Journal of Advances and Scholarly Researches in Allied Education
Vol. 16, Issue No. 6, May-2019, ISSN 2230-7540

A Study on the Usage of Computerized Drone System for Security

Alisha Y. Warke[1]* Aryan Prasad[2]

[1] Sr. Analyst, Capgemini Technology Services India Ltd., Bengaluru

[2] Research Assistant, Kutch Nav Nirman Abhiyan, DPS School, Kutch, Gujarat

Abstract – Unmanned aerial vehicle technology covers everything from the aerodynamics of the drone, materials in the manufacture of the physical UAV, to the circuit boards, chipset and software, which are the brains of the drone.

A typical unmanned aircraft is made of light composite materials to reduce weight and increase maneuverability. This composite material strength allows military drones to cruise at extremely high altitudes.

Drones are equipped with different state of the art technology such as infrared cameras, GPS and laser (consumer, commercial and military UAV). Drones are controlled by remote ground control systems (GSC) and also referred to as a ground cockpit.

An unmanned aerial vehicle system has two parts, the drone itself and the control system.

The nose of the unmanned aerial vehicle is where all the sensors and navigational systems are present. The rest of the body is full of drone technology systems since there is no space required to accommodate humans.

The engineering materials used to build the drone are highly complex composites designed to absorb vibration, which decrease the sound produced. These materials are very light weight.

Keywords: Computerized, Drone, System, Security

----------X----------

INTRODUCTION

Drones come in a wide variety of sizes, with the largest being mostly used for military purposes such as the Predator drone. The next in size are unmanned aircraft, which have fixed wings and require short runways. These are generally used to cover large sections of land, working in areas such as geographical surveying or to combat wildlife poaching.

Drones can fly in both GNSS and non-satellite modes. For example DJI drones can fly in P-Mode (GPS & GLONASS) or ATTI mode, which doesn't use GPS.

Highly accurate drone navigation is very important when flying especially in drone applications such as creating 3D maps, surveying landscape and SAR (Search & Rescue) missions.

When the quadcopter is first switched on, it searches and detects GNSS satellites. High end GNSS systems use Satellite Constellation technology. Basically, a satellite constellation is a group of satellites working together giving coordinated coverage and synchronized so that they overlap well in coverage. Pass or coverage is the period in which a satellite is visible above the local horizon.

The radar technology will signal the following on the remote controller display;

- signal that enough drone GNSS satellites have been detected and the drone is ready to fly.
- display the current position and location of the drone in relation to the pilot.

- record the home point for 'Return To Home' safety feature.

Most of the latest drone have 3 types of Return to Home drone technology as follows;

- Pilot initiated return to home by pressing button on Remote Controller or in an app.
- A low battery level, where the UAV will fly automatically back to the home point.
- Loss of contact between the UAV and Remote Controller with the UAV flying back automatically to its home point.

The latest high tech drones are now equipped with collision avoidance systems. These use obstacle detection sensors to scan the surroundings, while software algorithms and SLAM technology produce the images into 3D maps allowing the drone to sense and avoid.

The Mavic 2 uses both Vision and Infrared sensors fused into a vision system known as Omni-directional Obstacle Sensing.

The DJI Mavic 2 obstacle sensing system is top drone technology. The Mavic 2 will sense objects, then fly around obstacles in front. It can do the same when flying backwards. Or hover if it is not possible to fly around the obstacle.

This technology is known as APAS (Advanced Pilot Assistance System) on the DJI Mavic 2 and Mavic Air drones.

Gyros stabilization technology give the drone its smooth flight capabilities.

The gyroscope works almost instantly to the forces moving against the drone keeping it flying or hovering very smoothly. The gyroscope provides essential navigational information to the central flight controller.

The inertial measurement unit (IMU) works by detecting the current rate of acceleration using one or more accelerometers. The IMU detects changes in rotational attributes like pitch, roll and yaw using one or more gyroscopes. Some IMU include a magnetometer to assist with calibration against orientation drift.

The Gyroscope is a component of the IMU and the IMU is an essential component of the drones flight controller. The flight controller is the central brain of the drone.

The motors and propellers are the drone technology, which move the UAV into the air and to fly in any direction or hover. On a quadcopter, the motors and propellers work in pairs with 2 motors / propellers rotating clockwise (CW Propellers) and 2 motors rotating Counter Clockwise (CCW Propellers).

A video camera is mounted on the unmanned aerial vehicle and this camera broadcasts the live video to the pilot on the ground. The ground pilot is flying the aircraft as if they were on-board the aircraft instead of looking at the aircraft from the pilot's actual ground position.

FPV allows the unmanned aircraft to fly much higher and further than you can from looking at the aircraft from the ground. First Person View allows for more precise flying especially around obstacles.

FPV allows unmanned aerial vehicles to fly very easily indoors, or through forests and around buildings.

Drones such as the DJI Mavic use integrated controllers and intelligent algorithms to set a new standard for wireless high definition image transmission by lowering latency and increasing maximum range and reliability.

Live video and maximizing the range of the transmission is fascinating drone technology.

The flight control system communicates with a PC Assistant through a Micro-USB cable. This allows configuration of the UAV and to upgrade the drone firmware.

USAGE OF COMPUTERISED DRONE SYSTEM FOR SECURITY

A very simple description of a drone is that it is a flying computer with a camera or sensor attached. Like computers, drones have firmware software, which send commands to the physical components in the aircraft or remote controller.

Drone manufacturers release firmware upgrades to fix bugs and add new features to the aircraft, remote control unit or software if it is used to fly the drone.

The front LED indicators light up to indicate the nose of the UAV.

The rear LEDs flight indicators light up to indicate the various status of the drone when power on, getting a firmware upgrade and flying.

It is a good to understand what the flashing LEDs on your quadcopter indicate.

Mobile networks can assist with drone identification, authorization, and geo fencing. Mobile networks are equipped with a variety of tools to identify and authorize users and devices that can access the networks. The International Mobile Equipment Identity (IMEI) is

used to identify the mobile device, and the International Mobile Subscriber Identity (IMSI) is used to identify the user in a mobile network. The subscriber and connectivity provider profiles are embedded in the SIM card, or dynamically provisioned on demand to the embedded SIM (eSIM) or embedded Universal Integrated Circuit Card (eUICC). This ensures a tamper resistant solution for drone identification. On the other hand, IMEI and IMSI can be utilized to support other drone identification solutions, providing a robust and secure way to bootstrap certificate-based solutions to identify, authenticate and authorize drones, pilots, and individual drone operations.

There are two main solution categories for drone identification: local broadcast solutions and network publishing solutions. Mobile networks can support both. Local broadcast can utilize the LTE sidelink V2X communication capabilities that can be integrated into mobile chipsets, while network publishing solutions are inherently supported by the data connectivity provided to mobile subscribers. One of the benefits of using mobile technology for both identification modes is that communication is encrypted and uses a secure channel for both local broadcast as well as network publishing mechanisms. A key advantage of cellular solutions is that enabled smartphones can be used to access both the broadcast and network publishing information so that specialized receivers are not required.

In addition to identifying drones, their positions over time need to be monitored as well. This is important to ensure that drone traffic management systems have up-to-date information about the locations of individual drones as well as to be able to locate any drone in the airspace.

An important component of drone tracking solutions is the use of GNSS systems. Drones retrieve their positional information from GNSS readings and then, to support tracking, they communicate this information to a central server, a component of the drone traffic management system. The shortcoming of this self-reporting solution is that the telemetry data provided by a drone can be easily altered by a malicious user without detection by the drone traffic management system.

Mobile systems also provide an independent location tracking mechanism. The cellular mobile positioning system (MPS) can be used both to validate and act as a backup to the drones' self-reported location information. The MPS system can provide a location estimate with tens of meters of accuracy. This precision is enough to validate the telemetry data. In addition, the MPS positioning information can also be used if the drone fails to report telemetry because of, for example, a malfunction. In this case, MPS positioning information may be used to continue monitoring no-flight zone violations, or even to detect potential crash landings along with an approximate position of the incident.

Safe drone operations require physical infrastructure across cities and throughout a country. Mobile infrastructure is widely and relatively evenly distributed infrastructure that may be used to co-locate additional systems, like the ones introduced below, to support drone operations.

While the previously introduced solutions using mobile technology for identification and tracking of drones apply to drones using cellular communication, to protect from malicious users we need to be prepared for drones that use other technologies for communication, or for drones that do not emit radio signals to evade detection. Different technologies are being developed to detect drones based on radio emission, low altitude radar, video or audio detection combined with triangulation. All these technologies need to be deployed throughout the area they are protecting. Installing these devices along with mobile infrastructure is a cost-effective way to roll out drone detection systems.

Mobile infrastructure locations provide installation options for the hardware devices as well as power and reliable network connection. Similar to detection systems, drone defense solutions need to be deployed to act upon a rogue drone that poses a public safety risk. Drone defense devices need the same infrastructure – that is, physical installation, power and reliable network connectivity.

Regular drone operations also require services such as weather sensors, charging stations and safe emergency landing locations. These services can be co-located with mobile infrastructure – for example, on rooftops or within a secured area along mobile infrastructure in rural areas.

DISCUSSION

Wireless drone communication can potentially be provided over licensed and unlicensed spectrum. Unlicensed spectrum is shared spectrum in which users do not receive exclusive access to channels. This spectrum is intended to facilitate innovation and, for this purpose, it includes light regulations. Therefore, this spectrum is more prone to interference than licensed spectrum, as the latter requires exclusive licenses that include regulatory requirements to fulfill.

There are essentially three options for providing drone communication over licensed spectrum: satellite technology over satellite spectrum, deployment of a dedicated drone terrestrial network over licensed spectrum, or use of the existing terrestrial mobile network over licensed mobile spectrum. Satellite technology might provide good

outdoor coverage, however the drawbacks are high latency, low throughput and higher cost. The drawbacks of deploying a dedicated terrestrial network also include increased costs, as well as the time it takes to build out a system that has adequate coverage for drones.

The existing terrestrial mobile network already has significant coverage with low latency, high throughput and low cost. Further, communication over mobile networks has been proven to be secure and robust. Therefore, while different technologies may be used, we at Ericsson believe that the existing terrestrial network is the most cost-efficient and reliable alternative for drone communication.

Mobile networks can provide a proven and flexible communication channel to support the various requirements of drone use cases from low latency to high bandwidth scenarios. At the same time, the use of licensed bands and encrypted communication increases the safety of drone applications. 4G LTE and the upcoming 5G networks support a variety of capabilities that fit well with drone requirements. For reliable command and control communication, mobile networks can provide flexible differentiated QoS matching the needed reliability, latency and throughput.

Communication security is already inherent within the architecture of mobile networks and provided at many levels from encryption on the radio link to higher layer security mechanisms. For collision avoidance and drone identification, the sidelink capability provides a secure mechanism to exchange broadcast type messages to nearby entities in addition to network connectivity. Drone tracking is supported by the mobile positioning service and can be queried from the mobile network and integrated into the drone traffic management systems. Industry forums, like GSMA and CTIA have prepared position papers to highlight the potential of mobile networks for drones.

The existing terrestrial LTE networks can provide good mobility support to the initial deployment of a small number of drones. New mobility management challenges may arise for higher drone densities or more difficult radio environments. As shown by simulation and field trial results documented in the 3GPP technical report [8], in some scenarios the mobility performance of drone user equipment is worse compared to a terrestrial user equipment. Two main problems have been identified: (1) When drones move through the sidelobe nulls of base station antennas, the default mobility procedures might be too slow for successful execution; (2) drones experiencing line-of-sight propagation conditions to many neighbor cells that cause comparably high interference levels may have difficulty in establishing and maintaining connection to the network.

Performance enhancing solutions can be used to optimize mobile connectivity to provide improved performance for the drones while maintaining the performance of ground mobile devices. Next generation 5G networks will have higher capacity in providing connectivity services to both terrestrial and aerial devices. New advanced technologies have been introduced in 5G networks.

CONCLUSION

Wide-area network coverage is needed to safely expand low-altitude drone operations for beyond visual line-of-sight missions. Mobile networks provide wide-area secure wireless connectivity, utilizing proven technology based on mobile licensed spectrum and global standards. We have evaluated the performance of mobile networks for airborne drone communication and found that already today, LTE networks are capable of supporting the initial deployment of low-altitude drones. The significantly improved capabilities of 5G networks will provide more efficient and effective mobile connectivity for large-scale drone deployments with more diverse applications. Further, we believe that in addition to wireless communication, drone traffic management systems should utilize the sophisticated and proven identity management and tracking capabilities of mobile networks. Ericsson will continue to work actively in the relevant forums to align mobile network capabilities with drone communication and traffic management requirements.

REFERENCES

1. L. Atzori, A. Iera, G. Morabito (2010). The internet of things: A survey, Computer networks, 54, pp. 2787-2805.

2. J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami (2013). Internet of Things (IoT): A vision, architectural elements, and future directions, Future Generation Computer Systems, 29, pp. 1645-1660.

3. D. POPA, D.D. POPA, M.M. CODESCU (2017). Reliabilty for A Green Internet of Things, Buletinul AGIR nr, pp. 45-50.

4. S. S. Prasad, C. Kumar (2013). A green and reliable internet of things, Communications and Network, 5, pp. 44.

5. C. Zhu, V.C. Leung, L. Shu, E.C.H. Ngai (2015). Green Internet of Things for the smart world, IEEE Access, 3, pp. 2151-2162.

6. S. Sala (2009). Information and Communication Technologies for climate change adaptation, with a focus on the agricultural sector, Thinkpiece for CGIAR Science Forum Workshop on “ICTs

transforming agricultural science, research, and technology generation," Wageningen, Netherlands, pp. 16-17.

7. H. Eakin, P.M. Wightman, D. Hsu, V.R. Gil Ramón, E. Fuentes Contreras, M.P. Cox, T.A.N. Hyman, C. Pacas, F. Borraz, C. González-Brambila (2015). Information and communication technologies and climate change adaptation in Latin America and the Caribbean: a framework for action, Climate and Development, 7, pp. 208-222.

8. A.P. Upadhyay, A. Bijalwan (2015). Climate change adaptation: services and role of information communication technology (ICT) in India, American Journal of Environmental Protection, 4, pp. 70-74.

9. N. Zanamwe, A. Okunoye (2013). Role of information and communication technologies (ICTs) in mitigating, adapting to and monitoring climate change in developing countries, International conference on ICT for Africa.

10. A. Mickoleit (2010). Greener and smarter: ICTs, the environment and climate change, OECD Publishing.

Corresponding Author

Alisha Y. Warke*

Sr. Analyst, Capgemini Technology Services India Ltd., Bengaluru