Contingency Clarification Protocols for Reliable Counter-Drone Operation

ABDULHADI SHOUFAN, Member, IEEE
ERNESTO DAMIANI, Senior Member, IEEE
Khalifa University, Abu Dhabi, UAE

Counter-drone technology plays a vital role in protecting airspace against unwanted and malicious drones. Counter-drone systems increasingly rely on unmanned traffic management services, such as remote identification and flight authorization enforcement, for the detection and mitigation of unauthorized activities on the part of unmanned aerial vehicles (UAVs). These services support automated drone identification and verification of the drone activity's compliance before taking any enforcement action. Available drone identification standards, such as ASTM F3411-22 for drone remote identification (DRI), specify key requirements for entities involved in UAV operations. However, DRI systems can fail for many technical and nontechnical reasons related to the drone itself, its operator, the identification system, other involved service suppliers, or the communication between these actors. On the other hand, experience has shown that even licensed drone operators can violate permitted flight parameters mistakenly or for unavoidable reasons. In such contingency situations, the counter-drone system should perform additional checks and interact with relevant agents before classifying the drone as illegal and taking action against it. This article presents a set of protocols to formalize the interaction between the counter-drone system and relevant agents to clarify possible failures and violations. The goal is to complement current DRI systems mitigating the effect of erroneous drone identification and supporting reliable decision-making. The simulation of worst-case scenarios shows that executing the clarification protocols takes just a few seconds, and this delay is only notable in situations where immediate action is required to neutralize illegal drones.

Manuscript received 12 April 2023; revised 11 July 2023; accepted 3 September 2023. Date of publication 11 September 2023; date of current version 8 December 2023.

DOI. No. 10.1109/TAES.2023.3313573

Refereeing of this contribution was handled by G. Chen.

This work was supported by the Khalifa University through the Center of Cyber-Physical Systems.

Authors' addresses: Abdulhadi Shoufan and Ernesto Damiani are with the Center of Cyber-Physical Systems, Khalifa University, Abu Dhabi 127788, UAE, E-mail: (abdulhadi.shoufan@ku.ac.ae; ernesto.damiani@ku.ac.ae). *(Corresponding author: Abdulhadi Shoufan.)*

I. INTRODUCTION

The market of unmanned aerial vehicles (UAVs), popularly known as *drones*, is rapidly growing with diverse applications in construction, agriculture, insurance, the oil and gas industry, film-making, parcel delivery, journalism, law enforcement, and civil defense [32]. Despite this, the management of UAVs operation in urban areas is still in the exploratory stage [59]. We can neither get our online orders delivered by drones nor ride a taxi drone, although today's UAVs are technically ready for such applications [25]. Indeed, flying a drone is associated with security, privacy, and safety threats that challenge the penetration of UAVs in the urban airspace [10], [33]. Safety is, without doubt, a critical aspect of drone operation. Worldwide reports on drone incidents and intrusions highlight the criticality of this issue [26], [27].

Counter-drone technology [also referred to as *counter-unmanned aerial systems* (CUAS)] plays a vital role in protecting the airspace against unwanted and malicious drones. Fig. 1 shows the two main functions of a typical counter-drone system: detection & classification and interdiction. For detecting and classifying drones, different technologies, such as radar, optical systems, and acoustic sensors, are used followed by signal processing systems and machine learning [12], [50]. Similarly, a wide range of interdiction solutions are available, such as jamming, catching, or shooting [35], [43].

Unmanned traffic management (UTM) services, such as drone remote identification (DRI), can make counter-drone operations more effective [39]. When connected to a UTM, the counter-drone system can identify a drone and verify its flight authorization in the 4-D space of interest, as shown in Fig. 2. Instead of classifying all sighted drones as unwanted, the counter-drone system can now differentiate between legal and illegal UAV operations. This allows for controlled drone use in or close to sensitive areas.

Some preliminary work has been done on standards for DRI, including the European EN 4709-002:2020 [14] and the US ASTM F3411-22 [15]. The latter provides a partial list of the entities involved in drone operation, such as the UAVs, their operators, and the *observers*, which include antidrone enforcement systems. Furthermore, DRI proposals encourage the establishment of international *UAV registries* enabling observers to use remote identification messages broadcasted by UAVs to access trustworthy information about the drone and their operators. The proposed standards, however, do not cover *contingency* situations.

Contingency planning and management is an essential objective of drone operations [22]. Altun et al. [11] classified contingency hazards in unmanned aircraft systems into five categories: technical failures, human-related failures, data-related issues, infrastructure-based failures, and environmental events. Technical failures primarily affect drone operation and cause malfunctions, such as loss-of-link, GPS failure, navigation degradation, camera failures, and engine and power failures. Human-related failures essentially stem from the performance of pilots due to distractions for the

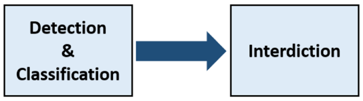

Fig. 1. Conventional counter-drone system.

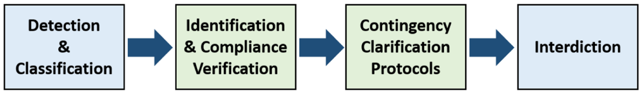
Detection & Classification
Identification & Compliance Verification
Contingency Clarification Protocols
Interdiction

Fig. 2. UTM-enhanced counter-drone system with proposed contingency clarification protocols.

pilot in command, medical issues, perception, and decision errors. Data-related problems can arise from cyberattacks or the provision of inaccurate or delayed geofence data, weather, or terrain data. Infrastructure-based failures often affect vertiports and lead to availability issues, surface contamination, or debris that may interfere with takeoff or landing. Environmental events, such as adverse weather conditions, volcano eruptions, air pollution, and bird strikes, can cause contingency situations [11].

Several authors addressed contingency planning and management. For example, Pang et al. [38] proposed an approach to estimate the UAV trajectory by utilizing the extended Kalman filter when the drone loses the GPS signal. Various machine vision-based methods for self-localization and autonomous landing in emergency cases were presented [40], [54]. Also, several authors addressed lost-link situations, e.g., when the drone loses its Internet connection, and proposed solutions that allow the drone to complete the mission [4], [61]. In addition to such reactive solutions to specific contingency issues, several authors proposed architectures and frameworks to automate contingency management and integrate it into UTM systems, e.g., [16], [21], and [52].

This previous research has focused solely on the operational aspect of contingency management and failed to consider the influence of contingencies on the decision-making process of counter-drone systems. Indeed, various technical, human-related, infrastructural, data-related failures, as well as environmental events can cause a drone to appear unlawful to a CUAS, leading to an incorrect neutralization decision. For example, the following holds.

1) UAVs can fail to broadcast their remote identification messages permanently or temporarily.
2) The remote identification receiver of the CUAS system can fail to receive or decode drone self-identification.
3) UTM service providers can fail to update relevant registries or to do this on time.
4) Communication with UTM services can fail for technical reasons.
5) UAV operators can exceed the permitted flight time by mistake or for an urgent reason.
6) UAV operators can deviate from the approved mission trajectory by mistake or for admissible *force majeure* reasons, e.g., direct danger to humans.

These examples suggest that counter-drone systems may interpret contingency situations as violations although this is not necessarily the case. For reliable enforcement decisions, counter-drone systems should be able to disambiguate these cases and clarify them, as illustrated in Fig. 2.

The clarification of contingency situations is a complex task that requires checks beyond the scope or control of counter-drone systems. For instance, if a counter-drone system detects a UAV that does not broadcast its identification messages, the system has no means to verify whether this issue is due to noncompliance with regulations or just because of a technical failure. Indeed, clarifying the reason for the missing identification is essential for performing a correct classification of the drone and deciding whether action should be taken against.

This article presents a set of protocols that can help counter-drone systems to solve ambiguity issues related to drone identification and authorization. Our solution leverages the information provided by UTM services and enables counter-drone systems to interact with relevant entities to remove ambiguities about detected drones. We claim that disambiguation facilitates the accurate classification of drones and supports informed and accountable action against illegal ones. While indispensable for airspace and public safety, counter-drone systems are sensitive and controversial [20]. Improving their performance is crucial for its acceptance and wide deployment. The clarification protocols proposed in this article present an important step toward this goal.

The rest of this article is organized as follows. Section II describes the related work. Section III specifies the requirements for the clarification protocols. Section IV describes the protocols in detail. Section V describes the implementation and evaluation of the proposed protocols. Finally, Section VII concludes this article.

II. Related Work

A. UTM Systems

The concept of UTM refers to an ecosystem for controlling the operation of unmanned aerial systems [30], [59]. Data exchange is at the core of UTM where authorized unmanned service suppliers (USS) provide cloud-based services to different stakeholders. Examples of these services include UAV control [60], efficient and fair unmanned traffic control [24], flight planning and scheduling [8], [51], geofencing [48], path optimization and collision avoidance [23], weather and contingency management [36], [42], orchestrating of UAV services [18], and supporting the Internet of Drones [9].

Civil aviation authorities are making use of UTMs to introduce and support regulations. Two well-known examples include remote identification and automatic authorization [19]. The European Union Aviation Safety Agency has published the Commission Delegated Regulation (EU) 2020/1058 that mandates the equipment of drones with a remote identification system [3]. Similarly, the FAA in the

USA published a final rule for remote identification in January 2021 [2]. According to this rule, the remote identification message should contain information about the drone's identity, location, altitude, velocity, the control station's location and elevation, a time mark, and emergency status. A database with remote ID information should provide three levels of access. Level 1 includes public information, such as the UAS unique identifier. Level 2 provides information to designated public safety and airspace management officials, e.g., information about the drone owner. Level 3 contains information relevant to the aviation authority and certain federal, state, and local agencies, e.g., tracking data. On the other hand, the FAA has implemented a system referred to as Low Altitude Authorization and Notification Capability (LAANC) [29]. This system automates the application and approval process for airspace authorizations. Its operation goes as follows: the drone pilot submits a request through an LAANC USS. The request is checked against multiple airspace data sources by the FAA. If approved, the pilot receives the authorization in near real time.

UTM systems are still in their infancy. Some authors have highlighted key challenges and issues in the design of these systems. Wolter et al. [57] pointed out multiple obstacles in the current experimental setups, which relate to standardization, information quality, and the transition from human-centric design to automation. Other authors addressed the security of UTM systems and presented their vulnerabilities to various cyber and physical attacks [7], [9], [47]. The lack of a consistent legal framework for UTM system operations was highlighted in [44]. The authors described the fundamentals of such a legal framework that should provide the needed certainty for all stakeholders.

B. Counter-Drone Systems

The counter-drone industry has boomed in recent years. A report published by the "Center for the Study of the Drone" at Bard College shows that there are 537 CUAS on the market [34]. Researchers showed wide interest in this field, especially regarding the detection and classification of small UAVs.

Counter-drone systems can use a variety of technologies for drone detection and classification [56]: radar [28], acoustic detectors [12], computer vision [31], and radio frequency [5]. Each technology has its advantages and disadvantages. For example, low-cost frequency-modulated continuous wave radars are highly resistant to fog, cloud, and dust, and they do not require line of sight. However, their effectiveness in detecting drones is limited due to the small radar cross sections of drones. Acoustic detectors, such as microphone arrays, are cost effective and do not require line of sight. However, they are sensitive to ambient noise and wind conditions, and they require a comprehensive database of acoustic signatures for different types of drones. Computer vision-based detection can utilize low-cost camerassuch as CCTVs, and leverage deep learning techniques for classification. However, computer vision detectors require line of sight, and their performance can be affected by adverse weather conditions, such as dust, fog, cloud, and daytime lighting unless thermal or laser-based cameras are employed. On the other hand, radio frequency-based detectors employ low-cost sensors and do not require line of sight, offering long-range capabilities. However, they are not effective for drones operating in autonomous mode since these drones are typically not controlled using radio frequency signals. In critical areas, a combination of multiple technologies, known as multimodal technologies, can be utilized to complement each other's strengths and weaknesses [45].

Parallel to the advances in detection and classification technologies, researchers investigated technical solutions for drone interdiction. Wyder et al. [58] classified these technologies according to their impact on the target drone, coming up with three main categories: signal interception, propeller restriction, and aerial takedown. Due to its undisruptive nature, signal interception has received substantial attention for UAV interdiction in urban areas. Depending on the operation mode of the drone, Roth et al. [43] identified two methods of signal interception-based interdiction: drone hacking and GPS spoofing. Propeller restriction refers to capturing uncooperative drones, usually by using a net. The net is launched either manually by a skilled operator on the ground or autonomously by another flying drone [13]. Finally, a variety of aerial takedown technologies was presented. These include hunting by eagles [37] and shooting by machine guns or laser [43].

C. Coordination Between UTM and Counter-Drone Systems

Despite the close relation between UTM services and counter-drone systems, interoperability between these systems remained unaddressed in the literature. Recently, Park et al. [39] presented a comprehensive review of counter-drone systems and highlighted the necessity of integrating DRIs and counter-drone systems. Sandor [46] highlighted the need to define the problems, the scope, and the operational environment of UTMs. The author defined and classified many functions related to UTM and interestingly listed surveillance among key UTM services, mentioning a panoply of technologies for the detection of cooperative and noncooperative vehicles. However, the author did not mention interdiction, a critical function of a counter-drone system. Apart from this, we are not aware of any literature that has addressed counter-drone operations in a UTM context.

III. REQUIREMENT SPECIFICATION

In this section, we first describe the functional requirements for the clarification protocols highlighting the problems to be resolved and the clarification outcomes. Based on the functional requirements, the essential technical requirements for executing the protocols are identified. Finally, the performance requirements for the protocols are specified.

A. Functional Requirements

The clarification protocols work based on the following assumptions.

1) All drones must be registered and operated by certified pilots.
2) Any drone in flight must broadcast remote identification as per regulations.
3) Any drone flying in the operation zone of a CUAS is required to have authorization. The authorization data should contain information about the drone ID and the mission's date, time, and path.
4) Remote identification and authorization data must be accessible through registries.

The contingency clarification protocols address the following cases.

1) The CUAS receives no remote identification.
2) The CUAS receives an unknown remote identification.
3) The CUAS receives an expired remote identification.
4) The CUAS finds no flight authorization data for the drone.
5) The CUAS observes a violation of the authorized flight time.
6) The CUAS observes deviation from the authorized flight path or zone.

The execution of the clarification protocol should lead to one of three alternative decisions, given as follows.

1) Tolerate the drone violation or noncompliance.
2) Interdict/disable the drone immediately.
3) Interdict/disable the drone after a timeout.

The type of enforcement action (immediate or after a timeout) depends on the risk associated with violation or noncompliance. In particular, in the case of low risk, the operator can be granted a grace period to stop the operation and land the drone safely.

Furthermore, to support accountability in counter-drone operations, the system should meet two additional requirements, given as follows.

1) Any enforcement decision should be taken by a central authority, e.g., civil aviation authority.
2) The decision should be legally disputable through a court.

B. Technical Requirements

To meet the functional requirements specified above, the following technical provisions are needed.

1) In addition to detection, tracking, and interdiction technologies, the CUAS should include technology for receiving and analyzing UAVs' remote identification messages.
2) The CUAS should have access to a DRI registry that maintains drone identification information.

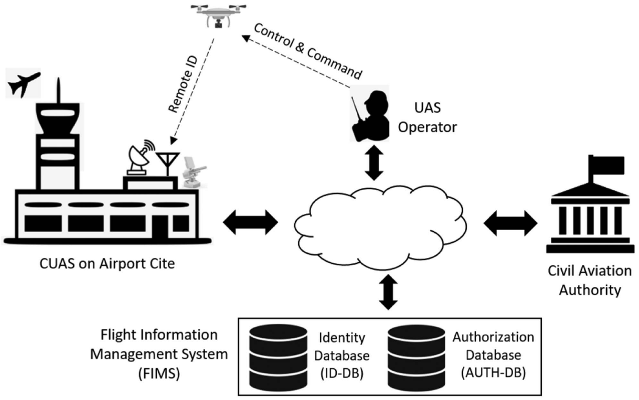
Remote ID
Control & Command
UAS Operator
CUAS on Airport Cite
Civil Aviation Authority
Flight Information Management System (FIMS)
Identity Database (ID-DB)
Authorization Database (AUTH-DB)

Fig. 3. CUAS system integrated into a UTM system.

3) The identification database should be kept up-to-date by the authority or any authorized agent. Legacy/expired IDs shall be marked as such, but not removed from the database.
4) The CUAS should have access to a database that maintains information about authorized missions in the CUAS's area of interest.
5) The authorization database (AUTH-DB) should be kept up-to-date by the authority or any authorized agent.
6) The CUAS needs a communication link with the authority.
7) During the flight, drone operators need to be connected to the Internet and respond to authority inquiries immediately.

Fig. 3 illustrates the CUAS connected to the authority and the flight information management system (FIMS). The FIMS includes an identity database (ID-DB) and an AUTH-DB. To execute the clarification protocols, the CUAS system should be granted access to ID-DB at level 2 or 3, depending on the authority of these systems, see Section II-A. We further assume that the ID-DB database is available and protected against security attacks so that the CUAS can use it to verify the authenticity of a received remote ID.

Furthermore, we suppose that mission authorizations are logged in the AUTH-DB. Database and include information about the drone ID and the mission date, time, path, or zone. The counter-drone system should have access to the AUTH-DB to verify the authorization of a detected drone. The AUTH-DB database must be protected against security attacks.

The effective range of the proposed detection and identification system is primarily determined by the remote identification technology employed onboard the drone. Present regulations in many countries mandate the use of standard WiFi or Bluetooth technology for broadcasting the remote ID, resulting in a limited identification range of a few hundred meters. However, the ASTM standard introduces network-based remote identification, eliminating this limitation in areas with adequate mobile network coverage. Regarding detection and classification capabilities, the range

TABLE I
Outcomes of Protocol 1 (Clarify Missing ID Transmission)

	Operator Response	Risk Assessment	Authority Response to Operator	Authority Response to CUAS
CASE 1	No response	No	NA	Authorize immediate interdiction
CASE 2	I am not flying	No	NA	Authorize immediate interdiction
CASE 3	I am already transmitting my ID	Yes	Order mission completion or stop	Order mission tolerance or authorize timed interdiction
CASE 4	I am not able to restore ID	Yes	Order mission completion or stop	Order mission tolerance or authorize timed interdiction
CASE 5	I restored ID transmission	No	NA	Verify ID restoration
CASE 6	Unconfirmed ID restoration	Yes	Order mission completion or stop	Order mission tolerance or authorize timed interdiction

depends on the sophistication of the technology utilized. Advanced radar systems, for instance, can detect small drones at distances of up to 10 km [1].

C. Performance Requirements

The overall architecture shown in Fig. 3 allows the CUAS to access the UTM databases and interact with relevant agents to clarify contingency cases. Executing the clarification protocols is associated with computation and communication overhead that can delay the CUAS's response to malicious drones. Therefore, we define the *minimum delay* as a principal nonfunctional requirement for the proposed clarification protocols.

IV. PROTOCOL DESCRIPTION

In this section, we describe the clarification protocols in detail. We first outline the contingency case that initiates the respective protocol. Then, we explain its functionality using a table to summarize the protocol outcomes and sequence diagrams that illustrate the messaging, as far as needed. The messages are highlighted in capital letters in the text.

A. Protocol 1—Clarify Missing Remote Identification

The objective of this protocol is to clarify the situation when the CUAS detects a drone but does receive a remote identification from it. In this case, the CUAS queries the AUTH-DB to verify if there is an authorization for *any* mission in the current time and zone. If this is the case, the CUAS extracts the identity of the operator of the authorized mission. We call this a *potential operator* of the sighted drone. The goal of Protocol 1 is to verify whether this potential operator is the actual operator. The CUAS initiates this protocol by sending a message called NO ID BUT POTENTIAL OPERATOR to the authority. This message includes the ID of the potential operator. The authority sends a CHECK/RESTORE ID TRANSMISSION message to the potential operator and receives one of four responses or no response as outlined in Table I (CASE 1 to CASE 5). Next, we describe how to treat each of these cases as well as CASE 6 that occurs when the CUAS does not confirm ID restoration in response to CASE 5.

In the case of no response (CASE 1) or when the operator confirms that he or she is not flying (CASE 2), the authority may have no possibility for further checks. Hence, it sends an INTERDICT IMMEDIATELY message to the CUAS. The latter performs the interdiction and reports this to the authority. The authority may investigate the case, issue a fine, or file a lawsuit case if needed, see Fig. 4.

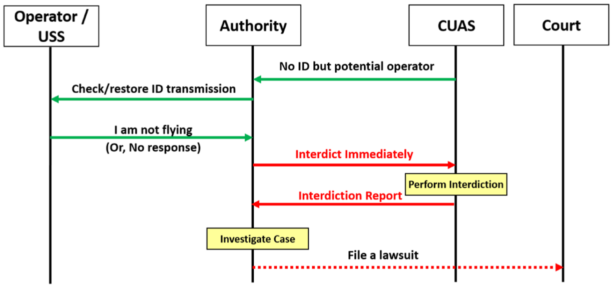

Fig. 4. Protocol 1 (CASE 1 and CASE 2). The CUAS does not receive an ID from the detected drone. The drone operator either does not respond or confirms that he/she is not flying.

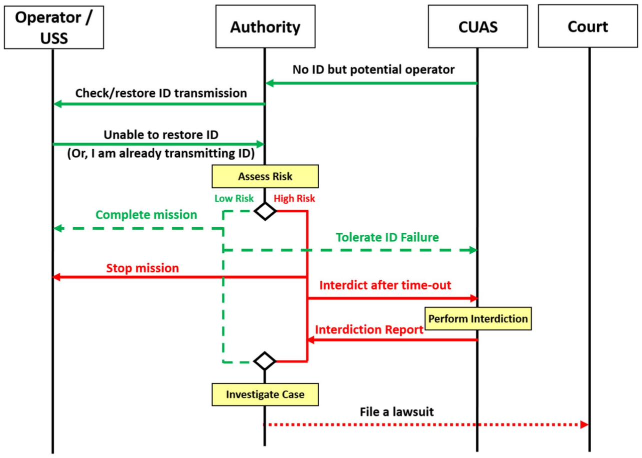

Fig. 5. Protocol 1 (CASE 3 and CASE 4). The drone operator claims that he or she is already broadcasting remote ID or unable to restore transmission.

CASE 3 occurs when the operator denies that the drone is not broadcasting remote identification. In this case, the operator replies to the authority by sending the message I AM ALREADY TRANSMITTING ID. CASE 4 occurs when the operator confirms that the drone is not broadcasting remote identification, and this cannot be restored at the moment, e.g., due to a technical issue. For this, the operator sends the message UNABLE TO RESTORE ID, see Fig. 5. In both cases, the authority may conduct a fast risk assessment. Risk severity evaluation may take into account available information on the importance of the drone mission and the criticality of the respective fly zone. If the estimated risk is low, the authority sends a TOLERATE ID FAILURE message to CUAS and a COMPLETE MISSION message to the operator. In contrast, if the risk is high (or in case a zero-risk policy is preferred), the authority sends a STOP MISSION message to the operator and an INTERDICT AFTER TIME-OUT message to the CUAS. Receiving this message, the CUAS takes action against the drone after the time-out specified in this message.

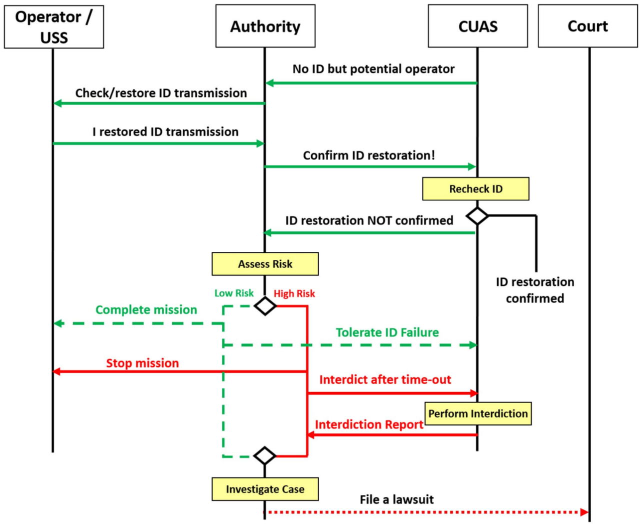

Fig. 6. Protocol 1 (CASE 5 and CASE 6). The drone operator claims that ID transmission is restored.

TABLE II
Outcomes of Protocol 2 (Clarify Unknown ID Issue)

	Description	Authority Response to Operator	Authority Response to CUAS
CASE 1	No technical issues, unregistered ID	NA	Authorize immediate interdiction
CASE 2	Correct ID, issue with the ID-BD	Order mission stop	Authorize timed interdiction
CASE 3	Correct ID, issues with both databases	NA	Order mission tolerance

In CASE 5, the operator confirms that he has restored the ID transmission by sending the message I RESTORED ID TRANSMISSION to the authority, see Fig. 6. The latter asks the CUAS for confirmation by sending a CONFIRM ID RESTORATION! message. The CUAS verifies if the remote identification signal is available. If yes, it sends an ID RESTORATION CONFIRMED, otherwise, an ID RESTORATION NOT CONFIRMED message to the authority. Upon unconfirmed ID restoration (CASE 6), the authority acts according to the risk level, as illustrated in Fig. 6.

B. Protocol 2—Clarify Unknown Identity

This protocol aims to handle the situation when the CUAS receives a remote ID but does not find any related entry in ID-DB or AUTH-DB. This issue can be caused by a technical, data-related, or communication failure related to the databases. Alternatively, the detected drone could be unregistered and flying illegally without registration. The CAUS initiates this protocol by sending the authority an UNKNOWN ID message with the unrecognized identity. The latter performs necessary checks to verify if the provided ID exists and the source of failure causing the database misses. Depending on the result of these checks, we identify three cases as summarized in Table II.

CASE 1 occurs when the authority does not detect any failure related to the databases and concludes that the sighted drone is not registered. As a response, it sends an INTERDICT IMMEDIATELY message to the CAUS, as depicted in Fig. 7. If a forensic investigation is desired, the authority may request the CUAS to use nondestroying enforcement for the interdiction.

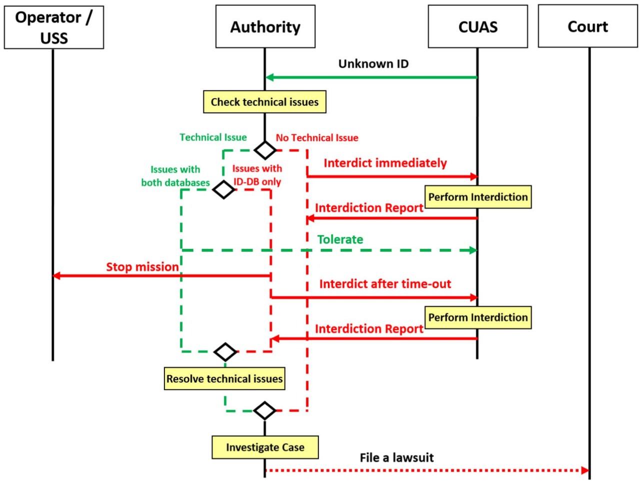

Fig. 7. Protocol 2 (All cases). Clarify unknown ID.

TABLE III
Outcomes of Protocol 3 (Clarify Missing ID in ID-DB)

	Description	Authority response to CUAS
CASE 1	Unresolved technical issue in ID-DB	Tolerate ID failure
CASE 2	Resolved technical issue in ID-DB	Confirm ID restoration

In CASE 2, the authority detects a failure in the ID-DB, which prevents the CUAS from retrieving the ID from this database. However, it finds no issue in the AUTH-DB. It concludes that the drone is registered but not authorized to fly. In this case, the authority sends a STOP MISSION message to the operator and an INTERDICT AFTER TIME-OUT message to the CUAS.

In CASE 3, the authority identifies issues in both databases. In this case, it sends a TOLERATE message to the CUAS indicating that the received ID is original and should be provisionally accepted until the database issues are fixed.

C. Protocol 3—Clarify Missing ID in ID-DB

This protocol clarifies the situation when the CUAS receives a remote ID but does not find the corresponding entry in the ID-DB. At the same time, the AUTH-DB shows that the drone with the received ID is authorized to operate in the respective time and zone. In this case, the CAUS sends the authority an ID-BD MISS message that contains the received remote ID. The latter checks if the ID-DB has any technical issues. If yes, the authority sends the CUAS a TOLERATE ID FAILURE message and works on resolving the issue, see CASE 1 in Table III. CASE 2 occurs when the problem can be resolved quickly by the authority. In this case, the latter requests the CUAS to confirm the ID restoration. Note that the drone operator is not involved in this protocol.

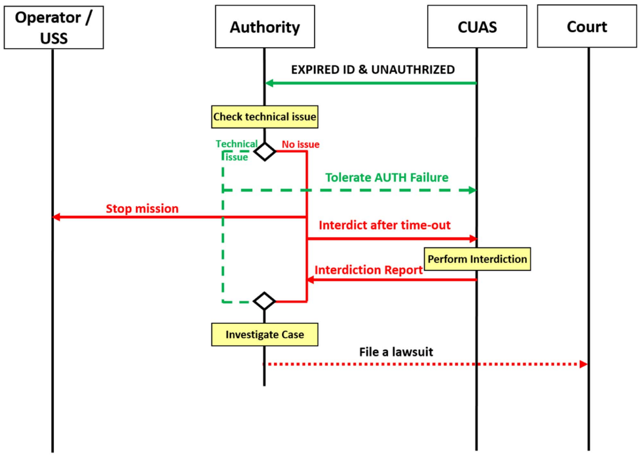

Fig. 8. Protocol 4 (clarify unauthorized and expired ID).

TABLE IV
Outcomes of Protocol 5 (Clarify Authorized but Expired ID)

	Description	Authority response to CUAS
CASE 1	Unresolved technical issue in ID-DB	Tolerate expired ID
CASE 2	Resolved technical issue in ID-DB	Confirm valid ID entry

D. Protocol 4—Clarify Expired ID and Unauthorized Mission

This protocol clarifies the situation when the CUAS receives a remote identification but the ID-DB shows that the drone registration is *expired*. In addition, the AUTH-DB contains no mission authorization for the sighted drone. In this case, the CAUS sends the authority the message EXPIRED ID AND UNAUTHORIZED, as shown in Fig. 8. The authority checks if there are any issues related to the databases. If no, it sends a STOP MISSION message to the operator and an INTERDICT AFTER TIME-OUT message to the CUAS. In contrast, if the authority identifies a technical issue in the databases, it sends a TOLERATE AUTH FAILURE message to the CUAS and works on fixing the problem.

E. Protocol 5—Clarify Authorized Mission Despite Expired ID

This protocol clarifies the situation when the CUAS receives a remote identification but the ID-DB shows that the drone registration has expired. However, the AUTH-DB contains a mission authorization for the drone. This situation can be caused by technical issues related to the ID-DB or human errors leading to providing a performance authorization without proper checking of the ID validity.

To handle this situation, the CAUS sends the authority an EXPIRED ID BUT AUTHORIZED MISSION message. The latter sends a TOLERATE EXPIRED ID message to the CUAS and works on fixing the problem. Alternatively, the authority updates the ID-DB immediately and requests the CUAS to confirm. Table IV summarizes the outcomes of this protocol.

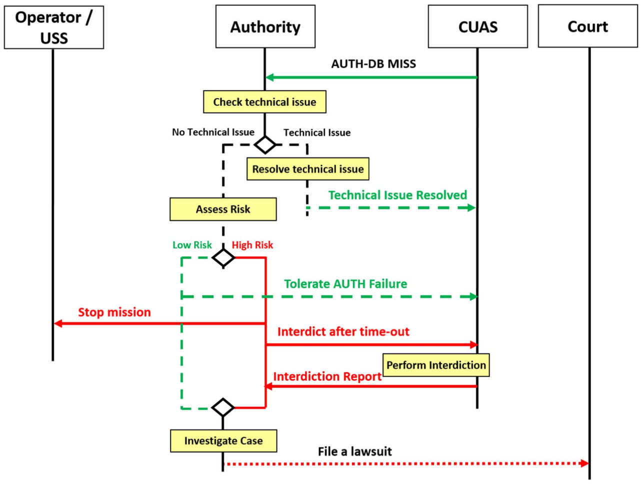

Fig. 9. Protocol 6 (clarify flying without authorization).

TABLE V
Outcomes of Protocol 6 (Clarify Flying Without Authorization)

	Description	Risk Assessment	Authority Response to Operator	Authority Response to CUAS
CASE 1	Technical issue with AUTH-DB	No	NA	Technical issue resolved
CASE 2	No technical issue High risk	Yes	Order mission stop	Authorize timed interdiction
CASE 3	No technical issue Low risk	Yes	Order mission completion	Order mission tolerance

F. Protocol 6—Clarify Flying Without Authorization

This protocol clarifies the situation when the received remote ID is in ID-DB and valid, but there is no corresponding authorization in the AUTH-DB. In this case, the CUAS sends an AUTH-DB MISS message to the authority, as shown in Fig. 9. The latter checks if the missing authorization is due to a technical or data-related issue (CASE 1), see Table V. If this is the case, the authority updates the database and sends the message AUTH-DB MISS RESOLVED to the CUAS; otherwise, it assumes that the operator is flying without permission and performs a fast risk assessment. Depending on the outcome of this assessment, the authority can request the operator to stop the mission and send the CUAS an INTERDICT AFTER TIME-OUT message (CASE 2). If the risk level is low, the authority can request the CUAS to tolerate the mission (CASE 3).

G. Protocol 7—Clarify Flight Zone Violation

This protocol clarifies the situation when the drone flies beyond the authorized zone. The CUAS sends an AREA VIOLATION message to the authority, as shown in Fig. 10. The latter requests the operator to RETURN TO AUTHORIZED AREA. Table VI summarizes five possible cases for clarifying this situation.

In CASE 1, the operator does not respond to the request. In this case, the authority requests the operator to stop the mission and authorizes the CUAS to neutralize the drone after a time-out. The operator can deny the flight zone violation (CASE 2) or claim that he cannot return the

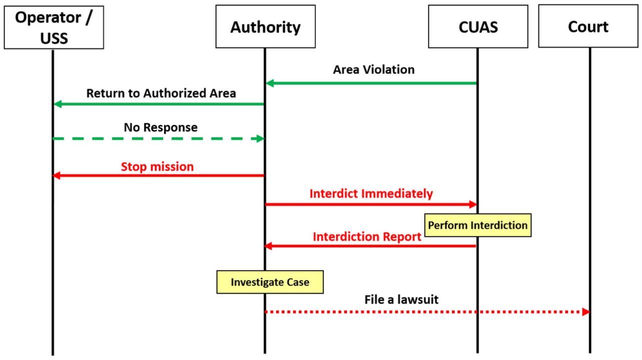

Fig. 10. Protocol 7 (clarify area violation, CASE 1). The operator violates the flight zone and does not respond to the authority.

TABLE VI
Outcomes of Protocol 7 (Clarify Area Violation)

	Operator Response /Description	Risk Assessment	Authority Response to Operator	Authority Response to CUAS
CASE 1	No response	No	Order mission stop	Authorize timed interdiction
CASE 2	I am already flying in authorized area	Yes	Order mission completion or stop	Order mission tolerance or authorize timed interdiction
CASE 3	I cannot return to authorized area	Yes	Order mission completion or stop	Order mission tolerance or authorize timed interdiction
CASE 4	I returned to authorized area	No	NA	Verify return to authorized area
CASE 5	Unconfirmed return to authorized area	No	Order mission stop	Authorize timed interdiction

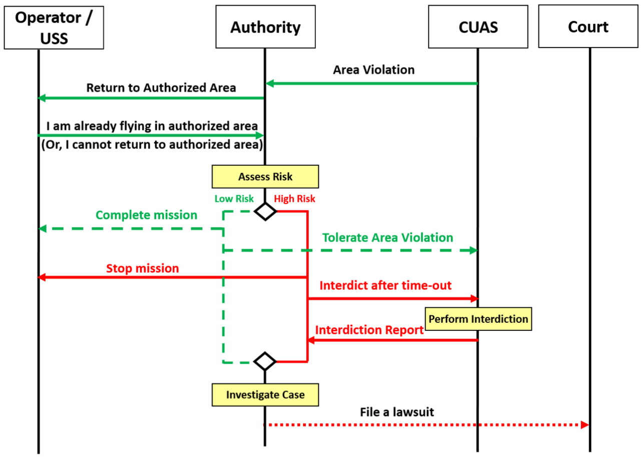

Fig. 11. Protocol 7 (clarify area violation, CASE 2 and CASE 3). The operator responds to the authority message.

drone to the authorized zone for any reason (CASE 3). In these cases, the authority decides based on the risk level, as detailed in Fig. 11. In CASE 4, the operator confirms that he has returned to the authorized area. The authority asks the CUAS to validate this. If the CUAS disconfirms, the authority requests the operator to stop the mission and the CUAS to interdict the drone after a time-out. This same decision can be taken when the operator violates the authorized area fly zone repeatedly (CASE 5).

H. Protocol 8—Clarify Flight Time Violation

This protocol is similar to Protocol 7. It clarifies the situation when the drone is found to exceed the authorized flight time. The CUAS sends a TIME VIOLATION message to the authority. The latter requests the operator to stop the mission. When the operator does not respond to this request, the authority requests the CUAS to neutralize the drone after a time-out. When the operator denies the time violation or claims that he cannot stop the mission for any reason, the authority decides based on the risk level similar to Protocol 7. When the operator confirms that he stopped the mission. The authority asks the CUAS to validate. If the CUAS disconfirms, the authority requests the operator to stop the mission and the CUAS to interdict the drone after a time-out. This same decision can be taken when the operator violates the authorized area fly zone repeatedly.

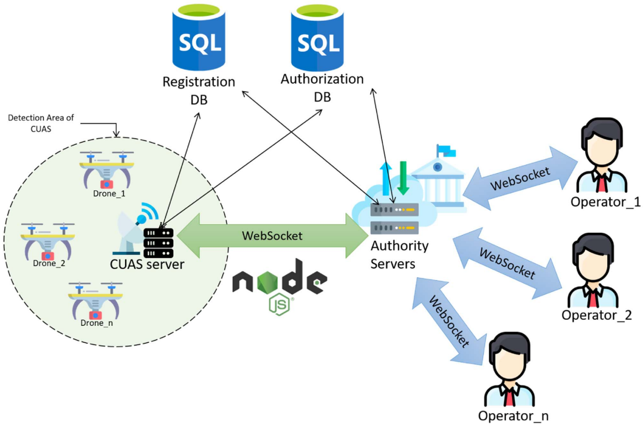

Fig. 12. Overview of the simulation environment.

V. SYSTEM SIMULATION AND EVALUATION

We first validated the proposed protocols using MATLAB. We created state machines to model the interaction between the CUAS, the authority, and the operator with the help of the Stateflow toolbox [53]. The simulation allowed us to identify and debug different types of errors, such as unreachable states, missing transitions, and deadlocks.

To evaluate the performance of the protocols, we then built an event-driven application using Node.js [55], an open-source WebSocket protocol [41], and SQL databases, as illustrated in Fig. 12. The system allows the creation of full-duplex connections for message exchange between the server (authority) and the clients (CUAS and UAV operators), and can handle multiple operators, drones, and missions. The *async* library was used in both the CUAS and authority scripts to handle multiple requests in an asynchronous nonblocking mode [6]. The system was simulated on a desktop machine with an Intel Core i9-8950HK CPU running at 2.90 GHz and 32 GB RAM.

The objective of the simulation is to estimate the *clarification time*, i.e., the wall-clock time elapsed between the detection of a drone and receiving a decision message from the authority. For this, we designed multiple scenarios to model diverse behaviors and mimic different responses to authority messages paying attention to protocol executions that correspond to worst-case clarification times. We used scripts to simulate multiple scenarios for the same drone

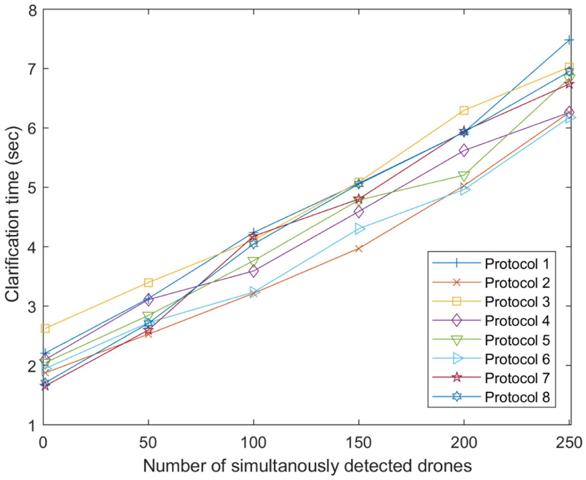

Fig. 13. Clarification time of executing the proposed protocols for different numbers of drones.

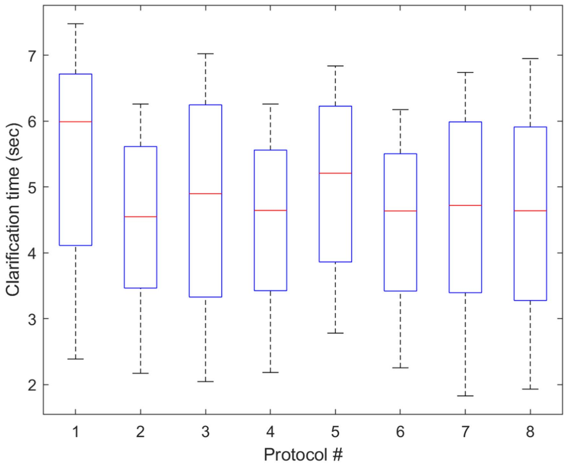

Fig. 14. Clarification time of proposed protocols for 250 drones.

and employed the *child_process* module to launch multiple scripts and simulate numerous drones.

Fig. 13 summarizes the simulation results showing the average clarification time for different protocols and varying numbers of drones from 1 to 250 in steps of 50. We explain this diagram by an example. Assume that the CUAS system has detected 50 drones that are all broadcasting their remote identification but the CUAS cannot find any of these IDs in the ID-DB. The CUAS would initiate protocol 3 to clarify these issues. The simulation results in Fig. 13 show that, in this case, every drone requires an average of 3.3 s to be clarified. The box-and-whisker plot in Fig. 14 demonstrates the data distribution more clearly. Taking Protocol 1 and the case of 250 drones as an example, we can see that the system can clarify 75% of the cases in less than 7 s while the maximum clarification time is 7.5 s only.

We evaluate the clarification time t_{clarify} based on its contribution to the total response time t_{response} of the counter-drone system, as illustrated in Fig. 15. Here, $t_{\text{d\&c}}$, t_{out}, and $t_{\text{interdiction}}$ refer to the time needed to detect and classify the drone, the timeout before initiating the interdiction, and the interdiction time, respectively. Accordingly, the impact of the clarification time on the response time can be defined by the following ratio:

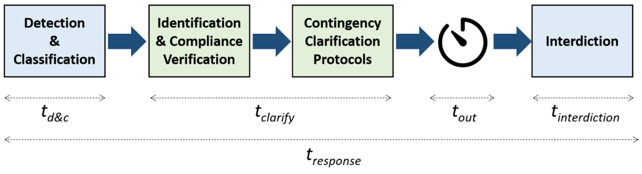
Detection & Classification
Identification & Compliance Verification
Contingency Clarification Protocols
Interdiction
$t_{d\&c}$
$t_{clarify}$
t_{out}
$t_{interdiction}$
$t_{response}$

Fig. 15. Illustrating the components of the CUAS's response time.

TABLE VII
Impact of Clarification on System Latency

Protocol Outcome	Impact of clarification on response time
Tolerance	$R = 2.5/(1.16 + 2.5 + \infty) = 0\%$
Interdiction after a timeout	$R = 2.5/(1.16 + 2.5 + 25) = 9\%$
Immediate interdiction	$R = 2.5/(1.16 + 2.5 + 0) = 68\%$

$$R = \frac{t_{\text{clarify}}}{t_{\text{d\&c}} + t_{\text{clarify}} + t_{\text{out}} + t_{\text{interdiction}}}. \tag{1}$$

In the following, we evaluate R for the case of a single drone where $t_{\text{clarify}} \approx 2.5$ s in the worst case according to the simulation. For this, we first provide some estimation for $t_{\text{d\&c}}$, t_{out}, and $t_{\text{interdiction}}$.

Detection and classification time ($t_{\text{d\&c}}$)*:* Reports on the time needed to detect and classify a drone are scarce. Basak et al. [17] proposed a combined drone detection and classification framework using YOLO Lite. They reported a mean inference time of 1.16 s for detecting and classifying one drone.

Timeout (t_{out})*:* The timeout depends on the outcome of the clarification protocol as follows.

1) When the decision is to interdict the drone immediately, then $t_{\text{out}} = 0$.
2) When the decision is to tolerate the drone, then $t_{\text{out}} = \infty$.
3) When the decision is to interdict the drone after a timeout, then t_{out} should be around what an operator typically needs to stop the mission, e.g., by landing the drone safely. Landing a drone takes place at low speeds, e.g., 4 m/s according to [49]. So, if a multirotor drone flies at an altitude of 100 m, the landing would take around 25 s.

Interdiction time ($t_{\text{interdiction}}$)*:* This time depends on the used technology. Jamming is one of the fastest solutions due to its nonkinetic nature. Although the jamming signal should be directed to reduce side effects, the market is rich in off-the-shelf solutions with omnidirectional jammers that block communication immediately after being switched on. The interdiction time of such systems would be negligible.

Based on these estimations, Table VII summarizes the impact of the clarification time on the CUAS's response time for the three outcomes of decisions: tolerance, interdiction after a timeout, and immediate interdiction. Accordingly, when the authority decides to tolerate the drone, the clarification time has no impact. When the drone is to be neutralized after a timeout of 25 s, the clarification time extends the response time by 9%. In the case of immediate interdiction, the clarification time worsens the response time by 68%. In other words, the clarification would delay the interdiction by approximately 2.5 s.

VI. DISCUSSION

According to the performance evaluation, the use of clarification protocols can significantly affect the response of the counter-drone system only when the drone is identified as illegal and requires immediate neutralization. However, even in such cases, the delay in response is only a few seconds. This delay is a compromise for dealing with legal UAVs that may have technical or nontechnical issues. Whether or not to accept this compromise depends on the criticality of the particular zone and the level of experience with drone operations in and around that zone. Such experience can provide insight into the likelihood of encountering contingency issues versus illegal operations, but unfortunately, there is currently no data available to inform these decisions. Future research may shed light on this topic.

There are some limitations to this study, specifically related to the accuracy of determining clarification time. The simulation was run on a single computer without real networking, whereas a real deployment would involve a distributed system that introduces network and communication delays. In addition, the simulation assumed that the authority and operators would respond without delay, which may not be practically feasible. Therefore, actual implementation and real-time measurements in the future could provide more accurate timing data. Furthermore, the protocols were implemented at the application layer, but in a real deployment, security measures at lower layers, such as using SSL sessions between the CUAS and encrypted messaging with the authority server, could be beneficial. Lastly, the study did not define message formats, as this is not relevant at this stage of research and should be addressed in the context of standardization activities.

VII. CONCLUSION

Currently, the development of UTM systems and counter-drone systems is taking place independently, while drone operators are still benefiting from the current legal situation, which prohibits the interdiction of aerial vehicles. Many efforts are ongoing to change this situation, leading to precise regulations for counter-drone operations. Like always, however, regulations matter for those who plan to follow them. Management of drone operations must be able to deal with malfunctions, technical failures, and malicious users. Real-time coordination of the drone and counter-drone operation is a challenge. We claim that the protocol suite proposed in this article provides the first organic approach to this problem, and our simulation results are promising. However, we are fully aware that real deployments and pilot tests are required to fully understand all details of the problem and the hurdles to overcome. We hope that the proposed protocols will provide guidance to system developers working on integrating CUAS and UTM systems and attract attention to the need for standardization.

REFERENCES

[1] Weibel Scientific A/S, "Counter-UAS - What is a drone detection radar," Accessed: Jul. 09, 2023. [Online]. Available: https://weibelradars.com/drone-detection/what-is-drone-detection/#:text=Our%20drone%20detection%20radars%20are, and%20high%2Dpower%20systems%20respectively

[2] Federal Aviation Administration, "UAS remote identification overview," 2021. [Online]. Available: https://www.faa.gov/uas/getting_started/remote_id/

[3] European Union Aviation Safety Agency, "Commission delegated regulations (EU) 2020/1058," 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020R1058&from=EN

[4] G. Airlangga and A. Liu, "A novel architectural design for solving lost-link problems in UAV collaboration," in *Proc. 28th Asia-Pacific Softw. Eng. Conf.*, 2021, pp. 380–389.

[5] S. Al-Emadi and F. Al-Senaid, "Drone detection approach based on radio-frequency using convolutional neural network," in *Proc. IEEE Int. Conf. Inform., IoT, Enabling Technol.*, 2020, pp. 29–34, doi: 10.1109/ICIoT48696.2020.9089489.

[6] S. Alimadadi, A. Mesbah, and K. Pattabiraman, "Understanding asynchronous interactions in full-stack JavaScript," in *Proc. 38th Int. Conf. Softw. Eng.*, 2016, pp. 1169–1180.

[7] R. Alkadi, N. Alnuaimi, C. Y. Yeun, and A. Shoufan, "Blockchain interoperability in unmanned aerial vehicles networks: State-of-the-art and open issues," *IEEE Access*, vol. 10, pp. 14463–14479, 2022.

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

[9] A. Allouch et al., "UTM-chain: Blockchain-based secure unmanned traffic management for Internet of Drones," *Sensors*, vol. 21, no. 9, 2021, Art. no. 3049.

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

[11] A. T. Altun, Y. Xu, and G. Inalhan, "Contingency management concept generation for U-space system," in *Proc. Integr. Commun., Navigation Surveill. Conf.*, 2022, pp. 1–12.

[12] M. Z. Anwar, Z. Kaleem, and A. Jamalipour, "Machine learning inspired sound-based amateur drone detection for public safety applications," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2526–2534, Mar. 2019.

[13] M. J. Armstrong, G. R. Hutchins, and T. A. Wachob, "Interdiction and recovery for small unmanned aircraft systems," US Patent 10,401,129, Sep. 3, 2019.

[14] ASD-STAN, *Direct Remote ID—Introduction to the European UAS Digital Remote Id Technical Standard*," Aerospace and Defence Industries Association of Europe Standardization, Brussels, Belgium, 2020.

[15] *Standard Specification for Remote ID and Tracking*, ASTM Standard ASTM F3411-19, 2019. [Online]. Available: http://www.astm.org/cgi-bin/resolver.cgi?F3411-19

[16] J. E. Baculi and C. A. Ippolito, "Onboard decision-making for nominal and contingency SUAS flight," in *Proc. AIAA Scitech Forum*, 2019, Art. no. 1457.

[17] S. Basak, S. Rajendran, S. Pollin, and B. Scheers, "Combined RF-based drone detection and classification," *IEEE Trans. Cogn. Commun. Netw.*, vol. 8, no. 1, pp. 111–120, Mar. 2022.

[18] O. Bekkouche, M. Bagaa, and T. Taleb, “Toward a UTM-based service orchestration for UAVs in MEC-NFV environment,” in *Proc. IEEE Glob. Commun. Conf.*, 2019, pp. 1–6.

[19] K. Belwafi et al., “Unmanned aerial vehicles’ remote identification: A tutorial and survey,” *IEEE Access*, vol. 10, pp. 87577–87601, 2022.

[20] P. Boucher, “Domesticating the drone: The demilitarisation of unmanned aircraft for civil markets,” *Sci. Eng. Ethics*, vol. 21, no. 6, pp. 1393–1412, 2015.

[21] H. Newton, M. J. C. Acheson, and I. M. Gregory, “Dynamic vehicle assessment for intelligent contingency management of urban air mobility vehicles,” in *Proc. AIAA Scitech Forum*, 2021, Art. no. 1001.

[22] C. Capitán, J. Capitán, R. A. Castaño, and A. Ollero, “Threat management methodology for unmanned aerial systems operating in the U-space,” *IEEE Access*, vol. 10, pp. 70476–70490, 2022.

[23] A. Chakrabarty, C. A. Ippolito, J. Baculi, K. S. Krishnakumar, and S. Hening, “Vehicle to vehicle (V2V) communication for collision avoidance for multi-copters flying in UTM–TCL4,” in *Proc. AIAA Scitech Forum*, 2019, Art. no. 0690.

[24] C. Chin, K. Gopalakrishnan, M. Egorov, A. Evans, and H. Balakrishnan, “Efficiency and fairness in unmanned air traffic flow management,” *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 9, pp. 5939–5951, Sep. 2021.

[25] C. Courtin, M. J. Burton, A. Yu, P. Butler, P. D. Vascik, and R. J. Hansman, “Feasibility study of short takeoff and landing urban air mobility vehicles using geometric programming,” in *Proc. Aviation Technol., Integration, Operations Conf.*, 2018, Art. no. 4151.

[26] G. Darroch, “Gatwick airport: Drones ground flights,” *BBC*. Accessed: Dec. 20, 2018. [Online]. Available: https://www.bbc.com/news/uk-england-sussex-46623754

[27] DeDrone, “Worldwide drone incidents,” 2020. [Online]. Available: https://www.dedrone.com/resources/incidents-new/all

[28] M. Ezuma, C. K. Anjinappa, M. Funderburk, and I. Guvenc, “Radar cross section based statistical recognition of UAVs at microwave frequencies,” *IEEE Trans. Aerosp. Electron. Syst.*, vol. 58, no. 1, pp. 27–46, Feb. 2022.

[29] FAA, “UAS data exchange (LAANC),” 2020. [Online]. Available: https://www.faa.gov/uas/programs_partnerships/data_exchange/

[30] Federal Aviation Administration, “Unmanned aircraft system (UAS) traffic management (UTM) concept of operation,” Federal Aviation Administration, Washington, DC, USA, Tech. Rep. UTM ConOps v2.0, 2020.

[31] A. G. Haddad, M. A. Humais, N. Werghi, and A. Shoufan, “Long-range visual UAV detection and tracking system with threat level assessment,” in *Proc. IEEE IECON 46th Annu. Conf. Ind. Electron. Soc.*, 2020, pp. 638–643, doi: 10.1109/IECON43393.2020.9254816.

[32] M. Hassanalian and A. Abdelkefi, “Classifications, applications, and design challenges of drones: A review,” *Prog. Aerosp. Sci.*, vol. 91, pp. 99–131, 2017.

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

[34] A. H. Michel, “Counter-drone systems,” 2019. [Online]. Available: https://dronecenter.bard.edu/files/2019/12/CSD-CUAS-2nd-Edition-Web.pdf

[35] T. Multerer et al., “Low-cost jamming system against small drones using a 3D MIMO radar based tracking,” in *Proc. Eur. Radar Conf.*, 2017, pp. 299–302.

[36] N. Neogi, S. Bhattacharyya, D. Griessler, H. Kiran, and M. Carvalho, “Assuring intelligent systems: Contingency management for UAS,” *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 9, pp. 6028–6038, Sep. 2021.

[37] J. O’Malley, “The no drone zone,” *Eng. Technol.*, vol. 14, no. 2, pp. 34–38, 2019.

[38] B. Pang, M. E. Ng, and K. H. Low, “UAV trajectory estimation and deviation analysis for contingency management in urban environments,” in *Proc. AIAA Aviation Forum*, 2020, Art. no. 2919.

[39] S. Park, H. T. Kim, S. H. L. Joo, and H. Kim, “Survey on anti-drone systems: Components, designs, and challenges,” *IEEE Access*, vol. 9, pp. 42635–42659, 2021.

[40] T. Patterson, S. McClean, P. Morrow, G. Parr, and C. Luo, “Timely autonomous identification of UAV safe landing zones,” *Image Vis. Comput.*, vol. 32, no. 9, pp. 568–578, 2014.

[41] V. Pimentel and B. G. Nickerson, “Communicating and displaying real-time data with websocket,” *IEEE Internet Comput.*, vol. 16, no. 4, pp. 45–53, Jul./Aug. 2012.

[42] C. Reiche, A. P. Cohen, and C. Fernando, “An initial assessment of the potential weather barriers of urban air mobility,” *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 9, pp. 6018–6027, Sep. 2021.

[43] J. Rothe, M. Strohmeier, and S. Montenegro, “A concept for catching drones with a net carried by cooperative UAVs,” in *Proc. IEEE Int. Symp. Safety, Security, Rescue Robot.*, 2019, pp. 126–132.

[44] R. Ryan, S. Al-Rubaye, G. Braithwaite, and D. Panagiotakopoulos, “The legal framework of UTM for UAS,” in *Proc. IEEE/AIAA 39th Digit. Avionics Syst. Conf.*, 2020, pp. 1–5.

[45] S. Samaras et al., “Deep learning on multi sensor data for counter UAV applications–A systematic review,” *Sensors*, vol. 19, no. 22, 2019, Art. no. 4837.

[46] Z. Sándor, “Challenges caused by the unmanned aerial vehicle in the air traffic management,” *Periodica Polytechnica Transp. Eng.*, vol. 47, no. 2, pp. 96–105, 2019.

[47] A. Shoufan, C. Y. Yeun, and B. Taha, “ESIM-based authentication protocol for UAV remote identification,” in *Proc. Secur. Privacy Internet Things: Architectures, Techn., Appl.*, 2021, pp. 91–122.

[48] M. Stevens and E. Atkins, “Geofence definition and deconfliction for UAS traffic management,” *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 9, pp. 5880–5889, Sep. 2021.

[49] I. Suroso and E. Irmawan, “Analysis of UAV multicopter of air photography in new Yogyakarta International Airports,” *TELKOMNIKA*, vol. 17, no. 1, pp. 521–528, 2019.

[50] B. Taha and A. Shoufan, “Machine learning-based drone detection and classification: State-of-the-art in research,” *IEEE Access*, vol. 7, pp. 138669–138682, 2019.

[51] Y. Tang, Y. Xu, and G. Inalhan, “An integrated approach for on-demand dynamic capacity management service in U-space,” *IEEE Trans. Aerosp. Electron. Syst.*, vol. 58, no. 5, pp. 4180–4195, Oct. 2022, doi: 10.1109/TAES.2022.3159317.

[52] E. H. Teomitzi and J. R. Schmidt, “Concept and requirements for an integrated contingency management framework in UAS missions,” in *Proc. IEEE Aerosp. Conf.*, 2021, pp. 1–17.

[53] Inc. The MathWorks, “Stateflow toolbox,” 2021. [Online]. Available: https://www.mathworks.com/products/stateflow.html

[54] C. Theodore et al., “Flight trials of a rotorcraft unmanned aerial vehicle landing autonomously at unprepared sites,” in *Proc. Annu. Forum Proc.-Amer. Helicopter Soc.*, 2006, vol. 62, Art. no. 1250.

[55] S. Tilkov and S. Vinoski, “Node.js: Using JavaScript to build high-performance network programs,” *IEEE Internet Comput.*, vol. 14, no. 6, pp. 80–83, Nov.-Dec. 2010.

[56] J. Wang, Y. Liu, and H. Song, “Counter-unmanned aircraft system(s) (C-UAS): State of the art, challenges, and future trends,” *IEEE Aerosp. Electron. Syst. Mag.*, vol. 36, no. 3, pp. 4–29, Mar. 2021.

[57] C. Wolter, L. Martin, and K. Jobe, “Human-system interaction issues and proposed solutions to promote successful maturation of the UTM system,” in *Proc. IEEE/AIAA 39th Digit. Avionics Syst. Conf.*, 2020, pp. 1–7.

[58] P. M. Wyder et al., “Autonomous drone hunter operating by deep learning and all-onboard computations in GPS-denied environments,” *PLoS One*, vol. 14, no. 11, 2019, Art. no. e0225092.

[59] C. Xu, X. Liao, J. Tan, H. Ye, and H. Lu, “Recent research progress of unmanned aerial vehicle regulation policies and technologies in urban low altitude,” *IEEE Access*, vol. 8, pp. 74175–74194, 2020.

[60] J. Zhou, D. Sun, I. Hwang, and D. Sun, “Control protocol design and analysis for unmanned aircraft system traffic management,” *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 9, pp. 5914–5925, Sep. 2021.

[61] J. Zhou and C. Kwan, “A high performance contingency planning system for UAVs with lost communication,” in *Proc. IEEE Int. Conf. Prognostics Health Manage.*, 2018, pp. 1–8.

Abdulhadi Shoufan (Member, IEEE) received the Dr.-Ing. degree in computer engineering from Technische University Darmstadt, Darmstadt, Germany, in 2007.

He is currently an Associate Professor of electrical engineering and computer science with Khalifa University, Abu Dhabi, United Arab Emirates. His research interests include drone security, safe operation, embedded security, cryptography hardware, learning analytics, and engineering education.

Ernesto Damiani (Senior Member, IEEE) received the Ph.D. degree in computer science from the University of Milan, Milan, Italy, in 1994.

He is currently a Full Professor with the Università degli Studi di Milano, Milan, Italy, the Senior Director of the Robotics and Intelligent Systems Institute, and the Director of the Center for Cyber Physical Systems (C2PS), Khalifa University, Abu Dhabi, United Arab Emirates. He is also the Leader of the big data area with the Etisalat British Telecom Innovation Center (EBTIC) and the President of the Consortium of Italian Computer Science Universities (CINI). He is also a part of the ENISA Ad-Hoc Working Group on Artificial intelligence cybersecurity. He has pioneered model-driven data analytics. He has authored more than 650 Scopus-indexed publications and several patents. His research interests include cyber-physical systems, Big Data analytics, edge/cloud security and performance, artificial intelligence, and machine learning.

Dr. Damiani was the recipient of the Research and Innovation Award from the IEEE Technical Committee on Homeland Security, Stephen Yau Award from the Service Society, Outstanding Contributions Award from IFIP TC2, Chester-Sall Award from IEEE IES, IEEE TCHS Research and Innovation Award, and Doctorate Honoris Causa from INSA-Lyon, France, for his contribution to Big Data teaching and research.