Privacy and Confidentiality Issues in Drone Operations: Challenges and Road Ahead

Savio Sciancalepore
Eindhoven University of Technology, Eindhoven, Netherlands
s.sciancalepore@tue.nl

***Abstract*—[1]While drone-based civilian services and applications are appearing on the market at a high pace, recent efforts in the security and privacy community mainly focused on drone detection and neutralization when unauthorized invasions occur. Conversely, more attention must be paid to unveiling potential privacy and confidentiality threats to drone users and operators arising from using such a technology. Such threats, emerging from drones' adoption for entertainment and business operations, are increasingly concerning due to the recently-introduced regulation on the Remote Identification of Unmanned Aircraft (Remote ID (RID)), mandating persistent disclosure of identity and location of the drone at run-time. This paper sheds some light on the aforementioned context, identifying several privacy and confidentiality threats connected to regular drone operations. Such threats originate from the nature of the drones' ecosystem and actors and are magnified by the adoption of the RID regulation. For all the identified threats, we pinpoint similarities with issues faced in other research domains, potential solutions, and constraints owing to the drone technology, making the solutions conceived therein hardly applicable for drone-based services. The final result is a set of appealing research challenges, calling for joint efforts from Academia and industry.**

***Index Terms*—Unmanned Aircraft; IoT; Privacy Enhancing Technologies; Security.**

I. Introduction

Unmanned Aircraft (UA), a.k.a. *drones*, are gaining increasing momentum in Academia and industry due to their flexibility and suitability for many automated challenging tasks. To cite a few, delivery companies are using both autonomous and remotely-piloted drones for goods delivery, critical infrastructures are deploying them for assisting equipment maintenance, and emergency operators are relying on them for search-and-rescue in challenging and hazardous environments [1]. The explosion of such technology is also supported by numbers, with leading companies reporting approx. 9.64 millions drones active at the end of 2022 and the related market valued at minimum USD 47.38 billion by 2029 [2].

Despite the enormous application spectrum, drones represent the classical dual-use technology usable for malicious purposes. At the time of this writing, a large part of the research on drones in the security and privacy domain focused on the detection of their presence in unauthorized areas, the design of various methods to take over their control or force them to move away, as well as the identification of spying activities [3]. Regional aviation regulatory authorities also worked to regulate drone flights, laying the basis for timely misbehavior detection, smooth operator identification, and sanctions application. In this context, the US-based Federal Aviation Administration (FAA) emitted the first regulation on the Remote Identification of Unmanned Aircraft, namely, RID, forcing all commercial drones to regularly broadcast plaint-text information on their identity, current location and details of the related ground control station. Such regulation applies for almost any commercial drone and in any condition, excluding a few FAA-recognized areas, and other regional authorities are following the same example [4].

In this context, researchers paid little attention to security and privacy issues potentially affecting drone users and operators, arising from the usage of such technology. Such issues first originate from the nature of the drone ecosystem, and they further magnify due to the introduction of RID regulations. Indeed, as per its nature, the drone technology is possibly subject to capture, especially when the moving entity is far from the physical control of the operators. This technological feature, independent from enforcing RID regulations, enables attackers to access information stored onboard, generating possible privacy and confidentiality issues. Additional privacy concerns can emerge from the large variety and geographical distribution of the actors involved in commercial drone production and deployment. Indeed, drone manufacturers (possibly different from service providers) often keep remote access and super-user privileges in the system for diagnostics, maintenance, and firmware updates. In this context, compliance with RID regulations generates additional concerns, allowing for remote passive tracking of real-time location and linking drone paths to the identification information.

Although some previous contributions such as [5] partially outlined some of the issues, they only consider a subset of the possible privacy and confidentiality threats, and they do not consider their magnification when coupled with the RID regulation, soon applicable worldwide. Moreover, such contributions did not demonstrate the potential unsuitability of currently available solutions for drone-based applications.

Contribution. In this paper, we provide several contributions. First, we identify and describe several novel confidentiality and privacy issues affecting users, industrial and government operators using commercial drones for entertainment and business-related activities. We characterize and classify a range of threats emerging from the unintentional and

[1]This is a personal copy of the authors. Not for redistribution. The final version of the paper will be available soon through the digital library IEEExplore.

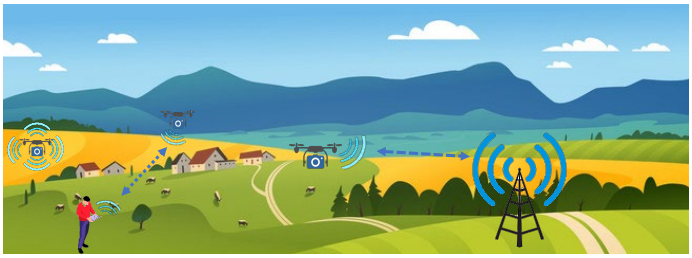

Figure 1. Reference System Model. Commercial drones frequently operate in scenarios with a non-persistent Internet connection, being connected and accessible by users and manufacturers only intermittently and forced to execute real-time tasks onboard.

intentional disclosure of sensitive information, emerging either from the composition of drone-based networks or from the compliance to RID regulations. Moreover, for all the identified threats, we highlight similarities with security and privacy issues faced in other research domains. Finally, we discuss how the constraints of drone-based networks complicate a straightforward application of solutions conceived in different domains to our scenario of interest, making them only sometimes fully applicable. Such findings call for further research and innovative solutions from both Academia and industry.

Overall, this contribution sheds light on the privacy and confidentiality issues arising when adopting drones, especially when handling sensitive data onboard. As a distinctive novel contribution, rather than proposing new solutions, we argue that currently available ones from other domains often do not apply to drone operations in the wild, fostering additional research.

Roadmap. The rest of the manuscript is organized as follows. Section II introduces the reference system and adversary model, Section III derives privacy and confidentiality threats arising when operating drones, Section IV puts forward possible solutions to such threats based on similarities with other research areas, while also identifying research challenges complicating their straightforward application in the drone ecosystem. Finally, Section V concludes the paper.

II. Reference System and Adversary Model

Here, we introduce the reference system and adversary model. Such models are essential to identify the information drones need for their correct operations and the tools that the adversary can use to threaten them.

Fig. 1 depicts the reference system model considered in this paper, while Tab. I summarizes the specifications and capabilities offered by some drones used as a reference for the following discussion. We consider generic Unmanned Aircrafts, a.k.a. drones, which can be autonomous, semi-autonomous, or remotely piloted, possibly via a remote controller. Being battery-powered, drones feature energy constraints, i.e., they have limited energy available for their operations. For example, the DJI Mini 2 has a battery capacity of 2,250 mAh, providing a flying time of approx. 30 mins. At the same time, more constrained drones such as the Crazyflie 2.1 feature a flying time of only 7 minutes by default. Although some drones have processing constraints (e.g., the Crazyflie 2.1 has a Cortex M-4 processor), drones usually have regular computational capabilities, e.g., ARM Cortex A15 or octa-core CPUs. However, energy constraints also cause processing limitations. Indeed, executing computationally intensive tasks at full processing power drains more energy from the battery per unit of time, reducing, in turn, the drone's lifetime. Thus, drones should limit computationally intensive tasks to avoid affecting planned operations significantly. In line with modern capabilities and features, drones feature various sensors and peripherals, including GNSS receivers (allowing precise position estimates), accelerometers, magnetometers, gyroscopes, various types of inertial measurement units, barometers, cameras for video acquisition, and possibly microphones.

We consider drones compliant with the RID specification. As per the regulation in [6], independently of their take-off weight, drones should broadcast wirelessly messages containing their unique identifier, location, speed, pilot location, timestamp and emergency status. Such regulation applies everywhere, excluding a few FAA-recognized areas. Drones should emit such messages at least once per second using WiFi or Bluetooth, with no mandatory encryption nor authentication [7]. Thus, we consider drones equipped with wireless communication capabilities. They include at least a WiFi module operating in the 2.4 GHz band (and possibly in the 5 GHz band), either integrated onboard or connected as an external peripheral. Such a module allows both to broadcast RID-compliant messages and connect to the drones remotely, e.g., for issuing navigation commands and retrieving sensors and video feeds, typically in a given range from the drone's location (from 1 to 30 km). Some drones also feature a connection to the cellular network, used to provide data, receive commands, and also for remote access to the drone. Remote access might be required for installing software and firmware updates, as well as for remote maintenance and diagnostics by the manufacturer. Depending on the deployment location, drones might not feature a persistent Internet connection, especially in remote and hard-to-reach areas. Before the deployment, drones typically are in controlled locations, where they recharge and feature an Internet connection. Thus, if they need a specific setup or pre-configuration before their mission, they can download updated information from the Internet at this time. However, persistent Internet connection might only be available sometimes later, during operation. Such a constraint implies that real-time critical operations should occur offline, relying mostly on the computational, energy, bandwidth, and storage capabilities available in the field.

Adversary Model. The adversary envisioned in this paper features both passive and active capabilities. First, we assume the adversary can access the drone and its local storage and content, e.g., by capturing it. Such access can be performed either remotely, e.g., via the WiFi link of the

Table I
SPECIFICATIONS AND CAPABILITIES OF SOME EXEMPLARY DRONES AVAILABLE IN THE MARKET. NOTE THAT EACH MODEL IS CHARACTERIZED BY ONE OR MORE CONSTRAINTS ON THE CPU, BATTERY CAPACITY, STORAGE AND COMMUNICATION FEATURES.

Model	**CPU**	**Battery Capacity [mAh]**	**Storage**	**Communication [GHz]**	Range [m]	**Flying Time [mins]**
DJI Mini 2	32-bit Quad-core ARM Cortex A15, up to 2.3 GHz	2,2250	SD-Card	[2.400-2.4835], [5.725-5.850]	4,000	30
DJI Mavic 3	32-bit Quad-core ARM Cortex A15, up to 2.3 GHz	5,000	up to 1 TB	[2.400-2.4835], [5.725-5.850]	30,000	46
Skydio 2	64-bit octa-core Kryo™ 300, up to 2.2 GHz	5,410	SD-card	[5.18-5.24], [5.725-5.85]	6,000	27
Crazyflie 2.1	Cortex M4 at 168 MHz	240	1 MB	[2.400-2.4835]	1,000	7

drone, or physically, independently from the deployment of RID. In the case of physical drone access, the adversary can use active capabilities to capture the drone, e.g., jamming the drone-controller communication link or spoofing (if possible) the messages coming from the ground control station. Moreover, the adversary features a receiving Radio Frequency (RF) antenna, that they can tune to the channel the drones use for communication. Thus, the adversary can access all the information broadcasted by drones, including, e.g., the plain-text ones in RID messages, such as the drone's location, identifier, and operators' data. Here, we highlight that the WiFi range typically installed on commercial drones easily reaches $1,000$ m, making the broadcasts not limited to a *local* domain. However, decreasing such range to reduce information exposure only provides *security-by-obscurity*, reducing, in practice, the effectiveness of technologies such as RID without any noticeable security benefits.
Overall, the final objective of the adversary is to obtain private or confidential information about the drone.

III. PRIVACY AND CONFIDENTIALITY THREATS

In this section, we point out several issues targeting drone users and operators in terms of privacy (i.e., connected to the personal sphere of the user) and confidentiality (i.e., connected to non-personal information known by the user). We distinguish between *Ecosystem-related Threats*, i.e., drone capture and unauthorized access by curious manufacturers, and *RID-related Threats*, namely, plain-text drones' location disclosure, plain-text drones' unique identity disclosure, and plain-text drones' operator location disclosure. We highlight that the forced compliance to RID only makes it easier for the adversary to extract (some type of) information from the drone, worsening existing *Ecosystem-related* privacy and confidentiality issues.

Drone Capture. Due to their mobile nature, drones often operate far from the user/owner, being at risk of de-touring and capture by malicious parties. For instance, an adversary can capture the drone by jamming the Global Positioning System (GPS) or the controller WiFi signal, which causes most commercial drones to land immediately. They can also combine jamming with GPS spoofing, easily achievable through low-cost Software-Defined Radios (SDRs). When the drone is captured, they can extract all the information stored onboard, e.g., the identity of the drone, its location, its path, and other data stored internally. As an example, consider a drone which uses onboard face recognition (e.g., products developed by companies such as Aerialtronics or software like Face-6). If the drone is captured, the details about the identity and the face of the user might be exposed, leading to privacy issues which might even be legally accountable in some countries.

Unauthorized Access by Curious Manufacturers. Designing and assembling commercial drones requires diverse and expensive expertise. Thus, most commercial companies buy drones from external manufacturers specializing in designing and assembling such technology. However, such manufacturers often keep remote access to the drone after delivery, e.g., for diagnostics, remote maintenance, and application of software/firmware updates. Recall that remote access typically involves super-user rights on the system. Thus, such manufacturers might access the system when connected to the Internet and exfiltrate any information stored onboard [8]. Based on the company's business type, such information might include potentially confidential and IP-protected algorithms and source code, as well as private user information (e.g., face details, as in the example mentioned above). Not only information that is sensitive by definition might be stolen (e.g., sensitive user data), but other information, such as the list of trusted intermediaries and companies of a service provider, defined, e.g., within an access control policy, might generate unexpected business concerns.

Plain-text Drones' Location Disclosure. The RID rule requires almost all commercial drones to broadcast the current location in clear text over the 2.4 GHz wireless channel, from take-off to landing [6]. However, the indiscriminate disclosure of such a location generates confidentiality and privacy threats. Indeed, although enabling easier accountability [9], RID enables malicious parties to precisely track the drone through simple passive wireless receivers, e.g., to capture it when the surrounding environment is specifically suitable for this scope. In turn, especially in the case of semi-autonomous operations, the disclosed locations might reveal side information, leading to the disclosure of autonomous navigation algorithms, which are typically

Table II
SUMMARY OF THE MOST REPRESENTATIVE IDENTIFIED CONFIDENTIALITY AND PRIVACY THREATS, ENABLING INFORMATION, AND POTENTIAL IMPACT.

Threat Origin	Threat Type	Enabling Information	Impact
Ecosystem	Confidentiality	Algorithm Source Code Disclosure	IP-protected information leakage
Ecosystem	Privacy	Personally-identifiable Information Disclosure	Leakage of Private Data (e.g., faces, access control policies)
Remote ID	Confidentiality	Drone Location Disclosure	Drone Capture
Remote ID	Privacy	Drone Path Disclosure	User Home/Work address, Preferences, Places
Remote ID	Confidentiality	Drone Identity Disclosure	Company Storage Site, Companies Relationships
Remote ID	Privacy	Operator's Location Disclosure	Relationship Drone-Operator unveiled, drone capture

confidential and IP-protected. At the same time, the location occupied by the drone and the travelled trajectory might also reveal personal information about the operator, such as his home/work address and personal preferences (e.g., if the drone consistently starts/stops at specific places). Without RID, to know the drone's location, attackers had to either connect to the drone and be authorized to access location information or see it. With RID, they can access location information cheaply through wireless channel eavesdropping, easing the attack.

Plain-text Drones' Unique Identity Disclosure. Besides location, the RID rule also forces the disclosure of the unique identifier of the drone. When coupling such a unique identifier with location information, confidentiality and privacy issues arise. For instance, in the case of drone-based goods deliveries, leaked identity and location might reveal the location of the storage site of a company, as well as the existence and extent of relationships among companies or users. In this context, not only might malicious entities acquire data on their own, but they can also exploit bad practices by third parties in storing and manipulating such information. The latter is the case of the recent data leak discussed in [10], where a user logging data through the DJI Aeroscope app left such data freely available on the public Internet. Independently from the intention of the user of the DJI app to make such data publicly available, the simple availability of such apps on the market enables anyone to retrieve and disclose the identity of RID-enabled drones in the area of interest with no consent, highlighting and worsening privacy issues. The unauthorized access to the identity of the drone previously required the attacker to capture the drone. With RID in place, attackers can access such information more easily, eavesdropping on the wireless channel.

Plain-text Drones' Operator Location Disclosure. The RID regulation also mandates the broadcasting of the drones' operator data, i.e., the latitude, longitude, and altitude coordinates of the ground control station(s) piloting the drone. As for the two items discussed above, drone operators' data are also broadcasted in plain text, enabling any receiver to discover the pilot's location. For almost all drone applications, such location data might be sensitive, as they could further ease attacks on the drone communication link, such as location-based jamming of the control station. Moreover, such data might allow inferring the relationship between an operator and a group of drones, potentially revealing additional private information. The existence of such a problem has also been acknowledged by working groups specifically dedicated to integrating the RID regulation into local airspaces, such as the IETF Working Group *drip*. Similarly to the previous case, access to the pilot's location previously required the attacker to see the pilot or capture the drone. With RID in place, the attacker only needs to listen RID messages.

We summarize the above-discussed threats in Tab. II, highlighting the most representative threats, the information enabling such threats, and the potential impact of the information leakage.

IV. POTENTIAL SOLUTIONS AND RESEARCH CHALLENGES

In this section, we identify similarities between the described threats and issues faced in other research areas, as well as available technologies used to solve such threats in those domains. For each potential solution, we extract challenges specific to the drone ecosystem, making the integration of such technologies complex and possibly paving the way for future research. Fig. 2 provides an explicit connection between the threats identified in Sec. III and the viable solutions described below.

Tamper-proof Drone Hardware. To protect the drone against tampering and exfiltration of private information once captured, tamper-proof hardware can be used, such as Secure Elements (SEs) and Trusted Computing Bases (TCBs). However, integrating such hardware technologies onboard a commercial drone might face several challenges. First, such solutions require dedicated hardware, which is often difficult to integrate onboard and connect with peripherals and flight controllers. Also, such hardware might increase the drone's weight, reducing its lifetime and forcing sub-optimal design choices. Finally, integrating one or more SEs on board might raise the cost of the drone significantly, decreasing the appeal of the users towards using drones. Note that, in this context, *zero-trust network security* approaches do not represent a viable solution. Indeed, there are no verifiable operations involved, and as the drone itself can be compromised, the security perimeter for online drone-based services is basically non-existent. Therefore, dedicated low-cost, lightweight, and efficient solutions, possibly including hardware-software co-design, are needed to keep tamper-proof trusted drones appealing to customers.

Private Processing Onboard. The likely snooping of the manufacturer on information stored onboard the drone

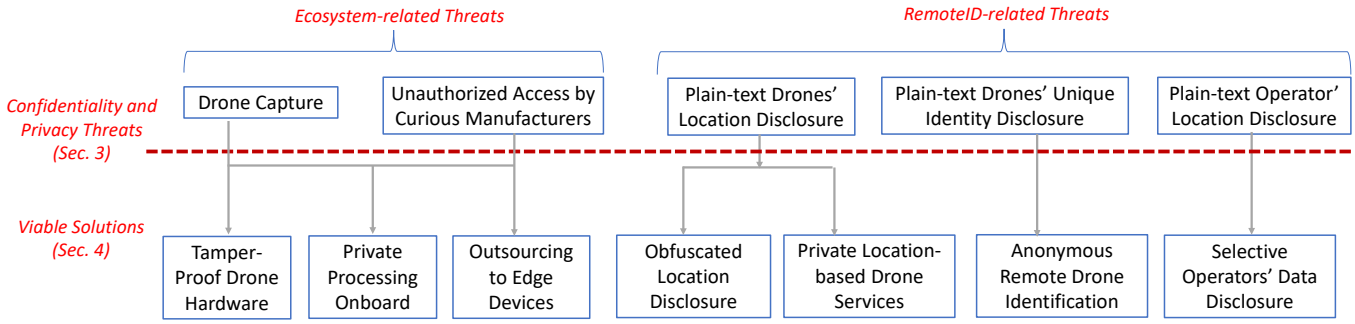

Figure 2. Mapping between the confidentiality and privacy threats identified in Sec. III and the viable solutions discussed in Sec. IV.

requires such information not to be stored as plain text on the drone. An option might be to rely on information stored on servers available on the public Internet and to interact with such servers whenever operations on sensitive data are required. However, drones likely operate in scenarios with intermittent Internet connectivity (see Sec. II), limiting the effectiveness and applicability of such a strategy. Thus, in many applications, drones must store sensitive information onboard securely, e.g., obfuscated or encrypted, to still allow for the execution of the required operations, such as search and comparison.

In this context, many Privacy-Enhancing Technologies (PETs) can theoretically address the identified issues by letting operations occur reliably in the encrypted domain. For instance, Secure Searchable Encryption (SSE) schemes allow searching for values or keywords in an encrypted database, and Homomorphic Encryption (HE) techniques allow either addition or multiplication among private values to occur in the encrypted domain. Recently, Fully Homomorphic Encryption (FHE) schemes allowing addition and multiplication in the encrypted domain were also released.

Unfortunately, many PETs are well-known processing-intensive and memory-hungry operations, such as in the case of HE, Secure Function Evaluation (SFE), and SSE. Also, many of them require a semi-trusted third party online while executing the operations in the encrypted domain. Still, they might be hard to deploy and reach when drones operate in remote locations. Thus, the straightforward integration of such schemes on drones would be challenging and cause too much overhead, leading to excessive computation times, congestion, and ultimately, a significant reduction of the drone's lifetime — all negatively impacting the quality of the offered service. Therefore, new tailored PETs are required to guarantee timely and reliable service while preventing data leakage to curious manufacturers.

Outsourcing to Edge Devices. Considering the likely snooping on onboard data by untrusted manufacturers and the lack of a persistent Internet connection, another option might be outsourcing sensitive computations to Edge devices possibly deployed on-site, close to where the drone is operating.

In this context, secure and trusted outsourcing strategies such as Secret Sharing (SS) techniques and Federated Learning (FL) strategies already offer the required theoretical and practical support [11]. However, additional threats and constraints apply here. Indeed, edge devices are usually provided by untrusted users, which might actively work to trace back sensitive and private information, possibly colluding with other users/devices connected to the network. Moreover, edge devices are often as constrained as drones in processing, storage, and bandwidth, limiting the application of existing traditional outsourcing techniques. Therefore, new tailored research is required to address private outsourcing from drones to constrained edge devices.

Anonymous Remote Drone Identification. When protecting information in RID messages, message encryption is not an option as it would break compliance with the specification. Instead of disclosing static unique identifiers in each RID message, drones might keep compliance with the RID rule by broadcasting messages using rolling ephemeral identities. Assuming a passive eavesdropper does not know how many drones are flying in its reception radius, such rolling identifiers would make it more difficult to associate a message to a specific flying drone, anonymizing the broadcasted message.

Here, two significant research challenges arise. First, standalone receivers listening to incoming drone messages should be able to authenticate the message, either directly or by relying on third parties. Moreover, when misbehavior occurs, dedicated third-party authorities should be able to verify the infringement of any rules and disclose the actual identity of the drone. The enforcement of such requirements implies the application of specific algorithms for the generation of the ephemeral identity and the authentication materials, recalling the large body of work done in the context of (anonymous) online e-voting [12]. However, the application of such techniques for anonymous remote drone identification faces additional challenges specific to the drone domain, such as the limited processing power of the signer, the limited access to the Internet on both the signer and the verifier, the little energy available on the signer, the mobile nature of the drone, and the limited available bandwidth. The problem faced here differs from anonymous authentication in the domain of Vehicular Ad-Hoc NETwork (VANET), as RID messages are broadcast, while VANET message exchanges

Table III
SUMMARY OF IDENTIFIED VIABLE SOLUTIONS, AVAILABLE TOOLS AND TECHNOLOGIES POTENTIALLY ABLE TO IMPLEMENT THEM, AND CONSTRAINTS SPECIFIC TO THE DRONE DOMAIN, MAKING THEIR INTEGRATION FURTHER CHALLENGING.

Viable Solutions	Available Tools and Technologies	Domain-Specific Constraints
Tamper-Proof Drone Hardware	TCBs, SEs	Integration into existing hardware; Weight increase; Cost increase.
Private Processing Onboard	SFE, HE, FHE	Deployment of (Semi-) Trusted Third Party; Limited processing, bandwidth, storage, and energy on the drone; Lack of persistent Internet connection.
Outsourcing to Edge Devices	FL, SS	Limited processing, bandwidth, storage, and energy on the drone; Lack of persistent Internet connection.
Anonymous Remote Drone Identification	Anonymous e-voting schemes	Limited processing, bandwidth, storage, and energy on the signer; Lack of persistent Internet connection; Requirements of RID rule.
Obfuscated Location Disclosure	Differential Privacy	Requirements of RID rule; Highly-correlated location disclosures; Limited processing and energy on the drone.
Private Location-Based Drone Services	Private Location-Based Services (LBSs)	Limited processing, bandwidth, storage, and energy on the drone; Lack of persistent Internet connection.
Selective Operators' Data Disclosure	Encryption	Requirements of RID rule; Limited processing and energy on the drone; Limited space available into single WiFi frame; Key storage into exposed device;

are typically unicast. To complicate the integration further, consider that RID also imposes identity disclosure at least once every second. Also, it would be desirable not to use more than a single broadcast wireless message to provide remote identification to minimize the impact of potential packet losses. Therefore, we need new research and solutions in this domain, tailored to the unique system requirements and constraints of heterogeneous commercial drones. A preliminary solution in this direction is [13], but work is still needed to reduce overhead and adapt to more constrained drones.

Obfuscated Location Disclosure. Several technical solutions are available to protect the indiscriminate disclosure of location data, mainly conceived for providing privacy-preserving LBSs, such as location obfuscation based on Differential Privacy [14].

However, several major challenges arise in the drone domain. Indeed, most drones have limited processing, energy, and bandwidth, possibly requiring optimizing current strategies and developing dedicated solutions. Moreover, when compliance with RID is required, the disclosure of location information (at least) once every second makes multiple location disclosures highly correlated, reducing the effectiveness of solutions in the privacy-preserving LBS domain significantly.

Another research problem is the disclosure of the location of misbehaving drones. Indeed, in line with the previous discussion about anonymity, misbehaving drones should be identified, and their actual location should be disclosed to the parties on the field when needed to allow for timely threat neutralization. Such a requirement implies the design and deployment of dedicated solutions that, to the best of the authors' knowledge, are both unique and challenging based on the tight constraints of the drone ecosystem. We remark that, although the FAA does not exclude the implementation of encryption techniques for RID, no solutions providing encryption for RID messages are available and neither planned, so far.

Private Location-Based Drone Services. Besides location sharing occurring for complying with RID regulations, drones might also require location sharing when using location-based services, e.g., search-and-rescue operations, telecommunication services, and collision avoidance. In this context, solutions protecting drones' location should also ensure the provisioning of location-based services to the drones, which is crucial for their correct and smooth operations. This problem shares similarities with privacy-preserving LBS for Cloud and social networks, where users would like to enjoy location-based services while not revealing their location [15]. Similarly, privacy-preserving collision avoidance techniques share similarities with private proximity testing solutions previously applied in the LBS context. However, additional constraints apply to the drone scenario. Indeed, most drones are even more constrained than mobile phones in processing, energy, and bandwidth availability, possibly requiring the development of dedicated solutions.

Selective Operators' Data Disclosure. Although the RID regulation requires broadcasting of operators' data, such data might be *protected* so that only authorized parties can access them, limiting uncontrolled information disclosure. Different encryption algorithms can be considered here, including symmetric and asymmetric techniques. On the one hand, the traditional pros and cons of symmetric and asymmetric encryption schemes should be considered. For example, symmetric schemes are computationally lighter than asymmetric ones but also more vulnerable to key leakage, which is particularly relevant for the drone domain (see the

following discussion on tamper-proof drone hardware). On the other hand, we should consider the requirements imposed by the RID rule. Indeed, drones should deliver RID messages at least once per second, and their data should occupy no more than a single WiFi frame. Also, other requirements might apply based on the constraints of the specific application. For instance, some applications might require the messages to be retrievable by authorized parties not equipped with a persistent Internet connection. In contrast, other applications may require the ciphertext to have the same size as plain text bytes for backward compatibility purposes. Combining all the mentioned constraints and requirements makes this problem challenging and worthy of dedicated research.

Tab. III summarizes our discussion by linking the described solutions to tools and technologies available in closely related research areas and to domain-specific constraints. Most of the identified constraints refer to the limited processing, bandwidth, storage, and energy available on the drone and the lack of a persistent Internet connection. Also, consider that drones often leverage proprietary Operating Systems (OSs) and kernels, making it hard to compile source code running on traditional IT systems. Finally, the enforcement of RID imposes additional requirements on the performance of such schemes, magnifying the problems further.

V. Conclusion

In this paper, we described and motivated several confidentiality and privacy issues arising from the regular deployment and operation of commercial drones. We identified several pieces of sensitive information likely to be stored onboard a drone when used for commercial operations, possibly leading to privacy leakages. Such privacy issues are firstly related to the features of the drone ecosystem, and they are further magnified by the enforcement of the recent RID regulation, reducing the effort of the attackers to acquire such information. We discussed the practical threats and impact of data leakages, and we also put forward possible solutions anchored in scientific literature conceived in other research areas, e.g., privacy-preserving location-based services and anonymous e-voting. Considering the device, system, and networking constraints characterizing drone operations, we also identified conflicting research challenges to address to finally protect against such threats. Through our paper, we would like to raise the attention of Academia and Industry on the urgency of the described threats and the likely unsuitability of solutions currently available for solving the problem to finally unleash the full potential behind the drone technology in existing application domains.

Acknowledgements

This work has been supported by the INTERSCT project, Grant No. NWA.1162.18.301, funded by the Netherlands Organisation for Scientific Research (NWO). The findings reported herein are solely responsibility of the authors.

References

[1] P. Boccadoro, et al., "An Extensive Survey on the Internet of Drones," *Ad Hoc Networks*, vol. 122, p. 102600, 2021.

[2] Fortune Business Insights, "Commercial Drones Market Size," https://www.fortunebusinessinsights.com/commercial-drone-market-102171, 2022, (Accessed: 2024-Jul-21).

[3] S. Park, et al., "Survey on Anti-Drone Systems: Components, Designs, and Challenges," *IEEE Access*, vol. 9, pp. 42 635–42 659, 2021.

[4] K. Belwafi, et al., "Unmanned Aerial Vehicles' Remote Identification: A Tutorial and Survey," *IEEE Access*, vol. 10, pp. 87 577–87 601, 2022.

[5] A. Svaigen, et al., "Design Guidelines of the Internet of Drones Location Privacy Protocols," *IEEE IoT Magaz.*, vol. 5, no. 2, pp. 175–180, 2022.

[6] FAA, "UAS Remote Identification Overview," 2021, Available Online: https://www.faa.gov/uas/getting_started/remote_id/.

[7] Tedeschi, P. et al., "Privacy-Aware Remote Identification for Unmanned Aerial Vehicles: Current Solutions, Potential Threats, and Future Directions," *IEEE Transactions on Industrial Informatics*, 2023.

[8] N. Schiller, et al., "Drone Security and the Mysterious Case of DJI's DroneID," in *NDSS*, 2023.

[9] Drone DJI, "This free app tracks nearby drone flights using Remote ID data," https://dronedj.com/2022/10/04/remote-id-drone-tracking-app/?utm_source=dlvr.it&utm_medium=twitter&s=08, 2022, (Accessed: 2024-Jul-21).

[10] DroneXL, "80,000 Drone IDs Exposed in DJI Aeroscope Data Leak," https://dronexl.co/2022/10/17/80000-drone-ids-dji-aeroscope-data-leak/?utm_source=rss&utm_medium=rss&utm_campaign=80000-drone-ids-dji-aeroscope-data-leak, 2022, (Accessed: 2024-Jul-21).

[11] Z. Shan, et al., "Practical Secure Computation Outsourcing: A Survey," *ACM Computing Surveys*, vol. 51, no. 2, Feb. 2018.

[12] M. Alsadi and S. Schneider, "Verify My Vote: Voter Experience," *E-Vote-ID 2020*, p. 280, 2020.

[13] E. Wisse, et al., "A^{2}RID–Anonymous Direct Authentication and Remote Identification of Commercial Drones," *IEEE Internet of Things J.*, 2022.

[14] C. Bettini, "Privacy Protection in Location-Based Services: A Survey," in *Handbook of Mobile Data Privacy*. Springer, 2018, pp. 73–96.

[15] H. Jiang, et al., "Location Privacy-preserving Mechanisms in Location-based Services: A Comprehensive Survey," *ACM Computing Surveys*, vol. 54, no. 1, pp. 1–36, 2021.

Biographies

Dr. Savio Sciancalepore is an Assistant Professor at TU/e, Eindhoven, Netherlands. He received his Master's and PhD degrees in 2014 and 2017 from the Politecnico di Bari, Italy. From 2017 to 2020, he was Post Doctoral researcher at HBKU, Doha, Qatar, and he joined TU/e in 2021. In 2018, he received the award for the best PhD Thesis in Information and Network Security in EU from the ERCIM Security, Trust, and Management Working Group of the Internet Engineering Task Force. His research interests cover network security and privacy issues in Wireless, Mobile and Internet of Things systems.