Drone Registration and Remote ID

Here's why the establishment of a robust identity management solution for UAS can't be left 'up in the air.'

By Amit Ganjoo, ANRA Technologies

With the drone market expecting exponential growth over the next few years and a large number of anticipated users, an Unmanned Aircraft Systems Traffic Management (UTM) system that does not require constant human monitoring and surveillance yet ensures the safety, security, and control of drones in the low-altitude airspace is key.

UTM system stakeholders should have the ability to remotely identify an Unmanned Aircraft System (UAS) and make strategic decisions—launch, execution, and/or termination of airspace operations— related to mission management. The procedures and interfaces also need to ensure that only authenticated and approved UAS can operate in the given airspace.

Ultimately, the goal of the UTM project would be to develop an independent, self-directed, and scalable system that will manage and monitor the drones and their flights. Factoring in inputs from external sources such as obstacles, terrain, weather, airspace, command and control (C2) links, and performance data, the system would make this data available to all operators/service providers. In addition, the system also has to be capable of sending notifications to external stakeholders like public safety, state, and local agencies. Furthermore, all this must be handled in a safe and secure fashion.

MULTIPLE UTM EFFORTS UNDERWAY

Of the several efforts underway in the UTM space, the predominant one is the NASA UTM program, an alliance between NASA and various industry partners, including ANRA Technologies.

There are other similar initiatives that are being kicked off across the globe by various countries. These programs require the synergistic efforts of different stakeholders worldwide and an alliance between regulators, the private industry, and academic institutions. ANRA is

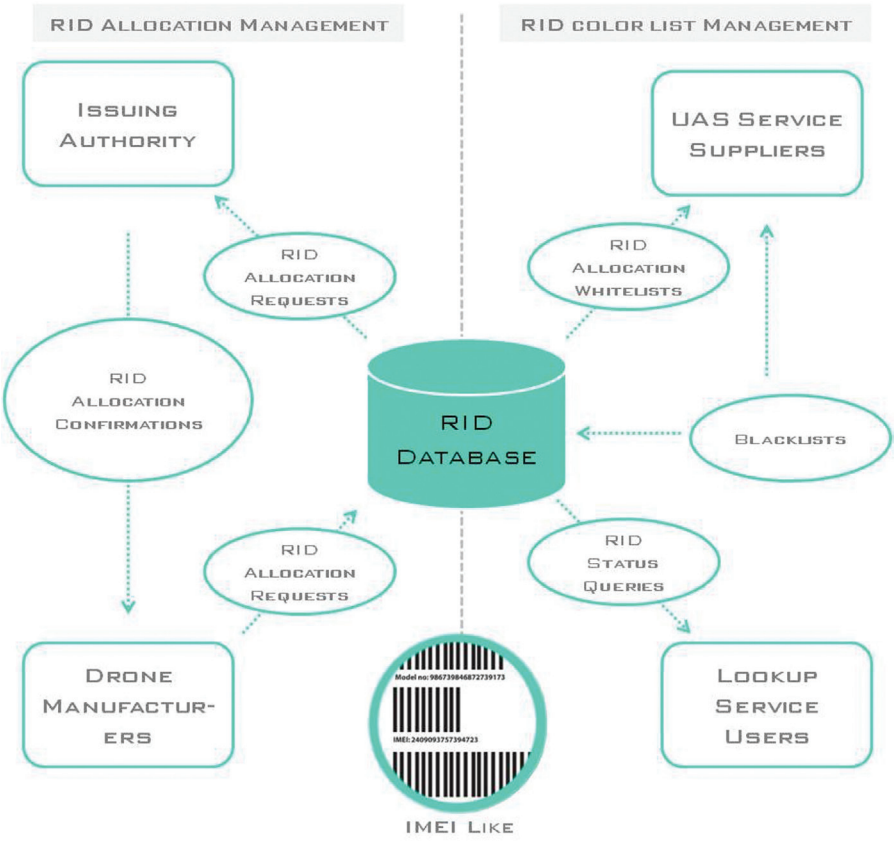

Figure 1: Logical Architecture Overview (Image courtesy ANRA Technologies)

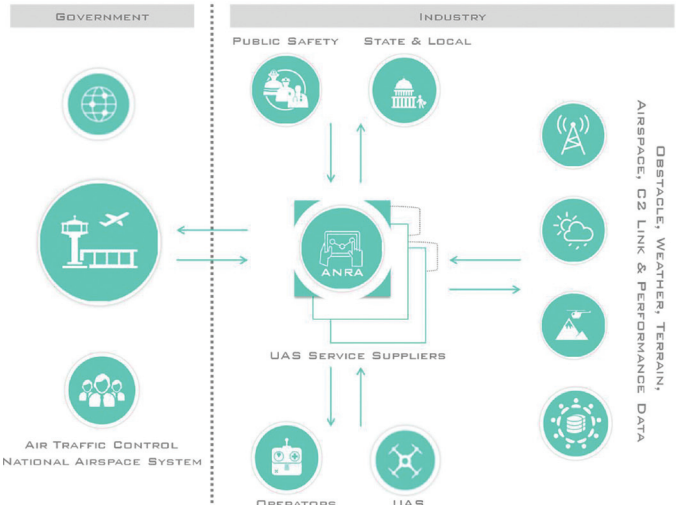

Figure 2: RID Allocation and Management (Image courtesy ANRA Technologies)

one such private partner working to create and coordinate the technologies to accommodate and realize the UTM vision.

Additionally, the Global UTM Association (GUTMA) is a non-profit consortium of worldwide UTM stakeholders. Its purpose is to foster the safe, secure, and efficient integration of drones in national airspace systems. Its mission is to support and accelerate the transparent implementation of globally interoperable UTM systems.

REGISTRATION AND REMOTE IDENTIFICATION

A remote identification methodology should enable public or private entities concerned about a drone flight in close proximity to report an identifier number to the authorities, who would then have the tools to investigate the complaint without infringing on operator privacy.

The use of a remote identification system would protect drone user information and any confidential information about the nature and objective of the drone missions. Monitoring and reporting potential complaints by the public about safety, inappropriate drone usage, or damage to public or personal property would be handled by using the broadcasted drone identifier. The identifier would keep the public informed about, for example, the drone's surveillance capabilities, without releasing personal information about the drone operators unless they are involved in unauthorized flights.

Drone identifications of different types can be made available to the users via an online system using the drone registration number as the primary key.

MANAGING AUTHORITY

There needs to be a structured process for life cycle management of the Remote ID (RID). This includes not only the initial allocations, but also subsequent enforcement leveraging color list management, as shown in Figure 2. A centralized RID database needs to be managed by an authoritative entity such as the International Civil Aviation Organization (ICAO) at a global level or each country's Civil Aeronautics Administration (CAA).

However, the key is that all these systems need to be federated and managed in a similar fashion to how current International Mobile Equipment Identify (IMEI) allocation and management works for telecom networks or how domain registry and the Domain Name System (DNS) work in the Internet domain.

POTENTIAL IDS

There is no reason for the industry stakeholders to reinvent the wheel. Plenty of existing technologies and solutions can be leveraged to build ID frameworks for Registration and Remote ID. The types of RIDs worth considering include International Mobile Equipment Identity (IMEI) or the Media Access Control (MAC) address of a radio on board the drone.

International Mobile Equipment Identity (IMEI)—Based on cellular standards, the IMEI is a unique number that can identify 3GPP and mobile as well as some satellite devices but not the subscriber. Being a universally adopted system for cellular devices it can be used for drone identifications also. Even though industry can leverage IMEI concepts from the cellular realm, this ID can be shared over other noncellular communication links as well via a service layer application residing on the drone.

Radio Media Access Control (MAC) Address—Bluetooth Inquiries expose the MAC address of each radio on board the drone. The MAC address is unique to each radio, so it can serve as a unique drone identifier.

Anyone with the proper receiver RF or Bluetooth can obtain those transmissions from the drone, but only law enforcement officials or aviation regulators would be able to use that registration number to identify the registered owner. This system would be similar to automotive license plates, which allow anyone to identify a nearby vehicle they believe is operating improperly, but which can only be traced to its owner and operator by authorities.

IDENTIFICATION CHANNELS

Any unique RID used by the drone can be shared or made available to the relevant stakeholders via the following two approaches:

- Radio frequency transmission to local receivers using existing UA antennas and modified C2, or new "ADS-B Like" protocols including one or more open standards
- A network-based identification system, likely over cellular networks as well as the internet

Going forward the majority of drones will potentially leverage and rely on commercial wireless broadband solutions for either C2 or real-time sensor data management and transfer. These next generation networks will have to support a highly diverse range of new applications, user requirements, and connected devices, sensors, robotics, mission-critical wireless communication, and automated manned and unmanned vehicle systems.

The only way all this can become a reality is by continuing to evolve existing wireless technologies, cellular and noncellular, and by working on new licensed or unlicensed radio access technologies. These next generation networks will be heterogeneous networks using a myriad of wireless technologies such as cellular, millimeter wave, Wi-Fi, etc.

In addition to long and medium range RF links, low-power and range technologies such as DSRC and Bluetooth can also be considered. Passive

discovery of Bluetooth devices is relatively straightforward because most Bluetooth devices periodically issue Inquiry or Page packets to discover or attempt association with other Bluetooth devices. However, a more deterministic mechanism for discovering other devices is for an active sniffer to issue frequent Inquiry packets on all channels. The sniffer that is inexpensive and simple to operate would start with the first channel, issue an Inquiry packet, and listen for Inquiry responses for some number of milliseconds before repeating the process on the next channel. This works because Bluetooth devices are required to respond to Inquiry packets. Class 1 Bluetooth radios work at up to 100 meters with realistic ranges of 30 meters. Furthermore, Bluetooth operates in the public spectrum, so active sniffers would violate no FCC rules or laws.

Even though these technologies will evolve to support the throughput and latency requirements for safe drone operations, one of the key challenges we will face is agile, reliable, safe, and secure support for different use cases and user requirements. We as the industry need to consider all key technical areas and explore ways of integrating "security by design" principles into commercial drone ecosystem development.

SECURITY CONSIDERATIONS

As drones and other IoT applications in general become more widespread, we will need new service delivery models that involve new actors in the ecosystem. Virtualization and cloud infrastructures will be leveraged to provide flexibility, scalability, and the ability to deliver richer services quickly. Data access wireless networks will need to provide users and other third parties access via APIs for granular control and security of the services. This paradigm shift will enable innovative capabilities but also create complex security challenges.

If we peel the layers further, we can group the security focus into the following sections that warrant review and collaborative solutions from us as the industry.

- Key management
- Denial of service (DoS) protection
- Identity management

KEY MANAGEMENT

Communication for the majority of commercial drones as well as other IoT devices is constrained today to using short-range communication protocols such as 802.11 Wi-Fi. Most commercially available drones utilize a 2.4 GHz ISM band command and control link.

A typical implementation includes wireless end points or sensors that communicate between themselves using point-to-point or mesh networking capabilities. Typically, the nodes that participate in this architecture are provisioned with cryptographic material that supports confidential, authenticated, and integrity protected communications amongst themselves and to/through the gateway(s). The underlying cryptographic material and services required depends on the protocols that are being used (both communication and messaging) and the security objectives of each. In addition to keys required for communication protocols, messaging protocols (e.g., MQTT, CoAP, DDS) also levy cryptographic algorithms and key material. Although some messaging protocols only support username/password, many provide options for using symmetric keys, key pairs, and certificates to secure communication between devices.

A majority of the solutions implemented today leverage symmetric keys but going forward using asymmetric keys should also be considered. We also need to consider alternative trust models that enable flexibility in establishing trust models across heterogeneous devices, access technologies, network domains, and communication modes.

With the introduction of next generation broadband technologies and their evolution to 5G, IoT drone solution developers will be able to redesign their products with broad, direct access to the cloud and new capabilities for peer-to-peer communications. This requires flexible key management capabilities that support a variety of use cases.

Denial of Service (DoS) protection—Mission critical services like drones in particular require highly available, low-latency, and highly reliable communication systems. As more devices like drones are connected to the wireless broadband networks, the networks will be exposed to DoS attacks targeting the limited resources of specific services, much like botnet-driven distributed denial of service attacks in the internet. Drone operations need to account for this possibility and plan for mitigation of such attacks by having redundant interfaces as well as extensive fail-safes integrated in the solution.

Identity Management—There is a lot of talk about Identification Systems for drones, however this needs to be more than just identifying the drones. The established identity can be the basis to accomplish further security goals, such as policy-based access control decisions to resources within that system or recording of actions mapped to their actors to establish an auditable transaction history (e.g., through blockchain-based transaction integrity preservation).

There is a wide range of identities involved in a typical commercial drone ecosystem, and it is not about the identification of the drone by itself. These identification needs exist at every layer of the stack, in every segment of the architecture. For example, drones might need to be identified as hardware trust anchors, but then you have IP endpoints, cloud service instances, network services, virtualized network function instances, subscribers and administrators, and many more.

All of those identities need to be defined, provisioned, maintained, validated, revoked, etc., so we require a robust Identity Management solution that captures the entire life cycle of this management task.

Amit Ganjoo is the Founder and CEO of ANRA Technologies and has over 20 years of aviation, telecom and wireless experience in both the federal and the commercial space. He's a licensed pilot and an experimental aircraft builder, following a lifelong passion in aviation. Until December, he acted as the co-chair for FCC's Technical Advisory Council (TAC) for 5G and IoT, which included ground and airborne autonomous vehicles. He was the Director of Engineering and Principal Architect at Ericsson, providing telecom solutions to Commercial Customers and Federal Government, where he was the recipient of the Athena Award. Ganjoo was also the Chief System Architect for Navy 4G LTE Sea Pilot deployed as part of the U.S.S. Kearsarge Expeditionary Strike Group. He delivered a one of a kind turn-key, secure, unmanned airborne/afloat autonomous 4G LTE Network with applications to directly support the war fighter.