

Remote ID for Rapid Assessment of Flight and Vehicle Information

Abraham K. Ishihara*

Stinger Ghaffarian Technologies, Inc, Moffett Field, CA, 94305

Joseph Rios†

NASA, Moffett Field, CA, 94305

Priya Venkatesan‡

Stinger Ghaffarian Technologies, Inc, Moffett Field, CA, 94305

The ability to rapidly identify UAS in the field has emerged as a critical need for the integration of small UASs into the national airspace and counter-uas operations. This paper proposes an architecture for rapid retrieval of UAS information leveraging NASA’s current Unmanned Aircraft System (UAS) Traffic Management (UTM) system. The proposed architecture utilizes UTM components: FIMS (Flight Information Management System), USS (UAS Service Supplier), and vehicle registration and model database in order to provide assessment of the UAS reported in the field including the ability to distinguish between participating and non-participating UTM actors. Detailed system descriptions are provided and preliminary results from field tests conducted during UTM TCL (Technical Capability Level) 3 are discussed. It is found that 94% of the remote ID look-ups were successful. The average time of a look-up is found to be 1.2 seconds. Failure cases are examined and recommendations on next steps to advance UAS remote identification are provided.

I. Introduction

By 2024, the commercial drone market is estimated to reach 17 billion US dollars [1]. Much of this growth can be attributed to significant venture capital investment over the last several years coupled with more capable UAS platforms targeting information and value-add services. Agriculture applications, for example, continue to drive market demand in the areas of crop monitoring, spraying, and soil and crop health. UAS package delivery is projected to save up to 50 billion US dollars as a result of 50 million drone deliveries per day [2].

With the potential of millions of drones simultaneously accessing the airspace in the near future, there is significant concern regarding the ability to distinguish participating from non-participating actors in the Unmanned Aircraft System (UAS) Traffic Management (UTM) system. There have been increasing reports of criminals and organized crime leveraging advancements in drone technologies in order to surveil targets [4], deliver contraband to prison inmates [5], and smuggle narcotics across borders [12]. Recently in Staten Island, NY, a hobbyist UAS unwittingly entered airspace where a Blackhawk UH-60M assigned to the 82nd Airborne Division was located [15]. The quadrotor collided with the Blackhawk causing damage to the main rotor blade.

In response to these events, Counter-UAS or C-UAS has emerged as a critical need in both the public and private sectors [16, 17]. Although legal challenges abound [18], there has been recent venture capital investment in companies such as Citadel Defense Co. and Securus Technologies [20]. Over 230 counter-UAS products currently exist or are under development worldwide spanning a range of technologies including radar, active and passive optics, acoustics, electromagnetic emissions, and magnetic field detection [21]. While counter-UAS technologies continue to make inroads with respect to detection of one or more vehicles in cluttered environments (for example, an urban setting), rapid UAS identification and the ability to distinguish participating from non-participating actors in the UTM system remains a significant challenge. For comprehensive, end-to-end counter-UAS solutions, four components are required (collectively referred to herein as DIAD and depicted in Fig. 1): (1) **Detect UAS**; (2) **Identify UAS**; (3) **Assess safety and risk metrics**; (4) **Defeat UAS** (disable or thwart mission objectives).

*NASA Ames Research Center, Moffett Field, CA., AIAA Member

†NASA Ames Research Center, Moffett Field, CA., AIAA Senior Member

‡NASA Ames Research Center, Moffett Field, CA., AIAA Member

The **Detect** block refers to process by which a collection of phenomenological data is acquired by one or more sensors (active or passive [21]) and processed via sensor fusion or other techniques in order to locate and track a potential drone as it traverses its flight path. The block labeled **Identify**, which is the primary focus of this paper, constitutes the point in the flow where information is gleaned from the detect block and provides registration and/or position information to a public safety USS (discussed below) to ‘look-up’ or acquire corresponding information in the UTM system. The information provided by the UTM system could include vehicle performance specifications, past flight data including detailed trajectory and planning information, current and future flight plan information and owner contact details.

Historical information could be useful in order to predict anomalous behavior. While it is not known the type of traffic patterns that may emerge* as the UTM system unfolds, machine learning techniques could be used to identify in near real-time unusual flight patterns arising from witting or unwitting actors. For example, package delivery trajectories may follow relatively predictable patterns given a set of known parameters such as vehicle type, time of year, location, weather, and other economic metrics. At the same time, delivery routes may be located near assets vulnerable to a potential UAS threat that would require rapid intervention to defend.

Assessment, the third block, comprises the garnering and processing of all relevant information from the detect and identify blocks as well as additional information regarding the asset to be protected. Risk metrics are evaluated and a decision is made as to how to defeat the potential threat, if any. This leads to the **Defeat** block and its options will depend on the progression of counter-UAS technologies as well as the rules and regulations that are under consideration presently. Further discussion of detect, assess, and defeat is beyond the present scope.

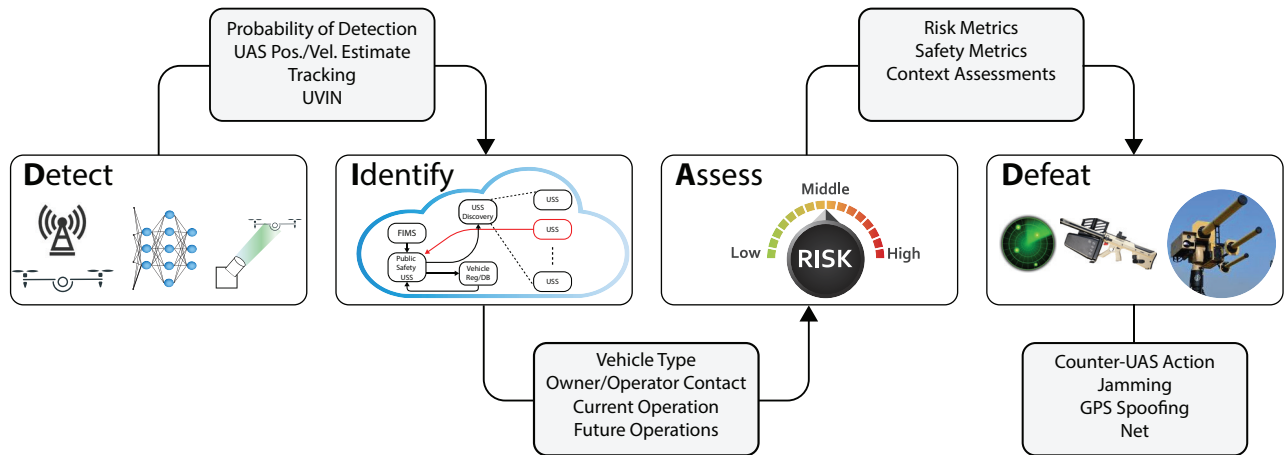


Fig. 1 Detect Identify Assess Defeat (DIAD)

The primary contributions of this paper are as follows: (1) initial architecture for remote ID in the context of the UTM system, (2) description of the preliminary prototype deployed, and (3) initial assessment of the system used in UTM TCL3 field tests conducted February through June 2018.

The remainder of this paper is as follows: In Section II, a brief description of the problem and relevant background information on the NASA UTM project is presented. In Section III, the initial remote ID architecture and scenarios are discussed. The main results are presented in Section IV and summary in Section V.

II. Background and Previous Results

By 2021, the combined number of commercial and hobbyist UASs could reach 6 million [23]. The scale, type, risk, and increasing complexity of the potential UAS operations would likely overwhelm the existing Air Traffic Management (ATM) system. To address this challenge, NASA developed an initial concept termed Unmanned Aircraft System (UAS) Traffic Management (UTM) in 2015 [24] which provided a research platform to test and integrate innovative strategies and solutions. In collaboration with the FAA, UTM has evolved and consists of a suite of services [25] to aid the management of complex UAS operations in uncontrolled (Class G) airspace. It establishes safe, efficient, and secure

*Traffic patterns will likely be driven by market need and regulatory requirements which are currently evolving.

mechanisms for UAS operators to share flight operation intent and receive common situational awareness. The elements of UTM consist of: (1) USS (UAS Service Supplier) which is the entity that receives flight operations from a UAS operator and provides support for deconfliction, conformance monitoring, and communication with FIMS; (2) FIMS (Flight Information Management System) which is the centralized gateway of information between the USSs and FAA; (3) SDSP (Supplementary Data Service Supplier) which is the entity that provides data or services to USSs or UAS operators. Further description of the UTM system and its interplay between ATC services can be found in [25].

In 2018, NASA worked with six test sites to demonstrate UTM Technical Capability Level (TCL) 3 which explored the following elements: (1) Moderate Population; (2) Moderate Traffic Density; (3) Suburban Applications; (4) Mixed Operations; (5) Vehicle to Vehicle Communication; (6) Public Safety Operations. The test sites were located in Alaska, North Dakota, Nevada, New York, Texas, and Virginia.

In support of the UTM project, a vehicle registration and model database, called Vehicle Registration and Model Database (VRMD). The VRMD enables the storage and retrieval of detailed vehicle-specific information for use in trajectory performance analysis and potential counter-UAS applications. The total number of manufacturers that currently exists in the database is 168 and total number of distinct vehicles types (available to select as part of the registration process) is 474. This includes both publicly available vehicles and custom vehicles (vehicles built or customized for this test or are otherwise not publicly available). Fig. 2. summarizes the current state of VRMD.

As part of UTM TCL3 field test (across the six test sites), approximately 124 vehicles registered via the NASA VRMD system. The registered vehicles include vehicles that were reserved for backup and vehicles that failed and were replaced during the course of preparation for the testing events. Sixteen of the vehicles were used for simulation. Registration was facilitated by a web-portal made publicly available and partners from the test sites were provided access through NASA's access and identity control system. Prior to performing any testing, all vehicles that were anticipated to fly had to register and provide detailed vehicle model specifications.

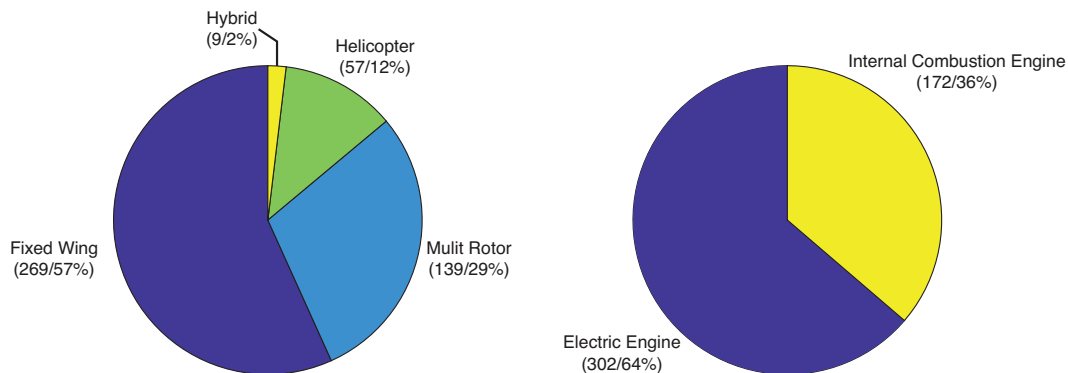


Fig. 2 UTM Vehicle Registration and Model Database (VRMD) Summary. At the time of this writing, the database contains 474 distinct vehicle types that operators can select from during the registration process. Each vehicle type has associated with it detailed model specifications which can be queried via the VRMD API.

The process of registering a vehicle involves selecting the vehicle type from a vehicle list (containing the 474 vehicle types) and entering additional vehicle instance (the realization of a vehicle type) information. Upon its creation, VRMD issues a universally unique identifier (version 4 UUID), which is used as the UTM Vehicle Identification Number (UVIN). Binding UVINs to GUFIs (Globally Unique Flight Identifiers) used by USSs enable rapid access to vehicle and operation specific data for remote ID and other data analyses.

Having discussed the UTM background, the TCL3 testing phase, and the VRMD, the remote ID architecture is now described.

III. UTM Remote ID System

A. Architecture

The remote ID architecture that was implemented in UTM TCL3 is shown in Fig. 3. The primary objective of the remote ID concept is to test and validate a list of scenarios where identification of a vehicle is required by an authorized

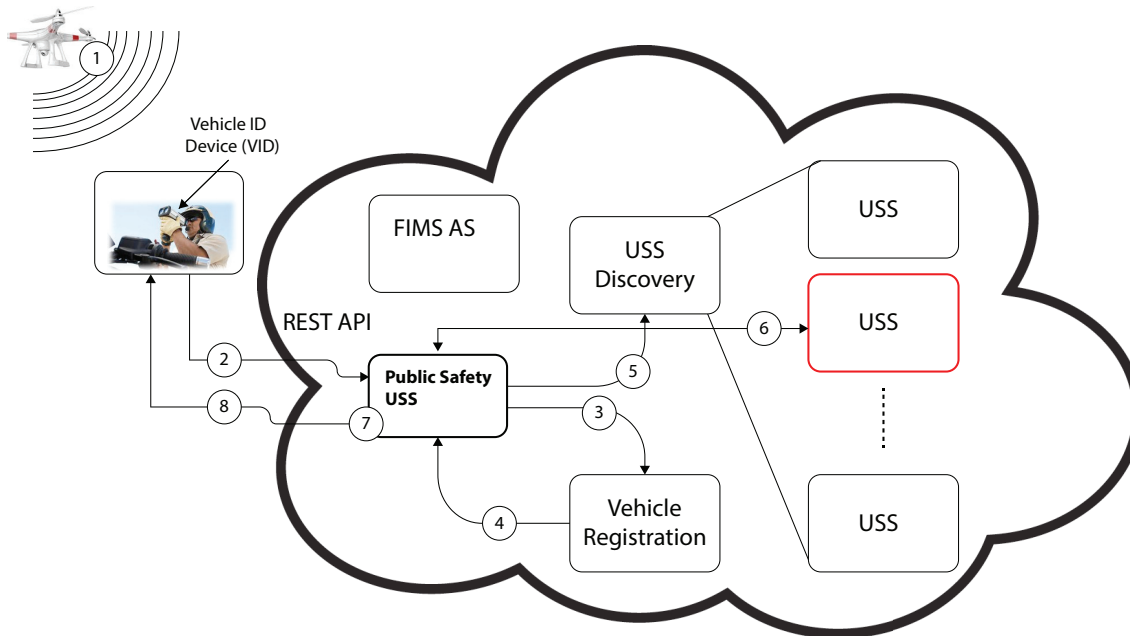


Fig. 3 UTM Remote ID Flow Diagram

entity working near the operation. An example of this scenario is when a police officer observes a UAS flying overhead and requires the following:

- 1) Identification of the UAS owner and contact
- 2) Vehicle properties including class (fixed-wing, quad, etc.)
- 3) Current flight plan, vehicle speed and heading, and future operations
- 4) UTM state of the corresponding flight plan, e.g. ROGUE, NON-CONFORMING, etc.

Given the above information, the officer may assess the situation and choose the appropriate counter-UAS measure. It is important to note that a counter-measure might be as simple as contacting the owner/operator and conveying that the vehicle should not be there. If the owner/operator, ‘turns the vehicle around’ then that mission was effectively ‘defeated’ from the public safety officer’s point of view.

The test sites conducted one or more of the test scenarios discussed below. Each test scenario involves (1) a UAS to be remotely identified and zero or more UASs nearby that may also be simultaneously broadcasting drone identification information, (2) a public safety USS, (3) a public safety user who performs the remote UAS identification and validates the results of the tests, and (4) a USS that receives the original flight plan for the UAS to be identified (note that certain tests which do not include vehicle registration and/or proper flight plan submission to a USS excluded this component). A public safety USS is a USS that has been granted by FIMS the *PUBLIC_SAFETY* role. Bound to this role are a number of public safety permissions enabling it to request information from other USSs and query VRMD to obtain detailed vehicle information required for remote ID. A public safety user is a person who is registered with a public safety USS and has relevant credentials/authorization to communicate with it using a suitable device (tablet, phone, etc) over the public internet. Test sites determined and provided the appropriate hardware and software for both the UAS to be identified and the public safety user (the sensors are described in Section IV).

The remote ID system for identifying a UAS is a multi-step process. Also, some specific use cases may not require each step. The steps are as follows:

- Step 1:** A UAS is detected by one or more sensors corresponding to the **Detect** block in Fig. 1. This includes any additional information such as the broadcast of position and UVIN (registration) data.
- Step 2:** After acquiring the information, the Vehicle Identification Device (VID)[†] transmits an HTTP GET request to a public safety USS.

[†]In this paper, the device that detects the vehicle and transmits the information to the public safety USS is referred to as the VID. However, in general this could be any system and need not be a portable device.

- Step 3:** If the information received contains a UVIN, the public safety USS requests information from the UTM Vehicle Registry and Model Database (VRMD). The public safety USS has specialized roles that enable it to access required vehicle information including make, model, owner contact information, and other properties.
- Step 4:** The response from VRMD is also returned indicating whether the vehicle has been found or not and the additional information required for remote ID.
- Step 5:** The public safety USS sends a request to the USS Discovery Service. The USS Discovery Service receives the request and retrieves the ‘owning’ USS instance (highlighted in red in Fig. 3). This request is based on the UVIN and/or reported 4d position estimate of the UAS as determined by the VID (Detect block in Fig. 1). An illustration of this process for two overlapping USS instances is shown on the left side of Fig. 4. A USS instance is a specific realization defined by a bounding rectangle. A USS may instantiate zero or more USS instances to support its missions.
- Step 6:** The public safety USS then performs an inquiry to the ‘owning’ USS to retrieve additional information such as the current flight operation submitted (GUFIs), current UTM state, position and velocity of the UAS (if identified), and future flight operations. Depending on the scenario, the ‘owning’ USS instance many need to be selected from a list of candidate USS instances. This is illustrated on the right side of Fig. 4. UTM operation states include states such as ACTIVE, ROGUE, NON-CONFORMING, AND CLOSED. Further information can be found in [27].
- Step 7:** The public safety USS assembles all relevant pieces of information and performs Drone Observation Resolution (DOR) - a process where it provides its ‘best’ estimate of the observed vehicle and its status with respect to the UTM ecosystem. This could be challenging when there exists multiple overlapping USSs and multiple operations overlapping in time and space. In addition, position updates and other messages could be used to fine-tune the estimate.
- Step 8:** The DOR is assembled and returned to the VID for display to the public safety user.

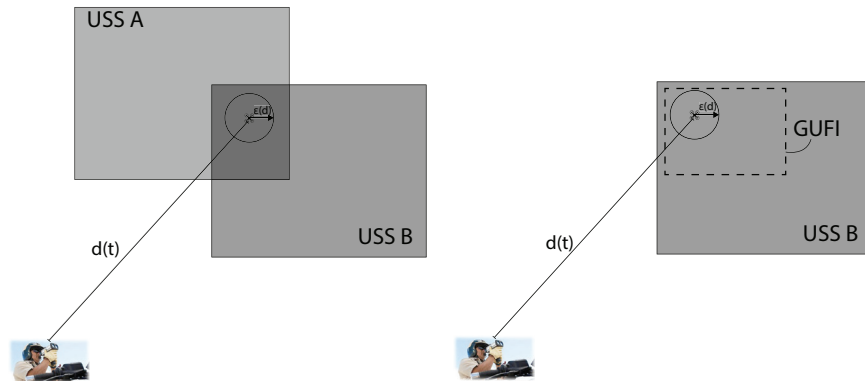


Fig. 4 [Left]: Overlapping USS Instances. The UAS location transmitted by the VID is located in a region of intersection between two USS Instances. Both USS Instance IDs are returned to the public safety USS. [Right]: VID position reported contained in operation (identified by a GUFi) associated with USS Instance B.

B. Remote ID Test Scenarios

Having described the general flow of information, the remote ID test scenarios that were considered[‡] as part of UTM TCL3 testing are now discussed. As indicated above, not all paths were traversed since some scenarios do not, for example, involve the broadcast of a UVIN to the VID. When the positions of the vehicle or the VID, are referred to, WGS-84 [28] is assumed.

Scenario 1: *Valid UVIN; flight plan & observation consistent*

The UAS transmits a valid UVIN to the VID and its coordinates are also estimated by the VID[§]. The

[‡]Not all of these scenarios were fully field tested.

[§]In the event that the VID is unable to provide an estimate, the position of the VID itself could be used as the best estimate provided the detection range is small relative to the UAS movement capabilities.

public safety USS receives the UVIN and the vehicle coordinates. DOR determines

- UVIN is valid
- Flight plan submitted is consistent with the observation

The results are packaged and sent back to the VID. The public safety user records results on the reporting template.

Scenario 2: *Valid UVIN; flight plan & observation inconsistent*

The UAS transmits a valid UVIN to the VID and its coordinates are also estimated by the VID. The public safety USS receives the UVIN and vehicle coordinates. DOR determines:

- UVIN is valid
- Flight plan submitted is inconsistent with the observation (for example, a rogue operation)

The results are packaged and sent back to the VID. The public safety USS user records results on the reporting template.

Scenario 3: *Valid UVIN; no flight plan submitted*

The UAS transmits valid UVIN to the VID and its coordinates are also estimated by the VID. The public safety USS receives the UVIN and vehicle coordinates. DOR determines

- UVIN is valid
- There is no flight plan submitted by the operator of the vehicle with an operating time range that coincides with the observation time.

The results are packaged and sent back to the VID. The public safety USS user records the results on the reporting template.

Scenario 4: *Unregistered (or expired) UVIN*

The UAS transmits a UVIN to the VID and its coordinates are also estimated by the VID. The public safety USS receives the UVIN and vehicle coordinates. DOR determines

- There does not exist an entry in the vehicle registration database or that the UVIN has expired

The results are packaged and sent back to the VID. The public safety USS user records the results on the reporting template.

Scenario 5: *No transmission; valid flight plan*

The UAS does not transmit a UVIN to the VID, however, its coordinates are estimated by the VID. The public safety USS receives the vehicle coordinates. DOR determines

- There exists at least one flight plan that is consistent with the transmitted coordinates.
- There are valid UVINs of the vehicle(s) whose flight plan(s) is (are) consistent with the observation and notes lack of transmission

The results are packaged and sent back to the VID. The public safety USS user records the results on the reporting template.

Scenario 6: *No transmission; no flight plan*

The UAS does not transmit a UVIN to the VID, however, its coordinates are estimated by the VID. The public safety USS receives the vehicle coordinates. DOR determines

- There does not exist a flight plan that is consistent with the transmitted coordinates
- This is a non-UTM participating vehicle

The results are packaged and sent back to the VID. The public safety USS user records the results on the reporting template.

IV. Main Results

In this section, the remote ID tests that were performed as part of UTM TCL3 field testing that occurred during the February-June 2018 time-frame are discussed. Remote ID tests were performed at the North Dakota, New York, and Virginia test sites. Data from the NY and ND test sites are presented below.

Fig. 5. summarizes the vehicles that participated, including several performance specifications. Scenarios 1 and 5 described above are reported.

ND Test Site: All remote ID tests occurred at Camp Graphton North located near Devils Lake Municipal Airport (KDVL). All tests included three vehicles simultaneously operating near one another. Two vehicles (Altavian Nova F700 and SharperShape A6) always flew as ‘participating’ vehicles, that is, they were registered and filed flight plans with a USS. One vehicle (Vapor) served as the ‘non-participating’ or intruder vehicle.






Vehicle	Test-Site	Manufacturer	Model	MTOW	Endurance	Range	Cruise
	ND	Altavian	Nova	14.8 [lb]	80 [min]	1.1 [mi]	30 [kts]
	ND	Sharper	A6	39.7 [lb]	75 [min]	1.1 [mi]	30 [kts]
	ND	Pulse Aerospace	Vapor 55	55 [lb]	60 [min]	4.9 [mi]	21.7 [kts]
	NY	DJI	S1000	24 [lb]	12 [min]	3.6 [mi]	9.72 [kts]
	NY	DJI	M100	7.9 [lb]	10 [min]	2.5 [mi]	9.72 [kts]

Fig. 5 Remote ID: Vehicle Specifications. A total of five vehicles took part in remote ID test scenarios during the UTM TCL3 field demonstrations (February-June 2018).

Two remote ID systems were examined, both using μ Avionix ADS-B technology. The first was a passive system where local area receivers were deployed and continually monitored for UVIN and position information transmission. This system could be deployed to locations where constant surveillance and situational awareness is required. It provides an additional data and verification layer. For example, if a vehicle unwittingly did not properly file a flight plan but was able to transmit its UVIN and position information, the system could determine the vehicle type, its properties, and contact the owner to assess whether or not this constituted a bad actor in the system.

In the second system, a handheld receiver was developed to provide a public safety officer to actively identify a vehicle. The receiver had internet connectivity and was able to query the public safety USS once UVIN and position information was received (see Fig. 3). Fig. 6. depicts one of the remote ID test flights that occurred on April 17, 2018 around 14:50 GMT.

NY Test Site: All remote ID flights were conducted at the NY UAS test site at Griffiss International Airport in Rome, NY. In each test, a DJI S1000 and M100 (see Fig. 5.) equipped with various sensor packages were flown. Three UAS Remote ID methods were tested: (1) ADS-B (using μ Avionix), (2) Secure Integrated C2, and (3) Infrared Light Beacon Encoding.

In the first method, μ Avionix Ping 2020 ADS-B transceivers were installed and programmed to transmit UVIN and position information over 978MHz. Multiple ground-based ADS-B receivers received the transmission and a smart phone application was used by the public safety officer to interface with the public safety USS.

The second method, termed secure integrated C2, leveraged the Internet Engineering Task Force (IETF) Host Identification Protocol (HIP). A primary advantage of HIP is its separation of identity and location as opposed to traditional TCP/IP architectures which combine them based on IP addresses leading to non-verifiable identities subject to spoofing and other forms of attack. Instead, identity is established based on 2048-bit RSA public keys [29].

In the third method, infrared light beacons were installed on each UAS and were programmed to transmit UVIN data at 1Hz. The public safety officers used handheld IR receivers connected to a smart-phone application that interfaces with the public safety USS. Generally, this technology required the public safety officers to be in closer proximity to the UAS being identified (see Table 3).

The primary metrics analyzed included detection and look-up latencies as well as the distances from the vehicle to the vehicle identification device (VID) at times of look-up. Remote ID detection latency is defined as the time duration (measured in seconds) from the initial detection by the relevant sensor suite to its acquisition of a UVIN, position, or other information required for a remote ID look-up. In Fig. 3., this is the time duration between steps 1 and 2. Remote

ID look-up latency is defined as the time duration (measured in seconds) from the initiation of the HTTP request by the VID to its corresponding HTTP response. In Fig. 3., this is the time duration between steps 2 and 8. A time of look-up is defined as the time (GMT) that step 2 occurs.



Fig. 6 Remote ID Look-Up Test: The blue trajectory depicts the A6 (participating multi-rotor) simulating a scenario of filming a sporting event. Also depicted in blue is its geo-fence. The Vapor (intruder helicopter), depicted in red, takes off and breaches the geo-fence of the A6. The public safety officer becomes aware of the intruder and uses its VID to identify the intruding vehicle. Two look-ups are shown by the white lines indicating the positions of both vehicle and public safety officer at the times of look-up. The average distance 179.45 [m] and time 1.13 [s] are computed over all data from the ND test site. Also shown is the Nova (participating fixed-wing) in yellow.

Overall, there were a total of three technologies examined in TCL3 Remote ID experiments[¶]. ADS-B based technology (using μ Avionix hardware) was tested most frequently (generated the highest number of lookup data). The second was secure C2 and the third was IR-based technology. Fig. 7. depicts this breakdown based on the percentage of look-ups by technology.

A total of 12 flights (12 distinct GUFIs) were flown for remote ID (8 at the NY test site and 4 at the ND test site) generating a total of 326 look-up data points. Table 1 shows the minimum, maximum, average, and standard deviation of the look-up latency times for all UTM remote ID look-ups. The last column, success percentage, indicates the percentage of the 326 look-ups that resulted in a success. A look-up is considered a success if there are no failures in the system preventing steps 1 through 8 in Fig. 3. from its completion. For example, a failure in step 1 could be due to obstruction from buildings/structures or environmental conditions such as sunlight, temperature, or humidity impacting the sensor technology employed. A failure in step 2 could be due to network failure from the VID to the internet (wifi or LTE signal strength for example). A failure in step 3 could be due to the unavailability of the vehicle registration service. Of the 326 look-ups, 306 or 93.87 percent resulted in a

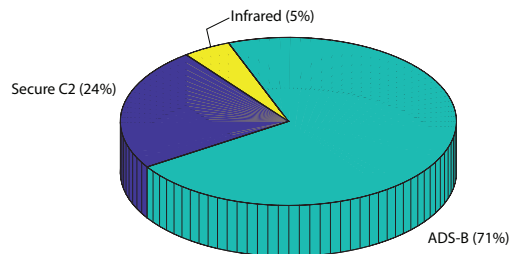


Fig. 7 Detection Technology Breakdown

Total Look-ups	Minimum Latency [s]	Average Latency [s]	Maximum Latency [s]	Standard Deviation [s]	Success Percentage
326	0.40	1.20	9.49	0.86	93.87

Table 1 Overall Look-up Latency Metrics. The minimum, maximum, average, and standard deviation of the latency times for all UTM remote ID look-ups are computed. This included whether or not the look-up resulted in a successful identification. In the last column the percentage of successful look-ups is reported.

success. 20 look-ups or 6.13 percent resulted in failure. Of the 20 failures there were 4 occurrences in tests that used the IR technology (see Fig. 7) and 16 occurrences in tests that used the secure C2 technology. Tests using the ADS-B technology did not result in any failure.

The failures in look-ups in the IR tests (4 out of 16 or 25%) were likely due to either the orientation of the vehicle or the position of the hand-held IR gun at the time of the look-up. Unlike in the secure C2 and ADS-B approaches, the public safety officer had to point the IR gun fairly accurately at the moving target for a period of about 0.25 [s] in order to receive the signal (UVIN data). Similarly, the transmission to the receiver of the light beacon mounted on the bottom of the vehicle is highly susceptible to aircraft orientation, speed, and environmental factors such as sunlight.

The 16 failures (21%) in the secure C2 tests were likely due to a public safety failure(see step 2 in Fig. 3.) due to an unanticipated heavy load during those tests. Specifically, this was due to the number of connections to the database (AWS RDS) that exceeded the allowable limit. Typically, this number is adjusted to optimize database performance. In addition, optimizing the connection pool maintained by the application could also have impact on performance. After this problem was identified and parameters were modified, these look-up failures did not persist.

It is found that the average look-up latency time was 1.2 [s] which is reasonable given that the HTTP request must ultimately traverse several network connections to disparate components (public safety USS, vehicle registration, USS discovery service, etc.). In addition, each component also has its own database connection which in most cases was an Amazon Web Service RDS (Relational Database Service). The maximum time was found to be 9.49 [s] which was likely due to increased traffic on the public safety USS or vehicle registration service and their dependencies. For example, the vehicle registration service used a third party authentication service that can result in intermittent delays of several seconds.

[¶]DSRC was used at the Virginia test site, however, data analysis of those flights are not included in this paper.

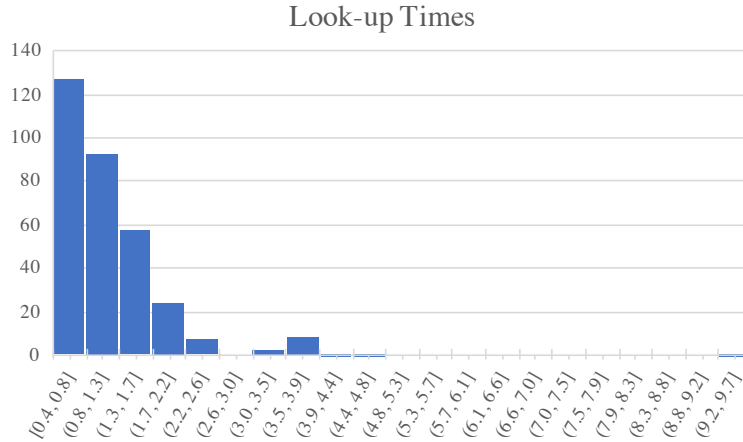


Fig. 8 Look-Up Time Histogram. The average look-up time was 1.2 [s]. The maximum (one occurrence) was 9.4 [s]. The standard deviation was 0.86 [s]. Delays were likely due to increased traffic on the public safety USS or vehicle registration service and their dependencies.

Minimum Latency [s]	Average Latency [s]	Maximum Latency [s]	Standard Deviation [s]
0.001	1.542	5.200	1.120

Table 2 Overall Detect Latency Metrics. The detect latency is defined by the time elapsed from when the detector acquires the relevant information to the time it becomes available to the software component that initiates the look-up.

Its important to distinguish the look-up latency from a failure. The 9.4 [s] latency is not considered a failure since the information requested at the time of look-up by the public officer was ultimately delivered. It is also depicted in Table 2 the detection latency statistics. This varied by technology since each one has different processing steps that enable the information (position and UVIN) to be processed and properly formatted for an HTTP request in step 2.

Also of interest is the distribution of distances from the vehicle to the VID or public safety officer at times of look-up. Overall, 26,588 vehicle position data elements were collected over 97 min of total flight time and linear interpolation was used to compute the distance from the vehicles to the public safety officers. Table 3 depicts the quartiles and the minimum and maximum statistics for the distances (in meters) based on the technology. The IR technology had the lowest range since the receiver had to be in closer proximity to the vehicle in order to obtain a detection.

Also of interest is the distribution of distances from the vehicle to the VID or public safety officer at times of look-up. Overall, 26,588 vehicle position data elements were collected over 97 min of total flight time and linear interpolation was used to compute the distance from the vehicles to the public safety officers. Table 3 depicts the quartiles and the minimum and maximum statistics for the distances (in meters) based on the technology. The IR technology had the lowest range since the receiver had to be in closer proximity to the vehicle in order to obtain a detection.

Technology	Min	Q1	Q2	Q3	Max
ADS-B	45.81	59.47	82.50	141.82	194.73
Infrared	54.52	57.33	66.72	73.18	84.24
Secure C2	48.18	57.96	88.78	111.70	163.95

Table 3 Distance at Times of Look-Up by Technology [m]

To summarize the results, there were a total of 12 flights, 326 look-up data points and a 94% success rate. The sensor technologies used had a significant impact on the data and success rate. For example, while the IR technology approach is promising, further research is needed regarding its detection range, susceptibility to environment factors, and vehicle orientation (Euler angles) and speed during a particular mission. In addition, if the public safety officer is required

to manage simultaneously two different devices (one for detection and one for interfacing with the public safety USS) this may impact the failure rate adversely especially when pointing accuracy is required. ADS-B technologies had the highest percent success rate, highest number of look-up tests, and the highest range (maximum distance) from the public safety officer at the time of look-up. This is likely due to the maturity of the technology (for example, the IR and secure C2 approaches was custom built specific to this test) and its general widespread familiarity.

While this analysis represents an important first step in remote ID using the UTM system, it is recommended that future remote ID experiments break the experiment into more focused subsets in order to analyze separately the

individual components. This includes sensor technologies, communication protocols, and the various s/w and network components that comprise Fig. 3.

V. Summary

This paper discussed the UTM remote ID framework and examined initial data collected during the UTM TCL3 field tests that were conducted February through June 2018. The proposed architecture utilized UTM components: FIMS (Flight Information Management System), USS (UAS Service Supplier), and vehicle registration and model database in order to provide assessment of the UAS reported in the field including the ability to distinguish between participating and non-participating UTM actors. Detailed system descriptions were provided and preliminary results from field tests were discussed. This included an analysis of the detect and look-up latencies and distances between the vehicles to be identified and the public safety officers. Future work should focus on (1) developing requirements for the latency metrics measured in this study which may depend on numerous factors including risk, geographic location, population density, etc., (2) the emerging technologies that enable remote identification of vehicles at longer distances, and (3) a more comprehensive and thorough analysis of the various UTM components and their network interconnections that play a critical role in remote ID.

Acknowledgments

The design, planning and scheduling, s/w development, communication support, and data collection for the 2018 UTM TCL3 field tests constituted an enormous endeavor and this acknowledgment captures only a small fraction of the individuals and effort involved. We acknowledge and thank Arwa Aweiss, Edgar Torres, and Hemil Modi for their tireless efforts in communicating with partners and ensuring data requirements were fulfilled. We acknowledge and thank Daniel Liddell and Shawn Li for their database support and meticulous analysis. We thank Daniel Mulfinger, David Smith, Confesor Santiago, and Sandra Lozito for their thorough review of this work and helpful feedback. We thank Jeff Homola, Marcus Johnson, Jaewoo Jung, Lawrence Markosian, Joey Mercer, and Irene Skupniewicz for helpful discussions throughout. We also thank Chris Theisen and Mark Reilly for helpful discussions on the remote ID data sets and providing invaluable insights. Lastly, we thank the effort of the entire UTM team without which no data would have been available for analyses.

References

- [1] "Global Market Insights," <https://www.gminsights.com/industry-analysis/consumer-drone-market>, March 2018.
- [2] Jenkins, D., Vasigh, B., Oster, C., and Larsen, T., *Forecast of the Commercial UAS Package Delivery Market*, Embry-Riddle Aeronautical University, 2017.
- [3] Barrett, D., "Burglars Use Drone Helicopters to Target Homes," <https://www.telegraph.co.uk/news/uknews/crime/11613568/Burglars-use-drone-helicopters-to-identify-target-homes.html>, May 18, 2015.
- [4] Margaritoff, M., "Australian Drug Cartel Used Drone to Spy on Police," <http://www.thedrive.com/aerial/12050>, 2017.
- [5] Craig, T., Russo, J., and Shaffer, J., "Eyes in the skies: the latest threat to correctional institution security," *Corrections Today*, 2017.
- [6] Ferrigno, L., "Ohio Prison Yard Free-For-All After Drone Drops Drugs," <https://www.cnn.com/2015/08/04/us/>, 2015.
- [7] Abbasi, W., "Inmates fly mobile phones, drugs and porn into jail – via drone," <https://www.usatoday.com/story/news/2017/06/15/inmates-increasingly-look-drones-smuggle-contraband-into-their-cells/102864854/>, 2017.
- [8] Bolster, K., and Rivera, R., "Prison employee fired after inmate escapes from Lieber Correctional," <http://www.wsmv.com/story/35816591/scinmate-captured-in-texas-with-guns-cash-phones-drone-mayhave-aided-escape>, 2017.
- [9] Guardian, T., "Escaped South Carolina Inmate May Have Used Drone-Delivered Wire Cutters," <https://www.theguardian.com/us-news/2017/jul/08/jimmy-causey-escaped-prisoner-south-carolina-drone>, 2017.
- [10] "BBC, Footage Shows Drone Delivering Drugs to Prisoners," <http://www.bbc.com/news/av/uk-36302136/footage-shows-drone-delivering-drugs-to-prisoners>, May 16, 2016.

- [11] Travis, R., “Threat From the Sky: 35 Drones Already Spotted at GA Prisons This Year,” <http://www.fox5atlanta.com/news/i-team/threat-from-the-sky-35-drones-already-spotted-at-ga-prisons-this-year>, 2017.
- [12] Repard, P., “In New Tactic, Smugglers Use Drone to Fly Meth over Mexican Border into San Diego, Officials Say,” <http://www.latimes.com/local/lanow/la-me-drug-smuggle-drone-20170819-story.html>, 2018.
- [13] Valencia, N., and Martinez, M., “Drone carrying drugs crashes south of U.S. border,” <http://www.cnn.com/2015/01/22/world/drug-drone-crashes-us-mexico-border/>, 2015.
- [14] Dinan, S., “Thirteen drones in four days: How drug smugglers are using technology to beat Border Patrol.” <https://m.washingtontimes.com/news/2018/jan/2/drones-fly-drugs-us-noborder-patrol-detection-tec/>, 2018.
- [15] Carey, B., “Army Confirms Black Hawk, Drone Collided Over New York City,” <https://www.ainonline.com/aviation-news/defense/2017-09-25/army-confirms-black-hawk-drone-collided-over-new-york-city>, September 25, 2017.
- [16] “Panel: Addressing the Counter-UAS Threat at Home and Abroad,” AUVSI Unmanned Systems – Defense. Protection. Security, 2018.
- [17] Snead, J., Seibler, J.-M., and Inserra, D., “Establishing a Legal Framework for Counter-Drone Technologies,” 2018.
- [18] Rupprecht, J., “7 big problems with counter-drone technology (drone jammers, anti-drone guns, etc.),” <https://jrupprechtlaw.com/drone-jammer-gun-defender-legal-problems>, 2018.
- [19] Wallace, R. J., Loffi, J. M., Quiroga, M., and Quiroga, C., “Exploring Commercial Counter-UAS Operations: A Case Study of the 2017 Dominican Republic Festival Presidente,” *International Journal of Aviation, Aeronautics, and Aerospace*, Vol. 5, No. 2, 2018, p. 8.
- [20] Geiver, L., “Early 2018 brings rush of counter-UAS activity,” <http://www.uasmagazine.com/articles/1829/early-2018-brings-rush-of-counter-uas-activity>, March 13, 2018.
- [21] Birch, G. C., Griffin, J. C., and Erdman, M. K., “UAS Detection Classification and Neutralization: Market Survey 2015,” Tech. rep., Sandia National Laboratories (SNL-NM), Albuquerque, NM (United States), 2015.
- [22] Buric, M., and De Cubber, G., “Counter remotely piloted aircraft systems,” *MTA review*, Vol. 27, No. 1, 2017, pp. 9–18.
- [23] Schaufele, R., Ding, L., Miller, N., Barlett, H., Lukacs, M., and Bhadra, D., “FAA Aerospace Forecast: Fiscal Years 2017-2037,” *Washington, DC*, 2017.
- [24] Prevot, T., Rios, J., Kopardekar, P., Robinson III, J. E., Johnson, M., and Jung, J., “UAS traffic management (UTM) concept of operations to safely enable low altitude flight operations,” *16th AIAA Aviation Technology, Integration, and Operations Conference*, 2016, p. 3292.
- [25] FAA, “Unmanned Aircraft Systems (UAS) Traffic Management (UTM) Concept of Operations,” , 2018.
- [26] Sandhu, R., Ferraiolo, D., Kuhn, R., et al., “The NIST model for role-based access control: towards a unified standard,” *ACM workshop on Role-based access control*, Vol. 2000, 2000, pp. 1–11.
- [27] NASA, “UTM models,” <https://app.swaggerhub.com/domains/utm/commons/v3>, 2018.
- [28] Smith, R. W., *Department of Defense World Geodetic System 1984: its definition and relationships with local geodetic systems*, Defense Mapping Agency, 1987.
- [29] Nikander, P., Gurtov, A., and Henderson, T. R., “Host identity protocol (HIP): Connectivity, mobility, multi-homing, security, and privacy over IPv4 and IPv6 networks,” *IEEE Communications Surveys & Tutorials*, Vol. 12, No. 2, 2010, pp. 186–204.