Privacy-Aware Remote Identification for Unmanned Aerial Vehicles: Current Solutions, Potential Threats, and Future Directions

Pietro Tedeschi, *Member, IEEE*, Fatima Ali Al Nuaimi, Ali Ismail Awad, *Senior Member, IEEE*, and Enrico Natalizio, *Senior Member, IEEE*

***Abstract*—The Federal Aviation Administration (FAA) recently introduced a new standard, namely, *remote identification*, to improve accountability for unmanned aerial vehicles (UAVs) operations. This rule requires UAV operators to broadcast messages revealing sensitive data, such as identity and location on the wireless channel. However, this leads to security and privacy concerns among UAV operators. Unauthorized parties may easily discover the location and identity of a UAV flying in a specific area and launch attacks on it such as using wireless jamming or tracking its activity. This review investigates and systematizes the main weaknesses affecting the *Remote ID* capability required of modern UAVs, and the approaches through which attackers can exploit these weaknesses to disrupt safety and accountability. Moreover, this article analyzes current solutions that mitigate privacy issues associated with *Remote ID*. Finally, we identify multiple challenges that require to be addressed by both industry and academia, and we propose future research directions to improve the security and privacy of UAVs.**

***Index Terms*—Anonymity, privacy, remote ID, security, unmanned aerial vehicles (UAVs).**

Manuscript received 30 January 2023; revised 25 April 2023; accepted 13 May 2023. Date of publication 5 June 2023; date of current version 19 January 2024. This work was supported in part by the Technology Innovation Institute, Abu Dhabi, UAE, and in part by a joint research grant between United Arab Emirates University and Zayed University (UAEU-ZU), under Grant 12R141. Paper no. TII-23-0287. *(Corresponding author: Ali Ismail Awad.)*

Pietro Tedeschi and Fatima Ali Al Nuaimi are with the Technology Innovation Institute, Autonomous Robotics Research Center, Abu Dhabi 9639, United Arab Emirates (e-mail: pietro.tedeschi@tii.ae; Fatima.alnuaimi@tii.ae).

Ali Ismail Awad is with the College of Information Technology, United Arab Emirates University, Al Ain 15551, United Arab Emirates, and also with the Centre for Security, Communications and Network Research, University of Plymouth, PL4 8AA Plymouth, U.K. (e-mail: ali.awad@uaeu.ac.ae).

Enrico Natalizio is with the Technology Innovation Institute, Autonomous Robotics Research Center, Abu Dhabi 9639, United Arab Emirates, and also with the Université de Lorraine, CNRS, LORIA, F-54000 Nancy, France (e-mail: enrico.natalizio@loria.fr).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TII.2023.3280325.

Digital Object Identifier 10.1109/TII.2023.3280325

I. Introduction

THE number of unmanned aerial vehicles (UAVs) and drone applications has increased in this decade owing to their excellent mobility, autonomy, and eco-friendly features. This enabling technology has been adopted in multiple fields such as military, delivery, agriculture, mapping, civil defense, and monitoring [1].

The market for UAVs will considerably grow in the coming years, from 26.2 billion USD in 2022 to 38.3 billion USD in 2027, which shows a compound annual growth rate (CAGR) of 7.9% [2]. This expansion is driven by applications such as surveillance and military operations, mapping, delivery, and transportation, thus, causing increased demand for advanced technology and an increase in the popularity of semiautonomous and autonomous vehicles. However, this increase in UAVs adoption is posing privacy and safety concerns [3], [4], [5]. For instance, the incidents of unauthorized access and invasion by amateur drones have been reported by UAV operators dealing with critical infrastructures (CIs), such as airports, seaports, and military areas; these unauthorized activities are responsible for considerable security, privacy, and safety concerns [6].

To uphold accountability for UAVs, and detect and identify malicious drones, multiple regulatory authorities have implemented regulations, such as the *remote identification* (*Remote ID*) standard of the US-based Federal Aviation Administration (FAA) [7], [8]. Furthermore, Europe, the American Society for Testing and Materials (ASTM), and the AeroSpace and Defence Industries Association of Europe - Standardization (ASD-STAN) are considering similar actions to ensure UAV and drone operators provide identification and location information that other parties can receive during the UAV's flight [9].

In brief, regulations that propose the implementation of *Remote ID* require UAVs to broadcast periodic messages by reporting their identity, speed, location, and information about the ground control station (GCS) (i.e., the operator) to ensure public safety and monitor aerial spaces. The *Remote ID* requirement of the US was enacted in April 2021. After September 2022, all UAV manufacturers are required to comply with the *Remote ID* standard, whereas operators are required to do so until September 2023 [10].

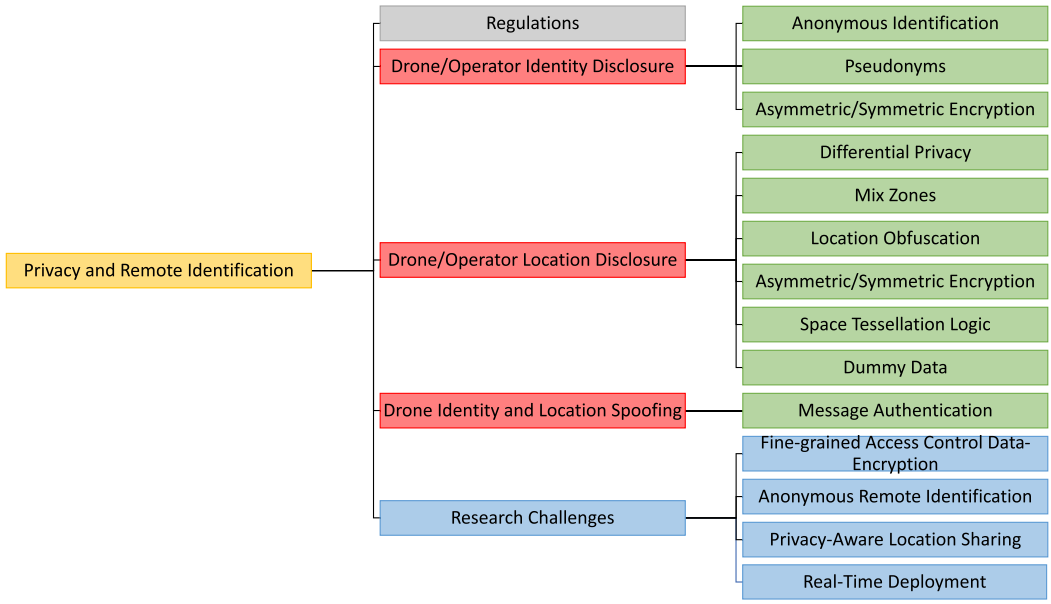

Fig. 1. Classification of scientific contributions per privacy issue. This contribution highlights considerable research challenges for each examined topic and identifies potential study areas.

However, the *Remote ID* requirement has raised privacy concerns among the UAV community, particularly. UAV operators dealing with CIs such as those in the retail, oil and gas, transportation, delivery, and health care industries. The broadcasting of cleartext data related to the identity and location of UAVs and their operators can enable malicious users to identify, and track UAVs and determine important information such as the locations of sensitive storage centers or the customer destination addresses of confidential/classified objects. For example, a UAV community opened a dispute recently about the privacy issues owing to the mandatory adoption of this rule will limit recreational and working activities [11].

Although the latest *Remote ID* standard provides the option to replace a long-term identity with an ephemeral one, such as a session identifier, no guideline or specification is provided to partially meet the privacy requests of UAV operators.

Despite its promising applications and prospects, applying the *Remote ID* standard to UAVs and drones has caused multiple privacy issues in academia, industries, and practitioners. Many studies, such as [12] and [13], have proposed the development of a secure protocol for drones and analyzed the vulnerabilities of and attacks on military and commercial drones. A few studies have proposed different solutions to mitigate the security and privacy issues of *Remote ID*.

An extensive review of the scientific literature suggests a requirement for a comprehensive review of the latest developments in this field. This article explores the primary privacy challenges to consider when imposing the *Remote ID* standard on UAVs and drones as well as the related countermeasures.

A. Our Contributions

This article fills the abovementioned gap by providing a comprehensive review of the latest developments regarding privacy issues, applications, solutions, and research challenges characterizing *Remote ID*, which affects operators or GCSs, and UAVs. This article introduces the current *Remote ID* regulations for tracking and identifying drones flying in defined airspace systems. Next, a reference scenario and an adversarial model are described. Furthermore, previously published privacy-preserving schemes related to *Remote ID* are surveyed and classified across multiple features, such as drone/operator identity privacy, location privacy, *Remote ID* requirement compliance, and communication technology (see Fig. 1 for a high-level overview). Moreover, this study presents the current attacks and threats affecting *Remote ID* and certain emerging research challenges to mitigate the aforementioned privacy issues, and discover future development directions. Previous studies on the privacy aspects of Internet of Drones (IoD), such as [10], [14], [15], [16], [17], have only focused on a limited number of vulnerabilities owing to *Remote ID*; an overview of potential defense strategies or countermeasures has not been provided. Therefore, an extensive study specifically designed to address the privacy concerns related to *Remote ID* is currently lacking.

B. Article Layout

The rest of this article is organized as follows. Section II provides an overview of the current regulations enabling drone tracking and identification. Section III describes the reference scenario and the adversarial model, followed by a study of multiple privacy-preserving schemes. Section IV describes the potential attacks and threats concerning the *Remote ID* standard. Then, the mechanisms and existing privacy-preserving techniques for *Remote ID* are discussed and compared in Section V. The emerging research challenges and future research directions are explained in Section VI. Finally, Section VII concludes this article.

II. Background

This section provides the background and fundamental concepts of standard *Remote ID* regulations for UAVs.

A. Remote ID

The set of *Remote ID* regulations published by the FAA allows any drone (and operator or GCS) to be identified and tracked by other parties in real time. The final *Remote ID* rule was released by the FAA in January 2021 and went into effect in April 2021. UAVs and their manufacturers have been required to comply with the *Remote ID* standard after September 2022, whereas operators have until September 2023 to comply with the requirements. The *Remote ID* rule requires UAVs to broadcast messages every second that contain at least the following information.

1) UAV ID: It is an identification code (identifier) of the UAV.
2) UAV position: It contains the global navigation satellite system (GNSS) coordinates such as latitude and longitude, altitude, and speed of the UAV.
3) Operator position: It contains the GNSS coordinates such as latitude and longitude and altitude of the operator or the ground control station.
4) Time stamp: It is the date and time of the broadcasted message.
5) Emergency code: It indicates whether the UAV is in an emergency state.

These requirements are applied from UAV takeoff until landing. From one side, according to the *Remote ID* specification, UAVs can use a network-based *Remote ID* via a persistent Internet connection with unmanned service supplier (USS) servers. From the other side, UAVs can adopt a broadcast-based approach to transmit the data over an industrial, scientific, and medical (ISM) frequency band $[2.4 \sim 2.5, 5.8]$ GHz such as Bluetooth/Wi-Fi via a *Remote ID* broadcast module. UAVs can operate without adopting a *Remote ID* module only in specific zones, namely, *FAA-Recognized Identification Areas* managed by organizations or educational entities.

B. Other Regulations

1) Europe: In 2015, the European Commission remarked on the importance of using *Remote ID* for safe, secure UAV operation in airspaces. In 2016, the European Union Aviation Safety Agency (EASA) proposed a "prototype" set of rules, namely, the Commission Regulation on Unmanned Aircraft Operations, which allows authorities to identify drones flying in airspaces using the following information: operator registration, UAV class, UAV operation type, geofencing status, UAV position and height. At the end of 2020, the EASA released rules obliging drones to broadcast their unique ID serial numbers, locations, and operator locations, without specifying any technology. By January 2023, all UAV operators in Europe should be following these rules [18].

2) France: French *Remote ID* rule requires UAVs to have unique identifiers, such as serial numbers. The mandatory data that should be broadcasted are the: 1) drone/operator location; 2) speed; 3) altitude. Operator registration is optional, and the data transmission interval is 3 s. Finally, the French *Remote ID* standard specifies Wi-Fi beacon technology as the communication technology [19].

3) Japan: In 2020, the Japanese Civil Aeronautics Act published the direct remote ID (DRID) standard document, which specifies the requirements that should be considered for UAV accountability. To summarize, the document states the following: 1) UAV registration has been mandatory since June 2022; 2) each UAV must be equipped with a *Remote ID* module; 3) a *Remote ID* message, containing the unique ID, serial number, position and speed, and authentication tag of the drone, must be broadcasted at least once per second to prevent common security attacks such as replay and man-in-the-middle; 4) one of the following communication standards should be used: Wi-Fi beacon, Wi-Fi NAN, Bluetooth Low Energy Long Range, and Bluetooth 5.x [20].

4) ASTM and ASD-STAN: The ASTM and ASD-STAN have defined a set of *Remote ID* guidelines to uphold the accountability of UAV operators. They have similar guidelines about the broadcasting of UAV identities and GNSS locations. As for communication technologies, the ASTM requires the use of Bluetooth 4.x and Wi-Fi NAN at 2.4 GHz; the use of Bluetooth 5.x and Wi-Fi NAN at 5.8 GHz is optional. The ASD-STAN specifies that Wi-Fi beacon is mandatory and Bluetooth 4.x is optional [21].

Table I (inspired by ASD-STAN [21]) summarizes the differences between the final *Remote ID* regulations of multiple countries.

III. Reference Scenario and Adversarial Model

This section introduces the reference scenario (see Section III-A) and adversarial model (see Section III-B) considered in this work in order to familiarize the reader with the privacy concerns linked to the broadcasting of cleartext *Remote ID* data. The assumptions in the scenarios highlight the common situations where *Remote ID* is adopted and provide examples of the capabilities and activities that a malicious actor can carry out.

A. Reference Scenario

The reference scenario, depicted in Fig. 2, assumes different UAVs u_j (remotely piloted, semiautonomous, or autonomous) flying around a given area to accomplish a mission. The GCS, which may be a person or a computer system, is responsible for the movements of a drone. In addition to the equipment available on most commercial drones, each UAV features a GNSS module, which estimates its real-time location with a maximum accuracy of δ meters, and an Instrumental Navigation System (INS). Each UAV is then assumed to broadcast standard-compliant *Remote ID* messages using an onboard common wireless transceiver such as a Wi-Fi or Bluetooth module. The UAVs may not have a persistent Internet connection with the GCS. According to the *Remote ID* rule, UAVs u_j have to broadcast sensitive data, such as their ID_j, position (latitude $lat_j(t)$, longitude $lon_j(t)$,

TABLE I
COMPARISON BETWEEN REMOTE IDENTIFICATION REGULATIONS; ● MEANS MANDATORY, ○ MEANS OPTIONAL, AND – MEANS UNSPECIFIED. STATEMENTS FULL NAMES: EUROPE (EU), FRANCE (FR), JAPAN (JP), AMERICAN SOCIETY FOR TESTING AND MATERIALS (ASTM), AND AEROSPACE AND DEFENCE INDUSTRIES ASSOCIATION OF EUROPE - STANDARDIZATION (ASD-STAN)

Feature	Remote ID	EU Rule	FR Rule	JP Rule	ASTM	ASD-STAN
UAV ID	●	●	●	●	●	●
UAV position	●	●	●	●	●	●
UAV direction	●	●	●	●	●	●
UAV speed	●	●	●	●	●	●
UAV altitude	●	–	●	●	●	○
UAV timestamp	●	●	–	●	●	●
UAV status	●	●	–	●	–	●
UAV category/Class	–	●	–	–	–	○
Operator ID	–	●	○	●	○	●
Transmission interval	1 s	–	3 s	1 s	1 – 3 s	1 – 3 s
Bluetooth 4.x	–	–	–	○	●	○
Bluetooth 5.x	–	–	–	○	○	●
Wi-Fi Beacon	–	–	●	○	–	●
Wi-Fi neighbor awareness networking (NAN) 2.4 GHz	–	–	–	○	●	●
Wi-Fi NAN 5 GHz	–	–	–	○	○	–

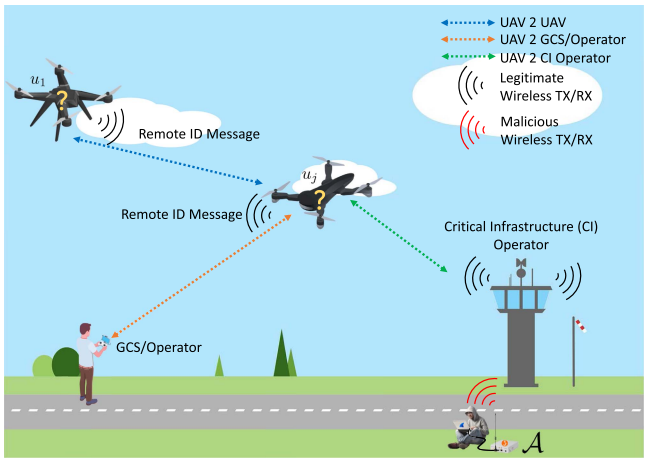

Fig. 2. Reference scenario. Several UAVs fly in a given area (one of them is controlled by a GCS/operator) and broadcast messages compliant with the *Remote ID* rule. An adversary $\mathcal{A}$ is eavesdropping on the wireless channel, and a CI operator monitors the area.

and altitude $alt_j(t)$), relative speed ($v_{(x,j)}(t)$, $v_{(y,j)}(t)$, and $v_{(z,j)}(t)$), GCS position, and the emergency code ϵ (if any) once every second or time t.

Furthermore, our scenario features a generic wireless receiver that can capture and collect the *Remote ID* packets transmitted by the UAVs on the selected radio channel. Based on the definition by the Drone Remote Identification Protocol (DRIP) working group (WG) of the Internet Engineering Task Force (IETF)-drone remote-id protocol [22], the generic observer can be an USS, and it is in charge of monitoring real-time traffic and enforcing airspace and violation control by reporting suspicious or unusual drone activity. The generic observer can be a CI operator or a generic user equipped with a laptop or a smartphone that can detect and decode *Remote ID* packets emitted by drones and access their contained information. Finally, the generic adversary $\mathcal{A}$ detailed in Section III-B is presented to highlight the security and privacy threats associated with *Remote ID*.

B. Adversarial Model

The main aim of the assumed adversary $\mathcal{A}$ is to disrupt the privacy of legitimate drones and forge (spoof) messages to be accepted or recognized by receivers as legitimate. The attacker can: 1) obtain the long-term identity and track the location of a specific UAV by collecting all data packets broadcasted *over the air* using a powerful wireless adapter (e.g., an ALFA Network card in *monitor mode* [23]) via WIRESHARK [24] or TCPDUMP [25]; 2) obtain the identity and track the position of the correspondent operator or GCS; 3) impersonate and spoof the location of a specific UAV while executing malicious activities, such that an UAV appears to behave legitimately. For example, the attacker can set up a software defined radio (SDR), such as a HackRF or a Universal Software Radio Peripheral (USRP), on its computer and start the spoofing activity using the GPS-SDR-SIM tool [26].

In this adversarial model, the $\mathcal{A}$ features both passive and active capabilities. On the one hand, $\mathcal{A}$ is a global, frequency-unbounded, and spatially unlimited passive eavesdropper, capable of detecting and receiving any message broadcasted by the UAV independently from the communication frequency and modulation. On the other hand, $\mathcal{A}$ can also generate fake messages, replay the received packets, spoofing the identity and the location of a legitimate UAV. Moreover, the attacker has access to significant computing power and/or a high-speed Internet connection, which allows it to outsource computational tasks. Although the attacker is unaware of the UAV location during the attack, standard Wi-Fi-enabled drones have a maximum range of around 6–7 km; however, as stated in [27], attacks against Wi-Fi can be launched outside this range. The assumed adversary does not aim to launch denial of service (DoS) attacks, such as jamming and packet flooding, because they are out of the scope of this contribution. Note that additional details about security attacks on drones are available in [28].

IV. *Remote ID* Attacks and Threats

This section identifies and discusses potential *Remote ID*-related privacy threats targeting UAVs and operators.

A. Drone Identity Disclosure

As per the FAA, beginning September 2023, every UAV should broadcast its identity in cleartext on wireless communication channels. Although this rule will improve the accountability and safety of aerial vehicles, it can threaten their privacy. An attacker aims to eavesdrop on wireless channels, capture packets, infer drone identities, and perform linking attacks. The attacker can collect sensitive information related to the UAV, such as the identity of its owner, and track it for other malicious activities [29].

B. Drone Location and Path Disclosure

The broadcasting of a drone's location (i.e., its GNSS coordinates) can help detect misbehaving and unauthorized UAVs and immediately identify potential collisions. However, it can enable an attacker to perform multiple malicious activities such as the capture, tracking, monitoring, and inference of sensitive data. Location-based attacks can reveal customer locations and company and CI storage sites, identify mobility patterns, and track UAV trajectories. Therefore, UAV operators or owners may want to conceal their UAV location information to protect their positions throughout their flight paths [30].

C. Operator Identity and Location Disclosure

The abovementioned threats to drones apply to UAV operators. The *Remote ID* standard obliges UAVs to broadcast in cleartext their GCS data such as their latitude, longitude, altitude, and identification code (which is optional). Operator data should be unlinkable between several messages; that is, an unauthorized observer should not be able to deduce any change (if any) in operator data between multiple messages, or infer the potential relationship between an UAV and an operator. Finally, a location-based attack can reveal the locations of depositories, customers, and military bases. For instance, in October 2022, attackers demonstrated that they collected the data of 80 000 Da-Jiang Innovations (DJI) drone identification codes, including the aircraft models, serial numbers, and pilot positions [31]. Furthermore, security researchers reverse engineered the *DroneID* radio protocol used by DJI drones and reported that the protocol broadcasted not only the Global Positioning System (GPS) location and unique identifier of each drone but also the GPS coordinates of its operator [32]. To address concerns about the public's ability to access the locations of drone pilots through the use of inexpensive software and radio devices, DJI is taking action by implementing certain measures: "This means that anyone with access to the software and cheap radio hardware can intercept and decode the drone's broadcasts to pinpoint the operator's location, potentially posing serious security and privacy concerns" [33].

D. Path Planning Algorithm Disclosure

The broadcasting of drone data, such as latitude, longitude, altitude, and speed, can enable an attacker to reverse engineer the shortest path or the best path algorithm that the UAV uses to reach a destination point using a data-driven approach. The attacker can capture data related to a particular drone and try to infer details using machine learning techniques on the algorithm behind it to generate the best path.

E. Drone/Operator Identity and Location Spoofing

Currently, the *Remote ID* does not define any security property, such as authentication and confidentiality. A *Remote ID* spoofing attack involves the creation or impersonation of the real identity of a UAV to hide or transmit fake data related to the occupied location. A generic aerial vehicle can appear legitimate, thus deceiving legitimate receivers such as CI operators, authorities, and neighboring UAVs. Furthermore, an attacker can inject false information (e.g., false emergency code), replay legitimate data, and broadcast false collision warnings by forcing other UAVs to critical maneuvers [14].

V. *Remote ID* Privacy-Preserving Solutions

The enforcement of security and privacy solutions for *Remote ID* has received minor attention over the last few years after the rule was announced on December 28, 2020. Therefore, the current industrial and academic efforts should be steered toward this direction. This study introduces a comprehensive classification of the scientific contributions that address the remote identification privacy concerns affecting UAVs and operator/GCS entities (summarized in Table II). Further, to conclude the critical discussion, Section V-A summarizes the main lessons learned.

Alkadi and Shoufan [34] addressed the security limitations of current UAV traffic management (UTM) systems, such as confidentiality, integrity, and availability, by proposing a decentralized UTM architecture to enforce airspace rules and regulations by leveraging mobile crowd sensing (MCS), and blockchain smart contracts. The main aim is to generate a drone identifier and verify it using the Ethereum platform. Moreover, they used the *Remix IDE* platform to write, execute, debug, and test solidity-based smart contracts before deploying them on the blockchain. Although the proposed approach complies with the standard *Remote ID* requirements, and provides detailed security analysis, drones' and operators' anonymity and authenticity are not considered. Furthermore, the proposed solution is not scalable to different scenarios, such as environments without persistent Internet connection.

Alsoliman et al. [35] presented a framework for anonymously verifying the authenticity of flying UAVs without revealing their flight paths or operator identities. This solution adopts a technique, namely *flight plan slicing* to divide the flight plan into segments, and the Boneh-Gentry-Lynn-Shacham (BGLS) aggregation signature scheme to sign anonymous *Remote ID* messages. As for the communication technology, they assumed

TABLE II
COMPARISON BETWEEN APPROACHES CONTEXTUALIZING PRIVACY-PRESERVING SOLUTIONS FOR *REMOTE ID*; ● INDICATES THAT A SPECIFIC FEATURE IS FULFILLED, AND ○ DENOTES THAT THE FEATURE IS NOT INCLUDED

Ref.	Method / Techniques	Drone ID Privacy	Drone Location Privacy	Operator ID Privacy	Operator Location Privacy	RID Requirement Compliance	Communication Technology	Platform/ Framework/ Simulation	Security / Privacy Analysis
[34]	Blockchain, Smart Contracts, MCS	○	○	○	○	●	Wi-Fi/ Bluetooth	Ethereum, Remix	●
[35]	Flight Plan Slicing, BGLS	●	●	●	○	●	Wi-Fi	Simulations	●
[36]	Differential Privacy, AES, Public Key Encryption	○	●	○	○	●	Wi-Fi	MATLAB R2020b	○
[37]	Decoy, Aggregation, Probabilistic Privacy Risk	○	●	○	○	●	○	Simulations	●
[38]	Obfuscation, Entropy-based	○	●	○	○	○	Wi-Fi, LTE	OMNeT++	●
[39]	Incremental Capsule Matching, RSA	○	●	○	○	○	Wi-Fi	Laptop, Raspberry-Pi, ESPCopter, MATLAB R2021b	●
[40]	eSIM, X.509 Certificates, AES, Elliptic Curve Cryptography (ECC), PIN	○	○	○	○	●	Wi-Fi	○	●
[41]	Mix Zones, Ant Colony Optimization	○	●	○	○	○	5G	IoDSim / OMNeT++	○
[42]	Mix Zones	○	●	○	○	○	5G	IoDSim / OMNeT++	○
[43]	MAVLink, ECDSA, El-Gamal ECC	●	○	○	○	●	Wi-Fi (IEEE 802.11b)	3DR-Solo Drone	●
[44]	MixDrones [42], ARID [43]	●	●	○	○	●	○	IoDSim / OMNeT++	●
[45]	Mix-Zones, k-anonymity, Dummy Data	○	●	○	○	○	IEEE 802.11	OMNet++	●
[46]	Elliptic Curve ElGamal, Capsule Tessellation Logic, Public Key Encryption	○	●	○	○	○	Wi-Fi (IEEE 802.11b)	3DR-Solo, MATLAB R2020b	●
[47]	Camenisch-Lysyanskaya (CS), Derler-Slamanig (DS), Bilinear Pairings	●	○	○	○	●	Wi-Fi (IEEE 802.11b)	Holybro X500, ESPcopter	●
[48]	Blockchain	●	●	○	○	●	5G	○	○
[49]	Elliptic Curve Integrated Encryption Scheme (ECIES), Keccak, Keccak Message Authentication Code (KMAC)	○	○	●	●	●	○	○	●

Wi-Fi usage to broadcast *Remote ID* messages. From the security perspective, they discussed different attack scenarios and security issues, such as impersonation and replay attacks, leaked Flight Certificate Vector (FCV), anonymity, and untraceability. About impersonation attacks, an unauthorized UAV can attempt to enter a restricted area without permission from the unmanned aircraft system (UAS) traffic controller. The UAV may attempt to create its own flight permissions and use them to generate *Remote ID* messages by impersonating a legitimate UAV (e.g., by leaking a public key certificate and the correspondent private key). For the replay attack, an unauthorized drone may try to intercept and replay a legitimate UAV's freshly broadcasted *Remote ID* message at a different time and/or location to gain access to a restricted area. Furthermore, misbehaving drones in a network may be hijacked, broken, or intentionally altered by their operators to deviate from their designated flight paths. However, dividing a UAV's flight plan into blocks of flight zones (bounded by time and location), each with its own public key, to achieve authentication anonymity for UAVs. The framework of the proposed solution is divided into two phases: setup and authentication. In the setup phase, the operator obtains the list of flight certificates (FA). The authentication phase involves two

mandatory steps: authentication request and authorization approval. This step is performed during flight because the drone is requested to authenticate itself by sending *Remote ID* messages. Authentication is achieved through the signing and verification of *Remote ID* messages via a BGLS scheme and elliptic curve digital signature algorithm (ECDSA). As for the communication technology, the authors assumed Wi-Fi adapters.

Brighente et al. [36] proposed a solution that guarantees only location privacy compliance with the *Remote ID* standard, and can detect violations of the no-fly zone areas by unauthorized drones. FAA regulations require all drones to broadcast information such as location and identity, which may enable an attacker to monitor a drone's behavior and capture the packets broadcasted wirelessly (via Wi-Fi) to increase awareness of the drone's location and identity. The proposed approach enhances the drones location privacy by implementing differential privacy and detecting invasions by unauthorized drones. The scheme comprises five phases: *1) registration*, where the legitimate entities register with a trusted third party (TTP) before their deployment; *2) differentially private Remote ID*, where they adopted the planar Laplace distribution for drawing a random point that depends only on the distance between the realization of the random variable and the actual UAV location; *3) encrypted location reports*, where ciphertexts containing precise location information are broadcasted; *4) area invasion detection* which introduces the area invasion detection process by describing the strategy of the solution implemented by the CIs operator to detect the attacks in a no-fly zone; *5) reporting phase* where the CIs operator reports malicious and attacking drones to TTP. The authors evaluated their scenario using MATLAB R2020b and real UAV flight data assuming the use of Wi-Fi communication technology. However, the authors did not provide a security analysis.

Ding et al. [37] focused on the location privacy issues in drone delivery. They assumed that an adversary can monitor a drone's path to force the disclosure of the customer's identity and delivery location. To mitigate this issue, they proposed a privacy risk assessment method that is based on the probability of connecting a particular customer with a specific vendor/supplier based on the delivery drone route. Then, they suggested methods of preserving the privacy of paths, such as the deployment of decoy vendors and the use of aggregation/obfuscation techniques. The authors have shown a very detailed privacy analysis.

Reddy et al. [38] aimed to mitigate attacks related to location privacy and tracking by obfuscating the current location of a UAV, and randomizing its trajectory to prevent an attacker from locating or tracking the drone. To this aim, they proposed three strategies based on the shortest path, random location, and dummy location without specifying details related to the *Remote ID* standard. The authors adopted location obfuscation, trajectory randomization, entropy-based metrics, and convex hulls. Furthermore, they assumed that the drone is equipped with multiple radio modules, such as IEEE 802.11 and long term evolution (LTE), for communication. They simulated the solutions via OMNeT++ and conducted a meaningful privacy analysis. However, efficient communication and collaboration between the user, server, and drone are necessary to locate and track a target effectively. The server provides the target's current location, and the drone observes and tracks it to respond and take action under the user's guidance (if it occurs on the ground).

Sciancalepore and George [39] proposed a new protocol called privacy-preserving trajectory matching (PPTM) to prevent collision between UAVs in a privacy-preserving fashion, that is, without disclosing any location data. Data such as UAV location and timestamps are essential for detecting and avoiding collisions in a timely manner; nevertheless, this information cannot be shared with others UAVs unless they are authorized parties. The main idea is based on the adoption of: 1) a tree-based algorithm, namely "Matching Incremental Capsule"; 2) a secure communication channel like transport layer security (TLS); and 3) a lightweight security protocol based on the Rivest–Shamir–Adleman (RSA) algorithm. For the performance assessment, the authors verified the solution in MATLAB R2021b and then deployed the protocol on a laptop, Raspberry Pi 3, and an ESPCopter drone assuming the Wi-Fi as communication technology. Moreover, the authors performed security analysis by the well-known automated verification tool ProVerif to prove that PTTM meets the standard security requirements.

To protect drone communications, Shoufan et al. [40] examined the security, safety, and privacy issues related to the FAA *Remote ID* standard. On the one hand, they proposed a *Remote ID* standard-compliant authentication protocol to secure communication. It authenticates the end-to-end and the broadcasted messages by using an embedded subscriber identification module (eSIM), a public key infrastructure, X.509 certificates, and the advanced encryption standard (AES) symmetric-key encryption algorithm. They tested their solution on a UAV developed by Government Telecommunication Authority. On the other hand, the authors conducted a security analysis with ProVerif, but they did not develop any mitigation technique against privacy issues introduced by the *Remote ID* regulation.

Svaigen et al. [41] introduced BioMixD, a bioinspired and traffic-aware mix zone placement strategy that leverages ant colony optimization for IoD location privacy. This solution exploits features such as traffic analysis, drone position, and airways congestion via mix-zones, a concept introduced in the field of vehicular ad hoc network (VANET) for pseudonym exchange between the UAVs. The proposed approach requires persistent communication with infrastructure elements, which may not always be available in UAV operations. The authors used the IoDSim simulator to evaluate the proposed solution for 5G and beyond-5G communication technologies. Although this work provided a brief security analysis of IoD privacy and security requirements and pursued location privacy preservation, the proposed approach does not comply with the *Remote ID* standard.

Svaigen et al. [42] proposed the MixDrones protocol, which is based on mix zones, "where drones can change their in-flight airways when they are inside a mix zone, aiming to embrace a large number of drones to protect and hamper the success of a location attack." Authors show that the MixDrones approach is robust against trajectory-based deanonymization attacks. The implementation has been done in a simulation environment, such as an IoDSim environment integrated with the INET framework

in OMNET++ simulator. However, this approach does not comply with the *Remote ID* standard.

Tedeschi et al. [43] highlighted the privacy issue related to the broadcasting of a drone's identity as per the *Remote ID* standard. To mitigate this privacy issue, the authors designed the anonymous remote identification (ARID) protocol, a standardized *Remote ID* security protocol. This approach leverages ephemeral pseudonyms that can only be linked to a UAV's long-term identifier and its operator by a trusted authority, such as the FAA. Furthermore, the proposed solution protects UAVs against spoofing and identity impersonation via message authentication by leveraging ECDSA for the authentication, and the Elliptic Curve ElGamal for the encryption. The authors integrated ARID with the MAVLink protocol on a 3DR-Solo drone (within 3DR Poky OS) by broadcasting frames using IEEE 802.11b. Moreover, they provided a security analysis in ProVerif to verify the UAV anonymity, message authenticity, protection against replay attacks, and partial protection against tracking.

Svaigen et al. [44] designed a real-time location-based attack to track a drone's trajectory based on its *Remote ID* message by strategically deploying eavesdroppers on the ground. To mitigate this issue, the authors integrated the solution proposed in [42] (MixDrones), and [43] (ARID) to protect the drone's location and identity information. Furthermore, they adopted zone service providers to provide shared access to drones and controlled airspace. They also evaluated the three solutions, namely, *Remote ID* (standard version without security features), ARID, and ARID+MixDrones in IoDSim, by providing a qualitative security analysis.

Svaigen et al. [45] presented a framework to guide the researcher on designing location privacy solutions for the IoD paradigm. The framework covers how to design a location privacy solution, define adversarial model, conduct experiments, evaluation, and analyze results. Furthermore, they discussed different techniques to increase location privacy, such as anonymization using mix zones, spatio-temporal obfuscation leveraging *k-anonymity*, use of dummy data by generating fake users and providing *k-anonymity*, and protocol-based solutions. Moreover, they proposed a framework, namely, MixDrones, and tested it by creating synthetic drone mobility traces generated by an *ad hoc* framework integrated with OMNet++. Moreover, they verified the effectiveness of the proposed approach in [42].

Tedeschi et al. [46] proposed a lightweight solution, namely, privacy-preserving collision avoidance (PPCA) for UAVs for colocation detection and collision avoidance in a privacy-preserving manner. Using the ElGamal encryption algorithm, this approach enables multiple UAVs to detect potential collisions by broadcasting wireless messages without revealing their locations. It allows nearby UAVs to agree on a secure path and temporary location by sharing using a secure wireless connection to avoid collisions. Moreover, the authors proposed a space tessellation logic based on the adoption of capsules by supporting the assumption with an experimental campaign on a 3DR Solo drone (using the 3DR Poky OS), and adopting the IEEE 802.11b protocol for broadcasting. Finally, they used ProVerif for the formal verification of the security features of PPCA. However, the contribution is not compliant with the *Remote ID* standard.

Wisse et al. [47] extended the ARID protocol proposed in [43]. The new protocol, namely Anonymous Direct Authentication and Remote Identification (A^2RID), is a suite of two protocols that guarantees UAV anonymity while broadcasting *remote-ID*-standard-compliant messages. They proposed to adopt two cryptographic schemes: 1) a processing-intensive but memory-lightweight solution that leverages Camenisch-Lysyanskaya ($CS-A^2RID$); 2) a computationally friendly but memory-consuming approach that adopts the Derler–Slamanig signature scheme ($DS-A^2RID$). Besides that, they used multiple cryptography techniques, such as the well-known ECIES, Cramer–Shoup cryptosystem, the digital signature scheme proposed by Boneh-Gentry-Lynn-Shacham, bilinear pairings, the Schnorr noninteractive zero-knowledge proof scheme, and a signatures of knowledge algorithm. The authors performed an extensive experimental campaign on real drones such as a Holybro X500 (for $CS-A^2RID$) and an ESPcopter (for $DS-A^2RID$). A formal security proof is provided via ProVerif. However, although this contribution provides a privacy-preserving scheme for the drones' identities and it complies with the *Remote ID* standard, it does not address other important issues such as the drone/operator location privacy.

Wu et al. [48] defined a blockchain-based privacy preservation solution for 5G drone communications. They introduce a high-level architecture that complies with the *Remote ID* standard. The authors described some approaches for protecting privacy regarding identifier management, data protection, and trajectory protection by leveraging well-known cryptographic techniques. In detail, they proposed the following blockchain-based privacy-preserving solutions for drones: an identification management approach, a data privacy protection approach, a trajectory privacy protection approach, and a drone network consensus mechanism. However, the authors did not perform any simulation or real implementation of the suggested solutions. Furthermore, they identified some research challenges and the limitations of their approach by considering the constraints of drone resources (energy, drone size, battery lifetime), and open issues that blockchain use can address to guarantee privacy preservation in drone communications.

Finally, Moskowitz et al. [49] submitted an IETF draft that describes a method of ensuring UAS operator/pilot privacy as per the *Remote ID* standard. At the time of writing, they are the only ones that have proposed a suite to address the privacy concerns of operators or GCSs (identifier and location). Their approach involves encrypting in place (the ciphertext has the same length as the cleartext), those fields containing operator sensitive data using a hybrid ECIES scheme. In detail, the authors used ECIES, and KMAC to ensure the privacy of drone operator. They introduced some potential security considerations of the proposed scheme.

A. Lessons Learned

This section summarizes the main lessons learned from the abovementioned investigation and cross-comparison of the security and privacy solutions for UAV deployments.

1) Security, Privacy, and Energy Tradeoff: Balancing security and energy efficiency can often be a challenging task. This is because achieving a high level of security usually demands more energy from UAVs than what is considered optimal, resulting in a less energy-efficient configuration. However, this balance can be achieved and certain limitations concerning UAV battery lifetime, usability, and reliability constraints can be addressed by minimizing power consumption and adopting secure, privacy-preserving solutions, as discussed in this contribution.

2) Cryptography Versus Physical-Layer Security: Modifying the receivers' and infrastructure software is a necessary step in implementing cryptography solutions. Thus, the expense of their integration should be carefully taken into account. Despite being effective, none of the abovementioned privacy-preserving solutions provide the implementation of physical layer anonymous communications [50]. However, over the past few years, many scientific contributions have notably promoted physical-layer security techniques for UAVs. Physical layer security features can be considered to build network architectures that are robust to several attacks, such as replay, spoofing, eavesdropping, and interference, to name a few. In cases for which standard cryptography techniques are unsuitable, network countermeasures and physical-layer security defensive schemes should be combined to provide a reliable communication channels. Nevertheless, implementing these advanced techniques usually increases receiver cost and complexity, which can significantly affect the energy budget of such devices. Thus, academia has expressed keen interest in the challenge of balancing energy and security, which remains a crucial aspect.

3) Secure Communication Protocols: The cleartext broadcasting of data related to a UAV or its operator identification and location can enable a malicious user to identify and track the UAV and its operator. This can lead to the discovery of sensitive information, such as the location of storage centers containing confidential or classified objects or the destination addresses of such objects for specific customers. In order to mitigate these issues and guarantee, at the same time, the accountability of UAVs and operators, it is necessary to provide a certain level of security and privacy for the protocol communications in a framework of to users worldwide. Finally, to limit the exposure of the cryptographic key material and execute the code in a secure area, the trusted execution environment (TEE) and the root of trust features should be considered.

4) Privacy-Aware Regulations: One of the main lessons from this contribution is that the transportation agencies of several governments are proposing different *Remote ID* rules that require different technical requirements as well. It is essential to standardise a generic remote identification rule for all UAVs to support the industry with the integration and development aspects. Further, as the next step, it is crucial that during the design of such regulations for UAV accountability, local and national authorities should take into account the concerns, risks, safety, and impact related to the privacy issues introduced to both UAVs and people.

VI. Research Challenges and Future Directions

This section highlights a few challenges and future research directions related to the security and privacy of *Remote ID*. Table III summarizes the attacks and the goals of a potential attacker covered in Section IV, the generic defense techniques presented in Section V, research challenges, and possible limitations.

A. Fine-Grained Access Control Data-Encryption

Data related to a drone and its operator, such as latitude, longitude, and altitude, should be known only to authorized parties; they should not be publicly available. For example, a drone or an operator can only allow authorized parties with the proper attributes (e.g., by leveraging the ciphertext/key policy—attribute-based encryption technique) [51] to open the broadcasted messages. Furthermore, *Remote ID* messages should be broadcasted at least once per second. The cryptographic payload broadcasted via Bluetooth or Wi-Fi should be compliant with the maximum transmission unit (MTU), i.e., one message per frame, without resorting to packet fragmentation. Finally, the solution should allow for opportunistic operator/drone data decoding by authorized parties without any explicit key establishment occurring at run-time.

B. Anonymous Remote Identification

The latest *Remote ID* rule allows UAV operators to partially protect their privacy by using session identifiers, known as a pseudonyms, rather than their UAVs' long-term identity for identification purposes. This feature enables unique identification by the FAA while maintaining the UAV's identity hidden. However, the *Remote ID* standard does not provide instructions on creating these identifiers or offer directions on their design. The enforcement of such a rule implies that the research community addresses the following challenges: 1) the anonymous authentic messages broadcasted by the operator/drone should be easily, and directly verified without referring to a TTP; 2) this latter should be able to verify and disclose the real long-term identity of a drone in case of misbehavior. Furthermore, the proposed solutions should be efficient in terms of processing, storage, bandwidth, and energy capabilities [43], [47]. Finally, promising mechanisms can be designed by considering the public key cryptography such as [43], or leveraging a lightweight physical unclonable function (PUF)-based privacy-preserving scheme for the authentication purposes [52], or by considering the application of physical layer security techniques for anonymous communications [53].

C. Privacy-Aware Location Sharing

Different solutions in the scientific literature have been discussed to ensure location privacy and avoid threats to aerial vehicles. For example, several mechanisms presented in this review are based on well-known techniques such as differential privacy, dummy data, encrypted space tessellation, mix-zones, data obfuscation, and *key-anonymity*, to name a few. According

TABLE III
MAPPING BETWEEN RESEARCH CHALLENGES, POTENTIAL SOLUTIONS, AND OVERALL LIMITATIONS FOR UAVS

Attack Types	Attack Goals	Defense Techniques	Research Challenges	Limitations
• Drone/Operator Location Disclosure	• Identify and target sensitive locations • Discover mission start and end point location	Asymmetric Cryptography, Attribute Based Encryption	Fine-grained Access Control Data-Encryption	*Remote ID* Law Enforcement Limited Computational Power Limited usage of Cryptographic Accelerators Limited Memory-Storage Limited Bandwidth Limited Battery-Lifetime Limited Bluetooth/Wi-Fi Maximum Transmission Unit Lack of Internet Connection Exposure of Crypto-Key Material Hard software integration
• Drone/Operator Identity Disclosure • Drone/Operator Location Spoofing	• Eavesdrop and infer the drone/operator identity • Perform linking attacks • Impersonate a legitimate drone/operator • Broadcast and injection of false data • Broadcast false collision warnings	Pseudonyms, Anonymous Signatures Scheme, Anonymous Broadcast Encryption, Blind and Anonymous Identity-Based Encryption	Anonymous Remote ID	
• Drone Location and Path Disclosure • Operator Location Disclosure • Path Planning Algorithm Disclosure	• Track and detect UAV location and trajectory • Collect sensitive data • Conduct traffic analysis	Differential Privacy, Mix-Zones, Data Obfuscation	Privacy-Aware Location Sharing	

to the abovementioned research challenges, a TTP should be able to identify and confirm the current location of a malfunctioning/misbehaving drone or operator, even when the drone is not been registered with federal authorities. This requirement will help authorities in taking prompt action. Moreover, the potential solutions to mitigate this issue should be efficient in terms of computational power, storage, bandwidth, and energy consumption. It would be beneficial to examine current air traffic regulations regarding location privacy and develop mechanisms to ensure compliance with law enforcement [45].

D. Real-Time Deployment

The real-time deployment of UAVs can pose a considerable number of issues. Some key points to be considered are listed below.

1) Performance and energy constraints: From the security and privacy perspective, it is worth considering the impact of adopting cryptography algorithms on the energy, computational cost, storage, and bandwidth overheads. In real-time deployment, the challenging aspects should consider the different types of UAV systems (from the small to the large ones), the time to execute the encrypt/decrypt operations, the memory footprint required in terms of random access memory (RAM) and read only memory (ROM), and finally, the size of payload that should be transmitted by leveraging a dedicated communication protocol, i.e., the number of packets and the time-slots to send a single packet. In this case, finding a suitable tradeoff for real-time deployments is crucial [54].
2) Safety concerns: Minimizing the risk of accidents is important because UAVs can endanger people and property, particularly if they malfunction or become uncontrollable. Therefore, precautions are necessary, such as by avoiding flying over crowded places or near airports. In this case, adopting safety risk assessment methodologies can help identify and assess active and latent safety hazards for drone operation, as well as predict the probability and severity of the consequences or outcomes of each operational risk before starting a mission [17].
3) Regulatory compliance: The deployment of UAVs in civilian airspaces strictly depends on the location. For example, UAVs may be prohibited from flying in certain zones, and some areas may have rules about the maximum altitude or the minimum distance that should be maintained from drones to buildings and people. Evaluating these requirements demands a considerable effort to comply with all the applicable regulations for different use case scenarios and countries [55].
4) Battery lifetime: Battery lifetime is an important aspect of real-time UAV deployment. Before starting a mission, the factors that can drain the UAV's lifetime should be examined via computer simulations because recharging or replacing batteries in remote or hostile areas is difficult [56].
5) Environment type and weather conditions: The type of environment, such as urban, rural and suburban, can affect UAV communications and pose multiple challenges to collision avoidance based on the number of obstacles. Thus, the type of the scenario requires special attention to flying country regulation for visual line of sight (VLOS), beyond visual line of sight (BVLOS), and extended visual line of sight (EVLOS) operations. Finally, weather conditions can affect UAVs, especially when they transport payload onboard, e.g., fog, rain, wind, air pressure/density, and temperature are parameters that require to be considered and predicted before real-time deployment [57].

VII. Conclusion

This article surveyed important privacy issues, threats, and potential solutions to mitigate *Remote ID* enforcement concerns. The contribution introduced a reference scenario, an adversarial model, and the limitations affecting the broadcasting of sensitive data, such as location and long-term identity. We explored, analyzed, and compared across distinctive features the current state-of-the-art on *Remote ID*, and prominent security and privacy schemes available in the literature. Furthermore, this article highlighted current research challenges and identified new limitations that should be addressed from the research and development perspective. Overall, the reported research challenges and the identified future research directions contribute to the remark that the design and testing of *Remote ID* standard-compliant privacy-preserving solutions for UAVs remain an active research domain for academia and industry.

Acknowledgment

The authors would like to thank the anonymous reviewers for their valuable feedback, which has significantly contributed to enhancing the quality of this work.

References

[1] 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.

[2] MarketsandMarkets Research Private Ltd., "UAV Market," Sep. 2022, Accessed: Jan. 21, 2023. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/unmanned-aerial-vehicles-uav-market-662.html?

[3] C. Lin, D. He, N. Kumar, K.-K. R. Choo, A. Vinel, and X. Huang, "Security and privacy for the internet of drones: Challenges and solutions," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 64–69, Jan. 2018.

[4] B. Nassi, R. Bitton, R. Masuoka, A. Shabtai, and Y. Elovici, "SoK: Security and privacy in the age of commercial drones," in *Proc. IEEE Symp. Secur. Privacy*, 2021, pp. 1434–1451.

[5] M. Min, W. Wang, L. Xiao, Y. Xiao, and Z. Han, "Reinforcement learning-based sensitive semantic location privacy protection for VANETs," *China Commun.*, vol. 18, no. 6, pp. 244–260, 2021.

[6] R. Altawy and A. M. Youssef, "Security, privacy, and safety aspects of civilian drones: A survey," *ACM Trans. Cyber- Phys. Syst.*, vol. 1, no. 2, pp. 1–25, Nov. 2016.

[7] FAA, "UAS remote identification overview," 2021, Accessed: Jan. 21, 2023. [Online]. Available: https://www.faa.gov/uas/getting_started/remote_id

[8] FAA, "Remote identification of unmanned aircraft," 2021, Accessed: Jan. 21, 2023. [Online]. Available: https://www.faa.gov/sites/faa.gov/files/2021-08/RemoteID_Final_Rule.pdf

[9] 911Security, "Comparing remote ID standards US, EU, FR," 2021, Accessed: Jan. 21, 2023. [Online]. Available: https://www.911security.com/comparing-remote-id-standards-us-eu-fr

[10] K. Belwafi, R. Alkadi, S. A. Alameri, H. A. Hamadi, and A. Shoufan, "Unmanned aerial vehicles' remote identification: A tutorial and survey," *IEEE Access*, vol. 10, pp. 87577–87601, 2022.

[11] Drone DJ, "Letter to FAA: Please reconsider your remote ID proposal," 2021, Accessed: Jan. 21, 2023. [Online]. Available: https://dronedj.com/2020/09/11/letter-to-faa-please-reconsider-your-remote-id-proposal/

[12] R. Cooley, S. Wolf, and M. Borowczak, "Secure and decentralized swarm behavior with autonomous agents for smart cities," in *Proc. IEEE Int. Smart Cities Conf.*, 2018, pp. 1–8.

[13] N. H. Motlagh, T. Taleb, and O. Arouk, "Low-altitude unmanned aerial vehicles-based Internet of Things services: Comprehensive survey and future perspectives," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 899–922, Dec. 2016.

[14] Y. Mekdad et al., "A survey on security and privacy issues of UAVs," *Comput. Netw.*, vol. 224, 2023, Art. no. 109626.

[15] P. Boccadoro, D. Striccoli, and L. A. Grieco, "An extensive survey on the internet of drones," *Ad Hoc Netw.*, vol. 122, 2021, Art. no. 102600.

[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.*, 2021, pp. 252–258.

[17] D. Lee, D. J. Hess, and M. A. Heldeweg, "Safety and privacy regulations for unmanned aerial vehicles: A multiple comparative analysis," *Technol. Soc.*, vol. 71, 2022, Art. no. 102079.

[18] European Union Aviation Safety Agency, "Easy access rules for unmanned aircraft systems," 2022. [Online]. Available: https://www.easa.europa.eu/en/document-library/easy-access-rules/online-publications/easy-access-rules-unmanned-aircraft-systems

[19] Drone Laws, "Drone laws in France," Jan. 2023. [Online]. Available: https://drone-laws.com/drone-laws-in-france/

[20] "Requirements for remote ID devices and applications," Nov. 2022. [Online]. Available: https://www.mlit.go.jp/koku/content/001582250.pdf

[21] AeroSpace and Defence Industries Association of Europe, "Remote ID rules and standards," 2021, Accessed: Jan. 21, 2023. [Online]. Available: https://asd-stan.org/

[22] D. Migault, M. Boucadair, and E. Vyncke, "Drone remote ID protocol (drip)," *Internet Eng. Task Force (IETF)*, 2022. [Online]. Available: https://datatracker.ietf.org/wg/drip/about/

[23] A. Rugo, C. A. Ardagna, and N. E. Ioini, "A security review in the UAVNet era: Threats, countermeasures, and gap analysis," *ACM Comput. Surv.*, vol. 55, no. 1, pp. 1–35, 2022.

[24] "Wireshark," Accessed: Apr. 8, 2023. [Online]. Available: https://www.wireshark.org/

[25] "TCPDUMP & LIBPCAP," Accessed: Apr. 8, 2023. [Online]. Available: https://www.tcpdump.org

[26] D. He, S. Chan, and M. Guizani, "Security in the Internet of Things supported by mobile edge computing," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 56–61, Aug. 2018.

[27] M. Vanhoef and F. Piessens, "Key reinstallation attacks: Forcing nonce reuse in WPA2," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*,2017, pp. 1313–1328.

[28] K.-Y. Tsao, T. Girdler, and V. G. Vassilakis, "A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks," *Ad Hoc Netw.*, vol. 133, 2022, Art. no. 102894.

[29] P. Gope and B. Sikdar, "An efficient privacy-preserving authenticated key agreement scheme for edge-assisted internet of drones," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 13621–13630, Nov. 2020.

[30] J.-P. Yaacoub, H. Noura, O. Salman, and A. Chehab, "Security analysis of drones systems: Attacks, limitations, and recommendations," *Internet Things*, vol. 11, 2020, Art. no. 100218.

[31] Drone DJ, "Over 80,000 DJI drone IDs exposed in data leak: Report," 2021, Accessed: Jan. 21, 2023. [Online]. Available: https://dronedj.com/2022/10/13/dji-drone-data-leak-us/

[32] H. Kesteloo, "DJI drone operator's location can easily be intercepted," Accessed: Apr. 9, 2023. [Online]. Available: https://dronexl.co/2023/03/02/dji-drone-operators-location-intercepted/

[33] H. Kesteloo, "DJI addresses concerns drone pilots' locations being public," Accessed: Apr. 9, 2023. [Online]. Available: https://dronexl.co/2023/03/09/dji-concerns-drone-pilots-locations-public/

[34] R. Alkadi and A. Shoufan, "Unmanned aerial vehicles traffic management solution using crowd-sensing and blockchain," *IEEE Trans. Netw. Service Manag.*, vol. 20, no. 1, pp. 201–215, Mar. 2023.

[35] A. Alsoliman, A. B. Rabiah, and M. Levorato, "Privacy-preserving authentication framework for UAS traffic management systems," in *Proc. 4th Cyber Secur. Netw. Conf.*, 2020, pp. 1–8.

[36] A. Brighente, M. Conti, and S. Sciancalepore, "Hide and seek: Privacy-preserving and FAA-Compliant drones location tracing," in *Proc. 17th Int. Conf. Availability, Rel. Secur.*,2022, pp. 1–11.

[37] G. Ding, A. Berke, K. Gopalakrishnan, K. H. Degue, H. Balakrishnan, and M. Z. Li, "Routing with privacy for drone package delivery systems," in *Proc. Int. Conf. Res. Air Transp. (ICRAT)*, 2022, pp. 1–8.

[38] S. R. Chinthi-Reddy, S. Lim, G. S. Choi, J. Chae, and C. Pu, "DarkSky: Privacy-preserving target tracking strategies using a flying drone," *Veh. Commun.*, vol. 35, 2022, Art. no. 100459.

[39] S. Sciancalepore and D. George, "Privacy-preserving trajectory matching on autonomous unmanned aerial vehicles," in *Proc. 38th Annu. Comput. Secur. Appl. Conf.*, 2022, pp. 1–12.

[40] A. Shoufan, C. Yeob Yeun, and B. Taha, "eSIM-based authentication protocol for UAV remote identification," *Secur. Privacy Internet Things: Architectures, Techn., Appl.*, pp. 91–122, 2021.

[41] A. R. Svaigen, A. Boukerche, L. B. Ruiz, and A. A. Loureiro, "BioMixD: A bio-inspired and traffic-aware mix zone placement strategy for location privacy on the internet of drones," *Comput. Commun.*, vol. 195, pp. 111–123, 2022.
[42] A. R. Svaigen, A. Boukerche, L. B. Ruiz, and A. A. F. Loureiro, "Mix-Drones: A mix zones-based location privacy protection mechanism for the internet of drones," in *Proc. 24th Int. ACM Conf. Model., Anal. Simul. Wireless Mobile Syst.*, New York, NY, USA, 2021, pp. 181–188.
[43] P. Tedeschi, S. Sciancalepore, and R. Di Pietro, "ARID: Anonymous remote IDentification of unmanned aerial vehicles," in *Proc. Annu. Comput. Secur. Appl. Conf.*, New York, NY, USA, 2021, pp. 207–218.
[44] A. R. Svaigen, A. Boukerche, L. B. Ruiz, and A. A. F. Loureiro, "Is the remote ID a threat to the drone's location privacy on the internet of drones?," in *Proc. 20th ACM Int. Symp. Mobility Manage. Wireless Access*, New York, NY, USA, 2022, pp. 81–88.
[45] A. R. Svaigen, A. Boukerche, L. B. Ruiz, and A. A. Loureiro, "Design guidelines of the internet of drones location privacy protocols," *IEEE Internet Things Mag.*, vol. 5, no. 2, pp. 175–180, Jun. 2022.
[46] P. Tedeschi, S. Sciancalepore, and R. Di Pietro, "PPCA - privacy-preserving collision avoidance for autonomous unmanned aerial vehicles," *IEEE Trans. Dependable Secure Comput.*, vol. 20, no. 2, pp. 1541–1558, Mar./Apr. 2022.
[47] E. Wisse, P. Tedeschi, S. Sciancalepore, and R. Di Pietro, "A^2RID - Anonymous direct authentication and remote identification of commercial drones," *IEEE Internet Things J.*, vol. 20, no. 2, pp. 1541–1558, Mar./Apr. 2023.
[48] Y. Wu, H.-N. Dai, H. Wang, and K.-K. R. Choo, "Blockchain-based privacy preservation for 5G-enabled drone communications," *IEEE Netw.*, vol. 35, no. 1, pp. 50–56, Jan./Feb. 2021.
[49] R. Moskowitz, S. W. Card, and A. Wiethuechter, "UAS operator privacy for RemoteID messages," *Internet Eng. Task Force (IETF)*, 2022. [Online]. Available: https://www.ietf.org/id/draft-moskowitz-drip-operator-privacy-11.html
[50] X. Sun, D. W. K. Ng, Z. Ding, Y. Xu, and Z. Zhong, "Physical layer security in UAV systems: Challenges and opportunities," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 40–47, Oct. 2019.
[51] Y. Zhang, R. H. Deng, S. Xu, J. Sun, Q. Li, and D. Zheng, "Attribute-based encryption for cloud computing access control: A survey," *ACM Comput. Surv.*, vol. 53, no. 4, pp. 1–41, Aug. 2020.
[52] G. Geltink, "Concealing KETJE: A lightweight PUF-based privacy preserving authentication protocol," in *Proc. Lightweight Cryptogr. Secur. Privacy: 5th Int. Workshop*, Aksaray, Turkey, 2017, pp. 128–148.
[53] Z. Wei, C. Masouros, H. V. Poor, A. P. Petropulu, and L. Hanzo, "Physical layer anonymous precoding: The path to privacy-preserving communications," *IEEE Wireless Commun.*, vol. 29, no. 2, pp. 154–160, Apr. 2022.
[54] P. Chen et al., "Secure task offloading for MEC-aided-UAV system," *IEEE Trans. Intell. Veh.*, vol. 8, no. 5, pp. 3444–3457, May 2023.
[55] C. Stöcker, R. Bennett, F. Nex, M. Gerke, and J. Zevenbergen, "Review of the current state of UAV regulations," *Remote sens.*, vol. 9, no. 5, 2017, Art. no. 459.
[56] H. Guo and J. Liu, "UAV-Enhanced intelligent offloading for Internet of Things at the edge," *IEEE Trans. Ind. Inform.*, vol. 16, no. 4, pp. 2737–2746, Apr. 2020.
[57] Y. B. Sebbane, *Intelligent Autonomy of UAVs: Advanced Missions and Future Use*. Boca Raton, FL, USA: CRC Press, 2018.

Pietro Tedeschi (Member, IEEE) received the master's degree with honors in computer engineering from Politecnico di Bari, Bari, Italy, in 2017, and the Ph.D. degree in computer science and engineering from the College of Science and Engineering (CSE), Hamad Bin Khalifa University (HBKU), Doha, Qatar, in December 2021.

He is currently a Senior Security Researcher with Technology Innovation Institute, Autonomous Robotics Research Center, Abu Dhabi, United Arab Emirates, from January 2022. From 2017 to 2018, he was a Security Researcher with Consorzio Nazionale Interuniversitario per le Telecomunicazioni (CNIT), Trento, Italy, for the EU H2020 SymbIoTe project. His major research interests include security and privacy in unmanned aerial vehicles, wireless, Internet of things, cyber-physical systems, and applied cryptography.

Dr. Tedeschi is serving in the TPC of several conferences.

Fatima Ali Al Nuaimi received the bachelor's degree in January 2020 from the College of Information Technology (CIT), United Arab Emirates University (UAEU), Al Ain, United Arab Emirates, where she is currently working toward the master's degree, both in science of information security.

She has been a Senior Associate Researcher with Technology Innovation Institute, Autonomous Robotics Research Center, Abu Dhabi, United Arab Emirates (UAE), since June 2020. Her research interests include network security, neuroscience (BCI), and the Internet of Things (IoT).

Ali Ismail Awad (Senior Member, IEEE) received the Ph.D. degree in computer science from Kyushu University, Fukuoka, Japan, in 2012.

He is currently an Associate Professor with the College of Information Technology, United Arab Emirates University, Al Ain, UAE, where he is coordinating the master's program in information security from 2022. He is also a Visiting Researcher with the University of Plymouth, Plymouth, U.K. He has edited or coedited several books and authored or coauthored several journal articles and conference papers in the areas of his research interests. His research interests include cybersecurity, network security, Internet of Things security, and image analysis with biometrics and medical imaging applications.

Dr. Awad is an Editorial Board Member of the *Future Generation Computer Systems Journal*, *Computers & Security Journal*, *Internet of Things*, *Engineering Cyber-Physical Human Systems Journal*, *Health Information Science and Systems Journal*, and *Security, Privacy and Authentication Section by Frontiers*.

Enrico Natalizio (Senior Member, IEEE) received the master's (*cum laude*) and Ph.D. degrees in computer engineering from the University of Calabria, Arcavacata, Italy, in 2000 and 2005, respectively.

He is currently a Vice President of the Autonomous Robotics Research Center with the Technology Innovation Institute, Abu Dhabi, UAE, and a Full Professor with the LORIA Laboratory, Université de Lorraine, Nancy, France. From 2006 to 2010, he was a Researcher with the Titan Lab of the Universitè della Calabria, Italy. In October 2010, he joined POPS team with Inria Lille, France, as a Postdoc Researcher and from 2012 to 2018 he was an Associate Professor with the Université de technologie de Compiègne, France, and a Full Professor with the Université de Lorraine from September 2018. His research interests include UAV communications and networking, and IoT security and privacy.

Dr. Natalizio has been ranked in the top-2% world-wide scientists of the Stanford-University's bibliometric study for the year 2021.