Integrating Counter-UAS Systems into the UTM System for Reliable Decision Making

Abdulhadi Shoufan and Ruba Alkadi

Abstract—Despite significant progress, the deployment of UAV technology in commercial and civil applications is still lagging. This is essentially due to the risks associated with drone flights and the lack of coordinated technologies that would mitigate these risks. While Unmanned Aircraft System Traffic Management systems (UTM) are being developed worldwide to enable safe operation, the counter-drone technology operates on an all-enemy basis and regards any sighted drone as a threat. This situation is essentially caused by the lack of information exchange between stakeholders. Without the exchange of relevant information, a counter-drone system can misclassify drones and initiate erroneous interdiction procedures. This paper proposes a system that integrates counter-drone technology into the UTM system for information exchange and coordination using a set of clarification protocols towards accountable response to sighted drones. The system functionality and performance were evaluated by simulation.

Index Terms—UAV, Counter-UAS, UTM.

I. INTRODUCTION

The drone market is growing rapidly with diverse applications in construction, agriculture, insurance, oil and gas industry, film making, sky photography, parcel delivery, journalism, security, law enforcement, and civil defense [20]. Despite this, the operation of UAVs in urban areas is still in the exploratory stage [41]. That is, we neither get our online orders delivered by UAVs nor can we ride a taxi drone, although the technical capabilities of today’s UAVs allow for the deployment in such applications [13]. Indeed, flying a drone is associated with security, privacy, and safety risks which have limited the progress and penetration of UAV applications across many sectors in the urban airspace [5], [22]. Safety is, without doubt, the most urgent requirement when it comes to drone operation. This is confirmed by the frequent reports on drone incidents and intrusions worldwide [14], [15], [24].

To support safe drone operations and counter violations many technologies are available. These technologies can be divided broadly into three categories as depicted in Fig. 1. The first category encompasses preventive onboard solutions such as sense&avoid and geofencing [16], as well as response technologies such as parachuting and self-recovery systems [21]. The second category addresses illegal UAVs and includes counter-drone systems from detection to interdiction. Detection and classification use different modalities such as radar, images, acoustic, and radio-frequency signals [6], [37]. Malicious drones can be deactivated using diverse interdiction technologies such as jamming, catching, or shooting [26], [32]. Finally, UTM-driven technologies, including mission authorization systems and remote identification, have been put forward recently to coordinate UAV activities in the low-altitude airspace [8], [18].

While these technologies are supposed to complement each other towards safe airspace, the current implementations of category-2 and category-3 technologies lack the necessary level of integration and appear to follow conflicting goals: While UTM-driven technologies promote the legalization of drone operations, the counter-drone systems take a skeptical attitude towards safe airspace, the current implementations of these technologies appear to follow conflicting goals: While UTM-driven technologies promote the legalization of drone operations, the counter-drone systems take a skeptical position and consider any drone in the sky as a threat. This suggests that information exchange between UTM systems and counter-UAS systems is mandatory to avoid conflicts. These observations were already reported in the recent survey of counter-drone technology [30]. Hence, the first contribution of this paper is to propose a novel architecture for integrating CUAS systems in the UTM system (Section III). This architecture will allow the CUAS system to obtain information about the registration status of the sighted drone and whether it is authorized to perform the observed flight. With this information, the CUAS system can classify the drone as cooperative and tolerate its existence in the operation zone of the CUAS system. To access relevant information in the UTM databases, a CUAS system requires an initial knowledge about the drone. We propose to obtain this initial knowledge from the drone itself through the broadcast remote identification. Remote identification (RID) is becoming a core technology of UTM systems in many countries.

No matter how reliable these technologies are, technical and non-technical errors can occur:

1) The RID module on board the drone can fail.
2) The RID receiver of the CUAS system can fail.
3) A UTM system operator can fail to update the databases or to do so on time.
4) An inquiry to the UTM databases can fail for technical reasons.
5) The drone operator can exceed the permitted flight time by mistake or for an urgent reason.
6) The drone operator can deviate from the approved mission trajectory by mistake or for mandatory reasons.

Center of Cyber-Physical Systems, Khalifa University, Abu Dhabi, UAE (emails: Abdulhadi.shoufan, Ruba.alkadi @ku.ac.ae)
In none of these cases should a CUAS system immediately classify a drone as uncooperative and start an interdiction operation. On the other hand, the outcomes of such cases are indeed ambiguous and can indicate uncooperative or malicious drone operations that should be countered. These thoughts suggest that a counter-drone system needs more information to clarify such cases and classify them correctly towards a responsible decision. Therefore, the second contribution of this paper is to present a post-detection model for the drone and a set of protocols that help in clarifying ambiguous cases, see Section IV.

The developed models and protocols are evaluated by simulation. First, we used an appropriate Simulink toolkit to test the correctness of the model and protocols. Then, we implemented the same using Node.js to assess the performance of the system in a networked mode. The simulation setup and results are present in Section VI.

II. RELATED WORK

A. UTM Systems

The concept of unmanned traffic management (UTM) refers to an ecosystem for controlling the operation of unmanned aerial systems [18, 41]. Data exchange is at the core of UTM where authorized unmanned service suppliers (USS) provide cloud-based services to the different stakeholder. Examples of these services include UAV control [42], efficient and fair unmanned traffic control [12], flight planning and scheduling [23], geofencing [35], path optimization and collision avoidance [11], weather and contingency management [27], [31], orchestrating of UAV services [10], and supporting the internet-of-drones (IoD) [4].

UTM systems are still in the development stage. Some authors have highlighted several challenges and issues in the design of these systems. Wolter et al. pointed out multiple obstacles in the current experimental setups which relate to standardization, information quality, and the transition from human-centric design to automation [39]. Several authors addressed the security of UTM systems and presented their vulnerabilities to various cyber and physical attacks [4]. The lack of a legal framework for UTM system operations was highlighted in [33]. The authors described the fundamentals of such a legal framework which 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 counter-unmanned aerial systems (CUAS) on the market [25]. Researchers showed wide interest in this field, especially regarding the detection and classification of small UAVs. Different technologies were proposed including radar, radio-frequency detection, acoustic systems, and computer vision [3, 6, 17, 28]. Parallel to the advances in detection and classification technologies, some researchers investigated technical solutions for drone interdiction. Wyder et al. classified these technologies according to their impact on the target drone into three main categories: signal interception, propeller restriction, and aerial takedown [40]. Due to its undisruptive nature, signal interception has received substantial attention for interdiction in urban areas. Depending on the operation mode of the drone, Roth et al. identified two methods of signal interception-based interdiction: drone hacking and GPS spoofing [32]. Propeller restriction refers to capturing uncooperative drones usually using a net. The net could be launched either manually by a skilled operator on the ground or autonomously by another flying drone [7]. Finally, a variety of aerial takedown technologies was presented. These include hunting by eagles [29] and shooting by machine guns or laser [32].

C. Coordination between UTM and Counter-Drone Systems

Despite the strong relationship between UTM and counter-drone systems, the interaction between these systems remained unaddressed in the literature. Recently, Park et al. surveyed more than 180 publications on the literature of counter-drone systems. In their concluding remarks, they highlighted the necessity of integrating a well-defined drone identification scheme into counter drone systems. Sandor has highlighted that with the spread of UTM systems, we need to define the problems, the scope, and the operational environment [34]. The author defined and classified many functions related to UTM and interestingly suggested surveillance as a UTM service with different technologies for the detection of cooperative and non-cooperative vehicles. However, the author did not take into consideration the critical function of a counter-drone system which is interdiction. Apart from this, we are not aware of any literature that addressed the coordination of the UTM and counter-drone systems’ activities.

III. SYSTEM ARCHITECTURE

The proposed system architecture relies on and extends the UAS traffic management system (UTM) released by NASA [18]. The proposed architecture in Fig. 2 aims to grant CUAS systems access to the Flight Information Management System (FIMS). The latter should contain at least two databases: a database of the identities of registered drones (ID-DB) and a database of authorized missions (AUTH-DB). In the following,
we first describe the system agents in brief. Then, we describe
the databases and how the CUAS system interacts within the
UTM system.

The Authority in our architecture refers to the agent that
regulates and oversees civil airspace to assure safe and secure
operation by providing air navigation services and facilitating
air connectivity. All drones should be registered at the author-
ity. Additionally, operators can obtain mission authorization
directly from the authority or from authorized service sup-
pliers. The authority along with such service suppliers keeps
relevant information about drone registrations and mission
authorizations in the ID-DB and AUTH-DB databases.

The Unmanned Service Supplier (USS) is an entity that
provides services to subscribed UAS operators to help them
meet the operational requirements specified by the authority.
Operation planning, strategic and tactical de-confliction, re-
move identification, and airspace authorization are examples of
the services provided by a USS. An operator may subscribe
to one or more USS’s to use multiple services.

The UAS operator is a primary agent in the UTM system
who is responsible for operating the drone in different modes
for various purposes. UAS operators may opt to utilize a
USS or to provide their own services to meet regulatory
obligations. So, it is the operator’s responsibility to meet the
requirements established for the type of operation and the
associated airspace volume or route.

The Counter Unmanned Aerial System (CUAS) is an active
agent in the UTM architecture according to our proposal. By far, the deployment of anti-drone technology against civil
drones has been served as individual efforts by different
agents interested in protecting their territories against ma-
ligious drones or by law enforcement for protecting public
safety. We advocate for integrating the CUAS technology
into the UTM system to enable the exchange of information
between relevant agents and support coordinated efforts for
cooperative vs. uncooperative drone identification.

Finally, the Court is added as an agent to the system
to benefit from the information infrastructure for evidence
collection in case of legal conflicts. Basically, following to
any interdiction process, the authority can file a lawsuit to
the court to initiate forensics work. Similarly, a UAS operator
might file a lawsuit in case her or his vehicle was intercepted,
fined, or jammed unlawfully.

A. Identity Database (ID-DB)

Aviation authorities worldwide are mandating the deploy-
ment of remote identification to promote safe and account-
able drone operations. The European Union Aviation Safety
Agency (EASA) has published related regulations in March
2019 (Commission delegated regulation (EU) 2019/945) that
were amended in April 2020 ((EU) 2020/1058). These regula-
tions mandate that all unmanned aircraft should be equipped
with a remote identification system [2]. The FAA in the USA
has published a final rule for remote identification in January
2021 [1]. According to this, the remote identification message
should include information about the drone’s identity, location,
alitude, and velocity in addition to the control station location
and elevation, a time mark, and emergency status. A database
with Remote ID information should provide three levels of
access:

1) Level 1: Information available to the public (the UAS
unique identifier).
2) Level 2: Information available to designated public
safety and airspace management officials (personally
identifiable information).
3) Level 3: Information available to the FAA and certain
Federal, State, and local agencies (tracking data).

In our architecture, we propose including this database in
the FIMS. Certified CUAS systems should be given access
to this database on level 2 or 3 depending on the predeter-
mined authority of these systems. We further assume that this
database is available and its content is protected from security
attacks. Specifically, Remote ID entries in the database are
assumed to be authentic. This means that a CUAS can use the
ID-DB to verify the authenticity of a received Remote ID.

B. Authorization Database (AUTH-DB)

CUAS systems are usually used in protected areas such
as controlled zones around airports. But even in such areas,
drones can have a reason to fly, for example, to help fire-
fighters nearby. So, the CUAS needs a possibility to check
whether a detected drone has permission to fly in this area
and time. The FAA has implemented a system referred to
as Low Altitude Authorization and Notification Capability
(LAANC) [19]. This system automates the application and
approval process for airspace authorizations. Like Remote ID,
the LAANC is considered a part of the UTM ecosystem. UAS
service suppliers support the authorization process: A drone
pilot submits a request through a 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.

For our purpose, we propose that all mission authorizations
should be logged in AUTH-DB. An entry in this database
should include information about the drone ID and the mission
date, time, and area. Operators of counter-drone systems
should have access to the AUTH-DB to verify the performance
authorization of a detected drone. The AUTH-DB must be
protected against security attacks such as entry manipulation.

C. CUAS Interactions within the UTM System

The proposed architecture in Fig. [2] allows the CUAS to
interact with different agents in the UTM system and to per-
form different checks using the identity and the authorization
databases towards cooperative vs. uncooperative identification.
For this, we make the following assumptions:

1) Any drone in flight should share its ID remotely.
2) A CUAS has the necessary technology to receive the
Remote ID and check its authenticity and validity by
accessing the ID-DB.
3) The ID-DB should be kept up-to-date by the authority
or any certified USS. Nonetheless, legacy/expired IDs
are not removed from the database.
4) Any drone flying in the operation zone of a CUAS (i.e., the zone in which the CUAS is permitted to interdict), is required to have a performance authorization.
5) A performance authorization includes at least information about the drone ID as well as the date, time, and area of flight.
6) The CUAS has access to the AUTH-DB to verify whether a detected drone is authorized to fly in the respective area and time.
7) The AUTH-DB should be kept up-to-date by the authority or any certified agent.

In the following section, the CUAS interaction with the UTM system will be detailed by defining a post-detection model for the drone.

IV. POST-DETECTION MODEL FOR DRONES

Based on the architecture presented in the previous section, we model a drone from a CUAS perspective using the finite state machine illustrated in Fig. [3]. The transition from one state to another is triggered either by the result of some checks that the CUAS performs independently or by the outcome of some protocol execution between the CUAS and other agents. In the beginning, the system is set in the Surveillance state. When the CUAS identifies an object as a drone, it transits to the state Drone Detected. The machine states are highlighted using three colors:

1) The green color indicates the desired state which is reached through a successful check of some conditions. For example, when the CUAS verifies that the drone is transmitting a Remote ID, the next state would be ID Received. Furthermore, the model has two special green states in which the drone is tolerated despite some failures, as will be described in Section [4].
2) A drone that reaches a red state is an uncooperative one. It will be subject to an approved interdiction, which can be started immediately or after a timeout.
3) The orange color describes an ambiguous state of the detected drone. The CUAS essentially tries to clarify this state by executing some protocol involving other system agents. As a result, the drone either returns to a green state or moves to a red state.

We first explain the case of a cooperative drone, which is represented by the vertical green path. When a drone is detected, the CUAS receives its Remote ID. The successful reception of the ID is followed by verifying its authenticity. If the ID is authentic, the CUAS checks if it is available in the identity database (ID-DB). If this is the case, the ID’s expiry date is checked. If the ID is valid, the CUAS accesses the authorization database (AUTH-DB) to verify whether the drone is authorized to perform the observed mission. If the check is successful, the CUAS verifies if the drone is complying with the mission plan regarding the area and time. If this is the case, the FSM returns to the state Drone Detected. The CUAS can repeat these checks until the drone has completed its mission or disappeared from the detection range.

We now explain in brief what happens when any of the previous checks fails. Detailed descriptions of the different cases and protocols will follow in Section [5]. First, when the CUAS does not receive an ID from the drone (No ID Received), the CUAS uses knowledge about the flight time and drone location to inquire about a potential operator in the authorization database (AUTH-DB). If no such operator is found, the drone state changes to No ID & No Potential Operator. Depending on the CUAS policy and the authority, an Immediate Interdiction process can be started. In contrast, if the CUAS finds a potential operator in the AUTH-DB, the machine transits to the state No ID But Potential Operator. Herein, the CUAS reads the ID of the potential operator and initiates Protocol 1 to verify whether this ID belongs to the actual operator who is flying the detected drone. Executing this protocol can lead to one of four results:

1) Restoring the ID transmission by the operator.
2) Tolerating the ID transmission failure.
3) Immediate interdiction of the drone.
4) Delayed interdiction of the drone.

The CUAS should verify the authenticity of a received remote identification. When this verification is not successful, the CUAS classifies the drone as uncooperative. The next state is Fake ID leading to the state Immediate Interdiction. In contrast, if the ID is authentic, the CUAS looks for a related entry in the ID-DB. If no such ID is found, the next state will be ID not in ID-DB. The CUAS tries to clarify this situation by checking if the ID has a corresponding entry in the AUTH-DB. If this is not the case, the CUAS moves to the state Unknown ID and executes Protocol 2 to clarify the reason for the missing ID and the missing performance authorization. Executing this protocol can lead to one of four results:

1) Restoring technical issues causing database misses.
2) Tolerating the missing ID and authorization.
3) Immediate interdiction of the drone.
4) Delayed interdiction of the drone.

In contrast, if AUTH-DB has a related entry, the CUAS initiates Protocol 3 to clarify the reason for the missing ID in the ID-DB. Executing this protocol may lead to restoring the technical issue in the ID-DB or tolerating the missing ID.

An authentic and known ID can be invalid for different reasons. For example, the operator may miss renewing the registration (if required) or the authority/USS may miss updating the ID-DB on time. When the CUAS finds out that the received ID has expired (Expired ID), it checks if the AUTH-DB has authorization for this ID in the current time and area. If no entry is found, the drone moves to the state Expired ID & Unauthorized. Protocol 4 is initiated to clarify this state. Three outcomes are possible:

1) Restoring the technical issues in both databases.
2) Tolerating the expired ID and the missing authorization.
3) Delayed interdiction.

In contrast, if the CUAS finds a related entry in the AUTH-DB, it initiates Protocol 5 with two possible outcomes:

1) Restoring the technical issue related to the ID-DB.
2) Tolerating the expired ID.

If the received ID is adequate (authentic, known, and valid) but the AUTH-DB doesn’t have a performance authorization
Fig. 3. Post-detection model for drones from CUAS perspective. The drone is modeled as a finite-state machine. A cooperative drone passes multiple checks transiting from one green state to another. A drone that fails some check transits to an orange state that can trigger some clarification protocol.

for this drone, then Protocol 6 is executed. Three outcomes are possible:

1) Restoring the technical issue in the AUTH-DB.
2) Tolerating the missing performance authorization.
3) Delayed interdiction.

When the CUAS finds out that the drone is flying outside the area specified in the authorization certificate in the AUTH-DB, it executes Protocol 7. This protocol has one of the following outcomes:

1) Bringing the drone back to the authorized area by the operator.
2) Tolerating the area violation.

3) Delayed interdiction.

Finally, when the CUAS finds out that the operator has exceeded the mission time specified in the authorization certificate, it executes Protocol 8. This protocol has one of the following outcomes:

1) Terminating the mission by the operator.
2) Tolerating time violation
3) Delayed interdiction.

The states Tolerate ID Failure and Tolerate AUTH Failure can be reached from different states as described above. To keep the diagram clear, we did not draw the related transitions but used the numbers 1 to 6 to refer to them. Apart from this,
these states are equivalent to the states Valid ID and Authorized Mission, respectively. Nonetheless, if called twice (or another number of times depending on the authority policy), a protocol will generate an interdiction approval to avoid deadlocks. This means that the system does not tolerate a UAS operator who fails to clarify his identity repeatedly.

V. CLARIFICATION PROTOCOLS

The clarification protocols aim at resolving unclear cases towards an accurate classification of the detected drone. In this section, we describe these protocols by first explaining when a protocol is triggered. Then, we summarize the possible outcomes of the protocol using a table and describe its flow using a sequence diagram as far as necessary. For simplicity, we use simple natural language to label the exchanged messages. In the text, the labels are in capital letters for clarity.

A. Protocol 1: Clarify Missing ID Transmission

The objective of Protocol 1 is to clarify the situation when the CUAS does not receive an ID from the drone. In this case, the CUAS accesses the authorization database (AUTH-DB) to check if there is an operator who is authorized to fly in the respective time and zone. If such an entry exists in the database, the corresponding operator is regarded as the potential operator of the detected drone. The CUAS initiates Protocol 1 to clarify whether this potential operator the actual one is, i.e., the one operating the detected drone. First, the CUAS sends a message named 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 or his USS. The authority receives one of the responses or no response from the operator as outlined in Table I (CASE 1 to CASE 5).

In the case of no response (CASE 1) or when the operator confirms that he/she is already transmitting the ID (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, which may file a lawsuit case, see Fig. 4. The drone operator claims that he/she is unable to restore ID, or that he/she is not flying (CASE 2). Clarify the situation when the CUAS does not receive an ID from the drone. In these two cases, the drone operator either does not respond before the timeout or respond with a “I AM NOT FLYING” message.

In the case of no response (CASE 1) or when the operator confirms that he/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, which may file a lawsuit case, see Fig. 4.

When the operator confirms that he is already transmitting the ID (CASE 3) or that he is unable to restore his ID transmission for any reason (CASE 4), then the authority must conduct a risk assessment, see Fig. 5. The risk assessment should take into consideration the criticality of the mission and the no-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, 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 can interdict the drone after the time-out specified in this message.
would be regarded as an implicit confirmation. In contrast, if the ID restoration was not accomplished, the CUAS would re-send the message NO ID BUT POTENTIAL OPERATOR to the authority. The latter would consider the repeated reception of this message as an invalidation of the ID restoration. An invalidated ID restoration (CASE 6) prompts the authority to perform a fast risk assessment and to act depending on the assessed risk level as illustrated in Fig. 6.

![Fig. 6. Protocol 1 (Clarify Missing ID Transmission, CASE 5 and CASE 6). The drone operator claims that the ID is restored.](image)

**B. Protocol 2: Clarify Unknown ID Issue**

The objective of this protocol is to clarify the situation when the CUAS receives an authentic Remote ID but does not find a related entry, neither in the ID-DB nor in the AUTH-DB. This can have technical reasons related to the update or retrieval of these databases. In the worst case, however, receiving an unknown ID can indicate a security break. First, the CAUS sends an UNKNOWN ID message to the authority. This message includes the received Remote ID. The authority performs necessary checks to find out whether such an ID exists or whether there is a technical issue causing the misses in the databases. Depending on the result of these checks, three outcomes are possible as summarized in Table II.

![Fig. 7. Protocol 2 (Clarify Unknown ID Issue)](image)

**TABLE II**

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

In failure-free operation, all authentic IDs are expected to be in the ID database. If the authority finds no technical issues related to the databases, it assumes a security break (CASE 1) because the CUAS has already verified the authenticity of the received ID. For example, the operator can have access to the authority’s private key. As a response, the authority sends an IMMEDIATE INTERDICTION AUTHORIZATION message to the CAUS. To keep the drone intact for forensics analysis, the authority may request the CUAS to use a non-destroying technology for the interdiction in this case.

Alternatively, the authority may find out that the drone is registered but not authorized to fly (CASE 2). This means that the CUAS conclusion regarding the performance authorization was correct but there is a technical failure related to the ID-DB because it did not show the ID. In this case, the authority sends a STOP MISSION message to the operator and an INTERDICT AFTER TIME-OUT message to the CUAS.

Finally, the authority may identify a technical issue related to the management of both databases (CASE 3). In this case, the CUAS receives a TOLERATE AUTH FAILURE message. This message implies that the ID is authentic, so the CUAS does not need to recheck this.

**C. Protocol 3: Clarify Missing ID in ID-DB**

This protocol is used to clarify the situation when the CUAS receives an authentic Remote ID but does not find a related entry in the ID-DB and, at the same time, the AUTH-DB has a performance authorization for this ID in the respective time and area. At first glance, one may attribute this case to an administrative fault. In particular, we may assume that the authority had issued a performance authorization without checking the validity of the ID. While this scenario is possible, it is excluded from our analysis because we assumed in Section III-C that expired IDs are not removed from the database.

First, the CAUS sends an ID-BD MISS message to the authority. This message includes the received Remote ID. The authority performs necessary checks. If it identifies a technical
issue related to ID-DB management, it sends a TOLERATE ID Failure message to the CUAS and works on resolving the technical issue. Alternatively, the authority can resolve this issue and request the CUAS to confirm this restoration. The latter can respond explicitly or implicitly. Note that the operator is not involved in this protocol. The outcomes of this protocol are summarized in Table III.

D. Protocol 4: Clarify Unauthorized & Expired ID

![Diagram](image)

This protocol deals with a drone that is transmitting an authentic but expired ID. Also, the drone is not authorized to fly. In this case, the CAUS first sends the message EXPRESSED ID & UNAUTHORIZED MISSION to the authority. The authority performs necessary checks to find out if there are any technical issues related to the databases. If no issue is found, the authority sends a STOP MISSION message to the operator and a TIMED INTERDICT AUTHORIZATION. In contrast, if a technical issue is identified, the authority sends a TOLERATE AUTH FAILURE message to the CUAS and works on fixing the problem. The message sequence diagram of this protocol is shown in Fig. 8.

![Diagram](image)

E. Protocol 5: Clarify Authorized But Expired ID

This protocol is executed when the received Remote ID is authentic, included in the ID-DB, and valid; but there is no related performance authorization in the AUTH-DB. To clarify this situation, the CAUS sends an AUTH-DB MISS message to the authority, see Fig. 9. The latter checks if the missing authorization is due to a technical problem such as the lack of a timely update (CASE 1), see Table IV. If this is the case, the issue is resolved and the CUAS is informed by sending the message AUTH-DB MISS RESOLVED. Otherwise and depending on a risk assessment, the authority requests the operator to stop the mission and the CUAS to interdict after a time-out (CASE 2). Alternatively, the CUAS can be requested to tolerate this mission if the risk is low (CASE 3).

![Diagram](image)

F. Protocol 6: Clarify Missing AUTH

![Diagram](image)

This protocol is executed when the received Remote ID is authentic, included in the ID-DB, and valid; but there is no related performance authorization in the AUTH-DB. To clarify this situation, the CAUS sends an AUTH-DB MISS message to the authority, see Fig. 9. The latter checks if the missing authorization is due to a technical problem such as the lack of a timely update (CASE 1), see Table IV. If this is the case, the issue is resolved and the CUAS is informed by sending the message AUTH-DB MISS RESOLVED. Otherwise and depending on a risk assessment, the authority requests the operator to stop the mission and the CUAS to interdict after a time-out (CASE 2). Alternatively, the CUAS can be requested to tolerate this mission if the risk is low (CASE 3).

![Diagram](image)

G. Protocol 7: Clarify Area Violation

This protocol is executed when the received Remote ID is authentic, included in the ID-DB, and valid; but there is no related performance authorization in the AUTH-DB. To clarify this situation, the CAUS sends an AUTH-DB MISS message to the authority, see Fig. 9. The latter checks if the missing authorization is due to a technical problem such as the lack of a timely update (CASE 1), see Table IV. If this is the case, the issue is resolved and the CUAS is informed by sending the message AUTH-DB MISS RESOLVED. Otherwise and depending on a risk assessment, the authority requests the operator to stop the mission and the CUAS to interdict after a time-out (CASE 2). Alternatively, the CUAS can be requested to tolerate this mission if the risk is low (CASE 3).

![Diagram](image)
### TABLE VI

**OUTCOMES OF PROTOCOL 7 (CLARIFY AREA VIOLATION)**

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

If the operator does not respond to this message (CASE 1), the authority requests the operator to stop the mission and authorizes the CUAS to interdict the drone after a time-out, see Fig. 10.

When the operator contradicts the request by claiming that he did not exceed the permitted area (CASE 2) or when he declares that he cannot return to the authorized zone (CASE 3), the authority must perform a fast risk assessment to take an appropriate decision as detailed in Fig. 11.

In CASE 4, the operator confirms that he returned to the authorized area. The authority asks the CUAS for confirmation. If the latter invalidates the mission stop (CASE 5), the authority decides to request the operator to stop the mission and the CUAS to interdict after a time-out.

### VI. SYSTEM SIMULATION AND EVALUATION

To validate the post-detection model and the clarification protocols, we first developed a high-level model for the system in Matlab. The purpose of this model is to verify the functionality of the proposed system and to identify any errors such as unreachable states, missing transitions, and deadlocks. For this, we used the Stateflow Toolbox [38] that provides a graphical programming language to design and test combinatorial and sequential decision logic using state machines and flowcharts. Besides, this tool offers runtime and edit-time checks to ensure design consistency and completeness before implementation. We created three state machines using this toolbox: the post-detection model that runs on the CUAS side and two additional machines to model the behavior of authority and the operator. The three models were synchronized using global events and executed in parallel to analyze the interaction between the three agents. The toolbox generates sequence diagrams to visualize the system operation as illustrated in the example of Figure 12 that shows the sequence diagram of case 3 of Protocol 8.

In addition to this functional simulation, we implemented the models and protocols and conducted performance testing to evaluate the system behavior in real-time. The goal is to analyze the system performance under different scenarios and with multiple drones. For this purpose, we used Node.js that

---

1 Protocol 8 is very similar to Protocol 7. The operator response may lead to five possible outcomes with similar cases. For space reasons, we omitted the outcomes table and the sequence diagrams.
Fig. 12. Simulated sequence diagram of Protocol 8 CASE 3

This work is submitted to an IEEE journal.

Fig. 13. Overview of the simulation environment.

Fig. 14. Entity-relationship diagram showing the relationship between the drone, operator, and missions.

VII. DISCUSSION

To understand the impact of the clarification process on the system performance, we should consider the simulation results in the context of a full counter-drone operation that usually includes three steps: detection/classification, clarification, and interdiction. Remember that the system can decide to tolerate the drone as outlined in Figure 3. In such a case, the clarification time becomes insignificant because there is no need to counter the drone. In contrast, the clarification protocols can affect the system performance when the drone is classified as uncooperative and needs to be interdicted immediately or after a timeout. So, we have four delay components in total:

1) Detection and classification time.
2) Clarification time
3) Timeout
4) Interdiction time

We now discuss these time components and try to assign some example values analytically or based on the literature.
Reports on the time needed to detect and classify a drone are scarce. Recently, Basak et al. [9] proposed a combined drone detection and classification framework using Yolo Lite. They reported a mean inference time of 1.16 seconds for the detection and classification of one drone using a single signal. The timeout should be sufficient for at least allowing the operator to land his drone safely. Safe landing takes place at low speeds in the range of a couple of meters per second, e.g., 4 m/sec as reported in [36]. So, if the drone is at an altitude of 100m, the landing would take around 25 seconds. The interdiction time depends on the used technology. Jamming is one of the fastest solutions due to its non-kinetic nature. Although the jamming signal should be directed to reduce side effects, the market is rich in off-the-shelf solutions with omnidirectional interceptors that block the communication immediately after switching on. So, the interdiction time of such systems would be negligible. Finally, the simulation results showed that the clarification time is around 2.5 seconds in the case of one drone.

For these example values, we conclude that the contribution of the clarification time to the total system delay is $\frac{2.5}{1.16 + 2.5} = 68\%$, when immediate interdiction is required, $\frac{2.5}{1.16 + 2.5 + 25} = 9\%$, when the drone should be interdicted after a timeout or $\frac{2.5}{1.16 + 2.5 + \infty} = 0\%$, when the drone should be tolerated.

Although this quantitative analysis gives an overall estimation of the proposed solution, it has some limitations which make the results look optimistic or pessimistic. For example, our simulation ran on a single computer. While a real deployment would use distributed systems and servers that are typically faster, network delays would affect the clarification time. Furthermore, we considered a best-case interdiction time of zero which makes our results pessimistic. On the other hand, we did not include the operator’s response time during the clarification process. Indeed, real-time measurements on a working implementation of the system with detailed testing scenarios are indispensable for understanding the system’s capabilities and challenges.

Apart from the timing aspects, we concentrated on functional aspects of the system and did not implement security techniques, e.g., for message encryption and authentication. System security is extremely important for this application. Intruders could attack the system and inject fake messages that can lead to drone misclassification with fatal consequences. Finally, in the proposed system, we did not define the messages’ formats. We believe that such activities are beyond the scope of this research and should be addressed collectively by consortiums interested in standardization.

VIII. Conclusion

Currently, developers of UTM systems and counter-drone systems are working in parallel. Drone operators are still benefiting from the current legal situation that prohibits the interdiction of aerial vehicles. Many efforts are on the way to change this situation and we will soon see regulations for counter-drone operations. But like always, regulations are for those who follow them. The system must be prepared to deal with malfunctions, technical faults, and malicious users. The paper showed that the real-time coordination of the drone and counter-drone operation is not a trivial task. The simulation results are promising but real deployments and pilot tests are
required to understand the actual dimensions of the problem and the challenges to overcome. We hope that the proposed architecture, models, and protocols will give some directions for system developers to start integrating CUAS and UTM systems and address open issues.

REFERENCES

[1] Federal Aviation Administration. UAS Remote Identification Overview, 2021.

[2] European Union Aviation Safety Agency. Commission Delegated Regulations (EU) 2020/1058, 2020.

[3] Cemal Aker and Sinan Kalkan. Using deep networks for drone detection. In 2017 14th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), pages 1–6. IEEE, 2017.

[4] Azza Alloouch, Omar Cheikhrouhou, Anis Koubâa, Khalifa Toumi, Mohamed Khalgui, and Tuan Nguyen Gia. Utm-chain: blockchain-based secure unmaned traffic management for internet of drones. Sensors, 21(9):3049, 2021.

[5] Riham Altawy and Amr M Youssef. Security, privacy, and safety aspects of civilian drones: A survey. ACM Transactions on Cyber-Physical Systems, 1(2):1–25, 2016.

[6] Murad Zohaib Anwar, Zeeshan Kaleem, and Abbas Jamalipour. Machine learning inspired sound-based amateur drone detection for public safety applications. IEEE Transactions on Vehicular Technology, 68(3):2526–2534, 2019.

[7] Michael J Armstrong, George R Hutchins, and Timothy A Wachob. Interdiction and recovery for small unmanned aircraft systems, September 3 2019. US Patent 10,401,129.

[8] Cristin Barrado, Mario Boyero, Luigi Bruculieri, Giancarlo Ferrara, Andrew Hatley, Peter Hullah, David Martin-Marrero, Enric Pastor, Anthony Peter Rushton, and Andreas Volkert. U-space concept of operations: A key enabler for opening airspace to emerging low-altitude operations. Aerospace, 7(3):24, 2020.

[9] Sanjoy Basak, Sreeraj R Rajendran, David Martin-Marrero, and Bart Scheers. Combined rf-based drone detection and classification. IEEE Transactions on Cognitive Communications and Networking, 2021.

[10] Oussama Bekkouche, Miloud Bagaa, and Tarik Taleb. Toward a utm-based service orchestration for uavs in mec-nfv environment. In 2019 IEEE Global Communications Conference (GLOBECOM), pages 1–6. IEEE, 2019.

[11] Anjan Chakrabarty, Corey A Ippolito, Joshua Baculi, Kalmanje S Krishnakumar, and Sebastian Hening. Vehicle to vehicle (v2v) communications for collision avoidance for multi-copters flying in utm-tc4. In AIAA Scitech 2019 Forum, page 0690, 2019.

[12] Christopher Chin, Karthik Gopalakrishnan, Maxim Egorov, Antony Evans, and Hansa Balakrishnan. Efficiency and fairness in unmanned air traffic flow management. IEEE Transactions on Intelligent Transportation Systems, 2021.

[13] Christopher Courtin, Michael J Burton, Alison Yu, Patrick Butler, Parker D Vasick, and R John Hansman. Feasibility study of short takeoff and landing urban air mobility vehicles using geometric programming. In 2018 Aviation Technology, Integration, and Operations Conference, page 4151, 2018.

[14] Gordon Darroch. Gatwick airport: Drones ground flights. BBC, 2018-20-12.

[15] DeDrone. Worldwide drone incidents, 2020.

[16] Jan Dentler, Somasundar Kannan, Miguel Angel Oliveres Mendez, and Holger Voos. A real-time model predictive position control with collision avoidance for commercial low-cost quadrotors. In 2016 IEEE conference on control applications (CCA), pages 519–525. IEEE, 2016.

[17] Jędrzej Drozdowicz, Maciej Wiego, Piotr Sameczynski, Krzysztof Kulpa, Jaroslaw Krzonkalla, Maj Mordzonek, Marcin Bryl, and Zbigniew Jakielaszek. 35 ghz fm ew drone detection system. In 2016 17th International Radar Symposium (IRS), pages 1–4. IEEE, 2016.

[18] FAA. Unmanned aircraft system (uas) traffic management (utm) concept of operation. Technical report, 2020.

[19] FAA. Uas data exchange (laanc). https://www.faa.gov/uas/programs_partnerships/data_exchange/, 2020-29-02.

[20] Mostafa Hassanalian and Abdessattar Abdelkafi. Classifications, applications, and design challenges of drones: A review. Progress in Aerospace Sciences, 91:99–131, 2017.

[21] Geon-Hwan Kim, Imtiaz Mahmud, and You-Ze Cho. Self-recovery scheme using neighbor information for multi-drone ad hoc networks. In 2017 23rd Asia-Pacific Conference on Communications (APCC), pages 1–5. IEEE, 2017.

[22] Chao Lin, Debiao He, Neeraj Kumar, Kim-Kwang Raymond Choo, Alexey Vinel, and Xinxi Huang. Security and privacy for the internet of drones: Challenges and solutions. IEEE Communications Magazine, 56(1):64–69, 2018.

[23] Huan Liu, Xiaomiao Li, Guohua Wu, Mingfeng Fan, Rui Wang, Liang Gao, and Wtold Pedrycz. An iterative two-phase optimization method based on divide and conquer framework for integrated scheduling of multiple uavs. IEEE Transactions on Intelligent Transportation Systems, 2020.

[24] Georgia Lykou, Dimitrios Moustakas, and Dimitris Grzitalis. Defending airports from uas: A survey on cyber-attacks and counter-drone sensing technologies. Sensors, 20(12):3537, 2020.

[25] Arthur Holland Michel. Counter-drone systems, 2019.

[26] Thomas Muñoz. Alexander Ganis, Ulrich Prechtel, Enric Miralles, Askold Meusling, Jan Mietzner, Martin Vossiek, Mirko Loghi, and Volker Ziegler. Low-cost jamming system against small drones using a 3d mimo radar based tracking. In 2017 European Radar Conference (EURAD), pages 299–302. IEEE, 2017.

[27] Natasa Neogi, Siddhartha Bhattacharyya, Daniel Griessler, Harshita Kiran, and Marco Carvalho. Assuring intelligent systems: Contingency management for uas. IEEE Transactions on Intelligent Transportation Systems, 2021.

[28] Phuc Nguyen, Mahesh Ravindranatha, Anh Nguyen, Richard Han, and Tam Vu. Investigating cost-effective rf-based detection of drones. In Proceedings of the 2nd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use, pages 17–22, 2016.

[29] James O’Malley. The no drone zone. Engineering & Technology, 14(2):34–38, 2019.

[30] Seongjoon Park, Hyeong Tae Kim, Sangmin Lee, Hyoentae Joo, and Hawngnam Kim. Survey on anti-drone systems: Components, designs, and challenges. IEEE Access, 9:42635–42659, 2021.

[31] Colleen Reiche, Adam P Cohen, and Chris Fernando. An initial assessment of the potential weather barriers of urban air mobility. IEEE Transactions on Intelligent Transportation Systems, 2021.

[32] Julian Rothe, Michael Strohmeyer, and Sergio Montenegro. A concept for catching drones with a net carried by cooperative uavs. In 2019 IEEE International Symposium on Safety, Security, and Rescue Robotics (SSRR), pages 126–132. IEEE, 2019.

[33] Richard Ryan, Sara Al-Rubaye, Graham Braithwaite, and Dimitrios Panagiotakopoulos. The legal framework of utm for uas. In 2020 AIAA/IEEE 39th Digital Avionics Systems Conference (DASC), pages 1–5. IEEE, 2020.

[34] Zsolt Sándor. Challenges caused by the unmanned aerial vehicle in the air traffic management. Periodica polytechnica transportation engineering, 47(2):96–105, 2019.

[35] Mia Stevens and Ella Atkins. Geofence definition and deconfliction for uas traffic management. IEEE Transactions on Intelligent Transportation Systems, 2020.

[36] Indreswari Suroso and Erwinh Imrawan. Analysis of uav multicopter of air photography in new yogyakarta international airports. TELKOMNIKA, 17(1):521–528, 2019.

[37] Bilal Taha and Abdulhadi Shoufan. Machine learning-based drone detection and classification: State-of-the-art in research. IEEE Access, 7:13669–138682, 2019.

[38] Inc. The MathWorks. Stateflow toolbox, 2021.

[39] Cynthia Wolter, Lynne Martin, and Kimberly Jobe. Human-system interactions in air traffic flow management for uas. IEEE Transactions on Intelligent Transportation Systems, 14(11), 2019.