone manufacturers can find impractical and costly. However, this is not an issue for the upcoming planned revisions of the drone platform. Integrating the required hardware and software to support RID into the autopilot or flight controller subsystem will be part of the new design cycle. Table 4 presents the drones that are already Remote ID compatible and the existing modules to be mounted in the drones that will not comply with Remote ID. In the following subsections, we summarize the activities of some major companies in this area.

1) DJI

Da-Jiang Innovations, or DJI, established in 2006 in Shenzhen, Guangdong, China, is one of the leading drone manufacturers that shares around two-thirds of the world drone market [83]. DJI claims that current drone platforms only require a software update to their flight controller to enable RID without additional hardware. DJI has planned to support drone identification solutions since 2017 by re-utilizing current wireless links within their platforms to ground stations [84]. The software update implements broadcasting identification information over the C2 link initially used for video streaming. This link utilizes the frequency of 2.4GHz or 5GHz, depending on the platform. Drones that do not contain C2 or Wi-Fi NAN links will require add-on modules to broadcast identification information, such as Dronavia Beacon. After Jan 1, 2020, all new models will be equipped with DJI AirSense, which uses ADS-B technology for such applications. DJI implemented a remote identification solution based on Wi-Fi technology into a Mavic Air UAV. The experimental results show that drone identification is performed accurately using a DeDrone Drone scanner application installed on an Android operating system. The detailed information of the operator and the done's information, such as the location, speed, and drone serial plate, are reported in real-time on the phone's screen.

The Dedrone DroneScanner is still under prototyping and is not yet available publicly, but the application's source codes can be found on GitHub. The application can be compiled easily using Android Studio. It continuously scans and decodes Bluetooth, Wi-Fi, and Wi-Fi beacon signals for android phones. If any matches the specifiers for OpenDroneID signals, it adds that transmitter to a list to display the drone's location on a map and the detailed content of the OpenDroneID data. The application reads the Android feature flags to determine the supported technology (BLE 4.0 or BLE 5.0). It complies with the Bluetooth, Wi-Fi NAN, and Wi-Fi Beacon parts of the ASTM F3411 Remote ID standard and the ASD-STAN prEN 4709-002 Direct Remote ID standard.

2) PARROT

Parrot is a multi-technological company specializing in manufacturing different types of drones [85]. Parrot introduced the support of Direct Remote Identification after the software release FreeFlight 6.7 in June 2021 [86]. DRI implements the message structure of the Open Drone ID protocol as ASTM standard specifies. The broadcast is transmitted through a Wi-Fi module equipped with Parrot platforms based on Wi-Fi beacon technology. The beacons frame are captured by cellular phones as part of a standard channel scan operation that is automatically applied within any operational client device. The flight information is extracted from the beacon message using a mobile application, which is shown in real-time as a red line traces Parrot Anafi's path. Figure 14 illustrates a print screen of the Dedrone drone scanner application, where the red line traces Parrot Anafi's path while the flight information details are available on the info screen.

3) YUNEEC

Another notable drone manufacturer based and founded in Jiangsu, China, in 1999 is Yuneec International [87]. The company announced in May 2021 the support of FAA Remote ID to their flagship drones, H520 and H520E [88].

TABLE 4. RID companies; NET ID: networked identification, BR ID: broadcast identification, NR: not reported.

	Company/ System	Tech.		Capabilities						Requirement	Standard	Targets
		NET ID	BR ID	VLOS/ BVLOS	Range (feet)	Bitrate (mbps)	Latency (ms)	Energy (Wh)	Battery life (min)			
UAV with RID	Parrot/ ANAFI	✓	✓	BVLOS	≥13000	100	300	20	25	Wi-Fi; LTE; Certificate	NR	Public
	DJI/Mavic		✓	VLOS	260	60	170	43.6	27	Wi-Fi	ASTM	Public
	DJI/ phantom		✓	BVLOS	16400	100	220	89.2	30	Wi-Fi	ASTM	Public
	DJI/ inspire		✓	BVLOS	22704	100	220	97.58	27	Wi-Fi	ASTM	Public
	senseFly/ eBee X		✓	BVLOS	9840	100	NR	90	56-74	NR	ASTM	Drone owner
	Yuneec/ H520E		✓	BVLOS	11480	100	NR	31.32	30	Wi-Fi	ASTM	Authorities & Drone owner
RID modules	Unifly/ BLIP	✓	✓	BVLOS	650	0.270	NR	7.7	420	LTE Cat1; BLE V5.0	ASTM F3411	Authorities
	RelmaTech/ SIAM	✓	✓	BVLOS	500	0.270	NR	NR	NR	LTE; Wi-Fi	ASTM	Authorities
	Thales/ ScaleFlyt	✓	✓	BVLOS	≥400	NR	NR	NR	NR	LTE; Wi-Fi	ASTM,ASD -STAN	Public
	Czech/ Dronetag	✓	✓	BVLOS	4920	0.320	NR	1.8	480	LTE; BLE 4.0	ASTM	Public
	INVOLI/ KIVU	✓		BVLOS	≥400	0.270	2000	3.3	270	LTE	ASTM	Authorities

Existing users of Yuneec drones are only required to update the drone firmware with a Wi-Fi module to be integrated into the platform. The updated firmware uses the Wi-Fi module to broadcast the identification information of the drone.

4) PIXHAWK

Open-source platforms are not exempt from complying with RID regulations, and most are trying to engage RID within their systems. For example, the Pixhawk autopilot hardware is supported by the PX4 and Ardupilot autopilot software, which do not integrate RID by default. For this reason, several top-up software has been introduced to resolve this issue, such as Auterion SDK for PX4 [89]. The SDK implements the MAVlink protocol to transmit the identification information to the ground station to forward later data to a server through the internet. RID can also be enabled with Pixhawk through a hardware add-on such as Aerobits idME, which uses BLE technology for the broadcast RID [90]. Another hardware module is cubepilot, adapted by Pixhawk company to support broadcasting RID based on ADS-B IN receiver from uAvionics.

C. RID MODULES

Today, most existing drones do not have an integrated remote identification module. The research entities are developing new remote identification devices to incorporate within the current UAV to comply with the FAA regulation. For example, Unifly and Czech companies offer two remote identification modules that can be retrofitted on all existing drones on the market. The two modules broadcast the required information, such as the operator ID, drone identification, location, etc. The Unifly module supports the 4.0 Bluetooth technology, whereas the Czech module can simultaneously broadcast using BLE 4.0 and BLE 5.0. Demonstrations of the use of these two modules are reported on the company's website showing their efficiencies.

VI. RESEARCH

RID Research studies are too rare despite the acute need to implement this technology in the shortest time. This section reviews the research studies on google scholar by searching the term ''drone remote identification.'' In addition to the scarcity of information in this field, some research studies address the remote identification problem well, unlike others. Thus, we categorized this section into two subsections: focused research studies that are axed very well with the philosophy and regulation of RID; and joint RID-UAV research that can help identify drones.

A. FOCUSED UAV-RID RESEARCH

1) SECURITY OF RID

Securely broadcasting UAV data is the key to successfully creating a modern automated UAS Traffic Management (UTM) system. Many studies focus on security and privacy concerns, including authentication threats and the leakage of identity, location, and flying routes to enhance UAV flying safety and service quality [91]. There are two types of broadcasted data: public data and payload data which are confidential and should be prevented from being exposed to unauthorized entities. Previous works are conducted by

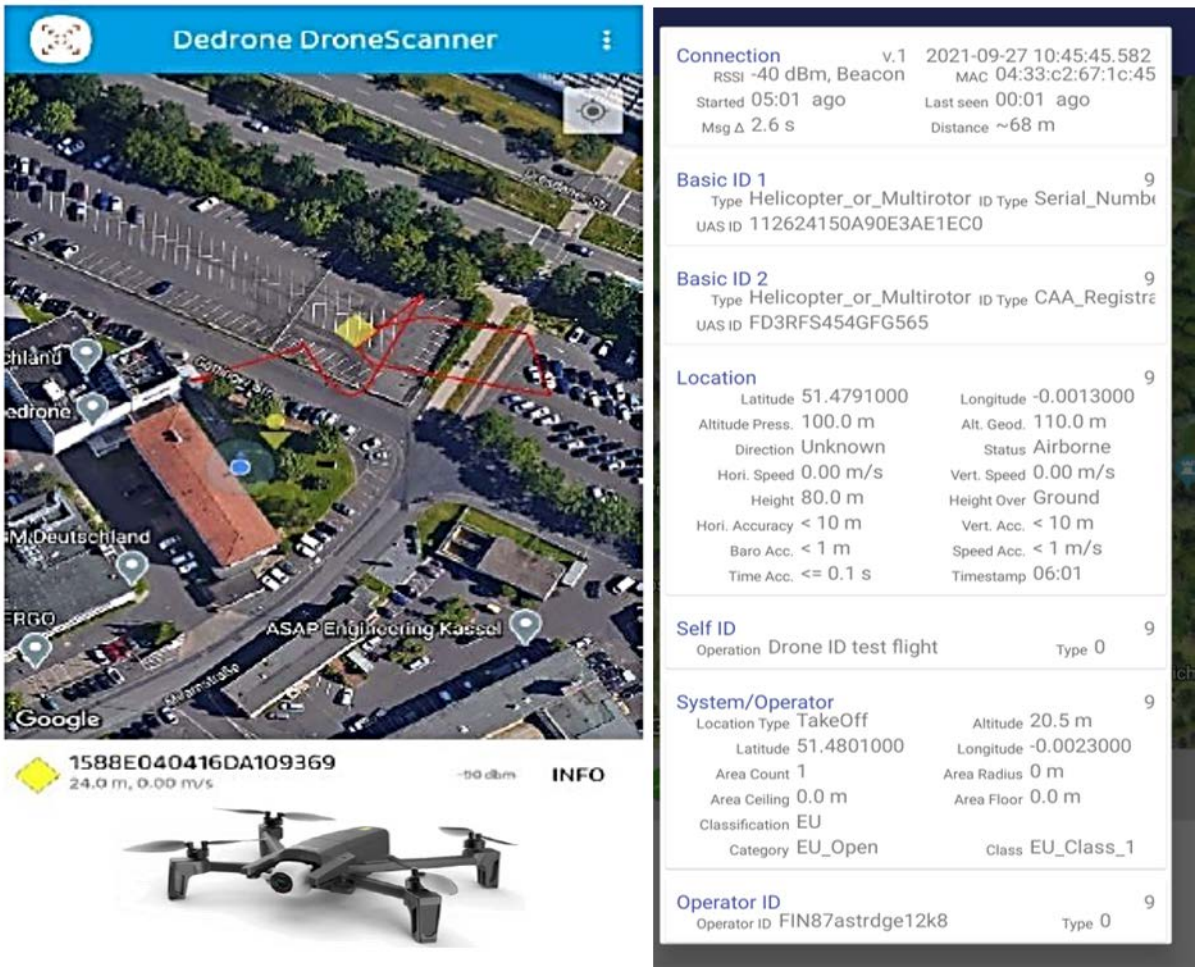


FIGURE 14. Wi-Fi beacon remote-ID (Parrot) [73].

our team to mitigate the risks associated with drone flights and to discriminate between cooperative and uncooperative drones [92]. The suggested system is a counter-drone technology integrated into the UTM system allowing information exchange and coordination using a set of clarification protocols for accountable response to sighted drones. The architecture allows the CUAS system to obtain information about the registration status of the sighted drone and whether it is authorized to perform the observed flight. The system contains two databases: a database of the identities of registered drones (ID-DB) and a database of authorized missions (AUTH-DB) containing updated information about drone registration and mission authorizations. The CUAS system is simulated to analyze its performance under different scenarios using multiple drones.

In [93], Tedeschi *et al.* proposed an Anonymous Remote IDentification of Unmanned Aerial Vehicles (ARID) to enable RemoteID-complaint anonymous remote identification of drones. The suggested solution allows the broadcasting of messages using ephemeral pseudonyms that only a trusted authority can link to the long-term identifier of the drone and its operator. Furthermore, ARID enforces message authenticity to protect drones against impersonation and spoofed reporting and generates negligible overhead on the trusted authority. ARID is implemented and validated on the 3DR-solo drone. The experimental results showed that the most demanding configuration takes only about 11.23 ms to generate a message and consumes 4.72 mJ of energy.

In [94], a decentralized UTM protocol is proposed to control airspace access to ensure high integrity, availability, and confidentiality of airspace operations. The suggested system addressed mainly the lack of a clear definition of protocols that govern a secure interaction between authorities, service providers, and end-users. The suggested solution is based on blockchain, smart contract technologies, and a mobile crowdsensing (MCS) mechanism to seamlessly enforce airspace rules and regulations governing UAV operations. The architecture is integrated with the Ethereum platform and verified using four innovative contract verification tools, Osiris, Slither, Oyente, and SmartCheck. The simulation results show the robustness of the code against many threats, such as man-in-the-middle, denial-of-service, and replay attacks.

Hashem *et al.* [95] proposed a novel drone ID architecture based on the Hyperledger Iroha blockchain, which is a block sequence. The administrator registers new drones to the networks and stores the public keys and certificates. The drone broadcasts the updated data directly to the blockchain if the Internet is available. Otherwise, drones send data to the connected ground control station, which will forward the received information on behalf of the drone. The observers receive messages via Bluetooth and Wi-Fi broadcast or poll the blockchain, and they can fetch the public key associated with a drone to validate the received messages. The authors showed its proof-of-concept implementation with the Drone remote identification protocol and the system's invulnerability against various attacks.

In [96], Xueping et al. proposed architecture for blockchain-based drone systems called DroneChain to secure drone communication during data collection and transmission and to preserve the integrity of collected data. DroneChain includes four main blocks: drones, a control system, a cloud server, and a blockchain network. The drones construct data as tuples: *DeviceID, Time, Location, Data* and send them to the controller, which forwards the data to the network block. The latter will hash the data and transform them into a Merkle tree node. Since each record will be stored in the cloud instantly, the data integrity can be verified at any time.

Despite the ADS-B being one of the optimal and promising solutions to broadcast the RID, this system does not contain a security mechanism [97], [98]. The ASD-B is vulnerable to attacks such as Eavesdropping, Jamming, and spoofing. Sudhindra *et al.* proposed a cryptography approach to overcome issues related to the security and sensitivity of the drone's data [99]. The concept is demonstrated in a hardware platform using a low-cost software-defined radio and an evaluation board equipped with an ARM processor. The suggested framework is based on the RTL-SDR library and integrates a symmetric-key encryption algorithm to encrypt/decrypt data. The architecture consumes one second to decode one ADS-B packet. In the same context, the researcher in [97] addressed the security failure of the ADS-B by proposing a new solution by exploiting some cryptographic primitives based on FFX encryption and then adapting them to the air traffic-monitoring scenario. The proposed solution is lightweight for congested data links and resource-constraint avionics. It also can tolerate package loss and disorders frequently occurring in ADS-B wireless broadcast networks.

2) POWER, PERFORMANCE, AND OTHER ASPECTS

Current research also focuses on the technical enhancement of the remote identification modules, such as the range, power consumption, and bit rate. For example, the horizontal broadcast range should be maximized ($\geq$ 1Km). Similarly, the vertical range should be greater than 500 m even if the UAV may not be flying this high [100]. Another design criterion is to keep the probability of false alarms less than one error/hour and the latency less than 3.5 s. Furthermore, the RID modules should have a minimal battery size to make them lightweight, which is one of the biggest challenges [101]. In [102], Jae *et al.* proposed an energy harvesting-based UAV identification network in which the UAVs harvest energy through radio frequency signals transmitted from ground control stations and then transfer their identification information to the ground receiver station (GRS). The time and bandwidth allocation balance the harvested energy and the achievable rate of UAVs.

A research team at the National Research and Development Corporation designed and developed a small RID transmitter powered by a lightweight Lithium-ion battery (3.8V, 1670 mAh), allowing it to broadcast information continuously for more than seven hours [103]. The evaluation was carried out in three approaches "horizontal distance between the transmitter and the evaluation receiver," "altitude of the transmitter," and "position of the transmitter." Bluetooth 5.0 technology is the wireless method used to broadcast RID where the maximum distance reached is about 300 m with a maximum communication success rate of 95%.

Omkar *et al.* present a study investigating the reliability and range of the LoRa to broadcast the remote ID [76]. This study quantifies the bit error rate performance and the spreading factors caused by two different interference scenarios to explore the impact on the reliability and coverage of the RID system based on the LoRa technology. MATLAB simulations show that lower spreading factors have limited range but have an advantage of shorter time-on-air and an increasing bit rate.

Using LoRa technology, Ghubaish *et al.* proposed a prototype based on low-cost LoRaWAN modules to identify and locate the UAVs [104]. The study shows that the UAV equipped with a LoRaWAN module that transmits the RID can be easily localized using several ground stations. The suggested architecture broadcasts the RID in a range of 600m while consuming only 1w. It is important to note that LoRa technology is considered an excellent candidate to transmit RID because it can spread signals for up to 10km for line-of-sight (LOS) conditions, using just a few watts [105], [106] and can reach distance range of 60 Km with less than 5% packet loss rate [71].

In [107], Chin *et al.* proposed an ADS-B based on low-power communication modules LoRa and APRS. These modules are tested in conjunction with the 4G network to broadcast the position for tracking and the flight data in a wide area using a quad-rotor to check the capability of the proposed infrastructure at low altitudes. The reported performance is encouraging and is verified with highly acceptable conditions under the Technical Capability Level (TCL3).

uFly framework is proposed in [108] to guarantee regular communication and optimize UAV flights. It allows the management of the drones' ADS-B communication traffic constrained by the airplanes' ADS-B. The uFly is implemented and verified within the UAV flight airspaces in different cities, and it ultimately revealed promising results in effectively

managing UAVs and keeping the ADS-B communication regular.

B. JOINT UAV-RID RESEARCH

In some studies, the term "remote identification" does not reflect the identification of drones defined by most regulations. However, it is used by some researchers to refer to detecting and identifying drones in images. In this context, some studies used different sources of information to identify UAVs such as radiofrequency signals [109], [110], [111], [112], [113], UAV sensors [114], [115], [116], acoustic fingerprints [117], [118], [119], [120], [121], etc. Such works are out of this review paper's scope because they do not align with the UAV-RID philosophy.

Other research studies use camera surveillance to identify drones using machine learning algorithms [112], [122], [123]. Such studies are considered because they represent an attractive joint alternative to remotely identifying UAVs. For example, in the research project undertaken in [124], Remote Drone Identification (ReDroId) is proposed based on visual RSA SecurID Tokens. ReDroId implemented an authentication scheme distinguishing between foe and friend drones by optically modulating the RSA token using flashing lights. A machine learning algorithm recognizes the flashing lights using a video surveillance camera. It converts the detected tokens to binary codes used to convert them to binary code, permitting identifying drones.

VII. DISCUSSION

Drone remote identification is indeed an indispensable technology for public and airspace safety. The regulations, standards, industrial solutions, and research work described in this paper build a framework to understand this technology's scope and inform related adoption, deployment, development, and research activities. For example, aviation authorities interested in making related rules can use this framework not only to have an overview of other countries' regulations but also to understand the scope of available standards and the capabilities of technical solutions to support a seamless rule-making process. Recall that the initially proposed rule-making by the FAA faced resistance from industry and users, which resulted in considerable changes and corresponding delays in issuing the final rule. In this section, we discuss the main opportunities and challenges of this technology.

A. RID OPPORTUNITIES

The primary function of RID is to identify a drone in the airspace and associate the drone with the operator by providing information about the location of the ground control station. This function is a core requirement for operating drones over people and at night. In addition to this primary function, RID provides several opportunities for advanced applications and services, airspace monitoring, and counter-drone systems.

1) OPPORTUNITIES FOR SAFE AIRSPACE OPERATION

The RID technology can support multiple applications, such as situational awareness and aircraft separation. Broadcast-based RID cannot support such applications due to the lack of a communication link to the drone. The FAA encourages –but not mandates– drone operators to equip with ADS-B In for increased traffic awareness if practicable [22]. On the other hand, the Internet Engineering Task Force has recognized the relevance of using remote identification to support Internet-based applications such as control and command (C2) beyond visual line-of-sight and detect & avoid (DAA). IETF aims to leverage existing Internet resources (protocols, standards, services, infrastructure, and business models) to support such applications. Still, not all applications require the user's device to have Internet connectivity. For example, an observer device can authenticate a remote identification message if the device is equipped with the necessary certificates.

2) OPPORTUNITIES FOR AIRSPACE MONITORING

In conjunction with public mobile devices, remote identification technology can provide a cost-effective opportunity to monitor airspace. The crowd's mobile devices can continuously sense RID messages and forward them to a central system for aggregation and evaluation. Such a solution is considered ideal for broadcast-based RID as it does not require the availability of an internet access point. However, this solution should be enhanced by a security solution to prevent false reports by the crowd. The amount of the received reports depends on the crowdedness of the area over which the drone is flying. In a crowded city center, for instance, the central server can receive hundreds of reports of the same drone, which is unneeded and can overload the system. From this viewpoint, the monitoring system should implement a periodic mechanism to treat a predefined number of reports for each drone to avoid overloading.

3) OPPORTUNITIES FOR RELIABLE COUNTER-DRONE OPERATIONS

Furthermore, remote identification presents an opportunity for counter-drone systems toward reliable decision-making. Currently, these systems support two main functions: detection and interdiction. Detection technologies include radar, computer vision, acoustic systems, and radio-frequency detectors [125], [126]. Interdiction solutions include jamming, catching, or shooting [127], [128]. This two-function concept of a counter-drone system is suited for sensitive zones where any sighted drone should be classified as illegal. Dividing the city airspace into sensitive and insensitive zones can be problematic in urban areas. Remote identification can mitigate this problem by allowing the counter-drone system to identify drones and differentiate between legal and illegal ones instead of classifying every drone as unwanted. Also, RID allows for controlled drone operations in or close to sensitive areas without being prevented by the counter-drone system.

B. RID LIMITATIONS AND CHALLENGES

Remote identification technology has several limitations and challenges that arise from its conception, design, or implementation. We discuss these in the following subsections.

1) SECURITY AND PRIVACY

The remote identification technology is vulnerable to a wide range of security attacks. The most critical issue is the ability of malicious drones to transmit fake identities while performing illegal missions. The fake identity can be arbitrary or masqueraded. Masqueraded identities are easy to obtain by intercepting remote identification messages from other drones since identity data is supposed to be public. Masquerading a drone identity is especially critical because it not only allows illegal operators to complete their missions without raising observer concerns. Innocent owners of the intercepted drone can also face prosecution because violations would be associated with their drones.

In addition to manipulating identities, an illegal drone can change other data in the remote identification message. For example, an operator can violate the approved mission plan and hide this violation by manipulating the location or velocity data in the remote identification message.

Remote identification requires compatibility with handheld devices such as mobile phones and tablets to allow observers to identify drones in their proximity and report annoying ones to authorities. Since drones can move at high speeds and disappear from the scene quickly, it is important to send reports with minimum delays using a system available to the public. However, such a system can open the door to various attacks. For example, malicious observers can send fake or falsified reports to cause harm to innocent drone operators or temporarily or indefinitely disrupt the service.

In large regions, multiple UTM service suppliers are needed to provide the required coverage. In remote identification, the ASTM standard differentiates between service and display providers. These providers should exchange information and communicate with other unmanned service suppliers in the UTM ecosystem. This distributed model of services adds additional risk to remote identification data, such as interception, spoofing, and manipulation.

This snapshot of issues shows that remote identification cannot be used without security enhancement. Indeed the authentication of remote identification data and reports is of high priority.

Operators' privacy is another challenge for drone identification. Revealing mission data along with the true drone identity and the operator's location can pose a risk to the businesses of some commercial operators. Therefore, different solutions, including encryption and anonymization, should be considered to address the privacy challenges. Such solutions would prevent the general public from knowing the true identity of the drone and its operator. Still, ground observers with special authorities such as law enforcement would have access to decryption or deanonymization services that help them find the true drone identity.

2) REMOTE IDENTIFICATION AMBIGUITY

Assume a ground observer who spots a drone in the near airspace. The observer starts the RID application on the mobile device. The application shows a drone at the expected location. Can the observer be sure that the drone displayed in the app is the same one seen in the sky? An illegal operator could fly an unregistered drone on a malicious mission and uses a ground transmitter to send fake RID to mislead ground observers. So, RID has an inherent ambiguity issue similar to car plates. Without further information, it is nearly impossible to assure that a car plate belongs to the vehicle it is placed on.

Associating a received RID with a sighted drone becomes more complex when multiple drones fly nearby, and the ground observer receives fewer RIDs than the number of the sighted drones. This ambiguity issue is hard to resolve. One solution was proposed in [129], where the observer is authorized to overtake control over the drone. In the case of ambiguity, the observer sends a command to the drone to perform a specific movement. When the drone responds to this command, it is considered legal. The observer should send the command securely to prevent other drones from imitating the response. Computer vision-based methods should be considered to disambiguate multiple and far drones. This disambiguation solution requires the involvement of a human observer, which can be error-prone and only deal with a limited number of drones near the observer.

3) TECHNICAL FAILURES AND DATA ACCURACY

As a technical system, remote identification can fail due to permanent or transient errors in the onboard RID module or the communication link. Also, location data included in the remote identification message be inaccurate or wrong due to interference affecting the IMU or erroneous information from the GPS modules [100]. Technical failures can be confused with safety or security violations by a ground observer who can make a wrong decision, e.g., to interdict the drone. This indicates that remote identification systems should be developed with high reliability using fault-tolerant systems methods such as adding redundancy modules, e.g., a redundant GPS device. Apart from this, ground observers should be able to obtain more information about violating drones before deciding to prevent them. For example, a dual system should be fitted into the NextGen of ADS-B to validate the position with the primary source.

4) RANGE LIMITATIONS

RID regulations and standards are driven by the requirement of supporting mobile devices such as tablets and mobile phones. This sets a significant constraint due to the limited capabilities of the embedded communication technologies, including WLAN and Bluetooth. Specifically, these technologies have a shorter range than what many or most high-end drones can fly in terms of altitude. Of course, flying above 400 feet (or whatever is specified by regulations) is already a violation. However, malicious users' interest is to remain

undetected in the first place. So, aligning the RID specification with the capabilities of standard mobile devices is a major issue [100].

Regardless of the solution chosen to broadcast the required information, there is a general desire for long-range identification. To overcome the lack of network connectivity and to support RID broadcast in remote areas, it is essential to complement the existing infrastructure with a non-terrestrial network using high-altitude platform stations and satellite technology [11]. Thus, the 6G network will be an excellent alternative to broadcast UAV identification because it is envisioned to provide integrated solutions with capabilities allowing the use of terrestrial and satellite communication within a single modem. Finally, radiofrequency is a reliable choice to broadcast remote identification, but it is not receivable by most mobile devices without a hardware upgrade.

5) ENERGY CONSTRAINTS

Another challenge to consider along the range question is energy consumption. An insufficient energy resource will cause the interruption of broadcasting data and mislead a ground observer to classify the drone as illegal. An independent energy source for the remote identification module should be considered to mitigate this issue. Possible solutions include solar panels or harvesting energy through radio frequency signals transmitted from the ground control stations as proposed in [102]. Another vital point to consider is power level regulations by communication authorities such as the FCC 47CFR15 and 47CFR18 by the International Telecommunication Union (ITU), which differ from one country to another. For example, the Effective Isotropic Radiated Power (EIRP) in Spain should not exceed 10 W against 400 W in the UK [130].

VIII. CONCLUSION

Drone remote identification will undoubtedly play an essential role in protecting the airspace against malicious and reckless drone operations and supporting public safety and privacy. This study has described the current activities in this area and provided details on related regulations in different countries, primary standards, industrial solutions, and research. Discussing the different opportunities and challenges provides hope in this technology and informs regulators, standardization bodies, industry, and researchers about what is still to do. The main lesson is that RID is an indispensable technology for airspace safety. It is as important as a car license plate for road traffic safety. However, associating the digital RID with the physical drone is a major challenge that should be overcome using advanced authentication and disambiguation solutions.

REFERENCES

[1] C. Pu and Y. Li, "Lightweight authentication protocol for unmanned aerial vehicles using physical unclonable function and chaotic system," in *Proc. IEEE Int. Symp. Local Metrop. Area Netw. (LANMAN)*, Jul. 2020, pp. 1–6.
[2] G. Cavone, N. Epicoco, R. Carli, A. Del Zotti, J. P. R. Pereira, and M. Dotoli, "Parcel delivery with drones: Multi-criteria analysis of trendy system architectures," in *Proc. 29th Medit. Conf. Control Autom. (MED)*, Jun. 2021, pp. 693–698.
[3] DroneDJ. *Traffic Monitoring Drones Proposed by Ohio Officials*. Accessed: Jun. 14, 2022. [Online]. Available: https://dronedj.com/2018/06/30/traffic-drones-ohio/
[4] A. Caruso, S. Chessa, S. Escolar, J. Barba, and J. C. Lopez, "Collection of data with drones in precision agriculture: Analytical model and LoRa case study," *IEEE Internet Things J.*, vol. 8, no. 22, pp. 16692–16704, Nov. 2021.
[5] S. U. Jan and H. U. Khan, "Identity and aggregate signature-based authentication protocol for IoD deployment military drone," *IEEE Access*, vol. 9, pp. 130247–130263, 2021.
[6] L. Wenguang and Z. Zhiming, "Intelligent surveillance and reconnaissance mode of police UAV based on grid," in *Proc. 7th Int. Symp. Mechatronics Ind. Informat. (ISMII)*, Jan. 2021, pp. 292–295.
[7] B. Aydin, "Public acceptance of drones: Knowledge, attitudes, and practice," *Technol. Soc.*, vol. 59, Nov. 2019, Art. no. 101180.
[8] R. Rumba and A. Nikitenko, "The wild west of drones: A review on autonomous-UAV traffic-management," in *Proc. Int. Conf. Unmanned Aircr. Syst. (ICUAS)*, Sep. 2020, pp. 1317–1322.
[9] C. Barrado, M. Boyero, L. Brucculeri, G. Ferrara, A. Hately, P. Hullah, D. Martin-Marrero, E. Pastor, A. P. Rushton, and A. Volkert, "U-space concept of operations: A key enabler for opening airspace to emerging low-altitude operations," *Aerospace*, vol. 7, no. 3, p. 24, Mar. 2020.
[10] M. S. Rahman, I. Khalil, and M. Atiquzzaman, "Blockchain-powered policy enforcement for ensuring flight compliance in drone-based service systems," *IEEE Netw.*, vol. 35, no. 1, pp. 116–123, Jan. 2021.
[11] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, H. Karimipour, G. Srivastava, and M. Aledhari, "Enabling drones in the Internet of Things with decentralized blockchain-based security," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6406–6415, Apr. 2021.
[12] J. J. Seibler Snead and D. Inserra, *Establishing a Legal Framework for Counter-Drone Technologies*. Washington, DC, USA: Heritage Foundation, 2018.
[13] *Commision Delegated Regulations (EU) 2020/1058*, European Union Aviation Safety Agency, Cologne, Germany, 2018.
[14] *UAS Remote Identification Overview*, Federal Aviation Administration, Washington, DC, USA, 2021.
[15] *ASTM F3411-19: Standard Specification for Remote ID and Tracking*, ASTM Int., West Conshohocken, PA, USA, 2019.
[16] Z. He and T. Tan, "Survey on worldwide implementation of remote identification and discussion on drone identification in China," in *Proc. IEEE 3rd Int. Conf. Civil Aviation Saf. Inf. Technol. (ICCASIT)*, Oct. 2021, pp. 252–258.
[17] *Remote Identification of Unmanned Aircraft*, Federal Aviation Administration, Washington, DC, USA, 2020. [Online]. Available: https://www.faa.gov/news/media/attachments/RemoteID/Final
[18] U-Space Teams, "U-space concept of operations," SESAR Joint Undertaking, Brussels, Belgium, White Paper 01, 2019.
[19] *Era of Rutm*, National Technological Initiative, Moscow, Russia, 2020.
[20] *Civil Aviation Administration of China Unmanned Aircraft System Traffic Management Information Service System (Beta Version)*, Second Research Institute of CAAC, Chengdu, China, 2020.
[21] C. Xu, X. Liao, J. Tan, H. Ye, and H. Lu, "Recent research progress of unmanned aerial vehicle regulation policies and technologies in urban low altitude," *IEEE Access*, vol. 8, pp. 74175–74194, 2020.
[22] *Remote Identification of Unmanned Aircraft—Final Rule*, Department of Transportation Federal Aviation Authority, USA, 2021.
[23] *Easy Access Rules for Unmanned Aircraft Systems (Regulations (EU) 2019/947 and (EU) 2019/945)*, EASA, Cologne, Germany, Sep. 2021.
[24] Civil Aviation Administration of China, "Concept of requirements: Identification of operating civil micro and small unmanned aircraft," Civil Aviation Admin. China, Beijing, China, Tech. Rep., 2021.
[25] Civil Aeronautics Act of Japan, "Overview of direct remote ID standard establishment," World Trade Org., Geneva, Switzerland, Tech. Rep., 2021.
[26] Joint Secretary to the Government of India, "The drone rules," Ministry Civil Aviation, New Delhi, India, Tech. Rep. AV-29017/37/2021-SDIT-MOCA, Aug. 2021.
[27] Director-General of Civil Aviation (DGCA), "Beyond visual line-of-sight operations for unmanned aircraft," Civil Aviation Authority Singapore, Singapore, Tech. Rep. AC UAS-2(0), 2019.

[28] Dubai Government, "Law no. (4) of 2020 regulating unmanned aircraft in the emirate of Dubai," Dubai Civil Aviation Authority, Dubai, United Arab Emirates, Tech. Rep., 2020.
[29] "Unmanned aircraft system (UAS) traffic management (UTM) concept of operation," Federal Aviation Admin., Washington, DC, USA, Tech. Rep., 2020.
[30] *81 FR 42063—Operation and Certification of Small Unmanned Aircraft Systems*, Dept. Transp. Federal Aviation Authority, USA, Aug. 2016.
[31] J. Trock and A. E. Matthews, "A new horizon in UAS regulation: Remote identification and operations over people," Air Space Lawyer, USA, Tech. Rep. 34, Jun. 2017.
[32] *Remote Identification of Unmanned Aircraft—Notice of Proposed Rulemaking*, Dept. Transp. Federal Aviation Authority, USA, 2019.
[33] Administration of Transportation Department and the Federal Aviation, "Part 107—Small unmanned aircraft systems," Code Federal Regulations, USA, Tech. Rep. 81 FR 42209, 2021.
[34] *Executive Summary—Final Rule on Remote Identification of Unmanned Aircraft*, U.S. Federal Aviation Authority, Washington, DC, USA, Dec. 2020.
[35] European Aviation Safety Agency (EASA), "Technical opinion: Introduction of a regulatory framework for the operation of unmanned aircraft," Eur. Aviation Saf. Agency, Cologne, Germany, Tech. Rep. A-NPA 2015-10, 2015.
[36] European Aviation Safety Agency (EASA), "Advance notice of proposed amendment: Introduction of a regulatory framework for the operation of unmanned aircraft," Eur. Aviation Saf. Agency, Cologne, Germany, Tech. Rep. NPA 2022-06, 2015.
[37] Drone Alliance Webmaster, "Drone traffic management in Europe, the views of the drone alliance Europe," Drone Alliance Europe, Brussels, Belgium, White Paper 06, 2016.
[38] Airports Council International, "Drones in the airport environment: Concept of operation and industry guidance," Airports Council Int. Europe, Brussels, Belgium, Tech. Rep., 2021.
[39] Global UTM Association Members, "Designing UTM for global success," Global UTM Assoc., Lausanne, Switzerland, Tech. Rep., Nov. 2020.
[40] Global UTM Association Members, "UAS traffic management architecture," Global UTM Assoc., Lausanne, Switzerland, Tech. Rep., Apr. 2021.
[41] European Aviation Safety Agency (EASA), "Prototype commission regulation on unmanned aircraft operations," Eur. Union Aviation Saf. Agency, Cologne, Germany, Tech. Rep. 2022/425, 2016.
[42] *Easy Access Rules for Unmanned Aircraft Systems (Regulations (EU) 2019/947 and (EU) 2019/945)*, EASA, Cologne, Germany, Mar. 2020.
[43] D. S. Bragin, D. R. Urazayev, A. A. Konev, and I. V. Cherepanova, "Onboard device for UAS remote identification," in *Proc. J. Phys., Conf.*, Aug. 2021, vol. 1989, no. 1, Art. no. 012044.
[44] *Provisions on Operations of Light and Small Unmanned Aircraft (Interim)*, CAAC Flight Standard Department, USA, 2015.
[45] *Number of Unmanned Aircraft Cloud Systems in China*. Accessed: Nov. 2020. [Online]. Available: https://baijiahao.baidu.com
[46] *Interface Specification of Unmanned Aircraft and Cloud System*, China Academy of Civil Aviation Science and Technology, Beijing, China, 2017.
[47] "Study on the regulation of UAS in Hong Kong," Netherlands Aerosp. Centre, Amsterdam, The Netherlands, Tech. Rep., 2018.
[48] *UAS Registration*, Gen. Civil Aviation Authority, Abu Dhabi, United Arab Emirates, 2021.
[49] N. S. S. Raj, J. Varghese, and G. R. Chandra, "Drones take-off towards legal regime in the united Arab Emirates," in *Proc. Int. Conf. Infocom Technol. Unmanned Syst. (ICTUS)*, Dec. 2017, pp. 689–693.
[50] "Unmanned aircraft system (UAS) and operations," Dubai Civil Aviation Authority, Dubai, United Arab Emirates, Tech. Rep., 2020.
[51] *CTA Standard, Small Unmanned Aerial Systems Serial Numbers (ANSI/CTA-2063)*, ANSI, New York, NY, USA, 2017.
[52] *Standardization Roadmap for Unmanned Aircraft Systems, Version 2.0*, ANSI, New York, NY, USA, 2020.
[53] *3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Numbering, Addressing and Identification (Release 13)*, document 3GPP TS 23.003 V13.5.0, 2016.
[54] W. S. Card, A. Wiethuechter, R. Moskowitz, and A. Gurtov, *Drone Remote Identification Protocol (DRIP) Requirements and Terminology*, document RFC 9153, Feb. 2022.
[55] W. S. Card, A. Wiethuechter, R. Moskowitz, S. Zhao, and A. Gurtov, "Drone remote identification protocol (drip) architecture," Internet-Draft draft-ietf-drip-arch-22, Internet Eng. Task Force, Fremont, CA, USA, Tech. Rep. draft-ietf-drip-arch-29, Mar. 2022.
[56] R. Moskowitz, T. Heer, P. Jokela, and R. T. Henderson, *Host Identity Protocol Version 2 (HIPv2)*, document RFC 7401, Apr. 2015.
[57] S. Josefsson and I. Liusvaara, *Edwards-Curve Digital Signature Algorithm (EDDSA)*, document RFC 8032, Jan. 2017.
[58] *Uncrewed Aerial System (UAS) Support in 3GPP*, document TS 22.125, 3GPP, Apr. 2022.
[59] *Study on Supporting Unmanned Aerial Systems (UAS) Connectivity, Identification and Tracking*, document TS 23.754, 3GPP, Mar. 2021.
[60] A. Ganjoo. (2020). *Drone Life*. Accessed: Jan. 31, 2022. [Online]. Available: https://dronelife.com/2020/02/19/the-deep-dive-into-remote-id-for-drones-what-it-is-what-it-means-and-whats-next/
[61] Thales Group. (2020). *Scaleflyt Remote ID: Identification & Gestion De Drones*. Accessed: Jan. 24, 2022. [Online]. Available: https://www.scaleflyt.com/remoteid
[62] *Unmanned Aircraft System (UAS) Traffic Management (UTM) Concepts of Operations, V2*, Federal Aviation Administration, Washington, DC, USA, Mar. 2020.
[63] S. Sciancalepore and R. Di Pietro, "SOS: Standard-compliant and packet loss tolerant security framework for ADS-B communications," *IEEE Trans. Dependable Secure Comput.*, vol. 18, no. 4, pp. 1681–1698, Aug. 2019.
[64] B. Stark, B. Stevenson, and Y. Chen, "ADS-B for small unmanned aerial systems: Case study and regulatory practices," in *Proc. Int. Conf. Unmanned Aircr. Syst. (ICUAS)*, May 2013, pp. 152–159.
[65] Y. Lin and S. Saripalli, "Sense and avoid for unmanned aerial vehicles using ADS-B," in *Proc. IEEE Int. Conf. Robot. Autom. (ICRA)*, May 2015, pp. 1–15.
[66] R. Yeniceri, M. Hasanzade, E. Koyuncu, and G. Inalhan, "Enabling centralized UTM services through cellular network for VLL UAVS," in *Proc. Integr. Commun., Navigat. Surveill. Conf. (ICNS)*, Apr. 2017, pp. 1–21, Paper 2E1–1.
[67] *Drone ADS-B Transceiver Datasheet*, uAvionix, Bigfork, MA, USA, 2000.
[68] C. M. Consiglio, B. Duffy, S. Balachandran, J. L. Glaab, and A. C. Muñoz, "Sense and avoid characterization of the independent configurable architecture for reliable operations of unmanned systems," NASA Langley Res. Center, Hampton, VA, USA, Tech. Rep. 20200002709, 2019.
[69] F. Minucci, E. Vinogradov, and S. Pollin, "Avoiding collisions at any (Low) cost: ADS-B like position broadcast for UAVs," *IEEE Access*, vol. 8, pp. 121843–121857, 2020.
[70] H. Lv, F. Liu, and N. Yuan, "Drone presence detection by the Drone's RF communication," *J. Phys., Conf.*, vol. 1738, no. 1, Jan. 2021, Art. no. 012044.
[71] M. H. M. Ghazali, K. Teoh, and W. Rahiman, "A systematic review of real-time deployments of UAV-based LoRa communication network," *IEEE Access*, vol. 9, pp. 124817–124830, 2021.
[72] F. Noor, M. A. Khan, A. Al-Zahrani, I. Ullah, and K. A. Al-Dhlan, "A review on communications perspective of flying ad-hoc networks: Key enabling wireless technologies, applications, challenges and open research topics," *Drones*, vol. 4, no. 4, p. 65, 2020. [Online]. Available: https://www.mdpi.com/2504-446X/4/4/65
[73] *Introduction to the European UAS Digital Remote ID Technical Standard*, ASD-STAN Standardization, Washington, DC, USA, Oct. 2021.
[74] N. Poursafar, M. E. E. Alahi, and S. Mukhopadhyay, "Long-range wireless technologies for IoT applications: A review," in *Proc. 11th Int. Conf. Sens. Technol. (ICST)*, Dec. 2017, pp. 1–6.
[75] S.-Y. Wang, J.-E. Chang, H. Fan, and Y.-H. Sun, "Performance comparisons of NB-IoT, LTE Cat-M1, Sigfox, and LoRa moving at high speeds in the air," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jul. 2020, pp. 1–6.
[76] O. Mujumdar, H. Celebi, I. Guvenc, M. Sichitiu, S. Hwang, and K.-M. Kang, "Use of LoRa for UAV remote ID with multi-user interference and different spreading factors," in *Proc. IEEE 93rd Veh. Technol. Conf. (VTC-Spring)*, Apr. 2021, pp. 1–7.
[77] M. Mozaffari, X. Lin, and S. Hayes, "Toward 6G with connected sky: UAVs and beyond," *IEEE Commun. Mag.*, vol. 59, no. 12, pp. 74–80, Dec. 2021.
[78] E. Murrell, Z. Walker, E. King, and K. Namuduri, "Remote ID and vehicle-to-vehicle communications for unmanned aircraft system traffic management," in *Communication Technologies for Vehicles* (Lecture Notes in Computer Science). Cham, Switzerland: Springer, 2020, pp. 194–202.

[79] A. Shoufan, C. Y. Yeun, and B. Taha, "*eSIM-Based Authentication Protocol for UAV Remote Identification*. Hoboken, NJ, USA: Wiley, 2021, ch. 4, pp. 91–122.
[80] A. Boekholt, "Switzerland launches first nationwide network remote identification service for drones," Swiss U-Space Implement., Swiss, Tech. Rep. 08, 2021.
[81] *Broadcast Location & Identification Platform (BLIP)*. Accessed: Jan. 25, 2022. [Online]. Available: https://unifly.aero/products/blip
[82] (2020). *RelmaTech*. Accessed: Jan. 24, 2022. [Online]. Available: https://www.relmatech.com/
[83] Insider Intelligence. (2020). *Here are the World's Largest Drone Companies and Manufacturers to Watch*. Accessed: Jan. 24, 2022. [Online]. Available: https://finance.yahoo.com/news/worlds-largest-drone-companies-manufacturers-192949252.html
[84] A DJI Technology. (2017). *What's in a Name? A Call for a Balanced Remote Identification Approach*. Accessed: Jan. 24, 2022. [Online]. Available: https://www.dropbox.com/s/v4lkyr2kdp8ukvx/DJI%20Remote%20Identification%20Whitepaper%203-22-17.pdf?dl=0
[85] DronesInsite. (2018). *Parrot Drone Company and Product Review | Bebop and AR Drones*. Accessed: Jan. 24, 2022. [Online]. Available: https://www.dronesinsite.com/drone-news/parrot-drone-company-review/
[86] ASD-STAN. (2021). *Introduction to the European UAS Digital Remote Id Technical Standard*. Accessed: Jan. 24, 2022. [Online]. Available: https://asd-stan.org/wp-content/uploads/ASD-STAN_DRI_Introduction_to_the_European_digital_RID_UAS_Standard.pdf
[87] Yuneec Website. (2021). *About us—Yuneec*. Accessed: Jan. 24, 2022. [Online]. Available: https://us.yuneec.com/
[88] (2021). *FAA Remote ID H520 and H520e Compliance—Yuneec*. Accessed: Jan. 24, 2022. [Online]. Available: https://us.yuneec.com/about-us/
[89] (2021). *Remote ID*. Accessed: Jan. 24, 2022. [Online]. Available: https://auterion.com/
[90] AEROBITS. (2021). *idME (remoteID)—Aerobits*. Accessed: Jan. 24, 2022. [Online]. Available: https://www.aerobits.pl/product/idme/
[91] L. Abualigah, A. Diabat, P. Sumari, and A. H. Gandomi, "Applications, deployments, and integration of Internet of Drones (IoD): A review," *IEEE Sensors J.*, vol. 21, no. 22, pp. 25532–25546, Nov. 2021.
[92] A. Shoufan and R. Alkadi, "Integrating counter-UAS systems into the UTM system for reliable decision making," 2021, *arXiv:2111.07291*.
[93] P. Tedeschi, S. Sciancalepore, and R. Di Pietro, "ARID: Anonymous remote identification of unmanned aerial vehicles," in *Proc. Annu. Comput. Secur. Appl. Conf.*, Dec. 2021, pp. 1–10.
[94] R. Alkadi and A. Shoufan, "Unmanned aerial vehicles traffic management solution using crowd-sensing and blockchain, 2021, *arXiv:2110.14979*.
[95] Y. Hashem, E. Zildzic, and A. Gurtov, "Secure drone identification with hyperledger Iroha," in *Proc. 11th ACM Symp. Design Anal. Intell. Veh. Netw. Appl.*, Nov. 2021, pp. 11–18.
[96] X. Liang, J. Zhao, S. Shetty, and D. Li, "Towards data assurance and resilience in IoT using blockchain," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Oct. 2017, pp. 261–266.
[97] H. Yang, Q. Zhou, M. Yao, R. Lu, H. Li, and X. Zhang, "A practical and compatible cryptographic solution to ADS-B security," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3322–3334, Apr. 2019.
[98] M. Strohmeier, V. Lenders, and I. Martinovic, "On the security of the automatic dependent surveillance-broadcast protocol," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 1066–1087, 2nd Quart., 2015.
[99] S. C. S. Nayak, "A cryptographic proof-of-concept for securing aircraft ADS-B data," RF Design, 2018. Accessed: Jan. 24, 2022. [Online]. Available: https://bit.ly/3QJ329I
[100] *Realizing Remote ID, Hidden Level*, High Level, Syracuse, NY, USA, Nov. 2019, pp. 1–16.
[101] L. Xie, J. Xu, and Y. Zeng, "Common throughput maximization for UAV-enabled interference channel with wireless powered communications," *IEEE Trans. Commun.*, vol. 68, no. 5, pp. 3197–3212, May 2020.
[102] J. C. Park, K.-M. Kang, and J. Choi, "Low-complexity algorithm for outage optimal resource allocation in energy harvesting-based UAV identification networks," *IEEE Commun. Lett.*, vol. 25, no. 11, pp. 3639–3643, Nov. 2021.
[103] H. Ishizuka, "Conducted a broadcast communication evaluation test that can remotely identify unmanned aerial vehicles," Tech. Rep., 2020. Accessed: Jan. 20, 2022.
[104] A. Ghubaish, T. Salman, and R. Jain, "Experiments with a LoRaWAN-based remote ID system for locating unmanned aerial vehicles (UAVs)," *Wireless Commun. Mobile Comput.*, vol. 2019, pp. 1–11, Oct. 2019.
[105] M. R. Seye, B. Gueye, and M. Diallo, "An evaluation of LoRa coverage in Dakar Peninsula," in *Proc. 8th IEEE Annu. Inf. Technol., Electron. Mobile Commun. Conf. (IEMCON)*, Oct. 2017, pp. 478–482.
[106] R. Ghanaatian, O. Afisiadis, M. Cotting, and A. Burg, "LoRa digital receiver analysis and implementation," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2019, pp. 1498–1502.
[107] E. C. Lin, C.-S. Hsieh, C.-C. Li, P.-C. Shao, Y.-H. Lin, and Y.-C. Yeh, "An ADS-B like communication for UTM," in *Proc. Integr. Commun., Navigat. Surveill. Conf. (ICNS)*, 2019, pp. 1–12.
[108] Y. Pan, S. Li, B. Li, B. Bhargav, Z. Ning, Q. Han, and T. Zhu, "When UAVs coexist with manned airplanes: Large-scale aerial network management using ADS-B," *Trans. Emerg. Telecommun. Technol.*, vol. 30, no. 10, Aug. 2019, Art. no. e3714.
[109] M. F. Al-Sa'd, A. Al-Ali, A. Mohamed, T. Khattab, and A. Erbad, "RF-based drone detection and identification using deep learning approaches: An initiative towards a large open source drone database," *Future Gener. Comput. Syst.*, vol. 100, pp. 86–97, Nov. 2019.
[110] M. S. Allahham, T. Khattab, and A. Mohamed, "Deep learning for RF-based drone detection and identification: A multi-channel 1-D convolutional neural networks approach," in *Proc. IEEE Int. Conf. Informat., IoT, Enabling Technol. (ICIoT)*, Feb. 2020, pp. 112–117.
[111] H. Gu, Y. Wang, G. Gui, S. Hong, H. Huang, J. Yang, M. Liu, J. Sun, and Y. Lin, "Radio frequency fingerprinting driven drone identification based on complex-valued CNN," in *Proc. 13th EAI Int. Conf. Mobile Multimedia Commun., Mobimedia, Cyberspace*, Aug. 2020, pp. 27–28.
[112] H. Kolamunna, T. Dahanayaka, J. Li, S. Seneviratne, K. Thilakaratne, A. Y. Zomaya, and A. Seneviratne, "DronePrint: Acoustic signatures for open-set drone detection and identification with online data," *Proc. ACM Interact., Mobile, Wearable Ubiquitous Technol.*, vol. 5, no. 1, pp. 1–31, Mar. 2021.
[113] A. Gumaei, M. Al-Rakhami, M. M. Hassan, P. Pace, G. Alai, K. Lin, and G. Fortino, "Deep learning and blockchain with edge computing for 5G-enabled drone identification and flight mode detection," *IEEE Netw.*, vol. 35, no. 1, pp. 94–100, Jan. 2021.
[114] S. Samaras, E. Diamantidou, D. Ataloglou, N. Sakellariou, A. Vafeiadis, V. Magoulianitis, A. Lalas, A. Dimou, D. Zarpalas, K. Votis, P. Daras, and D. Tzovaras, "Deep learning on multi sensor data for counter UAV applications—A systematic review," *Sensors*, vol. 19, no. 22, p. 4837, Nov. 2019.
[115] V. Sadhu, S. Zonouz, and D. Pompili, "On-board deep-learning-based unmanned aerial vehicle fault cause detection and identification," in *Proc. IEEE Int. Conf. Robot. Autom. (ICRA)*, May 2020, pp. 5255–5261.
[116] S. Hengy, M. Laurenzis, S. Schertzer, A. Hommes, F. Kloeppel, A. Shoykhetbrod, T. Geibig, W. Johannes, O. Rassy, and F. Christnacher, "Multimodal UAV detection: Study of various intrusion scenarios," *Proc. SPIE*, vol. 10434, pp. 203–212, Oct. 2017.
[117] O. A. Ibrahim, S. Sciancalepore, and R. D. Pietro, "Noise2Weight: On detecting payload weight from drones acoustic emissions," 2020, *arXiv:2005.01347*.
[118] S. Al-Emadi, A. Al-Ali, A. Mohammad, and A. Al-Ali, "Audio based drone detection and identification using deep learning," in *Proc. 15th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2019, pp. 459–464.
[119] S. Ramesh, T. Pathier, and J. Han, "SoundUAV: Towards delivery drone authentication via acoustic noise fingerprinting," in *Proc. 17th Annu. Int. Conf. Mobile Syst., Appl., Services*, Jun. 2019, pp. 27–32.
[120] J. Kim, C. Park, J. Ahn, Y. Ko, J. Park, and J. C. Gallagher, "Real-time UAV sound detection and analysis system," in *Proc. IEEE Sensors Appl. Symp. (SAS)*, Apr. 2017, pp. 1–5.
[121] N. Siriphun, S. Kashihara, D. Fall, and A. Khurat, "Distinguishing drone types based on acoustic wave by IoT device," in *Proc. 22nd Int. Comput. Sci. Eng. Conf. (ICSEC)*, Nov. 2018, pp. 1–4.
[122] L. Tao, T. Hong, Y. Guo, H. Chen, and J. Zhang, "Drone identification based on CenterNet-TensorRT," in *Proc. IEEE Int. Symp. Broadband Multimedia Syst. Broadcast. (BMSB)*, Oct. 2020, pp. 1–5.
[123] C. Y. Quan, O. L. W. Edmond, and S. Srigrarom, "Identification of drone thermal signature by convolutional neural network," in *Proc. Int. Conf. Unmanned Aircr. Syst. (ICUAS)*, Jun. 2021, pp. 63–70.
[124] B. Nassi, A. Levy, Y. Pirutin, A. Shabtai, R. Masuoka, and Y. Elovici, "ReDroId: Remote drone identification based on visual RSA SecurID tokens," in *Proc. Int. Conf. Electr., Comput., Commun. Mechatronics Eng. (ICECCME)*, Oct. 2021, pp. 1–9.

[125] M. Z. Anwar, Z. Kaleem, and A. Jamalipour, "Machine learning inspired sound-based amateur drone detection for public safety applications," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2526–2534, Mar. 2019.
[126] B. Taha and A. Shoufan, "Machine learning-based drone detection and classification: State-of-the-art in research," *IEEE Access*, vol. 7, pp. 138669–138682, 2019.
[127] T. Multerer, A. Ganis, U. Prechtel, E. Miralles, A. Meusling, J. Mietzner, M. Vossiek, M. Loghi, and V. Ziegler, "Low-cost jamming system against small drones using a 3D MIMO radar based tracking," in *Proc. Eur. Radar Conf. (EURAD)*, Oct. 2017, pp. 299–302.
[128] J. Rothe, M. Strohmeier, and S. Montenegro, "A concept for catching drones with a net carried by cooperative UAVs," in *Proc. IEEE Int. Symp. Saf., Secur., Rescue Robot. (SSRR)*, Sep. 2019, pp. 126–132.
[129] C. A. Bergan, E. H. Teague, and P. Guckian, "Local drone identification verification," U.S. Patent 17 193 312, Jul. 8, 2021.
[130] TWEVO Webmaster, "Radio regulation for drones," TWEVO Technol., Coimbra, Portugal, White Paper 11, Nov. 2017, pp. 1–9.

KAIS BELWAFI (Member, IEEE) received the M.Sc. degree in intelligent and communication systems from the Highest School of Engineering of Sousse, Tunisia, in 2012, and the Ph.D. degree in sciences and technology of information and communication from the University of Paris Seine, Cergy-Pontoise, France, in 2017. He is currently a Research Scientist with the Electrical and Computer Engineering Department, Khalifa University. His main research interests include the security of embedded systems, drone security, brain–computer interfaces, machine learning, signal processing, embedded and real-time systems, and HW/SW co-design.

RUBA ALKADI received the B.Sc. degree in electrical engineering from the American University of Sharjah, Sharjah, United Arab Emirates, in 2016, and the M.Sc. (by research) degree in engineering from Khalifa University, Abu Dhabi, United Arab Emirates, in 2018. She is currently a Research Associate with the Center of Cyber-Physical Systems, Khalifa University. Her research interests include unmanned aerial vehicles traffic management, machine learning, blockchain, and image processing.

SULTAN A. ALAMERI (Member, IEEE) received the B.S. degree in electrical and computer engineering from The Ohio State University, Columbus, OH, USA, in 2012, and the M.Sc. degree in electrical and computer engineering with focus on embedded systems from Khalifa University, Abu Dhabi, United Arab Emirates, in 2017, where he is currently pursuing the Ph.D. degree in electrical and computer engineering. He joined the defense industry in Abu Dhabi, in 2012, where he is also holding a position of the Head of the Department. His main research interests include artificial intelligence, embedded systems, and cybersecurity. He is a member of the IEEE-HKN.

HUSSAM AL HAMADI (Senior Member, IEEE) received the degree (Hons.) in computer engineering from Ajman University, in 2005, and the Ph.D. degree in computer engineering from Khalifa University, in 2017. He holds several international certificates in networking, business, and tutoring, like MSCA, MSCE, CCNA, CBP, and CTP. From 2005 to 2010, he was working as a Computer Consultant and a Tutor in several governmental and private institutions until joining Khalifa University as a Teaching Assistant, in 2010. He is currently a Research Scientist at the KU Center for Cyber-Physical Systems (C2PS), Khalifa University. His research interests include AI for security and security for AI, in addition to applied security protocols for several systems, such as software agents, SCADA, e-health systems, and autonomous vehicles. It also includes developing e-forensics and security methodologies for smartphones and drones. Since 2019, he has been the Secretary of the IEEE UAE Section. He is a Frequent Reviewer in several journals, including IEEE Access, IEEE Systems Journal, *KSII Transactions on Internet and Information Systems*, and *International Journal of Communication Systems*.

ABDULHADI SHOUFAN received the Dr.-Ing. degree from the Technische Universität Darmstadt, Germany, in 2007. He is currently an Associate Professor of electrical engineering and computer science at Khalifa University, Abu Dhabi. His research interests include drone security and safe operation as well as in embedded security, cryptography hardware, learning analytics, and engineering education.