Chapter 13
Role of Cyber Security in Drone Technology

B. Siddappaji and K. B. Akhilesh

Abstract Drones or Unmanned Aerial Vehicles are cyber-physical systems (CPS) meaning an integration of computation, networking, and physical processes. The main technology components of drones are physical structural airframe, propulsion system, embedded computing systems (ECS) such as ground control station (GCS), autopilot system, virtual radio link, multiple payloads, launch and recovery system. Drones systems are reliant on virtual cyber network and embedded computational system for their operation. Cyber security is meant for protecting technologies and processes. An attacker may misuse or manipulate the sensor input or functions, or he may simply disable them to cause denial of service attacks and make unwanted failsafe mechanisms. The drone has been identified as vulnerable to cyber-attacks because of their uniqueness of network and dispersed physical systems located in remote places and because of the cyber-attacks which can result in the defective operation of the control loop, denial of service, destruction and exfiltration, and information corruption. Hence, two important concerns need to be addressed for drones are cyber airworthiness safety and cyber reliability as well as security. In this paper, recent attack and failure of drones, drone network architecture, cyber security is introduced. Role of cyber security, standards, challenges, and requirements are presented.

Keywords Cyber-physical systems · Drone · Network architecture · Cyber security regulations · Standards · Cyber-attacks · Digital platform

B. Siddappaji (✉)
Aeronautical Development Establishment, DRDO, Bengaluru, India
e-mail: sidaps@gmail.com

K. B. Akhilesh
Department of Management Studies, Indian Institute of Science, Bengaluru, India
e-mail: kba@iisc.ac.in

K. B. Akhilesh and D. P. F. Möller (eds.), *Smart Technologies*,
https://doi.org/10.1007/978-981-13-7139-4_13

13.1 Introduction

The participating units (PU) of battlefield/warfare are intelligent sensor grid, command and control (C2) grid, and effector or shooter grid. The modern battlefield comprises system of systems network enabled and geographically dispersed connected via robust communication data link which is referred as network-centric warfare (NCW). NCW is a revolutionary step which provides flexibility, cooperation, dynamic, and real-time collaboration between grids, which introduce new dimensions and concepts to military power such as information superiority and decision superiority.

Drones are cyber-physical systems (CPS) which are one of the intelligent sensors/C2/shooters which provide persistence intelligence, surveillance, target acquisition and reconnaissance (ISTAR) to the C4ISTAR grid for effective directing, commanding, and controlling of the shooter grid kill-chain cycle. Basic technologies essential for drones are embedded computing systems (ECS), networking, information, and communication technologies (NICT), and sensing and actuating technologies (SAT).

Battlefield damage assessment, electronic warfare such as electronic protection, electronic support, electronic attack, airborne data relay, mobile communication, precision delivery of weapon to finish the enemy target, and real-time situational awareness of the battlefield are some of the other roles played by the UAVs in the modern battle space. UAVs success on battlefields in Afghanistan, Kosovo, and Iraq war has driven a demand for various types of UAVs and has established their importance in military operations. With this game changing tactics, autonomous UAVs systems carry varieties of payload to meet the modern battlefield requirements. UAVs provide real-time videos/still images and accurate geo-location of the target to the operational commanders at all level for swift decision making.

Drones are unique autonomous/semi-autonomous vehicles; they need to execute mission well under ambiguity and uncertain environment for long endurance; and they must be able to balance for system failures without external pilot/human intervention. This paper highlights the drone security aspects, drone communication aspects, various types of cyber-attacks and open research problems.

13.2 CPS Drones Are Key Enablers in Net-Centric Warfare

Unmanned aerial vehicles (UAVs)/drones are making significant impact for their continuing technological innovations and their diverse applications both in military and in commercial fields. In the military, UAVs are used for net-centric operations (NCO) missions as an intelligent sensor grid such as persistence intelligence gathering, surveillance and reconnaissance (ISR), and target acquisition (TA); the acquired data will be transferred to command and control (C2) via robust secure data link which may be within line of sight or beyond line of sight for decision making and

action will be taken to attack target using precision weapon shooter grid. In the commercial scenario, small UAVs landscape is emerging steadily IoT services such as border surveillance, disaster response, firefighting, law enforcement, precision agriculture, news coverage, land mapping, and personal use to mention a few. Small UAVs or drones are available in the market which is fully equipped with an HD camera controllable with an iPad for about $300.

The mechanized warfare has been dominated by the deployment of physical military assets such as tanks, ships, and aircraft in the battlefield. The coordination of military assets is achieved in a synchronized manner in accordance with the appropriate C2 and the defined missions accomplished independently of the other systems within the battle space. Mechanized warfare housed all the necessary sensors, decision makers, and weapons on dedicated platforms with limited radio-based voice and data communications which is less effective and less combat power.

On the other hand, NCW envisages the coordination of many assets, each with their own intelligence gathering or effects capabilities, in a near real-time framework. The key enablers of NCW are agility, configurability, currency and accuracy of information and the subsequent quality of decision making and speed of response.

Battlefield targets can be detected using multiple sensor technologies such as ground radar, human intelligence, UAVs, manned aircraft, helicopter, and satellites. UAVs are key enabling sensors and meet the following effective NCW operations:

- Near real-time dissemination of ISTAR data to C2;
- Data fusion techniques;
- Automated target recognition and tracking;
- Accurate time and space reference frameworks;
- Geo-location technologies;
- Data transmission to networks.

In the future, thousands of drones are deployed in the sky for the Internet of things (IoT) services such as e-commerce applications, precision agriculture, and package delivery operations. From January 2016, the drones registered in the USA exceed 2 lakhs in the beginning 20 days as per Federal Aviation Administration (FAA). In India, government, research and development institutions are allowed to deploy the drones for their missions, whereas private operators need to get permission from Directorate General of Civil Aviation (DGCA) a prior before putting the drones on the sky.

IoT services such as daylight and night surveillance using daylight TV camera/thermal infrared imaging technology, airborne data telemetry and algorithms to successfully track wild animals, disaster management at various places of India, 3D mapping, and precision agriculture such as soil quality study are done using Netra developed by DRDO-India forge has successfully carried out.

UAVs are integrated with high-definition IoT cameras and sensors to monitor Indian sensitive communal situations such as Ramadan procession in Lucknow, networked UAVs at Kumbh Mela in Uttar Pradesh, Ganesh Chaturthi processions in Maharashtra. The data were archived, disseminated, and transmitted to traffic police

officers over mobile phones to allow for instant diversions, vehicle, and crowd control in real time. UAVs assembled with IoT infrared and high-resolution imaging are being considered by the Indian security agency for border surveillance, coastal and maritime security, oil and natural gas pipeline monitoring, securing offshore assets, and urban security. UAV manufactured by China, DJI Phantom is being used in India by several Indian start-ups such as Funaster and Quidich for photography and video services. In India, drones for IOT Services are going to stay and one can say the future is unmanned and IoT unlimited.

Few important challenges need to be addressed before putting number of drones into the sky. First and foremost is traffic avoidance and collision system and secondly public safety and privacy. Therefore, traffic collision avoidance system (TCAS) is very important to implement in drones for maintaining safety of flight levels in airspace. In India, Director General of Civil Aviation (DGCA) authorities formulate air traffic control (ATC) procedures and processes. Acceptance by public is another important parameter that may limit the utilization of drones in the sky. This concern is logical as drones may disturb the privacy of persons by passing above them and remotely tracking their daily activities. Hence, safety measures and confidence of public are vital factors while putting drones for IoT services.

When drones are exploited for IoT services such as package delivery to customer, there need to be verification of drone and ensure it is for correct recipient or customer to distribute the parcel and not some other unidentified drone invading the customer premises. Hence to control the above, an efficient strategic planning of drone's route or navigation needs to be evolved.

IoT vision allows drones to become essential integral part of smart city infrastructure. IoT vision enables cyber-physical systems (CPS) to be connected 24×7, anytime, anywhere ideally using any kind of ubiquitous network and providing IoT services. Drones USP are low cost, versatile, ease of deployment, ease of reprogram during mission time, capable of measuring area, distance anywhere, and capable of flying in controlled and uncontrolled airspace. Drones encompass different technology components such as aviation packages, IoT sensors or payloads, customized software, and data link devices that provide radio links to the ground control station (GCS). The drone and GCS two parts jointly form a whole entity called UAV/drone-IoT thing.

13.3 Navigable Air Space and Drone Classifications

As per International Civil Aviation Organization (ICAO), navigable airspace is broadly categorized into controlled airspace and uncontrolled airspace. Instrumental flight rules (IFRs) and visual flight rules (VFRs) are used in the controlled airspace within ATC, and prior permission is required to enter the controlled airspace. Classes A, B, C, D, and E exist in this category. In the uncontrolled airspace, ATC permission is not required. Under this category, F and G classes exist.

Drones classification is based on the type of function or mission, range, altitude, endurance and all up-weight factors. Based on the functionality, drone can be categorized as target drone/ISR drone/package delivery/e-commerce drone, combat, research and development. Based on the range, altitude, endurance, and all up-weight, drones can be classified as nano-/micro-, mini-/small, medium-altitude long-endurance (MALE) and high-altitude long-endurance (HALE) drone. The maximum altitude of nano-/micro-drones is below 300 m, up to 5000 m-mini/medium, while anywhere above 5000 m are large drones. Regarding the range line-of-sight (LoS) communication, it is less than 3 km for micro/small drones and up to 250–300 km for the medium drones. However, the long-range, high-altitude and long-endurance large drones work beyond LoS (BLoS).

13.4 Cyber-Attack and Security Threats to Drones

With the advancement in technology, the application domains of drones are no more limited to laboratories or defense. They can also be used by hobbyists, pranksters, and troublemakers. This popularity may lead to an increase in the threats to the general public as well as chances of adverse usage of increasingly cheaper technology. After Iran's claim of RQ-170 capture, an in-depth study of UAV vulnerabilities has been done by several researchers including our advanced computing research laboratory (ACRL) team at the University of Toledo. Through our studies, it was understood how easily a UAV can be compromised and attacked. In 2012, North Korea launched a GPS jamming attack on its soil bordering South Korea, which disrupted the navigation of aircraft, ships, and ground vehicles. Several other works discuss recent attacks on UAVs. A recent news in The Washington Post detailed 47 biggest drone failures from 2001 to 2013 and the plan of US DoD to extend UAV operations to 110 bases in 39 states by 2017. It was noticed that until 2007, the number of reported cyber-attacks either in the civilian domain or to military systems were negligible compared to past few years. The primary reason behind the absence of attacks was the low popularity of these systems in the civilian domain, which didn't give adversaries much opportunity to study and exploit these systems. An earlier incident of satellite hacking was reported in 2007, which involved a British satellite being controlled by a terrorist group in 1999. In 2007, another news reported a US Satellite being used by LTTE (a Sri Lanka-based terrorist organization) to broadcast their messages and videos using some free bandwidth.

The first major case of an attack on a UAV system was the discovery of the recording of a UAV feed when some members of an Iraq-based terrorist group were captured in December 2009. The video feed was captured using a $26 software called Sky Grabber which was designed to capture free satellite-based entertainment channels, using a satellite antenna. This incident occurred due to the reason that terrorists discovered the vulnerability of the video feed being unencrypted. It came to the light later that this vulnerability was known to the Pentagon since the early 1990s. In September 2011, a malware was found in a control room computer of a

USAF Base, which was serving as a base station for UAV Command and Control Network. Later, it was declared as just a Keylogger, but clearly, was a huge threat to the national security. On the contrary, physical attacks on these drones pose a threat as loss of technology to adversaries and troublemakers. In December 2011, Iran claimed that it shot down a US RQ-170 stealth drone. In 2014, they again claimed that they have created a copy of that captured drone through reverse engineering the UAV design. In August 2014, Iran again claimed that they have shot down and captured an Israeli stealth, radar-evasive type drone called Heron which could be further reverse engineered and used against the US and its allies.

Through this discussion, we understand that it is important to evaluate the risk and vulnerability of a UAV for cyber-attacks based on its components including its comm-links, storage units, fault handling mechanisms, etc. Availability of a proper testbed to test these systems before the flight would lead to the prevention of midair collision and ground casualty. It would also help prevent any loss of human life and minimize investments in failed experiments. Recent increase in attack attempts on these unmanned systems has raised concern among defense as well as commercial manufacturers. With increasing autonomy level of these systems, concerns over their use have been ever increasing. These concerns necessitate the need for cost-effective and safe virtual simulation testbed environment for testing the accuracy of various security implementations in the drone system (UAS).

Being a cyber-physical system, a UAS is vulnerable to most network-oriented cyber-attacks but some of them can be more dangerous than others and can lead to a more unstable and vulnerable state of the UAS. Therefore, it is important to prioritize threats according to the risks they pose and their impact on the system once occurred. Based on this priority, threats should be addressed, and proper mitigation measures should be developed. The table below summarizes the major security threats to UAVs (Table 13.1).

13.5 Drone Communication Network Architecture

Long-range autonomous UAVs serve to provide ISTAR imagery using data links such as line of sight, satellite relay, airborne relay, forward pass concepts. Predator and Reaper UAVs have two C2 data links, a low bandwidth telemetry data link that describes the status of the UAV onboard systems, and a high bandwidth data link to stream the imagery and telemetry from the UAV's ISTAR sensors. Predator UAVs have a 200-Kbps outbound channel for command and control and a 3.2 Mbps return channel for data dissemination, The Global Hawk UAV, with operational data rates of up to 50 Mbps in the return channel (Fig. 13.1).

Table 13.1 Security threats to UAVs

Component/technology	Threat/attack
Satellite communication	Weak encryption
	Congestion due to traffic
	Availability attacks (Jamming, DoS, etc.)
Other radio comm links	Compromised UAVs
	Eavesdropping
	Radio jamming and DoS
	Location privacy attack
Unmanned aerial vehicle	GPS spoofing
	Fuzzing attack
	Hijacking and immobilization
	Gain scheduling attack
Ground control station	Malware injection
	Keylogger and other data extraction mechanisms
	Weak authentication
Command and control Messages	Weak message authentication
	Control channel jamming
Sensing	Sensor and actuator manipulation
	Spoofing

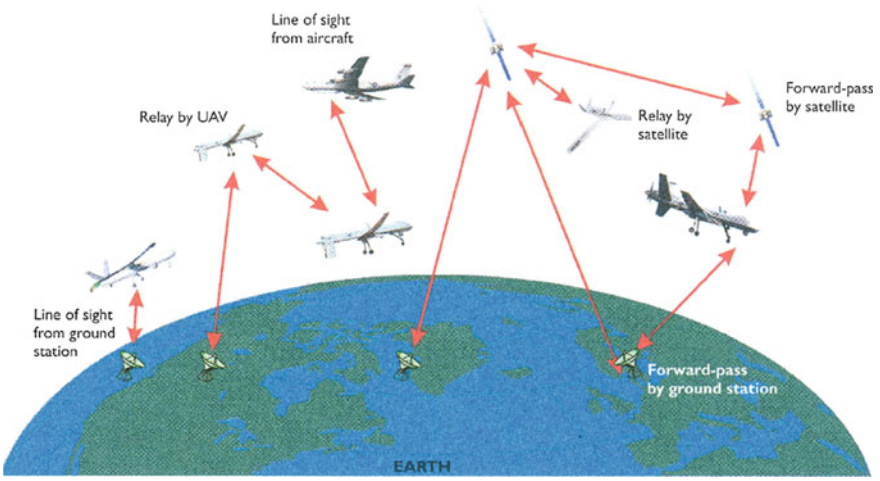

Fig. 13.1 Drone communication network architecture (Deakin 2010)

13.6 Cyber Security and Protective Risk Assessment Scheme

Drones are cyber-physical systems, which means their mission or applications are reliant basically on the close interaction between systems such as aircraft/GCS and computational elements such as flight control computer, data link, and other computational systems. Hence, the security is not only on the virtual network but also on the physical components also. Hence, there is a requirement for framework for the analysis of security issues in drones to be inclusive of the entire aircraft.

The diagram given below shows the risk assessment scheme containing integrity component, confidentiality, etc. In order to calculate the protective risk scheme, the probabilities are multiplied with the susceptibility value (Figs. 13.2 and 13.3).

13.7 Conclusion

Low cost, ease of deployment and accessibility of cheaper components/parts/software to build mini-drones has become possible. Small drones are now being exploited for recreational use in addition to research activities. Hence, it is very clear that incorrect or failure in writing programs for waypoint navigation will lead to accidents. It is very essential to provide security to both network and physical components by building suitable testbed simulation and environment.

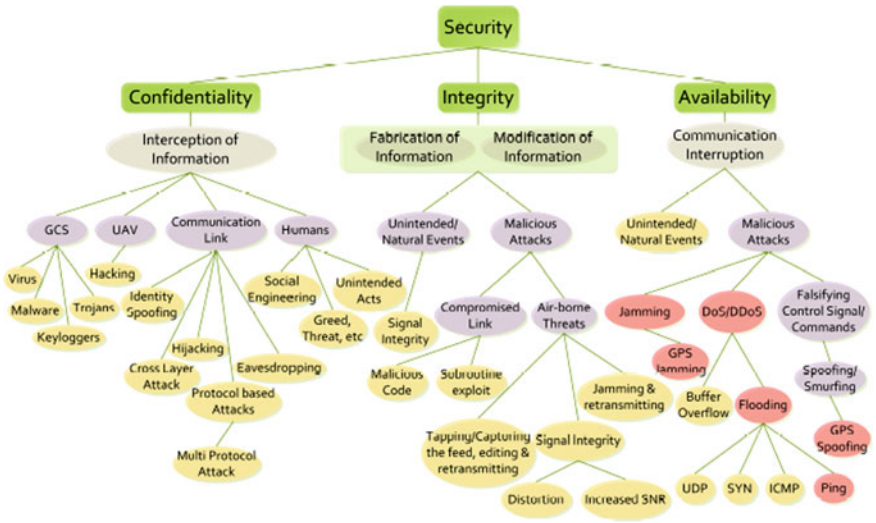

Fig. 13.2 Risk assessment scheme (Javaid 2015)

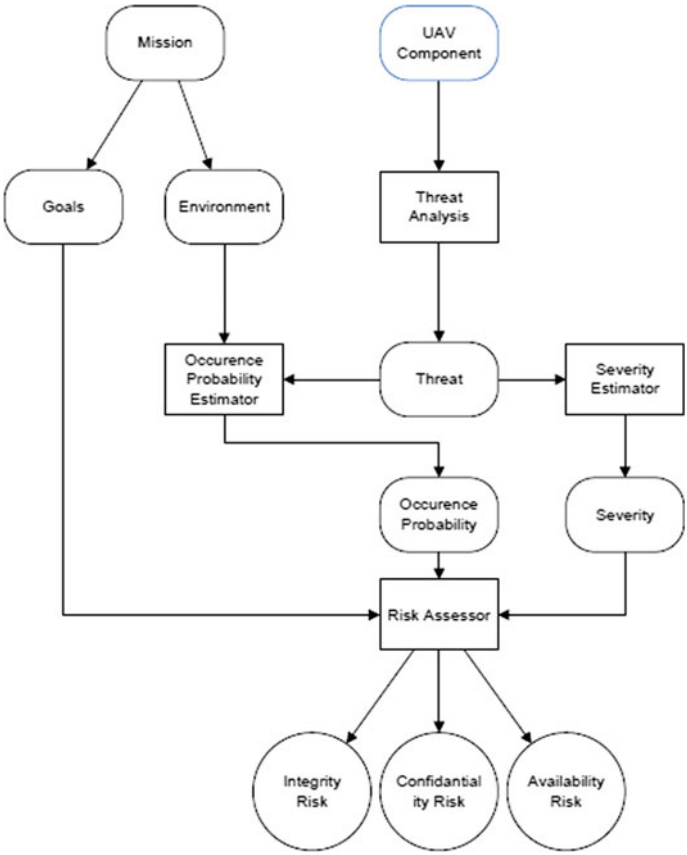

Fig. 13.3 Protective risk scheme (Javaid 2015)

This study logically highlights the current potential scenario of cyber security vision for drones. It also highlights the importance of cyber security in UAVs for integration and formulation of UAV policies for civilian use. In addition, it also draws the picture of IoT in the present context. Hence, such study is necessary for the researchers all over the world and aviation authorities of government to formulate policies and regulations for the mass use of UAVs in India as well as other parts of the world.

In order to provide security to drones, the following points may be considered: design security into all components rather than adding it in later; collect and retain least amount of information; know where information resides; know where it moves; encrypt everything; select vendor who share your vision, mission, and values; conduct a complete security audit of the environment as designed; and train staff on all risk elements associated with the drone infrastructure and associated data.

Active association by the research institutions/industries in the process of cyber security for drones is not only encouraged, but is very essential for the drone industry to grow and progress in an orderly fashion.

References

Borgen, K. Scratch build your own quad-copter! http://www.instructables.com/id/Scratch-build-your-own-quad-copter/step2/Materials/, August 2013. Online; Last accessed June 3, 2015.

Deakin, R. S. (2010). "Battlespace technologies" network-enabled information dominance 2010 Airtech House. "Unmanned systems Integrated Roadmap, FY2013-2038", US Department of Defence. Accessed at http://www.defense.gov/pubs/DOD-USRM-2014.pdf.

Javaid, A. Y. (2015). Cyber security threat analysis and attack simulation for unmanned aerial vehicle network, Theses