IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 4 September 2024, accepted 5 November 2024, date of publication 11 November 2024,
date of current version 26 November 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3495994

SURVEY

Cybersecurity Testing in Drones Domain: A Systematic Literature Review

EDA MARCHETTI, TAUHEED WAHEED, AND ANTONELLO CALABRÒ
ISTI-CNR, 56124 Pisa, Italy

Corresponding authors: Antonello Calabrò (antonello.calabro@isti.cnr.it) and Eda Marchetti (eda.marchetti@isti.cnr.it)

This work was supported in part by the Project RESTART under Grant PE00000001, and in part by the Project SEcurity and RIghts in the CyberSpace (SERICS) under National Recovery and Resilience Plan (NRRP) Ministero dell'Università e della Ricerca (MUR) Program funded by EU-NextGenerationEU under Grant PE00000014.

ABSTRACT The widespread use of unmanned aerial vehicles (UAVs) drone cybersecurity testing is becoming an emerging and evolving research area for cybersecurity and privacy issues avoidance and prevention. This paper contributes to guiding the research activity by systematically surveying the commonly adopted solutions and proposals for cybersecurity testing in the drone research domain. It highlights the research challenges and issues, classifies the current proposal, methodologies, and techniques, and suggests future directions. After gathering a collection of papers using automated inquiry of well-known digital libraries and snowballing techniques, a classification schema has been proposed and applied to the identified research works. Furthermore, research questions have been identified and answered through the performed classification. The paper provides an outlook on cybersecurity testing in drone environments. It also lists current criticalities, challenges, gaps, and future directions useful to improve drone quality and increase cybersecurity. The analysis reveals that the collected results point to a meaningful evolution and innovative approaches in cybersecurity testing within current research activities.

INDEX TERMS Drones, UAV, cybersecurity, testing.

I. INTRODUCTION

Drones, also called unmanned aerial vehicles or systems (UAV) or (UAS), are revolutionizing how we think and do in various sectors and contributing to efficiency, convenience, and innovation. Indeed, they are smart and flexible devices that can be easily equipped with sensors, cameras, and transmitters to satisfy the most challenging and practical difficulties. Valuable insights were drawn from a wide range of diverse fields, such as [1]:

- *Photography and Videography*: Drones equipped with high-end cameras capture images and videos of various environments and public and private events, enabling professional-grade content creation [2].
- *Delivery*: Started in 2015, the combined use of truck and drone delivery is quickly expanding. One of the main fields is parcel delivery. Many companies (like Amazon, DHL, and Alibaba) are evaluating using drones for last-mile delivery for faster and more efficient service [3]. Another important field is healthcare support, where drones can deliver medical supplies or transport medical samples, especially in remote or hard-to-reach areas [4].
- *Monitoring*: Many times, drones are used to monitor and manage the environment and specific situations. Examples are: i) Traffic Monitoring, for collecting real-time data on road conditions, helping with traffic control and alleviating congestion [5]; ii) Agriculture monitoring, for assessing field and animal conditions, optimising the use of resources and improving arrangements or yields [6]; iii) Environmental Monitoring, for instance, wildlife, tracking changes in ecosystems, and collecting data on air and water quality [7]. They assist researchers in understanding and protecting the environment, monitoring infrastructure like bridges, power lines, and pipelines, or inspecting difficult-to-reach or hazardous locations, reducing manual labor.
- *Search and Rescue Operations*: with the integrated use of different sensors and video devices, drones represent valid means for quickly exploring large areas, localising missing persons, or collecting critical information [8].

The associate editor coordinating the review of this manuscript and approving it for publication was Zhe Xiao.

- *Security and Surveillance*: for managing and controlling public events, borders, and private properties to improve situational awareness and monitoring capabilities [9].
- *Entertainment and education*: Drones can be used in outdoor events and light shows to experience remote-controlled flight. They also play an essential role in teaching concepts related to science, technology, engineering, and mathematics (STEM) [10].
- *Military use*: Drones can operate long distances, at high altitudes, and in challenging weather. They can be outfitted with advanced avionics and armaments. Recent wars demonstrated commercial drones can be used for tactical aims [11].

This non-exhaustive list highlights how eclectic the field of drone applications can be. For sure, new challenges and a more integrated use of them in our daily lives will appear as technology develops.

However, the pervasive use of drones opens the path to significant safety, security, and privacy concerns. These quality aspects are essential in any system or application for many reasons, such as the protection of sensitive data, the prevention of data breaches, the preservation of privacy, the prevention of cybercrime, the assurance of business continuity and integrity, and the assurance of trustworthiness [12]. In the case of drones, assuring cybersecurity could be even more critical due to their broad domain application fields and the complexity of their architecture. Indeed, drones can expose vulnerabilities and weaknesses in wireless communication systems, causing eavesdropping and unauthorized (data) access, tampering, remote hijacking, GPS spoofing (providing false GPS signals), or jamming (blocking GPS signals). They can also be infected with malware or Denial Of Service (DOS) attacks, compromising performance or data integrity.

Addressing cybersecurity challenges requires proactive risk management and joining activities and solutions applied at different stages of development. In this context, cybersecurity testing is recognised as one of the most effective means to assess adequate functional and non-functional quality levels and to prevent and remedy malfunctions. It assesses confidentiality, integrity, availability, authentication, authorization, and non-repudiation properties. It can also demonstrate conformance with security and privacy standards and protect against vulnerabilities and malicious and unexpected data and resource management.

Due to its pervasiveness, cybersecurity testing encompasses a variety of activities during the development process, consuming a large part of the production effort. This paper systematically surveys emerging cybersecurity testing technologies, solutions, and methodologies applicable to drone development and application. Indeed, despite the literature interest in drone cybersecurity, there needs to be a comprehensive classification of the studies focused on cybersecurity testing [12]. The analysis executed in this work shows that several authors deal with general cybersecurity challenges and opportunities but marginally address the testing problem [12].

The Systematic Literature Review (SLR) [13] on drone cybersecurity testing conducted over the last five years (2018-2023) presented here closes this gap. It also contains an automated search across six well-known digital libraries (Scopus, ACM, IEEE, and Springer). Iterations of snowballing have also been carried forward and backward (via Google Scholar) to find and classify pertinent research and solutions.

As a result, a total of **970** primary contributions have been scrutinized, of which **122** proposals eventually passed the selection and are surveyed here. The different testing approaches have been classified into three proposed research areas. In contrast, topics in each research area have been customized according to the proposal and content of the analyzed studies.

ROADMAP This survey is structured as follows: in the next Section II, the related work has been overviewed, analyzing the SoTa of the survey in Drone Cybersecurity Testing. Then, Section III describes the Research Questions (RQs) and the Research methodology applied. Section IV describes the classification process obtained from the proposed Research methodology while Section V details and results about the performed classification process. In Section VI the answers to the proposed RQs have been provided; in Section VII an evaluation of threats to validity has been proposed. Conclusions and future work are given in Section VIII.

II. RELATED WORK

This section's current paper is positioned according to the state-of-the-art surveys on Drone Cybersecurity. For this purpose, 47 surveys from 2018-2023 have been analyzed from the leading digital libraries (Scopus, ACM, IEEE, and Springer) and selected considering the following inclusion criterion: *The survey must include cybersecurity as one of the main topics*. The 24 selected related works are listed in Table 1 ordered by publication year.

In particular, for each work, Table 1 shows the *Publication year* (first column), the *Source* (second column), and the *Reference number*, i.e., the number of the paper as in the paper reference list (third column), the *Scope of the Survey* (fourth column), the primary cybersecurity *Classification Topics* (fifth column), and as defined in the following, the *Testing method* (sixth column) analyzed (if any).

Additionally, to better visualize the contribution of each of the selected surveys, a classification of their content according to the following topics has been performed:

- *Privacy*: The survey deals with the (data) privacy or regulations;
- *Drone Technology*: The survey analyses the (hw/sw) technologies useful for assuring cybersecurity;
- *Drone Architecture*: The survey analyses the architectural or by-design proposals for solving cybersecurity criticalities;

- *Specific attacks*: The survey focuses on specific cybersecurity attacks like intrusion detection, Denial-Of-Service;
- *Testing*: The survey focuses on specific testing approach approaches for solving cybersecurity issues.

In Table 1, all the analyzed contributions are reported, and most of them focus on the methods and approaches for solving cybersecurity issues at the architectural or technological level, proposing specific countermeasures. However, only a quarter of the surveys (6 over 24) offer testing as a possible solution for preventing and solving cybersecurity threats or vulnerability issues.

As highlighted by the analyzed survey papers, the increasing popularity of drones is driven by their cost-effectiveness, maneuverability, easy maintenance, and versatility in serving remote areas. However, in parallel with their diffusion, cybersecurity poses a significant concern [14]. Main challenges have been recognised in potential loss of flight data [15] or control [16], management of collaborative ecosystem [17], use of open-source platforms [18], or emerging technologies [19].

According to the survey papers analysis, the main findings on UAS Cybersecurity focus on threats and vulnerabilities at communication, network, software, or payload levels [19], [20], sometimes impacted also by human factors [21]. As in these papers usually, spoofing, intrusion detection, and Denial of Service are the common cyber-attacks on UAVs, emphasizing potential harm to individuals and the community [22], [23], [24], [25], [26]. Standard solutions for improving cybersecurity focus either on the adoption of technologies (such as AI, machine learning, authentication, cryptography techniques, blockchain-powered schemas) [19], [21], [22], [25], [27] or on the drone architectural model by proposing models, dataset, or specific networks [11], [15], [23], [28] or conceiving specific countermeasures (such as training algorithms, or simulation testing) [15], [16], [19], [29], [30], [31].

However, the investigation performed on this survey's papers highlighted three important challenges:

1) **CH1:** Despite the other IoT research fields, verification, validation, and testing activities are rarely considered an essential contribution to ensuring the required UAV cybersecurity level. Only 6 of the 24 surveys mention testing approaches [20], [22], [25], [27], [30], [32], and most of the time, they do not refer to standardized and controlled testing processes but limit themselves to the suggestion of fuzzy or penetration testing methodologies. Knowledge and understanding about testing still seem missing in the UAV research contest.
2) **CH2:** Research topics like privacy-preserving, ethical considerations, data quality management, and legal framework for forensic analysis post-illegal activities strictly connected with UAV cybersecurity and trustworthiness are rarely considered (7 surveys over 24) [14], [18], [19], [28], [31], [33], [34].
3) **CH3:** Security measures to mitigate cyber-attack risks and improve information confidentiality, authenticated access, software, data integrity, system availability, and accountability in UAVs are still missing in operating systems.

The scope of this survey is mainly to reply to the first challenge and, therefore, better understand the current state-of-the-art in UAV cybersecurity testing, highlighting the existing solutions and possible open issues.

III. APPLYING A SYSTEMATIC REVIEW METHODOLOGY

This section describes the methodology adopted for selecting and categorizing the papers related to cybersecurity testing in a drone environment. A set of papers has been collected and analyzed according to the guidelines for systematic reviews in software engineering research provided by Kitchenham and coauthors [49]. For the aim of completeness, the suggested procedural stages [49] are summarized below:

1) Defining the Research Questions;
2) Collecting the papers (see Section III-A);
3) Defining the classification procedure (see Section IV);
4) Analysing the results (see Section V);
5) Replying to the Research Questions (see Section VI).

The research questions have been defined by analyzing the results and the identified challenges of the related works (Section II). Thus, to satisfy the above-mentioned first stage (Defining the Research Questions), the following research questions have been identified (RQs):

- **RQ1**: What are the main objectives for drone cybersecurity testing?
- **RQ2**: What are the proposals (i.e., methods, techniques, and tools) mainly adopted in drone cybersecurity testing?
- **RQ3**: What are the challenges and issues in applying drone cybersecurity testing?
- **RQ4**: Which are the main application domains for drone cybersecurity testing?

A. TARGET PAPERS IDENTIFICATION

To satisfy the above-mentioned second stage (*Collecting the papers*) and select the *Target Papers Set* to be analyzed, a quality analysis process has been executed as shown in Figure 1.

Specifically:

- **Quality Analysis 1st Step:** To automatically select the paper, the following query has been defined:

  Q1: **"cybersecurity AND (drone OR uavs OR (aerial AND vehicle)) (testing OR validation OR verification)"**

  The terms `drone`, `UAVS`, and `aerial vehicle`, as well as the commonly adopted synonyms for testing, i.e., validation and verification, have been included to make the query as general as possible but able to provide meaningful results. By searching by title, abstract, and keywords on English papers from 2018 to 2023 the query has been executed over the following

TABLE 1. How surveys have been classified.

Publ. year	Source	Ref. n°	Scope of the survey	Size	Classification topics	Testing methods
2018	Scopus	[35]	It explores various evaluation techniques and approaches, including war planning situation awareness tools and decentralized anomaly-based detection techniques.	**27**	Drone Technology, Drone Architecture, Specific attacks	Specification-based; Real-time safety; Assessment algorithm
2018	IEEE	[36]	It overviews security concepts with a focus on attack surfaces. It analyses risk severity and security metrics	**58**	Drone technology Drone architecture Testing	Vulnerability risk analysis; Models for attack surface
2019	Springer	[33]	It focuses on the importance of government regulation and effective detection of drone spying as part of cybersecurity measures.	**29**	Privacy	No Specific topics
2019	Scopus	[34]	It focuses on UAV applications and concepts of drone services.	**109**	Privacy; Drone architecture	No Specific topics
2020	Scopus	[37]	It focuses on the use of drones, their vulnerabilities, and the need for comprehensive analysis of security vulnerabilities and countermeasures.	**411**	Drone technology; Drone architecture; Countermeasures	No Specific topics
2020	Scopus	[23]	It emphasizes privacy, various security threats and cyberattacksk like spoofing and denial of service attacks.	**23**	Privacy; Drone tech Architecture; Specific attacks	No Specific topics
2021	IEEE	[38]	It performs analysis of different types of cyberattacks, and discussion of countermeasures	**76**	Specific attacks Countermeasures	No Specific topics
2021	Scopus	[39]	It explores UAVs employed in the surveillance field for indoor and outdoor spaces.	**23**	Drone technology Drone architecture	No Specific topics
2021	IEEE	[25]	It classifies security issues, vulnerabilities, and attack of Drone Bugs Bounty Programs.	**22**	Specific attacks; Countermeasures; Testing	Vulnerability Assessment Penetration Testing
2021	IEEE	[40]	It explores defense mechanisms, operating systems' security and use of UAVs in industries.	**49**	Drone technology architecture; Countermeasures	No Specific topics
2022	IEEE	[41]	It proposes IDS (Intrusion Detection System) by utilizing deep learning anomaly-based detection methods for enhancing UAV swarms security.	**59**	Specific attacks Countermeasures	Evaluation used for testing IDS for UAV security.
2022	IEEE	[26]	It focuses on mitigation techniques for secure UAV communications in IoT applications.	**206**	Drone architecture; Specific attacks; Countermeasures	No Specific topics
2022	ACM	[42]	It explores adoption of AI for security-critical UAV tasks	**125**	Privacy Countermeasures	No Specific topics
2022	Scopus	[43]	It explores current standards related to UAV design, safety, communication and user training.	**200**	Privacy; Drone architecture; Countermeasures	Analyzing and classifying security threats.
2022	IEEE	[44]	It focuses on increasing awareness of the potential risks associated with UAV and proposed specific countermeasures to address these risks.	**23**	Drone technology Countermeasures	No Specific topics
2022	IEEE	[19]	It focuses on the protection of the IoD (Internet of Drones) and its integration of IoD with emerging technologies.	**88**	Privacy; Drone technology Arch; Specific attacks; Countermeasures	No Specific topics
2023	IEEE	[45]	It explores the potential security risks associated with hacking and cyber-attacks on UAV system components and communication.	**23**	Specific Attacks	No Specific topics
2023	Scopus	[16]	It explores the continuous updating of forensic methods and frameworks due to advancements in drone manufacturing	**108**	Drone technology Countermeasures	No Specific topics
2023	Scopus	[18]	It focuses on the challenges related to UAV security and privacy, trajectory and route planning techniques	**402**	Privacy; Drone technology	No Specific topics
2023	Scopus	[27]	It explores and analyzes defense methods such as physical layer security and intrusion detection.	**170**	Drone architecture; Specific attacks; Countermeasures; Testing	Fuzzy Testing
2023	IEEE	[46]	It focuses on the security of UAV-assisted IoT applications and the need for cost-effective security solutions.	**179**	Drone technology Testing	Configured testbed to detect against UAV-assisted IoT communication
2023	Scopus	[47]	It focuses on enriching semantic content and the potential for IoD to collect and complement existing datasets in the UC (Urban Computing) perspective	**177**	Drone architecture	No Specific topics
2023	Scopus	[48]	It focuses on Machine Learning (ML) based approaches to enhance UAV security in the field of transportation	**119**	Drone technology Drone architecture	No Specific topics
2023	Springer	[14]	It focuses on the lack of awareness among the various stakeholders to address drone cybersecurity challenges.	**327**	Privacy; Drone tech Arch; Specific attacks; Countermeasures	No Specific topics

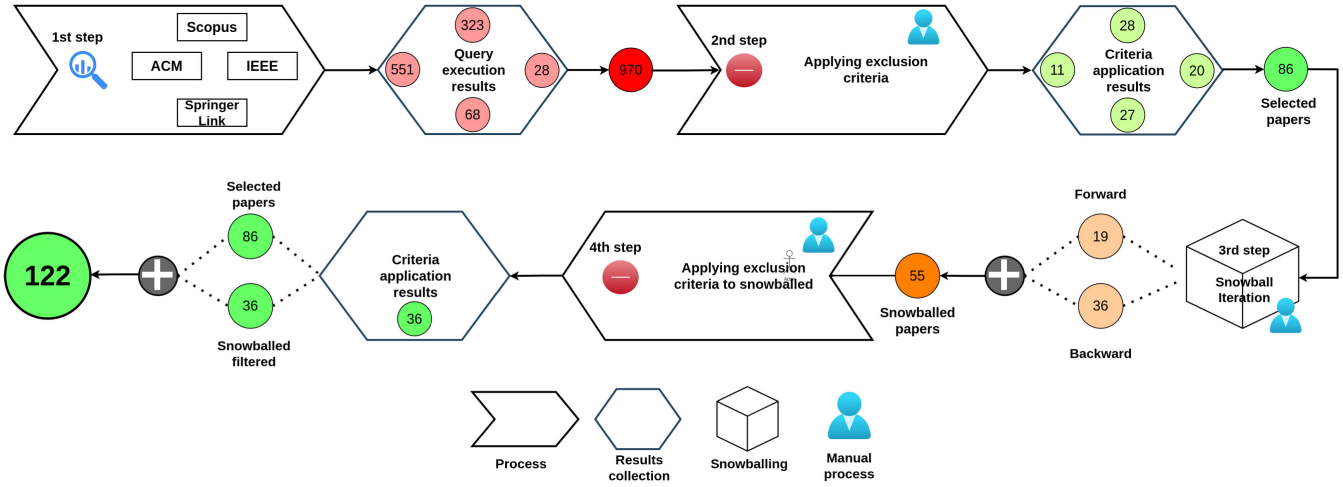

FIGURE 1. Methodology.

electronic sources: Scopus,[1] ACM Digital Library,[2] IEEE eXplore,[3] SpringerLink.[4] The execution provided the following results:

- Scopus: **323** papers;
- ACM Digital Library: **551** papers;
- IEEE eXplore: **28** papers;
- SpringerLink: **68** papers;

for an initial merged collection of **970** papers (excluding duplication).

- **Quality Analysis 2nd Step:** (See Figure 1) The 970 papers have been then processed by reading their title, abstract, and keywords and included or excluded from the collection according to the following criteria:
  - Exclude papers that do not specifically concentrate on drones;
  - Exclude papers that provide state-of-the-art reviews or surveys;
  - Exclude papers that do not qualify as original or comprehensive research publications, such as forwards, editorials, monographs, books, and contributions that are not peer-reviewed or are too brief;
  - Exclude poor-quality papers, such as those with unclear objectives that could have outlined a focused solution.

  This step largely reduced the papers provided the following results: Scopus reduced to **28**, ACM Digital Library reduced to **11**, IEEE eXplore reduced to **28**, and SpringerLink reduced to **27** papers. The total number of included papers was **86**.
- **Quality Analysis 3rd Step:** (See Figure 1) The accepted papers were manually enriched through a snowballing search [50]. The snowballing technique in systematic literature reviews involves using references and citations to discover additional relevant studies. There are two types of snowballing: *backward snowballing*, where the references have been examined to find earlier foundational works, and *forward snowballing*, where references have been used to look at subsequent studies that cite the initial articles. Snowballing is crucial for enhancing the comprehensiveness of a systematic literature review, helping to identify studies that traditional database searches might miss due to varying terminology or publication in less accessible sources. Thus, for each paper, the list of references (*backward snowballing*) and its citations list in Google Scholar[5] (*forward snowballing*) have been analyzed to collect additional pertinent studies not already included in the resulting set of papers.

  Moreover, **19** new additional papers were identified through forward snowballing, and **36** were identified through backward snowballing. Only studies in the 2018-2023 range have been considered per the query. Overall **55** new additional papers were identified.
- **Quality Analysis 4th Step:** (See Figure 1) The **55** paper identified by the snowballing process has been assessed with the exclusion criteria mentioned in step 2. As a result, **36** papers were selected for inclusion in the final set.

In conclusion, the overall *Target Papers Set* after backward snowballing includes **122** papers as schematized in Figure 1.

IV. CLASSIFICATION PROCESS

Several dimensions have been considered for classifying the *Target Paper Set*. The dimensions have been selected from the analysis of related work (Section II) and represent the

[1] http://www.scopus.com
[2] http://dl.acm.org
[3] http://ieeexplore.ieee.org
[4] https://link.springer.com
[5] http://scholar.google.com/

frequently used research areas, the commonly adopted terms, and the most relevant topic for replying to the RQs present in Section III. These general dimensions have been successively divided into sub-dimensions to better characterize the contribution of the analyzed paper. In particular, the dimension and relative sub-dimensions considered are:

- **Solution Layer:** Defines the target system layer of the paper solutions or proposal. Its sub-dimensions are described in Table 2.
- **Attack surface:** Describes the hardware or software level at which the attack has been solved or discussed. Its sub-dimensions are described in Table 3.
- **Service:** Describes the specific service (or component) on which the attack has been solved or discussed. Its sub-dimensions are described in Table 4.
- **Testing objective:** Describe the testing objective of paper. Its sub-dimensions are described in Table 5.
- **Testing strategy:** Defines the testing technique used in the paper. Its sub-dimensions are described in Table 6.
- **Perspective:** Describes which research perspectives are considered in the paper. Its sub-dimensions are described in Table 7.
- **Application domain:** Describes the application domain in which the paper proposal can be adopted. Its sub-dimensions are described in Table 8.

Taxonomy classification in [15], [16], [27], and [28].

V. TARGET PAPER ANALYSIS

This section reports details of the performed classification process on the 122 papers in the *Target Paper* set as a result of Section III. In particular, in Section V-A, the procure adopted for the paper classification is discussed, while in Section V-B, a detailed analysis is reported.

A. CLASSIFICATION PROCEDURE

To categorise the contribution, the following procedure has been performed:

1) Each paper was randomly assigned to two authors, who read the paper and made a first classification, deciding autonomously whether the contribution belongs to:
   - *Drone Cybersecurity*, the paper provides a solution for improving some cybersecurity aspects but does not explicitly refer to a testing procedure.
   - *Drone Testing*, the paper provides a solution for improving overall drone quality through a testing procedure but does not explicitly refer to specific cybersecurity aspects.
   - *Drone Cybersecurity Testing*, the paper provides a solution for improving the overall drone cybersecurity level through a specific testing procedure.
   - *Other*, the paper provides a valuable solution for improving drone quality but does not explicitly target cybersecurity aspects or testing procedures.

   The contributions classified as *Other* were excluded from further analysis because they are useless for this paper.

TABLE 2. Categorization proposal for identified Solution layer.

Solution layer	Description
Drone Hardware	The solution is related to the hardware of the UAV. i.e.Battery, Sensors, Motors, Radio transmitter/receiver.
Drone Software	The solution is related to the software of the UAV. i.e.OS, Firmware, Route planner.
Environment SW	The solution is related to software not on board of the UAV, such as ground control stations software and Data links.
Environment HW	The solution is related to hardware not on board of the UAV, such as hw of communication systems or ground control stations.
Communication (Drone↔RC)	The solution is related to the communication among Drone and Remote Controller.
Communication (Drone↔ENV)	The solution is related to the communication among Drone and Environment. i.e.Ground control station, Weather station, A-GPS ground station and infrastructure external to drone.
Other	All the solutions that not falls in previous category.

2) Each of the two authors continued classifying the remaining papers according to the seven dimensions and sub-dimensions presented in Section IV.
3) For each paper, the two obtained classifications (one per author) have been compared. In disagreement, the third author, who was not involved in the first step, acted as referee. He/she decided either to favor one of the two classifications' values or to keep both because they are equally pertinent.

Figure 2 depicts the final results. In particular, according to the first classification of the 122 papers, 44 have been classified as *Drone Cybersecurity*, 36 as *Drone Cybersecurity Testing*, two as *Drone Testing*, and 40 as *Other*. Details of this classification are reported in Appendix .

As highlighted in the figure, only 43% (36 over 82) of the papers are entirely in line with the focus of the proposed survey, i.e., Drone Cybersecurity Testing. However, because *Drone Cybersecurity* and *Drone Testing* are also important research topics for the overall cybersecurity and quality level of the UAV, they have been included in the detailed analysis in the remainder of this paper.

Figure 4 shows the distribution of the paper 82 papers belonging to the three categories over the years. As in the figure from 2021, there is a significant increase in the literature interest in *Drone Cybersecurity* and *Drone*

TABLE 3. Categorization proposal for identified attack surface.

Attack surface	Description
Onboard camera	SW or HW related to the UAV Cameras
Engine	SW or HW related to the UAV Engines
GPS	Attacks to the GPS Stack
Radio	Attacks to Wi-Fi or RF UAV functionalities
Network protocols	Attacks focused on the communication protocols (RF, Wi-Fi, Other)
Firewalls	Attacks to the network perimetral protection.
Database and storage	Attacks to the storage environment even if remote or on-board the UAV
Encrypted data	Attack on encrypted stored data compromising secrecy and allowing stolen sensitive information.
Route Planning	Attacks on route planning systems of the UAV.
Stakeholders	Attacks that impacts collaborations, or interactions, among UAV stakeholders.
Third-party system	Attacks exploit vulnerabilities in UAV third-party software or the supply chain.
Transponder	Attacks focused on UAV Transponder Hardware or Software.
Encryption	Attacks disrupt the confidentiality and integrity of the transmission channel among UAV and control station/remote control.
Other	All the solutions that not falls in previous category.

TABLE 4. Categorization proposal for identified service.

Service	Description
Authentication	System verifying identity to grant access to authorized users securely.
Authorization Access	Granting permission to access specific resources or functionalities securely.
Privacy-preserving	Protecting sensitive data while allowing useful analysis or access.
Digital rights management	Control and protection of digital content access and distribution rights.
Weather forecast	Collect data on future weather conditions such as humidity, temperature, and wind speed.
Air traffic controller	Systems that monitor and provide safe and well-coordinated movements in our airspace.
Routing algorithm	Algorithm determining the optimal path for efficient and optimized movements.
Communication protocols	Standards or rules for communication UAVs, multiple UAVs, and control stations.
Video Control System	Services for managing and analyzing video and images.
Transmission System	Systems for transmitting data, signals, in power efficient and reliable way.
Security protocols	Methods and rules ensuring secure communication and data exchange practices.

Cybersecurity Testing. Additionally, in the same period, *Drone testing* started to appear in the research context.

In trying to justify this behavior, several factors can be considered from a technological and commercial point of view. Regarding the former, the increasing drone battery charge life improves the length of flight time and the secure return-to-home process. Additionally, the miniaturization of different drone components, such as HQ cameras, allows the widespread adoption of drones in different application domains like videography, photography, agriculture, and inspection of broad areas. Moreover, improving stability during the flight and their user-friendly controls increase the use of drones by not expert pilots. Finally, the possibility of adding payloads to the drones allows them to be equipped with more sensors, thermal cameras, antennas/transmitters and be used for the widespread collection of real-time data. From the commercial point of view, the competition between vendors forces a cut down on drone prices and makes their costs affordable for various consumers. Additionally, the new regulations of airspace limits and capabilities, in conjunction with the abovementioned aspects, allow drones to grow in popularity and be used for continuous emergent scopes.

B. COLLECTED RESULTS

This section provides, through a set of figures, the results collected from the classification of the 82 papers belonging

TABLE 5. Categorization proposal for testing objective.

Testing objective	Description
Trusted behavior	Adherence to standards, compliance with ethical actions and confidence reliability.
Malware	Identification and mitigation of software to ensure system security continuity and availability.
Social networks	Correct and compliant functionality, security, and UX of social networks.
Spoofing	Detection and prevention of misleading identity impersonation.
Phishing	System's vulnerability to deceptive tactics, preventing and mitigating attacks.
Eavesdropping	Assessment and prevention of unauthorized interception.
Denial-Of-Service	Attacks that disrupt access to a service by overwhelming its resources.
Injection	Exploit vulnerabilities inserting malicious code or commands.
Ethical values	Principles promoting responsible and moral conduct in UAV development.
Laws principles	Laws and principles governing use, development, and ethics in UAV dev.
Tamper-proof	It involves a range of measures to ensure AV security and integrity.
Security-by-Design	Security-by-design in UAVs as their vulnerability to cyber-attacks and exploitation.
Hardware attacks	Attacks on UAV HW components to render them inoperable.
Data Privacy	Target personal data stored or collected by UAV.
Side-channel	Security vulnerability exploiting gaining access to extract information.
Safety	Mechanisms and methodologies to ensure reliably prevent harm to users or environment.
Trustworthiness	HW or SW components to ensure reliability and integrity of systems, data, and processes

to the categories *Drone Cybersecurity*, *Drone Testing*, *Drone Cybersecurity Testing*, according to the seven dimensions

TABLE 6. Categorization proposal for testing strategy.

Testing strategy	Description
Penetration	Evaluating system security by simulating attacks to identify vulnerabilities.
Fuzzy	Methodology for testing software with invalid, unexpected, or random data.
Combinatorial testing	Technique testing multiple combinations of input variables to uncover defects.
Model-based	The approach uses models to design and test system behavior.
Specification-based analysis	Testing addresses the analysis of system behavior against predefined specifications or requirements.
Ad-hoc	Approach or method improvised or created spontaneously as needed.
Configuration	Testing to ensure software or hardware configurations meet requirements and standards.
Random	The testing mechanism uses inputs chosen randomly without predefined patterns.
Formal methods	The strategies that leverage mathematical techniques to verify software correctness formally.
FSM	A testing strategy utilizing FSM to model and validate system behavior.
Exploratory	A testing approach emphasizing real-time exploration and learning to uncover defects.
Operational	Testing strategy assessing system functionality, performance, and reliability in real-world operational conditions
Usage-based	Strategy based on real or anticipated usage patterns, ensuring the system's robustness under varied conditions.

and sub-dimensions presented in Section IV. In each figure, green, yellow, and orange colors are associated respectively with *Drone Cybersecurity Testing*, *Drone Cybersecurity*, *Drone Testing* collected analysis data.

It is crucial to notice that according to the procedure described in Section V-A, a paper can be associated with one or more sub-dimensions. Therefore, the overall data reported

TABLE 7. Categorization proposal for perspective.

Perspective	Description
Research directions	Research that is aimed at discovering and responding to unanticipated problems and detours.
Issues	Problems related to the contribution that still need a practical or theoretical solution.
Challenges	Evolution related to the continuous and rapid evolution of drone technology.
Practical Solution	Scientific study and research that seeks to solve practical problems by proposing concrete solutions.

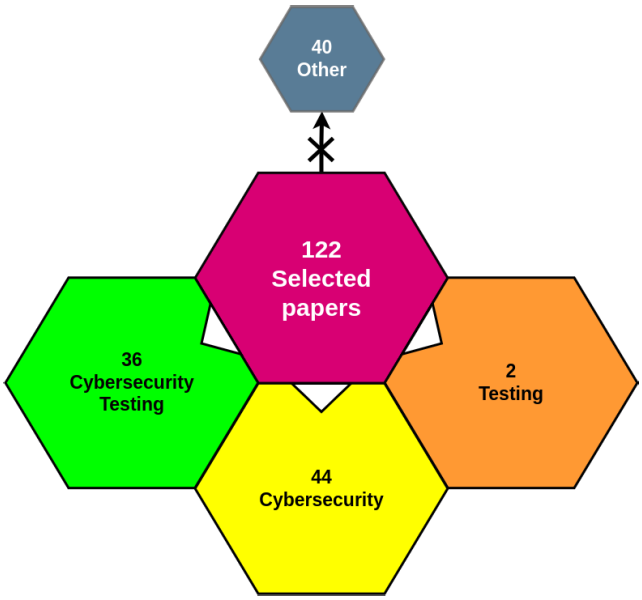

FIGURE 2. Classification groups.

in each table can be greater than 82 (total number of analyzed papers).

1) SOLUTION LAYER

Considering **Solution Layer** dimension and its sub-dimensions (as reported in Table 2), Figure 5 shows the obtained results.

As in the figure, the majority of papers focus on the Communication (Drone ↔ ENV) (42.68%),[6] Communication (Drone ↔ RC) (36.59%) or on Drone Software (37.80%), while few proposals target issues related to Drone Hardware (9.76%) or SW or HW environment (6.10% and 2.44% respectively). In particular, these last sub-dimensions are completely missed in the papers focusing on *Drone Cybersecurity Testing*.

[6]From hereafter, all the percentages are computed by the number of papers contributing to the sub-dimension divided by the overall paper set (82).

TABLE 8. Categorization proposal for application domain.

Application domain	Description
Photography and Videography	UAV used for aerial photo/video, capturing action from the air.
Goods Delivery	Aerial transportation of parcels, groceries, food, and other homecare products.
Healthcare Delivery	Transportation of medicines or other products related to the healthcare.
Vehicular Monitoring	Drones are used to capture driving errors, estimate driver gaps, provide an accurate collection of vehicle traffic data and detect dense traffic.
Agricultural monitoring	Drones are used to facilitate aerial surveillance of landscapes. Identify challenges such as water stagnation, pest infestations, or crop diseases.
Search and Rescue Operations	Leveraging emergency services, detecting distressed subjects, and capturing images or signals to accelerate finding missing people.
Security and Surveillance	It helps gather information about specific targets, enhancing situational awareness and response capabilities in various settings.
Entertainment and education	Drones are used for virtual reality, live streaming, and broadcasting, drone light shows and art, racing and gaming.
Military use	Intelligence gathering, target acquisition, precision strikes, force protection, surveillance, and reconnaissance, logistics, and combat operations.
Maritime System	Drones equipped with high-resolution cameras and LiDAR technology can capture detailed images and collect data on maritime infrastructure, such as ports, bridges, and offshore platforms.
Generic	Drones proposed approaches are validated general-purposely, not on a specific domain.

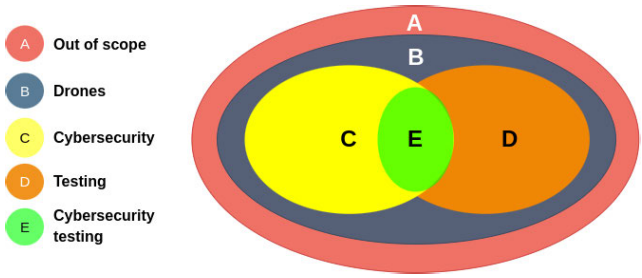

FIGURE 3. Groups categorization overview.

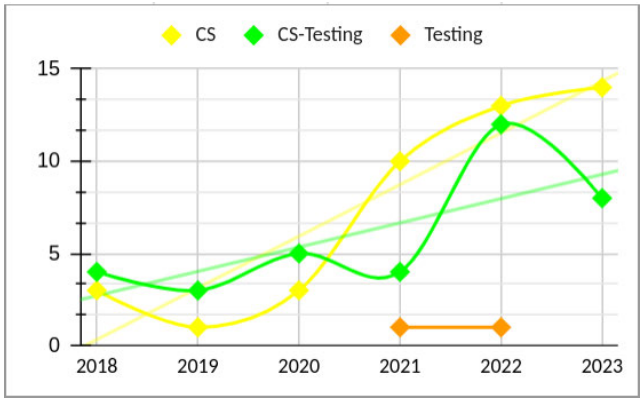

FIGURE 4. Distribution of papers by year and type.

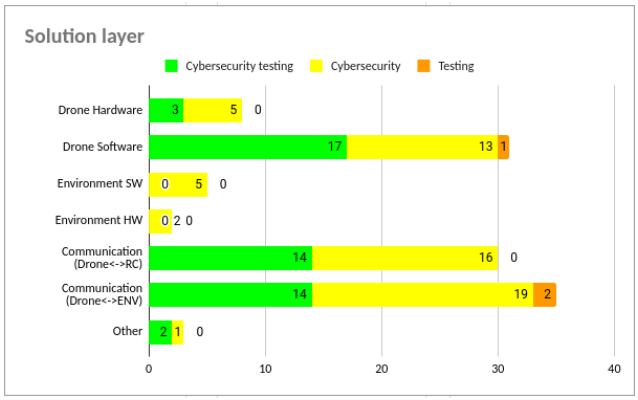

FIGURE 5. Solution layer distribution.

2) ATTACK SURFACE

Considering **Attack surface** dimension and its sub-dimensions (as reported in Table 3), Figure 6 shows the obtained results.

The data analysis reveals that most **Attack surfaces** focus on the main critical components of the drone architecture: Radio (19.51%), GPS (20.73%), Network protocols (14.63%), and Route planning (20.73%). Partial attention is devoted to Data storage and management (13.41%), Encrypted Data (7.32%), Encryption (7.32%), and Transponder (7.32%). It is essential to notice that other critical sub-dimensions such as Onboard camera, Engine, Firewalls, Stakeholders, and Third-party systems are entirely missed

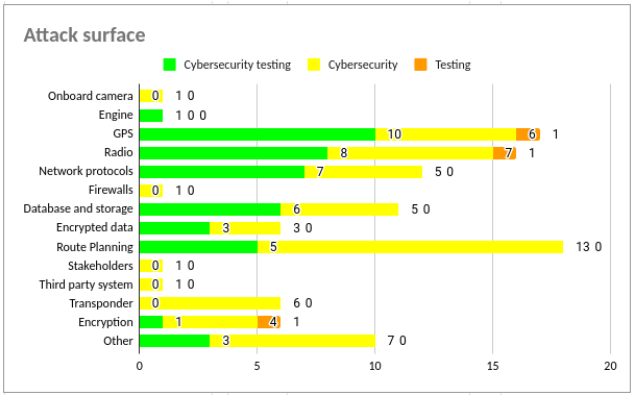

FIGURE 6. Attack surface results.

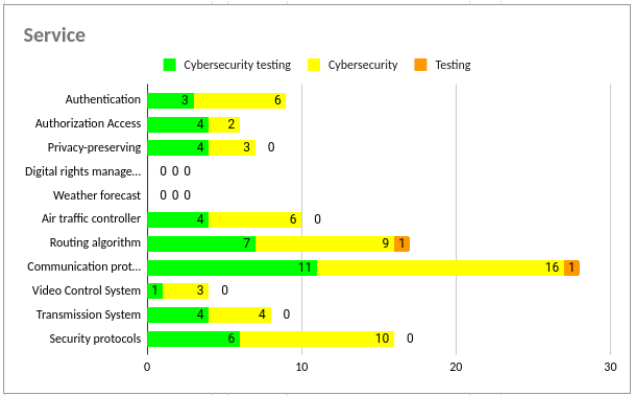

FIGURE 7. Service analysis results.

in the papers focusing on *Drone Cybersecurity Testing* and rarely targeted by those related to the *Drone Cybersecurity* with the percentage of 1,22%.

3) SERVICE

Considering **Service** dimension and its sub-dimensions (as reported in Table 4), Figure 7 shows the obtained results.

As in the Figure, most papers focus on Communication protocols (35.37%). Partial attention is devoted to Security protocols (20.73%), Routing algorithm (21.95%), Air traffic controller (12.20%) sub-dimensions, and limited consideration is reserved to Authentication (10.98%), Authorization Access (7.32%), and Privacy-preserving (8.54%), Transmission System (9.76%). The Video Control System sub-dimension is rarely considered (6.10%), while Digital Rights Management and Weather forecasts are wholly ignored.

4) TESTING OBJECTIVE

Considering **Testing objective** dimension and its sub-dimensions (as reported in Table 5), Figure 8 shows the obtained results.

Data analysis of the dimension of the **Testing objective** evidences two separate realities. While strong attention is devoted to Eavesdropping (23.17%), Spoofing (21.95%), Security-by-Design (19.51%), Denial-Of-Service

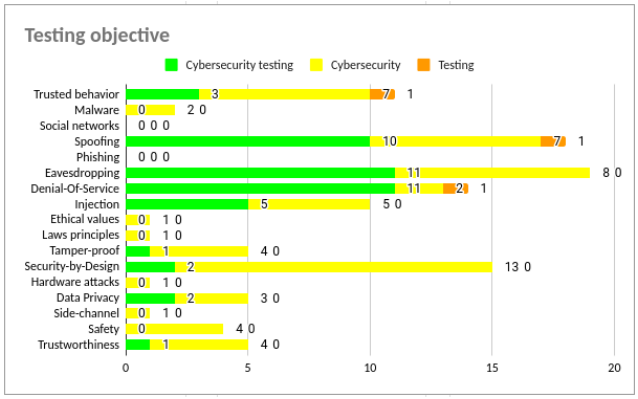

FIGURE 8. Testing objective results.

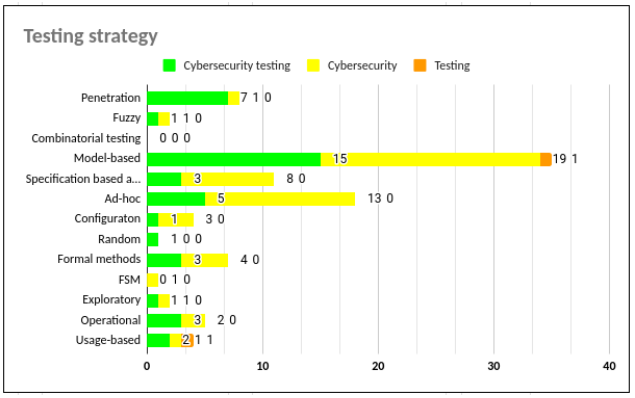

FIGURE 9. Testing strategy results.

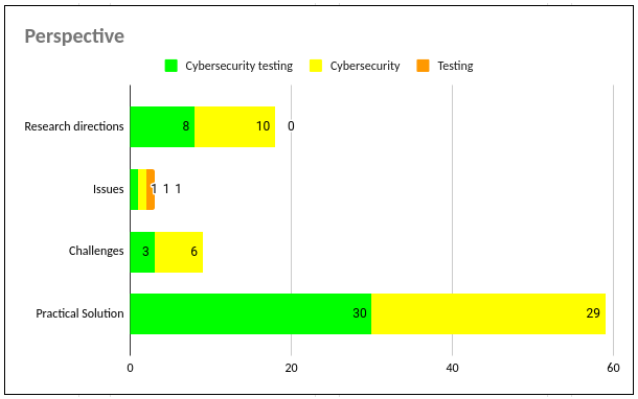

FIGURE 10. Perspective evaluation results.

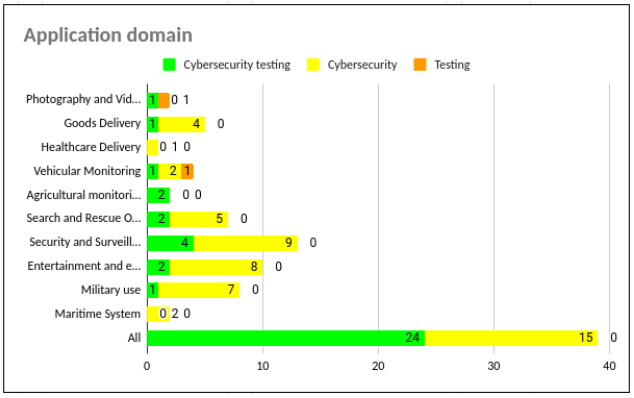

FIGURE 11. Application domain results.

(18.29%), Trusted behavior (13.41%), Injection (12.20%), other sub-dimensions like Tamper-proof (6.10%), Data Privacy (6.10%), Safety (4.88%), Trustworthiness (6.10%), are rarely considered. In addition, topics such as Malware, Ethical values, Law principles, Hardware attacks, and Side-channel are just considered by *Drone Cybersecurity* papers set with a percentage less than 2.5%, and others, such as Phishing and Social networks, are completely ignored.

5) TESTING STRATEGY

Considering **Testing strategy** dimension and its sub-dimensions (as reported in Table 6), Figure 9 shows the obtained results.

As in the figure, most papers focus on Model-based (43.90%), Ad-hoc (23.17%), Specification-based analysis (13.41%), sub-dimensions. Others like Penetration (10.98%), Formal methods (9.76%), Operational (6.10%), and Usage-based (4.88%) are rarely considered.

Very little attention is devoted to sub-dimensions like Fuzzy, Configuration, Random FSM, and Exploratory (percentage less than 2.5%), while others, such as Combinatorial testing, are entirely ignored.

6) PERSPECTIVE

Considering **Perspective** dimension and its sub-dimensions (as reported in Table 7), Figure 10 shows the obtained results.

Data analysis of the **Perspective** evidence that almost all the proposals focus on Practical Solutions (73.17%), some of them target Research directions (23.17%) or Challenges (10.98%) but rarely the Issues (3.66%).

7) APPLICATION DOMAIN

Considering **Application domain** dimension and its sub-dimensions (as reported in Table 8), Figure 11 shows the obtained results.

As in the figure, most papers provide generic solutions that are not conceived and focus on a specific application domain. Only exceptions are represented by Security and Surveillance, Entertainment and Education, and Military use (13%, 12%, and 11%, respectively) where focused solutions are provided. Particular attention should be devoted to Healthcare delivery, Photography and Videography, and Maritime systems that, even if very specific and critical from a cybersecurity point of view due to the widespread adoption, seem not to attract the attention of the current literature.

In conclusion, the overall picture from the classification process confirmed the challenges discussed in Section II. In particular, considering the first challenge

(**CH1** of Section II), as depicted in Figure 9, most of the papers focus on specific (predominantly machine-learning-based) or Ad-hoc testing strategies, and very few of them follow a controlled testing process as recognized by the best practice of software engineering [51]. Additionally, almost the totality of the papers dealing with Drone Cybersecurity Testing either put their attention only to communication issues, ignoring other critical cybersecurity architectural or software breaches (as highlighted in Figure 5 and Figure 7) or target specific cybersecurity objectives (as reported in Figure 8), proving that knowledge and understanding about testing need to be improved. Considering instead the second challenge (**CH2** of Section II), as showcased in Figure 7, and Figure 8, very few proposals take into consideration research topics like Privacy, Ethical values, and Law principles, meaning that cybersecurity and trustworthiness attributes are not fully taken in consideration in drone context. Finally, considering the last challenge (**CH3** of Section II), even if some proposals target confidentiality, Authentication, and Authorization issues (as in Figure 7), specific availability cybersecurity measures to mitigate cyber-attack risks are still missing in operating systems.

VI. REPLYING RQS

The data and results collected in the previous section have been used to answer the research questions introduced in Section III. The answers are provided considering mainly the paper belonging to the *Drone Cybersecurity Testing* group of papers because they are those closer to the RQs focus. However, when considered attractive, a global view (including also the *Drone Cybersecurity* and *Drone Testing* results) is provided. Each of the four sections is dedicated to a specific RQ.

A. REPLY TO RQ1

As reported in Section III, RQ1 refers to:

What are the main objectives for drone cybersecurity testing?

As already discussed in Section V-B and depicted in Figure 5, among the 82 papers analysed, a large portion of the proposals (i.e., the 79,27%) target Communication issues (Drone ↔ RC) and (Drone ↔ ENV).

Considering only the 36 papers belonging to *Drone Cybersecurity Testing* group, the percentage of papers dealing with communication problems is 77,78%, characterizing this issue as one of the primary objectives.

Therefore, in reply to RQ1, a detailed analysis of the specific testing objectives was performed better to understand the relationship between cybersecurity and communication issues. Thus, from the overall 82 paper set, the subsets of the papers dealing with communication problems have been extracted, obtaining the following selection:

- 25 fall in the *Drone Cybersecurity Testing* group of papers;
- 2 fall in the *Drone Testing* group of papers;
- 29 fall in the *Drone Cybersecurity* group of papers;

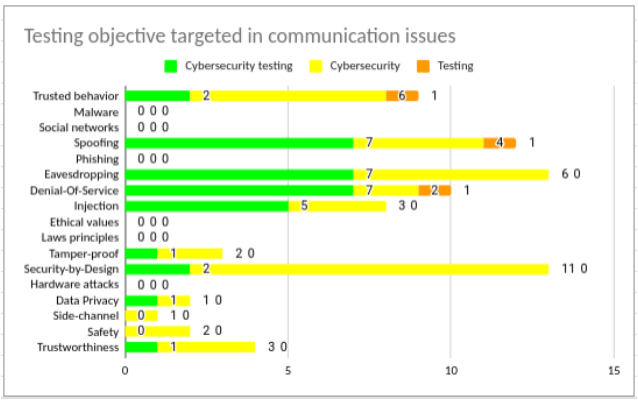

FIGURE 12. Testing Objectives of paper targeting communication issues.

For each of the three sub-sets, the data about the classification according to the `Testing Objective` dimension has been extracted, and results reported in Figure 12

The overall trend is confirmed by comparing these results with those presented in Figure 8. Indeed, as in the Figure, the objectives are majorly aligned with Eavesdropping (23.21%), Spoofing (21.42%), Security-by-Design (23.21%), Denial-Of-Service (17.85%), Trusted behavior (16.07%) and Injection (14.28%). Spoofing, Denial-Of-Service, Eavesdropping, and Injection are the main objectives, even considering only the 25 papers in the *Drone Cybersecurity Testing* group.

The collected evidence lets reply to RQ1:

The main objectives in Drone Cybersecurity Testing are the issues in Spoofing, Denial-Of-Service, Eavesdropping, and Injection focused on Communication (Drone ↔ RC) and (Drone ↔ ENV).

B. REPLY TO RQ2

As reported in Section III, RQ2 refers to:

What proposals (i.e., methods, techniques, and tools) are mainly adopted in Drone Cybersecurity Testing?

The data about the Attack surface reported in Figure 6 shows that most of the proposals in the *Drone Cybersecurity Testing* group focus on GPS, Radio, and Network protocols (GPS 10, Radio 8, Network protocols 7). In particular, as evidenced in Figure 7, the Services analyzed by the *Drone Cybersecurity Testing* papers group are mainly the Communication protocols (30%), the Routing Algorithms (19%), and the Security protocols (16%). Minor attention has been given to the Transmission System, Air Traffic Controller, Privacy-Preserving, and Authorization access that covers 16% each. Finally, as depicted in Figure 9, taking into consideration the Testing strategies, most of the *Drone Cybersecurity Testing* papers group contributions focus on Model-based testing (41.66%), Penetration testing (19.44%), and Ad-Hoc testing (13.88%). Minor attention has been dedicated to Specification-based analysis (8.33%), Formal methods (8.33%), Operational (8.33%), and Usage-based (8.33%).

To better address the RQ2, a correlated and detailed analysis has been performed considering the most frequent: (i) Attack surfaces (i.e., GPS, Radio, and Network protocols), (ii) Services (i.e., Communication protocols, the Routing Algorithms, and the Security protocols) and (iii) the applied Testing strategies. The collected results are detailed in Table 9.

As reported in the table's second column, 25 contributions have been analyzed (10 for GPS, 8 for Radio, and 7 for Network protocols). Rows labeled GPS, Radio, and Network protocols summarize the contribution percentage targeting the specific testing strategies for each selected attack surface. Overall pieces of evidence from the collected results are as follows:

- Configuration-based and Random testing approaches have never been applied in the analyzed papers. If, on the one hand, the latter can be justified because it aligns with the recent attitude of testing research to substitute random testing with Penetration testing; on the other hand, Configuration testing can be an important means to discover in advance possible setup issues and should be investigated more especially in case of Radio and Network Protocol.
- In general, for all the contributions, the Model-based approach is the most commonly adopted testing strategy. Especially for Network protocol, the percentage of Model-based is 57,14% and is considered the exclusive approach (with a percentage of 100%) for testing Communication Protocol and Routing algorithms. It is also very important for testing the Routing Algorithm of the GPS and the Communication Protocol of the Radio because it was adopted by 40% of the papers analyzed.
- For almost all the contributions, Penetration testing is the second adopted Testing strategy, especially when it is necessary to deal with security issues. Indeed, Penetration testing is considered the exclusive approach (with a percentage of 100%) for assessing the Security Protocol of Radio and Network Protocols and one of the most important (with a percentage of 50%) for the Security Protocol of GPS. Penetration testing is also considered important (with a percentage of 40%) for assessing the Communication Protocol of the Radio.
- For almost all the contributions (Attack surface and specifically its main services), Ad-hoc testing is the third adopted testing strategy, especially for the GPS and Network Protocols. Indeed, the paper authors decided that the tested surface (or its services) has peculiarities too specific to be addressed to the standard testing approach and prefer specific customized proposals. This is the case of the Communication Protocol of GPS and radio (with a percentage of 50% and 20%, respectively). However, the paper's authors do not specifically justify their choice. Therefore, it is unclear if they excluded the application of the standard testing approaches on purpose or because specific knowledge of the available testing strategies is not part of their background.

The detailed analysis confirms the results obtained by the global analysis, i.e., model-based testing is the most adopted approach.

To better investigate the motivation, a deeper analysis has been performed on the 15 papers, over the 36 belonging to the *Drone Cybersecurity Testing* group, that adopt Model-based testing (see Figure 9). Interestingly, results show that 60% of the contributions rely on behavioral or structural models or representations derived by adopting Artificial Intelligence (AI) or Machine Learning applications. Even if they are pertinent to the associated classification, they rely on a loose definition of Model-based testing. Indeed, the model is mainly derived from data collected during a learning period of system execution and does not refer to analysis or design system specification information (i.e., before the execution phase) as required from a more formal definition of model-based testing.

The collected evidence lets reply to RQ2:

The model-based testing specifically based on (AI) or Machine Learning is the main proposal adopted in Drone Cybersecurity testing, followed by Penetration testing, especially when security issues need to be specifically addressed. Most standard testing techniques are almost ignored (or applied without following the standard formal processes), and ad-hoc proposals are often the preferred choices, evidencing a generic lack of basic knowledge about the testing processes and procedures. Finally, *Attack surfaces* (such as *Engines, Onboard cameras, Firewalls*, and *Third-party systems*) and services (*Video control system, Digital rights management*) are almost excluded from the testing activity even if critical, especially from cybersecurity and privacy point of view.

C. REPLY TO RQ3

As reported in Section III RQ3 refers to:

What are the challenges and issues in applying Drone Cybersecurity Testing?.

As already discussed in Section V-B and depicted in Figure 5 because a large portion of the proposals target Communication issues (79,27% considering *Drone* $\leftrightarrow$ *RC* and *Drone* $\leftrightarrow$ *ENV*), is quite natural that also most of the challenges and issues identified in available literature refer to this context. However, as reported in Figure 5 there are solution layers completely ignored by the current state-of-the-art in *Drone Cybersecurity Testing* (such as SW and HW environments) that can represent per se opportunities for future research and testing practical investigations.

Similar analysis can also be performed for the other dimensions of Section V-B; the lack of interest shown by the *Drone Cybersecurity Testing* literature in some of the analysed sub-dimensions does not guarantee an absence of challenges and issues in that area. On the contrary, the ignored topic may represent a source of interesting investigation for avoiding vulnerabilities and possible cyber-attacks. Therefore, considering the *Attack surface* data schematized in Figure 6, further investigations can be necessary for the *Onboard cameras, Engines, Firewalls, Stakeholders,*

TABLE 9. Multimensional evaluation.

				Addressed Testing strategies									
Attack Surface	**N° of papers**	**Main targeted Services**	**Papers per service**	**Model Based**	**Penetration**	**Specification Based analysis**	**Formal Methods**	**Ad-hoc**	**Exploratory**	**Configuration**	**Operational**	**Usage Based**	**Random**
GPS	**10**			25%	16,67%	8,33%	8,33%	16,67%	8,33%	0	8,33%	8,33%	0
		Comm Protocols	1	0	0	0	0	50%	0	0	0	50%	0
		Routing Algorithm	3	40%	20%	20%	0	0	0	0	20%	0	0
		Security Protocols	2	0	50%	0	50%	0	0	0	0	0	0
Radio	**8**			25%	25%	12,5%	0	12,5%	0	0	25%	0	0
		Comm Protocols	5	40%	40%	0	0	20%	0	0	0	0	0
		Routing Algorithm	0	0	0	0	0	0	0	0	0	0	0
		Security Protocols	1	0	100	0	0	0	0	0	0	0	0
Network Protocols	**7**			57,14%	14,28%	0	0	14,28%	0	0	14,28%	0	0
		Comm Protocols	3	100%	0	0	0	0	0	0	0	0	0
		Routing Algorithm	1	100%	0	0	0	0	0	0	0	0	0
		Security Protocols	1	0	100%	0	0	0	0	0	0	0	0

Third-party systems, and *Transponder* while considering the services listed in Figure 7). Considering instead the Service dimension, future research activities can be devoted to *Weather forecasts* and *Digital rights management*.

Finally, focusing on the *Testing objective*, as showcased in Figure 5, considering the *Drone Cybersecurity Testing* papers group sub-dimensions like *Trusted behavior, Tamper-proof, Data Privacy*, and *Trustworthiness* are rarely considered the source of issues and topics such as *Malware, Social network, Ethical values, Law principles, Hardware attacks*, and *Side-channel* and safety completely excluded from the analyzed paper. As for the other dimensions, there is no specific justification for the lack of attention to these cybersecurity aspects considered critical in other IoT domains [52]. Therefore, these topics can be considered opportunities for future research and investigations.

The collected evidence lets reply to RQ3:

The main challenges and issues of Drone Cybersecurity Testing in various dimensions can be summarized in:

- *Software* and *Hardware Environment* for the *Solution Layer*;
- *Stakeholders* and *Third-party systems* for the *Attack Surface*;
- *Digital rights management* and *Video Control Systems* for the *Service*;
- *Data Privacy Trustworthiness Malware, Ethical values, Law principles* for the *Testing objective*.

D. REPLY TO RQ4

As reported in Section III, RQ4 refers to:

Which are the main application domains for drone cybersecurity testing?

As already discussed in Section V-B and depicted in Figure 11, a large portion of the proposals (i.e., the 29,26%) are not focused on any particular domain.

Also, considering, in particular, the proposals focused on *Drone Cybersecurity Testing* group, the situation is almost unchanged: most papers target generic Application domains (66,67%), and only some of them focus on *Security and Surveillance* (11,11%), *Agricultural monitoring* (5,55%), *Search and Rescue Operations* (5,55%), and *Entertainment and education* (5,55%).

The collected evidence lets reply to RQ4:

The main application domains for Drone Cybersecurity Testing are generic and not specifically conceived for a particular location domain.

VII. THREATS TO VALIDITY

The systematic survey has been developed considering the following threats to validity:

- *Initial paper selection*: the query and the procedure for papers' selection could have influenced the obtained results. To reduce this risk, the query was made as generic as possible, and the papers were selected in close agreement between all the authors with a careful inclusion and exclusion process along several iterations adopting, wherever possible, a conservative approach.
- *Source data*: the obtained results could have different behavior in case of depending on the selection of the electronic sources. The four most important digital libraries have been investigated to reduce the risk. Iterations of backward and forward snowballing have also been executed to ensure a very low chance of missing important papers.
- *Classification process*: The defined dimensions and sub-dimensions used in the classification process could have biased the final analysis. The classification items are the commonly used terms and definitions collected from

TABLE 10. Cybersecurity testing papers.

Ref. ID	Solution layer	Application domain
[53]–[55]	Communication Drone↔ENV)	Security and Surveillance
[56]	Communication (Drone↔ENV)	Agricultural monitoring
[27], [57], [58] [30], [59], [60] [61]	Communication (Drone↔ENV)	General purpose
[62]	Communication (Drone↔RC)	Security and Surveillance
[63]	Communication (Drone↔RC)	Entertainment and education
[64]–[66] [15], [67], [68] [69], [70]	Communication (Drone↔RC)	General purpose
[71]	Drone Hardware	Search and Rescue Operations
[72]	Drone Hardware	General purpose
[73]	Drone Software	Vehicular Monitoring
[74]	Drone Software	Search and Rescue Operations
[75]	Drone Software	Photography and Videography
[76]	Drone Software	Goods Delivery
[77]	Drone Software	Entertainment and education
[20], [24], [78] [79]–[81] [82]	Drone Software	General purpose
[83]	Other	General purpose

TABLE 11. Cybersecurity papers.

Ref. ID	Solution layer	Application domain
[33]	Communication (Drone↔ENV)	Entertainment and education
[31], [84], [85]	Communication (Drone↔ENV)	Military use
[86], [87]	Communication (Drone↔ENV)	Goods Delivery
[88], [89]	Communication (Drone↔ENV)	Search and Rescue Operations
[90], [91]	Communication (Drone↔ENV)	Security and Surveillance
[92]–[94]	Communication (Drone↔ENV)	General purpose
[95]	Communication (Drone↔ENV)	Maritime System
[21], [22], [29]	Communication (Drone↔RC)	Military use
[96]–[98] [99]	Communication (Drone↔RC)	Security and Surveillance
[17]	Communication (Drone↔RC)	Vehicular Monitoring
[100]	Communication (Drone↔RC)	Goods Delivery
[101]	Communication (Drone↔RC)	Entertainment and education
[15], [102], [103]	Communication (Drone↔RC)	General purpose
[104], [105]	Drone Hardware	Search and Rescue Operations
[106]	Drone Hardware	Security and Surveillance
[107], [108]	Drone Hardware	General purpose
[109]	Drone Software	Entertainment and education
[110]	Drone Software	Search and Rescue Operations
[111]	Drone Software	Security and Surveillance
[112]	Drone Software	Vehicular Monitoring
[28], [113], [114] [115]–[117]	Drone Software	General purpose
[118]	Other	General purpose

the related works (Section II) analysis. They have been selected through several iterations. However, even if the inclusion of further terms can be evaluated, the current set of dimensions and sub-dimensions is the first generic proposal for further research investigation in the drone environment.

- *Final paper selection*: initial paper selection could be biased by analyzing what is claimed in the abstract, title, and keywords. To mitigate this risk, a second iteration was performed, fully reading the text of the initial paper selection set and excluding those that were completely out of the scope.
- *Paper analysis*: Author knowledge and expertise may have influenced the paper analysis during the classification process. A random assignment of each paper to two authors has been performed to mitigate this issue. Additionally, the third author took the role of arbiter in the classification in case of disagreements.

TABLE 12. Testing papers.

Ref. ID	Solution layer	Application domain
[119]	Communication (Drone↔ENV)	Photography and Videography
[120]	Communication (Drone↔ENV)	Vehicular Monitoring

VIII. CONCLUSION

Considering Cybersecurity Testing as one of the most effective means to assess adequate functional and non-functional quality levels and to prevent and remedy malfunctions, the paper presented a systematic survey of the relative literature in the drone domain. Thus, 82 contributions have been selected from an initial set of 970 and analyzed according to a specific classification procedure. In particular, data collected have been used to reply to four research questions concerning the objectives, the proposals, challenges and issues, and the application domains mainly addressed by the contribution focusing on Cybersecurity Testing. The results of the systematic survey were then illustrated and discussed to identify future research directions.

As a general conclusion, the systematic survey evidenced that the drone application domain is still in continuous evolution, and only partial knowledge of the testing process and procedure is currently transferred in this complex environment. Indeed, loose concepts of model-based testing and penetration testing have been promoted as the main effective means for improving drone quality. Additionally, considering specific cybersecurity peculiarities, such as threats or vulnerability in authorization, privacy, and trustworthiness, only a few are currently addressed in the survey papers. A large margin of improvement is still possible from the technological and theoretical point of view.

Table 10 report Drone Cybersecurity Testing selected papers, Table 11 report Drone Cybersecurity selected papers while Table 12 report Drone Testing selected papers.

REFERENCES

[1] M. Ayamga, S. Akaba, and A. A. Nyaaba, "Multifaceted applicability of drones: A review," *Technol. Forecasting Social Change*, vol. 167, Jun. 2021, Art. no. 120677.

[2] E. Cheng, *Aerial Photography and Videography Using Drones*. Berkeley, CA, USA: Peachpit, 2015.

[3] N. Yanpirat, D. F. Silva, and A. E. Smith, "Sustainable last mile parcel delivery and return service using drones," *Eng. Appl. Artif. Intell.*, vol. 124, Sep. 2023, Art. no. 106631.

[4] M. Javaid, A. Haleem, I. H. Khan, R. P. Singh, R. Suman, and S. Mohan, "Significant features and applications of drones for healthcare: An overview," *J. Ind. Integr. Manage.*, vol. 2022, Sep. 2022, Art. no. 2250024.

[5] I. Bisio, C. Garibotto, H. Haleem, F. Lavagetto, and A. Sciarrone, "A systematic review of drone based road traffic monitoring system," *IEEE Access*, vol. 10, pp. 101537–101555, 2022.

[6] A. Hafeez, M. A. Husain, S. P. Singh, A. Chauhan, M. T. Khan, N. Kumar, A. Chauhan, and S. K. Soni, "Implementation of drone technology for farm monitoring & pesticide spraying: A review," *Inf. Process. Agricult.*, vol. 10, no. 2, pp. 192–203, Jun. 2023.

[7] J. Burgués and S. Marco, "Drone-based monitoring of environmental gases," in *Air Quality Networks: Data Analysis, Calibration & Data Fusion*. Cham, Switzerland: Springer, 2023, pp. 115–137.

[8] F. Steinhäusler and H. V. Georgiou, "Detection of victims with UAVs during wide area search and rescue operations," in *Proc. IEEE Int. Symp. Saf., Secur., Rescue Robot. (SSRR)*, Nov. 2022, pp. 14–19.

[9] G. U. Sai Theja, M. S. Murari, M. F. Singha, R. Patgiri, and A. Choudhury, "A survey on surveillance using drones," in *Proc. 14th Int. Conf. Contemp. Comput.*, Aug. 2022, pp. 250–257.

[10] K. Al-Dosari, Z. Hunaiti, and W. Balachandran, "A review of civilian drones systems, applications, benefits, safety, and security challenges," in *The Effect of Information Technology on Business and Marketing Intelligence Systems* (Studies in Computational Intelligence), vol. 1056, M. Alshurideh, B. H. Al Kurdi, R. Masádeh, H. M. Alzoubi, and S. A. Salloum, Eds. Springer, 2023, pp. 793–812, doi: 10.1007/978-3-031-12382-5_43.

[11] K. Chávez and O. Swed, "Emulating underdogs: Tactical drones in the russia-ukraine war," *Contemp. Secur. Policy*, vol. 44, no. 4, pp. 592–605, Oct. 2023.

[12] E. Athanasopoulos et al., "Blue book: A set cybersecurity roadmaps challenges for researchers policymakers," CyberSec4Europe Consortium, 2022.

[13] B. Kitchenham, "Procedures for performing systematic reviews," *Keele, U.K., Keele Univ.*, vol. 33, pp. 1–26, Jul. 2004.

[14] A. E. Omolara, M. Alawida, and O. I. Abiodun, "Drone cybersecurity issues, solutions, trend insights and future perspectives: A survey," *Neural Comput. Appl.*, vol. 35, no. 31, pp. 23063–23101, Nov. 2023.

[15] Y. Li, J. Pawlak, J. Price, K. Al Shamaileh, Q. Niyaz, S. Paheding, and V. Devabhaktuni, "Jamming detection and classification in OFDM-based UAVs via feature- and spectrogram-tailored machine learning," *IEEE Access*, vol. 10, pp. 16859–16870, 2022.

[16] V. Sihag, G. Choudhary, P. Choudhary, and N. Dragoni, "Cyber4Drone: A systematic review of cyber security and forensics in next-generation drones," *Drones*, vol. 7, no. 7, p. 430, Jun. 2023.

[17] A. Andreou, C. X. Mavromoustakis, J. M. Batalla, E. K. Markakis, and G. Mastorakis, "UAV-assisted RSUs for V2X connectivity using Voronoi diagrams in $6g^+$ infrastructures," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 12, pp. 15855–15865, Dec. 2023.

[18] K. Telli, O. Kraa, Y. Himeur, A. Ouamane, M. Boumehraz, S. Atalla, and W. Mansoor, "A comprehensive review of recent research trends on UAVs," 2023, *arXiv:2307.13691*.

[19] W. Yang, S. Wang, X. Yin, X. Wang, and J. Hu, "A review on security issues and solutions of the Internet of Drones," *IEEE Open J. Comput. Soc.*, vol. 3, pp. 96–110, 2022.

[20] S. Wu, Y. Li, Z. Wang, Z. Tan, and Q. Pan, "A highly interpretable framework for generic low-cost UAV attack detection," *IEEE Sensors J.*, vol. 23, no. 7, pp. 7288–7300, Apr. 2023.

[21] J. Li and J. Liu, "Sum rate maximization via reconfigurable intelligent surface in UAV communication: Phase shift and trajectory optimization," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC)*, Aug. 2020, pp. 124–129.

[22] S. Pohasii, S. Milevskyi, O. Bilotserkivskyi, V. Baranova, I. Ippolitova, and I. Pyvavar, "Cost-effective software and hardware complex to ensure security against unauthorized use of enemy commercial uavs on the combat territory," in *Proc. IEEE 4th KhPI Week Adv. Technol. (KhPIWeek)*, Sep. 2023, pp. 1–6.

[23] B. Ly and R. Ly, "Cybersecurity in unmanned aerial vehicles (UAVs)," *J. Cyber Secur. Technol.*, vol. 5, no. 2, pp. 120–137, Apr. 2021.

[24] A. Baird, H. Pearce, S. Pinisetty, and P. Roop, "Runtime interchange of enforcers for adaptive attacks: A security analysis framework for drones," in *Proc. 20th ACM-IEEE Int. Conf. Formal Methods Models Syst. Design (MEMOCODE)*, Oct. 2022, pp. 1–11.

[25] C. Kumar and S. Mohanty, "Current trends in cyber security for drones," in *Proc. Int. Carnahan Conf. Secur. Technol. (ICCST)*, Hatfield, U.K., Oct. 2021, pp. 1–5.

[26] G. K. Pandey, D. S. Gurjar, H. H. Nguyen, and S. Yadav, "Security threats and mitigation techniques in UAV communications: A comprehensive survey," *IEEE Access*, vol. 10, pp. 112858–112897, 2022.

[27] J. Colter, M. Kinnison, A. Henderson, S. M. Schlager, S. Bryan, K. L. O'Grady, A. Abballe, and S. Harbour, "Testing the resiliency of consumer off-the-shelf drones to a variety of cyberattack methods," in *Proc. IEEE/AIAA 41st Digit. Avionics Syst. Conf. (DASC)*, Sep. 2022, pp. 1–5.

[28] M. Liu, J. Chen, C. Du, and W. Yu, "Design and implementation of parallel simulation system for UAV swarms," in *Proc. WRC Symp. Adv. Robot. Autom. (WRC SARA)*, Aug. 2022, pp. 58–63.

[29] B. D. Deebak and S. O. Hwang, "Intelligent drone-assisted robust lightweight multi-factor authentication for military zone surveillance in the 6G era," *Comput. Netw.*, vol. 225, Apr. 2023, Art. no. 109664.

[30] Q. Abu Al-Haija and A. Al Badawi, "High-performance intrusion detection system for networked UAVs via deep learning," *Neural Comput. Appl.*, vol. 34, no. 13, pp. 10885–10900, Jul. 2022.
[31] N. Mäurer, C. Gentsch, T. Gräupl, and C. Schmitt, "Formal security verification of the station-to-station based cell-attachment procedure of LDACS," in *Proc. 18th Int. Conf. Secur. Cryptography*, 2021, pp. 603–610.
[32] S.-I. Conea and G.-C. Crişan, "Hybrid transportation system using trucks and drones," *Proc. Comput. Sci.*, vol. 225, pp. 3153–3162, Sep. 2023.
[33] Y. Zhi, Z. Fu, X. Sun, and J. Yu, "Security and privacy issues of UAV: A survey," *Mobile Netw. Appl.*, vol. 25, no. 1, pp. 95–101, Feb. 2020.
[34] M. Alwateer, S. W. Loke, and A. M. Zuchowicz, "Drone services: Issues in drones for location-based services from human-drone interaction to information processing," *J. Location Based Services*, vol. 13, no. 2, pp. 94–127, Apr. 2019.
[35] G. Choudhary, V. Sharma, I. You, K. Yim, I.-R. Chen, and J.-H. Cho, "Intrusion detection systems for networked unmanned aerial vehicles: A survey," in *Proc. 14th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2018, pp. 560–565.
[36] R. M. Fouda, "Security vulnerabilities of cyberphysical unmanned aircraft systems," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 33, no. 9, pp. 4–17, Sep. 2018.
[37] J.-P. Yaacoub, H. Noura, O. Salman, and A. Chehab, "Security analysis of drones systems: Attacks, limitations, and recommendations," *Internet Things*, vol. 11, Sep. 2020, Art. no. 100218.
[38] P.-Y. Kong, "A survey of cyberattack countermeasures for unmanned aerial vehicles," *IEEE Access*, vol. 9, pp. 148244–148263, 2021.
[39] E. Adorni, A. Rozhok, R. Revetria, and M. Ivanov, "Literature review on drones used in the surveillance field," in *Proc. Int. MultiConf. Eng. Comput. Scientists*, 2021, pp. 20–22.
[40] S. Iqbal, "A study on UAV operating system security and future research challenges," in *Proc. IEEE 11th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2021, pp. 0759–0765.
[41] L. M. Da Silva, I. G. Ferrão, and K. R. L. J. C. Branco, "A systematic mapping study in intrusion detection system for unmanned aerial vehicles security," in *Proc. Latin Amer. Robot. Symp. (LARS), Brazilian Symp. Robot. (SBR), Workshop Robot. Educ. (WRE)*, 2022, pp. 43–48.
[42] 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, Jan. 2023.
[43] 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, Aug. 2022, Art. no. 102894.
[44] N. Durfey and S. Sajal, "A comprehensive survey: Cybersecurity challenges and futures of autonomous drones," in *Proc. Intermountain Eng., Technol. Comput. (IETC)*, May 2022, pp. 1–7.
[45] P. Sanghavi and H. Kaur, "A comprehensive study on cyber security in unmanned aerial vehicles," in *Proc. 10th Int. Conf. Comput. Sustain. Global Develop. (INDIACom)*, Mar. 2023, pp. 804–811.
[46] M. Adil, H. Song, S. Mastorakis, H. Abulkasim, A. Farouk, and Z. Jin, "UAV-assisted IoT applications, cybersecurity threats, AI-enabled solutions, open challenges with future research directions," *IEEE Trans. Intell. Vehicles*, vol. 9, no. 4, pp. 4583–4605, Apr. 2024.
[47] L. M. S. Bine, A. Boukerche, L. B. Ruiz, and A. A. F. Loureiro, "Connecting Internet of Drones and urban computing: Methods, protocols and applications," *Comput. Netw.*, vol. 239, Feb. 2024, Art. no. 110136.
[48] H. Alqahtani and G. Kumar, "Machine learning for enhancing transportation security: A comprehensive analysis of electric and flying vehicle systems," *Eng. Appl. Artif. Intell.*, vol. 129, Mar. 2024, Art. no. 107667.
[49] P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner, and M. Khalil, "Lessons from applying the systematic literature review process within the software engineering domain," *J. Syst. Softw.*, vol. 80, no. 4, pp. 571–583, Apr. 2007.
[50] C. Wohlin, "Guidelines for snowballing in systematic literature studies and a replication in software engineering," in *Proc. 18th Int. Conf. Eval. Assessment Softw. Eng.*, May 2014, pp. 1–10.
[51] P. Bourque and R. E. Fairley, *Guide To the Software Engineering Body of Knowledge (SWEBOK)*, 3rd ed., Washington, DC, USA: IEEE Comput. Soc. Press, 2014.
[52] P. Williams, I. K. Dutta, H. Daoud, and M. Bayoumi, "A survey on security in Internet of Things with a focus on the impact of emerging technologies," *Internet Things*, vol. 19, Aug. 2022, Art. no. 100564.
[53] G. Bakirtzis, F. Genovese, and C. H. Fleming, "Yoneda hacking: The algebra of attacker actions," *ACM Trans. Cyber-Phys. Syst.*, vol. 6, no. 3, pp. 1–27, Jul. 2022.
[54] M. R. Manesh, J. Kenney, W. C. Hu, V. K. Devabhaktuni, and N. Kaabouch, "Detection of GPS spoofing attacks on unmanned aerial systems," in *Proc. 16th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2019, pp. 1–6.
[55] A. V. Savkin and H. Huang, "Navigation of a UAV network for optimal surveillance of a group of ground targets moving along a road," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 9281–9285, Jul. 2022.
[56] M. Rizwanullah, H. A. Mengash, M. Alamgeer, K. Tarmissi, A. S. A. Aziz, A. A. Abdelmageed, M. I. Alsaid, and M. I. Eldesouki, "Modelling of metaheuristics with machine learning-enabled cybersecurity in unmanned aerial vehicles," *Sustainability*, vol. 14, no. 24, p. 16741, Dec. 2022.
[57] S. Miao, Y. Li, and Q. Pan, "A preliminary study of UAV cyber traffic playback based on SDN," in *Proc. IEEE Int. Symp. Broadband Multimedia Syst. Broadcast. (BMSB)*, Jun. 2023, pp. 1–5.
[58] A. Aldaej, T. A. Ahanger, M. Atiquzzaman, I. Ullah, and M. Yousufudin, "Smart cybersecurity framework for IoT-empowered drones: Machine learning perspective," *Sensors*, vol. 22, no. 7, p. 2630, Mar. 2022.
[59] M. S. B. M. Fadilah, V. Balachandran, P. Loh, and M. Chua, "DRAT: A drone attack tool for vulnerability assessment," in *Proc. 10th ACM Conf. Data Appl. Secur. Privacy*, Mar. 2020, pp. 153–155.
[60] A. R. Svaigen, A. Boukerche, L. B. Ruiz, and A. A. F. Loureiro, "MixDrones: 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.*, Nov. 2021, pp. 181–188.
[61] P. Dhomane and R. Mathew, "Counter-measures to spoofing and jamming of drone signals," *SSRN Electron. J.*, Jan. 2020, doi: 10.2139/ssrn.3774955.
[62] H. Benkraouda, E. Barka, and K. Shuaib, "Cyber-attacks on the data communication of drones monitoring critical infrastructure," *Comput. Sci. Inf. Technol.*, vol. 8, no. 17, pp. 83–93, 2018.
[63] N. Pojsomphong, V. Visoottiviseth, W. Sawangphol, A. Khurat, S. Kashihara, and D. Fall, "Investigation of drone vulnerability and its countermeasure," in *Proc. IEEE 10th Symp. Comput. Appl. Ind. Electron. (ISCAIE)*, Apr. 2020, pp. 251–255.
[64] C. Gudla, M. S. Rana, and A. H. Sung, "Defense techniques against cyber attacks on unmanned aerial vehicles," in *Proc. Int. Conf. Embedded Syst., Cyber-Phys. Syst., Appl. (ESCS)*, in The Steering Committee of The World Congress in Computer Science, 2018, pp. 110–116.
[65] A. Ding, M. Chan, A. Hass, N. O. Tippenhauer, S. Ma, and S. Zonouz, "Get your cyber-physical tests done! Data-driven vulnerability assessment of robotic aerial vehicles," in *Proc. 53rd Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN)*, Jun. 2023, pp. 67–80.
[66] O. Westerlund and R. Asif, "Drone hacking with raspberry-pi 3 and WiFi pineapple: Security and privacy threats for the Internet-of-Things," in *Proc. 1st Int. Conf. Unmanned Vehicle Syst.-Oman (UVS)*, Feb. 2019, pp. 1–10.
[67] F. E. Salamh, U. Karabiyik, M. K. Rogers, and E. T. Matson, "Unmanned aerial vehicle kill chain: Purple teaming tactics," in *Proc. IEEE 11th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2021, pp. 1081–1087.
[68] N. Schiller, M. Chlosta, M. Schloegel, N. Bars, T. Eisenhofer, T. Scharnowski, F. Domke, L. Schönherr, and T. Holz, "Drone security and the mysterious case of DJI's DroneID," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2023, pp. 1–17.
[69] Z. Baig, N. Syed, and N. Mohammad, "Securing the smart city airspace: Drone cyber attack detection through machine learning," *Future Internet*, vol. 14, no. 7, p. 205, Jun. 2022.
[70] M. Shivers, C. Llanes, and M. Sherman, "Implementation of an artificial immune system to mitigate cybersecurity threats in unmanned aerial systems," in *Proc. IEEE Int. Conf. Ind. Internet (ICII)*, Nov. 2019, pp. 12–17.
[71] S.-Y. Chang, K. Park, J. Kim, and J. Kim, "Towards securing uav flying base station: Misplacement impact analyses on battery and power," in *Proc. Syst. Netw. Telemetry Anal.*, 2023, pp. 3–8.
[72] Z. Feng, N. Guan, M. Lv, W. Liu, Q. Deng, X. Liu, and W. Yi, "An efficient UAV hijacking detection method using onboard inertial measurement unit," *ACM Trans. Embedded Comput. Syst.*, vol. 17, no. 6, pp. 1–19, Nov. 2018.
[73] K. Han, "Employing automotive security to improve the security of unmanned aerial vehicles," *Frontiers Commun. Netw.*, vol. 4, May 2023, Art. no. 1122231.
[74] V. U. Ihekoronye, S. O. Ajakwe, D.-S. Kim, and J. M. Lee, "Cyber edge intelligent intrusion detection framework for UAV network based on random forest algorithm," in *Proc. 13th Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2022, pp. 1242–1247.

[75] F. Kateb and M. Ragab, "Archimedes optimization with deep learning based aerial image classification for cybersecurity enabled UAV networks," *Comput. Syst. Sci. Eng.*, vol. 47, no. 2, pp. 2171–2185, 2023.
[76] V. Dey, V. Pudi, A. Chattopadhyay, and Y. Elovici, "Security vulnerabilities of unmanned aerial vehicles and countermeasures: An experimental study," in *Proc. 31st Int. Conf. VLSI Design 17th Int. Conf. Embedded Syst. (VLSID)*, Jan. 2018, pp. 398–403.
[77] J. Gabrielsson, J. Bugeja, and B. Vogel, "Hacking a commercial drone with open-source software: Exploring data privacy violations," in *Proc. 10th Medit. Conf. Embedded Comput. (MECO)*, Jun. 2021, pp. 1–5.
[78] N. Syed, M. A. Khan, N. Mohammad, G. B. Brahim, and Z. Baig, "Unsupervised machine learning for drone forensics through flight path analysis," in *Proc. 10th Int. Symp. Digit. Forensics Secur. (ISDFS)*, Jun. 2022, pp. 1–6.
[79] I. Pekaric, D. Arnold, and M. Felderer, "Simulation of sensor spoofing attacks on unmanned aerial vehicles using the gazebo simulator," in *Proc. IEEE 22nd Int. Conf. Softw. Qual., Rel., Secur. Companion (QRS-C)*, Dec. 2022, pp. 44–53.
[80] C. S. Veerappan, P. L. K. Keong, V. Balachandran, and M. S. B. M. Fadilah, "DRAT : A penetration testing framework for drones," in *Proc. IEEE 16th Conf. Ind. Electron. Appl. (ICIEA)*, Aug. 2021, pp. 498–503.
[81] K. Das, C. Ghosh, and R. Karmakar, "Eavesdropping attack detection in UAVs using ensemble learning," in *Proc. 2nd Int. Conf. Electr., Electron., Inf. Commun. Technol. (ICEEICT)*, Apr. 2023, pp. 01–07.
[82] A. Ossamah, "Blockchain as a solution to drone cybersecurity," in *Proc. IEEE 6th World Forum Internet Things (WF-IoT)*, Jun. 2020, pp. 1–9.
[83] R. Guo, B. Wang, and J. Weng, "Vulnerabilities and attacks of UAV cyber physical systems," in *Proc. Int. Conf. Comput., Netw. Internet Things*, Apr. 2020, pp. 8–12.
[84] P. Tedeschi, S. Sciancalepore, and R. Di Pietro, "ARID: Anonymous remote identification of unmanned aerial vehicles," in *Proc. Annu. Comput. Secur. Appl. Conf.*, Dec. 2021, pp. 207–218.
[85] R. Restituyo and T. Hayajneh, "Vulnerabilities and attacks analysis for military and commercial IoT drones," in *Proc. 9th IEEE Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, Nov. 2018, pp. 26–32.
[86] F. Kong, B. Jiang, J. Wang, H. Wang, and H. Song, "Collaborative delivery optimization with multiple drones via constrained hybrid pointer network," *IEEE Internet Things J.*, vol. 11, no. 5, pp. 7739–7755, Mar. 2024.
[87] W. Najy, C. Archetti, and A. Diabat, "Collaborative truck-and-drone delivery for inventory-routing problems," *Transp. Res. C, Emerg. Technol.*, vol. 146, Jan. 2023, Art. no. 103791.
[88] A. A. Ahmed, A. Olumide, A. Akinwa, and M. Chouikha, "Constructing 3D maps for dynamic environments using autonomous UAVs," in *Proc. 16th EAI Int. Conf. Mobile Ubiquitous Syst., Comput., Netw. Services*, Nov. 2019, pp. 504–513.
[89] T. Nguyen, R. Katila, and T. N. Gia, "An advanced Internet-of-Drones system with blockchain for improving quality of service of search and rescue: A feasibility study," *Future Gener. Comput. Syst.*, vol. 140, pp. 36–52, Mar. 2023.
[90] L. Fu, P. T. Morón, J. P. Queralta, D. Hästbacka, H. Edelman, and T. Westerlund, "Is Alice really in wonderland? UWB-based proof of location for UAVs with hyperledger fabric blockchain," in *Proc. Int. Conf. FinDrones*. Cham, Switzerland: Springer, 2023, pp. 43–56.
[91] 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 (SP)*, May 2021, pp. 1434–1451.
[92] S. A. Ali, E. A. Mehrzi, A. A. Shamsi, S. A. Zaabi, K. A. Hemieri, and N. Ababneh, "Designing a secure and reliable emergency drone," in *Proc. 5th Int. Conf. Data Storage Data Eng. (DSDE)*, Feb. 2022, pp. 119–124.
[93] A. R. Sadik, B. Bolder, and P. Subasic, "A self-adaptive system of systems architecture to enable its ad-hoc scalability: Unmanned vehicle fleet–mission control center case study," in *Proc. 7th Int. Conf. Intell. Syst., Metaheuristics Swarm Intell.*, Apr. 2023, pp. 111–118.
[94] M. A. Lopez, M. Baddeley, W. T. Lunardi, A. Pandey, and J.-P. Giacalone, "Towards secure wireless mesh networks for UAV swarm connectivity: Current threats, research, and opportunities," in *Proc. 17th Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS)*, Jul. 2021, pp. 319–326.
[95] D. Dghaym, T. S. Hoang, S. R. Turnock, M. Butler, J. Downes, and B. Pritchard, "An STPA-based formal composition framework for trustworthy autonomous maritime systems," *Saf. Sci.*, vol. 136, Apr. 2021, Art. no. 105139.
[96] A. S. Nair and S. M. Thampi, "PUFloc: PUF and location based hierarchical mutual authentication protocol for surveillance drone networks," in *Proc. Int. Conf. Ubiquitous Secur.* Cham, Switzerland: Springer, 2021, pp. 66–89.
[97] A. Islam, K. Sadia, M. Masuduzzaman, and S. Y. Shin, "BUMAR: A blockchain-empowered UAV-assisted smart surveillance architecture for marine areas," in *Proc. Int. Conf. Comput. Advancements*, Jan. 2020, pp. 1–5.
[98] Y.-M. Kwon, J. Yu, B.-M. Cho, Y. Eun, and K.-J. Park, "Empirical analysis of MAVLink protocol vulnerability for attacking unmanned aerial vehicles," *IEEE Access*, vol. 6, pp. 43203–43212, 2018.
[99] G. Cho, J. Cho, S. Hyun, and H. Kim, "SENTINEL: A secure and efficient authentication framework for unmanned aerial vehicles," *Appl. Sci.*, vol. 10, no. 9, p. 3149, Apr. 2020.
[100] D. Mourtzis, J. Angelopoulos, and N. Panopoulos, "Unmanned aerial vehicle (UAV) path planning and control assisted by augmented reality (AR): The case of indoor drones," *Int. J. Prod. Res.*, vol. 62, no. 9, pp. 3361–3382, May 2024.
[101] G. Karmakar, M. Petty, H. Ahmed, R. Das, and J. Kamruzzaman, "Security of Internet of Things devices: Ethical hacking a drone and its mitigation strategies," in *Proc. IEEE Asia–Pacific Conf. Comput. Sci. Data Eng. (CSDE)*, Dec. 2022, pp. 1–5.
[102] Y. Hashem, E. Zildzic, and A. Gurtov, "Secure drone identification with hyperledger iroha," in *Proc. 11th ACM Symp. Design Anal. Intell. Veh. Netw. Appl.*, Nov. 2021, pp. 11–18.
[103] D. Chulerttiyawong and A. Jamalipour, "Sybil attack detection in Internet of flying things-IoFT: A machine learning approach," *IEEE Internet Things J.*, vol. 10, no. 14, pp. 12854–12866, Jul. 2023.
[104] J. Chen, Y. Zhang, J. Li, W. Du, Z. Chen, Z. Liu, H. Wang, and V. C. M. Leung, "Integrated air-ground vehicles for UAV emergency landing based on graph convolution network," *IEEE Internet Things J.*, vol. 9, no. 12, pp. 9106–9116, Jun. 2022.
[105] M. A. R. Estrada and A. Ndoma, "The uses of unmanned aerial vehicles—UAV's- (or drones) in social logistic: Natural disasters response and humanitarian relief aid," *Proc. Comput. Sci.*, vol. 149, pp. 375–383, Jun. 2019.
[106] Z. Fu, Y. Zhi, S. Ji, and X. Sun, "Remote attacks on drones vision sensors: An empirical study," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 5, pp. 3125–3135, Sep. 2022.
[107] G. Sternharz, J. Skackauskas, A. Elhalwagy, A. J. Grichnik, T. Kalganova, and M. N. Huda, "Self-protected virtual sensor network for microcontroller fault detection," *Sensors*, vol. 22, no. 2, p. 454, Jan. 2022.
[108] J. Kim, W.-H. Ko, and P. R. Kumar, "Cyber-security through dynamic watermarking for 2-rotor aerial vehicle flight control systems," in *Proc. Int. Conf. Unmanned Aircr. Syst. (ICUAS)*, Jun. 2021, pp. 1277–1283.
[109] A. Raja, J. Galvan, Y. Li, and J. Yuan, "UCLP: A novel UAV cybersecurity laboratory platform," in *Proc. 22st Annu. Conf. Inf. Technol. Educ.*, Oct. 2021, pp. 23–28.
[110] T. Nguyen, R. Katila, and T. N. Gia, "A novel Internet-of-Drones and blockchain-based system architecture for search and rescue," in *Proc. IEEE 18th Int. Conf. Mobile Ad Hoc Smart Syst. (MASS)*, Oct. 2021, pp. 278–288.
[111] A. S. Mohammed, A. Abul Hasanaath, A. Moinuddeen, and N. Mohammad, "A comparative study of drone forensic tools and techniques," in *Proc. Int. Conf. Intell. Data Commun. Technol. Internet Things (IDCIoT)*, Jan. 2023, pp. 752–758.
[112] S. Horovitz, I. Zexer, and B. Ganot, "UAVDome—Safe UAV transportation," in *Proc. IEEE 7th Int. Conf. Intell. Transp. Eng. (ICITE)*, Nov. 2022, pp. 214–222.
[113] M.-Á. Fas-Millán, F. Soro, O. Jung, and A. Shaaban, "Cybersecurity analysis in the UAV domain: The practical approach of the labyrinth project," in *Proc. ACM Conf. Inf. Technol. Social Good*, Sep. 2023, pp. 446–454.
[114] R. Nouacer, M. Hussein, P. Detterer, E. Villar, F. Herrera, C. Tieri, and E. Grolleau, "Towards a European network of enabling technologies for drones," in *Proc. DroneSE RAPIDO, Syst. Eng. Constrained Embedded Syst.*, 2023, pp. 1–11.
[115] E. Mantas and C. Patsakis, "Who watches the new watchmen? The challenges for drone digital forensics investigations," *Array*, vol. 14, Jul. 2022, Art. no. 100135.
[116] T. Ojo, H. Chi, and S. K. Erskine, "Unmanned aerial vehicle forensics investigation performance under different attacks," in *Proc. Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, Dec. 2022, pp. 958–964.

[117] A. Shafique, A. Mehmood, and M. Elhadef, "Detecting signal spoofing attack in UAVs using machine learning models," *IEEE Access*, vol. 9, pp. 93803–93815, 2021.
[118] A. R. Svaigen, A. Boukerche, L. B. Ruiz, and A. A. F. Loureiro, "Security in the industrial Internet of Drones," *IEEE Internet Things Mag.*, vol. 6, no. 3, pp. 110–116, Sep. 2023.
[119] E. Shaikh, N. Mohammad, and S. Muhammad, "Model checking based unmanned aerial vehicle (UAV) security analysis," in *Proc. Int. Conf. Commun., Signal Process., their Appl. (ICCSPA)*, Mar. 2021, pp. 1–6.
[120] D. Mourtzis, J. Angelopoulos, and N. Panopoulos, "Unmanned aerial vehicle (UAV) manipulation assisted by augmented reality (AR): The case of a drone," *IFAC-PapersOnLine*, vol. 55, no. 10, pp. 983–988, 2022.

EDA MARCHETTI received the degree (summa cum laude) in computer science and the Ph.D. degree from the University of Pisa. She is currently a Senior Researcher with CNR-ISTI. She has been responsible for CNR-ISTI of several national and international EU projects and actively participated in more than 20 national and international projects. Her research interests include software testing in general and, in particular, on introducing novel methodologies for testing emerging software technologies, cybersecurity, value-based, and ethical aspects. Her research topics include security and privacy testing, testing of access control systems, model-based testing, SOA and component-based testing, requirement management and assessment, monitoring business process, human-centric testing process management and scheduling, operational and structural testing, interoperability testing, domain-specific testing, product certification, and assessment.

TAUHEED WAHEED received the master's degree in software engineering from Bahria University, Islamabad, in 2017. He is currently pursuing the Ph.D. degree in cybersecurity for complex systems with the University of Pisa. He is a Research Associate with CNR. His research interests include cybersecurity, software engineering, requirements engineering, and software testing.

ANTONELLO CALABRÒ received the degree in computer science engineering. He is currently a Researcher with CNR-ISTI. He participated in different roles for CNR-ISTI to several national and international EU projects and actively participated in more than 15 national and international projects. His research interests include designing and developing smart monitoring infrastructure, responsive and adaptable complex event processing, and cybersecurity assessment. His research activities have been applied to several application domains, such as smart environments, SoSs, the IoT, vehicular networks, emerging technologies, and UAVs.

Open Access funding provided by 'Consiglio Nazionale delle Ricerche-CARI-CARE-ITALY' within the CRUI CARE Agreement