Security, Privacy, and Safety Aspects of Civilian Drones: A Survey

Article *in* ACM Transactions on Cyber-Physical Systems · November 2016

DOI: 10.1145/3001836

2 authors, including:

Riham Altawy
University of Victoria
36 PUBLICATIONS **711** CITATIONS

Security, Privacy, and Safety Aspects of Civilian Drones: A Survey

RIHAM ALTAWY and AMR M. YOUSSEF, Concordia Institute for Information Systems Engineering, Concordia University, Montréal, Québec, Canada.

The market for civilian unmanned aerial vehicles, also known as drones, is expanding rapidly as new applications are emerging to incorporate the use of civilian drones in our daily lives. On one hand, the convenience of offering certain services via drones is attractive. On the other hand, the mere operation of these airborne machines which rely heavily on their cyber capabilities poses great threats to people and property. Also, while the Federal Aviation Administration (FAA) NextGen project aims to integrate civilian drones into the national airspace, the regulation is still a work-in-progress and does not cope with their threats. This paper surveys the main security, privacy, and safety aspects associated with the use of civilian drones in the national airspace. In particular, we identify both the physical and cyber threats of such systems, and discuss the security properties required by their critical operation environment. We also identify the research challenges and possible future directions in the fields of civilian drone security, safety, and privacy. Based on our investigation, we forecast that security will be a central enabling technology for the next generation of civilian unmanned aerial vehicles.

CCS Concepts:•**General and reference** → **Surveys and overviews;**•**Security and privacy** → *Systems security;* Privacy protections;

Additional Key Words and Phrases: Unmanned Aerial Vehicles, Parcelcopters, Security, Safety, Privacy, Civilain Drones, Cyber-Physical Systems

ACM Reference Format:
Riham AlTawy and Amr M. Youssef, 2016. Security, Privacy, and Safety Aspects of Civilian Drones: A Survey. *ACM Trans. Cyber-Phys. Syst.* 1, 2, Article 7 (December 2016), 25 pages.
DOI: http://dx.doi.org/10.1145/0000000.0000000

1. INTRODUCTION

Not far in the past, trained certified pilots were the only persons who were granted authorization for flying aircraft. Nowadays, any individual can operate a flying machine within unregulated airspace. However, sharing the controlled airspace between manned aircraft and drones is a great challenge. Drones are Cyber-Physical Systems (CPSs) [Khaitan and McCalley 2015] which are also known as Unmanned Aerial Vehicles (UAVs). Projections forecast by the FAA stated that more than one million UAVs were going to be sold in 2015 [Addady 2015]. Indeed, such projections trigger concerns within the security society regarding cyber attacks [Hartmann and Steup 2013] against civilian drones [Villasenor 2014]. More precisely, with the FAA requiring mandatory registration of drones which holds the operators of drones accountable, the majority of the illegal use of drones will be achieved via their hostile acquisition, which can be established through exploiting their cyber vulnerabilities [Faughnan et al. 2013]. Additionally, most aviation standards set by regulatory bodies do not yet cover cyber-physical threats associated with the integration of drones into the national airspace, hence, the scope of our survey which attempts to bridge this gap.

Authors' address: R. AlTawy and A.M. Youssef, Concordia Institute for Information Systems Engineering, Concordia University, 1455 De Maisonneuve Blvd. W., Montréal, Québec, Canada.

DOI: http://dx.doi.org/10.1145/0000000.0000000

Currently the use of civilian drones is dominated by hobbyists for recreational purposes [Cai et al. 2014]. However, giant companies such as Amazon, Google, and Facebook are planning to employ drones for the delivery of goods and services. Indeed, one can predict that as the number of operating drones increases, more security, privacy, and safety threats will emerge. One of the well known problems caused by civilian drones is their interference with aviation systems.

UAVs are aircraft that can be operated either by remote control or autonomously using onboard computers. The physical elements onboard a drone employ a network of sensors and actuators which communicate with the ground control system via a wireless link. Accordingly, the UAV system is vulnerable to attacks that target either the cyber and/or physical elements, the interface between them, the wireless link, or even a combination of multiple components [Constantinides and Parkinson 2008]. A case where a military drone was taken over by an unauthorized party occurred when the Iranian cyber warfare unit was able to safely land a U.S. drone that allegedly violated its airspace [Hartmann and Steup 2013]. Although the exact scenario of the takeover is not commonly agreed upon, one course of events suggests that the takeover employed a mix of cyber attacks on the UAV where, firstly, all legitimate communications to the drone were interrupted by jamming both the satellite and ground control signals. Then, a GPS spoofing attack [Kerns et al. 2014; Shepard et al. 2012] was launched to feed the UAV with modified GPS data to make it land in Iran, tricking the drone into thinking that it was landing in its home base. Despite the fact that this attack was carried out on a military drone and our survey focuses on civilian drones, both types of UAVs employ similar core technologies, and accordingly, such an approach can be used to hijack civilian drones as well.

Drones can also be privacy and safety hazards [Clarke 2014; Boyle 2015]. In other words, the acceptance of the idea that intelligent machines equipped with infrared cameras and possibly microphones are flying over our heads and within our private airspace is completely dependent on the trust we have in the operator. However, with the expected increase in the number of civilian drones, it is next to impossible for a person to determine the operator of the UAV by only looking at it. In fact, if there are no proper regulations, drones can be easily used for illegal purposes ranging from surveillance and unauthorized tracking to even criminal uses such as targeted assassinations and terrorist attacks.

In this survey, we aim to raise awareness about the security, privacy, and safety aspects associated with the deployment of civilian drones into the national airspace. We particularly investigate their vulnerabilities to a cluster of possible attacks which can result in a malicious takeover or crashing of the drone, and analyze the security requirements of such systems. We also present a literature survey on the published works that offer solutions to some of the known vulnerabilities. Moreover, we highlight the physical challenges associated with the large scale deployment of civilian drones for the delivery of goods and services. From another perspective, we investigate how civilian drones can affect the security of people and their sense of privacy and safety. Furthermore, we identify the risks introduced by the integration of drones in national airspace. Finally, we discusses open problems and avenues for future research.

The rest of the paper is organized as follows. In the next section, a brief overview of the evolution of drones, their categories and high level architecture is given. In section 3, we give examples of how the national airspace is expected to accommodate civilian drones and how they can be used in both beneficial and harmful manners. Afterwards, in section 4, we investigate the security and safety threats targeting civilian drones where we identify both the cyber and physical threats that can target their different components, and define the expected security requirements of such systems. In section 5, we emphasize the privacy risks associated with the use of drones in the national

airspace, and give an overview of UAV systems designed for such malicious purposes and examples of mitigation techniques. Finally, we discuss open problems and future research directions, and summarize the main ideas presented in the paper.

2. THE EVOLUTION OF DRONES

According to [Marshall et al. 2015], the first drone was the fruit of a U.S. navy research project led by Elmer Sperry, the founder of the flight navigation control firm Sperry Corporation. Ever since, UAVs have been deployed for tasks which are characterized by being dangerous, dirty, and dull, commonly known as three Ds operations. Such operations are usually carried out outside of the cities where the human population is minimal [Marshall et al. 2015]. Thus, studying the effect of drone use on the security and safety of individuals was not of significant interest. Currently, civilian drones are becoming more popular among hobbyists and entrepreneurs, and with many companies pushing for deploying drones for delivery of goods and services, the national airspace is expected to get completely reshaped. The FAA mandatory registration of drones is effective in the event of the capture of a violating drone, but it does not provide any preventive solution. Accordingly, protecting civilian drones from adversaries and protecting individuals and their properties from malicious drones is still an open problem. In what follows, we give a brief overview of the different categories and control methods of drones, followed by the general architecture of UAV systems.

2.1. UAV Categories and Control

Drones vary drastically in size, some are as small as a match box and others are as large as manned aircraft and typically, the bigger the drone, the higher and longer it can fly. According to the European Association of Unmanned Vehicles Systems (EUROUVS) [VAN Blyenburgh 2003], UAVs are classified into: (i) Micro and mini drones with weights starting from several grams to 24kg, (ii) Tactical drones that weigh less than 1500kg, and (iii) Strategic drones which are the heaviest UAV platforms.

Controlling the actions of drones varies according to the degree of autonomy designed into the vehicle [Melzer 2013]. UAVs vary from being fully controlled remotely by an operator via manual electronic rudder or a complex ground control station to a fully autonomous control system where the drone navigates itself and depends on its sensors to perform a set of preprogrammed tasks. Within this range and depending on the degree of dominance exercised by a human operator, UAV control can be divided into three categories:

- *Remote Pilot Control (human-in-the-loop).* This type of control is also known as *operator static automation* where the control system is designed such that all decisions are taken by a remote human operator.
- *Remote Supervised Control (human-on-the-loop).* This type of control is commonly known as *adaptive automation*. It allows the drone to carry out the mission process independently from human commands and enables human intervention at the same time.
- *Full Autonomous Control (human-out-of-the-loop).*This class of control is also known as *system static automation* in which the drone carries out all the necessary decisions required for the successful completion of the mission.

Civilian drones that are used by hobbyists are usually remotely controlled by their operators. However, drones that are going to be used for the delivery of goods and services are expected to adopt a human-on-the-loop control model, where according to Amazon's proposal [Amazon 2015], one operator is going to be responsible for the supervision of a set of dispatched drones at the same time.

2.2. UAV System Architecture

Civilian UAV systems consist of three main elements which are the unmanned aircraft, the ground control station (GCS), and the communication data link [Marshall et al. 2015]. Moreover, the aircraft consists of an airframe, a propulsion system, a flight controller, a precision navigation system, and a sense and avoid system. Throughout our survey, we only focus on the building blocks that are relevant to our analysis, and hence consider that the aircraft contains a flight controller, a set of sensors, and actuators. Figure 1 provides a high level architecture of a UAV system and its main elements. In what follows, we give a brief overview of the main building components of civilian UAVs.

2.2.1. Flight Controller. The flight controller is the central processing unit of the drone. In addition to stabilizing the drone during its course, it reads the data provided by the sensors, processes it into useful information, and according to the type of control either relays this information to the GCS or feeds the actuator control units directly with the updated state. The flight controller implements the communication interface with the GCS. More precisely, commands from the GCS are processed by the flight controller which in turns affects the deployed actuators. Furthermore, the flight controller has a number of transmitter channels associated with the telemetric signals it can send to the GCS. The flight controller can have multiple sensors integrated onboard or communicate with an external sensor unit. The UAV system sensors include accelerometer, gyroscope, magnetic orientation sensor, global positioning system (GPS) module, and electro-optical or infrared camera.

2.2.2. Ground Control Station. A ground control station is an on-land facility that provides the capabilities for human operators to control and/or monitor UAVs during their operations. GCSs vary in size according to the type and mission of the drone. In other words, for recreational mini and micro drones, GCSs are small hand held transmitters used by hobbyist. For tactical and strategic drones, a large self-contained facility with multiple workstations is employed as the GCS. A GCS communicates with the drone through a wireless link to send commands and receive real-time data, thus creating a virtual cockpit.

2.2.3. Data Links. The data link refers to the wireless link used to carry control information between the drone and the GCS. The adopted communication link depends on the UAV operation range. Drone missions are categorized according to their distance from the GCS into Line-of-sight (LOS) missions where control signals can be sent and received via direct radio waves, and Beyond line-of-sight (BLOS) missions where the drone is controlled via satellite communications or a relaying aircraft which can be a drone itself [Marshall et al. 2015].

3. CIVILIAN DRONES AND THE PARCELCOPTERS

The term “Parcelcopters” refers to the aerial drones that are used for the purpose of delivering goods. Although delivery drones have not populated the north American skies yet, pressure from giant companies such as Amazon, Google, and Facebook on the FAA to clear their use is increasing. Meanwhile, in Germany, DHL is regularly using parcelcopters to deliver medicine twice a day to the island of Juist where drones autonomously cover a distance of 12km [Moormann 2015]. In what follows we give examples of the various uses of civilian drones.

3.1. Uses of Civilian Drones: The Good, the Bad, and the Ugly

Once regulated and cleared for national airspace, civilian UAVs can be used in many applications [Mohammed et al. 2014]. Most such applications are beneficial and are in-

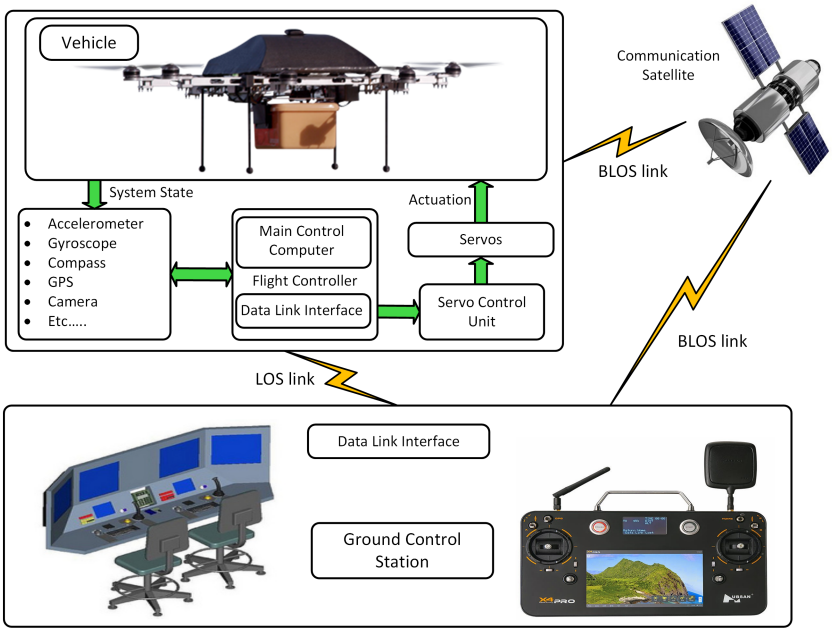

Fig. 1. High level architecture of a UAV system.

tended to overcome obstacles introduced by the dependence on a number of factors such as human availability, and geographical, spatial, and temporal conditions. In what follows we introduce some of the existing and potential uses of civilian drones including those that are beneficial and those that are injurious.

- *Internet access*: UAVs can be used to provide Internet access to individuals in rural areas which are not covered by conventional communication networks. Such proposals have been addressed by Facebook's Aquila solar powered drone and by Google which has acquired Titan Aerospace, a prominent maker of UAVs. Following a similar concept, low tech decommissioned military drones are being planned for use as WiFi hotspots by the Defense Advanced Research Projects Agency (DARPA) [News 2014] to serve the U.S. troops in secluded field areas.
- *Ambulance and medicinal services*: Drones can be used to deliver medicine and emergency response equipment to patients in areas which are hard to reach or require a long time when traditional delivery methods are adopted. In addition to the DHL medicinal parcelcopter project [Moormann 2015] in Germany, an ambulance drone project is proposed by Delft Technical University [TU Delft 2014], where an automated external defibrillator is delivered in response to cardiac arrest calls.
- *Cinematography and aerial photography*: Drones are currently used by filmmakers to approach aerial filming in ways that were not possible before which enriches the filming platform with new levels of creativity. They are also used by individual photographers to capture pictures with a bird's eye view [Rango et al. 2006]. Aerial photography is popular for both recreational and business purposes.
- *Natural disaster control*: UAVs are being used in disaster control and assessments since hurricane Katrina in 2005. Drones were deployed in affected areas that were cut off and the roads were blocked with fallen trees to assess the disaster consequences and check the state of survivors.

- *Construction, mining, and crop management*: Drones can be customized and used to perform specific tasks related to construction, mining, and agriculture. For example, in agriculture, drones can be used to fertilize and water crops.
- *Drug smuggling and prison breaks*: Several cases have been reported where drones were used to smuggle contraband drugs across the U.S-Mexico border [Valencia and Martinez 2015]. Also, on several occasions, drones have been used to smuggle phones, drugs, and cameras into prison facilities in the U.S [Reich 2015].
- *Targeted assassinations*: Although there are no reported cases where drones were used in assassinations among the civilian population, the concept is adopted in military missions and thus, it can be adapted within the civilian airspace. More precisely, while the acquisition of civilian drones with assault capabilities might be hard, they can be used in a kamikaze style for targeted assassinations. This concept has been demonstrated by the Israeli K1 suicide UAV [Eshel 2015] designed by the Aeronautics Defense Systems company in Yavne.

UAVs' integration into the national airspace is a key aspect of the FAA Next Generation Air Transportation System (NextGen) [FAA.gov 2015] which aims primarily to accommodate emerging technologies in a safer and greener approach. Such objective can only be fulfilled by granting drones more access to the national airspace and acceptance by the air traffic controlling authority. To gain the required acceptance, UAVs must demonstrate a sufficient level of safety and security. Indeed, such demonstration is only realizable upon identification, analysis, and finally settling a number of entangled and variably complex issues. An important challenging issue facing the drone integration process is how to control the airspace traffic. More precisely, when the airspace is going to be shared between drones and manned aircraft, the whole air traffic control system has to be redesigned in order to deal with the new and continuously variable operational parameters introduced by the integration of drones. In what follows, we highlight the air traffic control challenges associated by the wide introduction of UAVs in the same controlled airspace used by manned aircraft.

3.2. FAA Regulations and Airspace Management

Unlike commercial passenger and cargo aircraft, civilian drones are regulated by the FAA under special airworthiness categories [FAA.gov 2016]. Such categories include aircraft that are operated by civilians and used for recreation, aerial and agricultural surveying, weather control, and research and development. A special airworthiness certificate is issued for an individual aircraft under one of eight categories depending on the required purpose of operation. Such certificate is usually valid for one year. Additionally, the FAA requires the operator to attend a continuing airworthiness program and a maintenance training program.

Although the operation of drones and manned aircraft is regulated by a different set of rules, both are going to share the same airspace. Accordingly, air traffic control has to be conducted in a different manner in order to accommodate the integration of drones in the national airspace. All the air traffic communication, display, and information processing facilities have to be updated to handles traffic of both manned aircraft and drones. Also, air traffic controllers will be forced to interact with drones in ways different from those used with manned aircraft. For example, they have to be able to understand the actions of the drone without communication, manage traffic sequence, and even order unexpected flight procedures to maintain a safe operation. The impact of the added workload associated with managing both drones and manned aircraft on air traffic controllers is unexplored. More precisely, how their situational awareness and focus on airspace control are going to be affected is unknown. For that reason, NASA in collaboration with the FAA, has launched its UAV traffic

management (UTM) platform [Lozano 2016] as an initiative for an air traffic control system that manages both low flying drones and manned aircraft simultaneously. Just recently, NASA has put its UTM system to the test by flying twenty four different kinds of drones while simulating the operation of dozens of manned aircraft into the same airspace. In addition to the unknown consequences due to drones operation on air traffic controllers, in what follows, we list some examples of the challenges facing air traffic control agencies:

— Restricted see-and-avoid capabilities: Drone operators usually have a restricted view of airspace which is more evident when the drone is operating beyond line of site. Indeed, spotting the surrounding aircraft is hard from a computer screen.
— Delayed responses to instructions: Unless operating fully autonomous, control of the drone is solely dependent on control signals from the GCS. Accordingly, responses of the drone to air traffic control requests are delayed because all communication must be relayed through its operator in the GCS.
— Handling different sizes and speeds: Air traffic controllers must consider other factors when managing drone traffic. For example, light turbulence might affect small drones. Also, more separation is required between slow drones and fast manned aircraft.
— Extra workload on the operators: Operators have to be trained to efficiently handle another graphical user interface in order to respond to air traffic control requests while flying the drone in the same time.

The following section aims to investigate security and safety issues associated with the operation of the UAV system. Moreover, we assess the proposed strategies that offer solutions to some of the identified issues which can further help move the integration process forward.

4. SECURITY AND SAFETY ASPECTS IN CIVILIAN DRONES

The idea of having drones into the national airspace raises serious safety concerns for nearly all spectrum of the society which ranges from government facilities and aviation authorities to regular individuals. As a requirement for the NextGen initiative for integrating UAVs into the national airspace, drones are required to demonstrate a practical resolution for a sense-and-avoid feature [Angelov 2012]. In fact, the FAA regulation 14 CFR Part 91.113 states that drones must deploy an automated sense-and-avoid intelligent system that provides safety levels equal to or even exceeding that of manned aircraft. An example of proposals that offer a safer crashing scenario is proposed in [Ciarletta et al. 2016], where a safety parachuting system is dispatched at the sense of drone termination which aids in minimizing the damage when a collision is unavoidable. Nevertheless, the safety of UAVs remains an open issue.

In the case of civilian drones, functional safety [AlTawy and Youssef 2016] needs cyber-physical security. For that reason, their safe incorporation into the national airspace requires careful security analysis. Throughout the rest of the paper, we consider civilian drones that fall under the category that is required by the FAA for registration. Such drones have capabilities and weight limits that enable their use for malicious and harmful purposes. Moreover, we consider the UAV operator as the individual in control of the GCS and consequently, responsible for commanding the drone though its flight course. Also, we define the secure operation of the UAV as such operation that ensures the protection of the UAV system against cyber-physical threats resulting from intentional or unintentional actions. Also, we define the safe operation of a UAV system as the operation that ensures the protection of the system's surrounding environment, including people, property and other aircraft, from the unexpected consequences of the operation of the drone. From a high level perspective, a safe operation constitutes hazard avoidance, and safe take-off and landing.

The design of a UAV system should incorporate mitigation techniques which address the possible security threats. In what follows, we identify both the cyber and physical threats and classify them based on their target UAV component.

4.1. Cyber-Physical Threats

Cyber-physical attacks are generally categorized according to the power of the adversary [Chabukswar 2014] as follows:

- Revelation capabilities: refers to the power of the adversary to disclose the values of real-time data. For example, an adversary listening to unencrypted wireless information sent on the data link has such capabilities.
- Knowledge capability: which denotes the ability of the attacker to gain a prior knowledge of the system parameters. For instance, such capability is manifested in an attacker that has gained access to the onboard flight controller by falsely being authenticated as the legitimate GCS.
- Disruption capabilities: which refer to the ability of the attacker to interrupt the regular operation of the system.

Any attack carried out on UAVs requires one or more of the above capabilities. Figure 2 depicts examples of cyber attacks against different components of UAV systems. Most of the identified cyber attacks on drones can potentially lead to taking control of or crashing them. In what follows, we identify cyber attacks that target both the flight controller and GCS, and the communication data link.

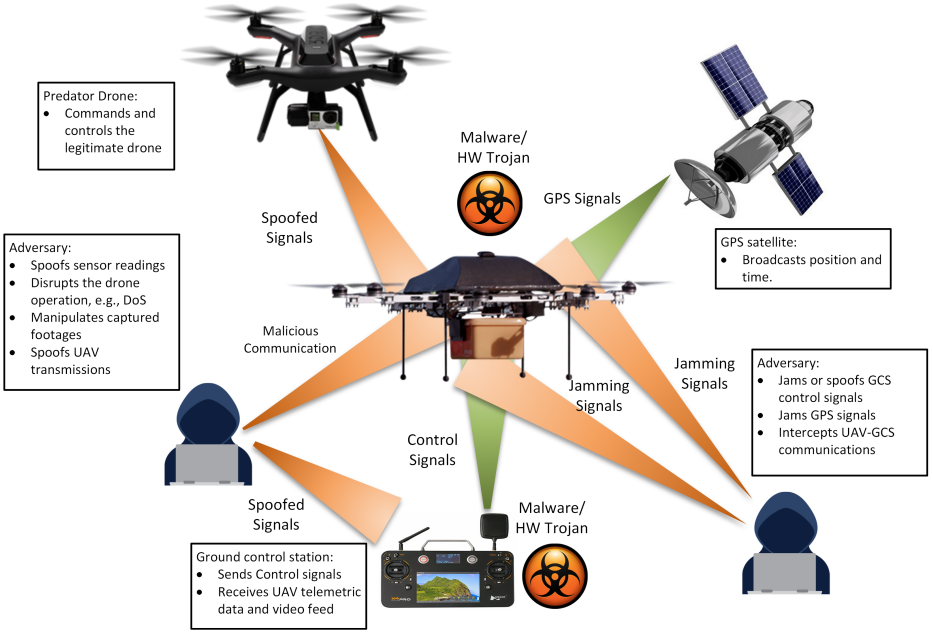

Fig. 2. Examples of cyber attacks that target the flight controller, ground control station and the data link

4.1.1. ***Attacks on the Flight Controller and Ground Control Station.*** The operation of the flight controller is solely dependent on the information received from the ground control station via the data link and acquired by its sensors from the surrounding environment [Mansfield et al. 2013]. Accordingly, attacks on both the flight controller and

ground control station that do not involve the data link are possible only if the attacker can access and manipulate the internal system communication or can fabricate the sensed physical properties in the surrounding environment. Due to the almost complete reliance of UAV operations on multiple inputs from the external environment, most of the attacks commence by external malicious modification of such inputs. In what follows, we identify attacks that target the onboard flight controller and GCS.

- Jamming or Spoofing the GPS Data. Navigation of UAVs depends on the GPS signals received and processed by the onboard GPS receiver. GPS broadcasts are freely accessible unencrypted and unauthenticated signals sent for civilian use. The open nature of the GPS signals enables spoofing attacks [Wesson and Humphreys 2013] where fake signals can be generated and fed to the attacked UAV with the aim of altering the geographical coordinates calculated by UAV's GPS receiver. Also, GPS signals can be easily jammed, thus cutting the external navigation feed to the UAV which renders the UAV in a disoriented state which can eventually lead it into crashing. GPS spoofing attacks on UAVs have been demonstrated in [Kerns et al. 2014], where a team from the University of Texas utilized a custom made GPS spoofing device located at about 0.3 mile from the UAV to generate a perfect replica of the GPS signals and feed them to the drone. Unable to verify the authenticity of the received signals, the drone started responding to the fake signals and was diving directly in to the ground. Normal operation was restored when the manual operator overrode the autonomous control mode. Authentication of GPS signals can offer a solution for GPS spoofing but enforcing it by traditional cryptographic approaches is a complex task and requires changes in the infrastructure of the satellite system. Other proposals for detecting GPS spoofing suggest checking the GPS observables which denote the signals' traveling time and consequently can indicate how far away the sources are [Wen et al. 2005]. Also, detecting sudden changes in signal power or observables within a tolerable range may be an indicator of the start of a spoofing attack. In addition to the common method of GPS spoofing which utilize a GPS signal generator to produce a counterfeit replica of the original one, GPS spoofing can also be achieved by embedding GPS malware in the GPS receiver to produce different location than the one calculated from the received satellites signals. A solution to overcome the consequences of jamming the GPS signals is to adopt an alternative navigation methods. For example, in [Wu et al. 2013], a vision and inertial navigation system is proposed to enable autonomous navigation when no GPS signals are received by the drone.

- Jamming or Spoofing the UAV Transmissions. It is expected that civilian drones will be equipped with an Automatic Dependent Surveillance-Broadcast (ADS-B)-like system which broadcasts the position and velocity of the aircraft every second to avoid collision with other manned or unmanned aircraft. Similar to GPS signals and because the intended receivers cannot be predetermined, ADS-B signals are unencrypted and unauthenticated [McCallie et al. 2011]. Such signals can be easily jammed or replaced by fake ones, leading the drone into an imminent collision due to the inability to detect or verify the ADS-B warning. Also, spoofing ADS-B signals can be used instead of GPS spoofing to take control of the aircraft. More precisely, an attacker can continuously feed the UAV with malicious ADS-B signals to trick it into diverting its course in order to avoid collisions, and ultimately directing it to the desired territory. Such false signal injection attacks were studied in [McCallie et al. 2011] where experiments with a cheap antenna resulted in the aircraft concluding that a midair collision was unavoidable. These attacks can be avoided in manned airplanes because a pilot can visually verify, on a radar system, the proximity of other aircraft and whether they are on a collision course. Other UAV signals include the telemetric data and video feeds sent to the ground control station. Spoofing such signals can directly influence the op-

erator commands which can possibly result in a drone crash. Verifying the authenticity of the drone signals by the GCS can be achieved using Message Authentication Code (MAC) schemes [Menezes et al. 1996]. Also, secure distance bounding protocols [Boureanu et al. 2014] may be used to determine the proximity of the source of the received signals and compare it to the last known location of the UAV.

- Manipulating the Captured Footage. Autonomous low-altitude UAVs rely on the video captured by their cameras for navigation and collision avoidance. Normally, the process starts by the flight controller requesting the captured video from the kernel of the operating system of the flight controller computer by issuing a system call [Deligne 2012]. An attacker who has knowledge of the system parameters and is able to gain access to the flight controller can intercept the system calls issued to the kernel and replace the genuine footage with a fabricated one. A direct consequence of this attack is the hijacking of the drone by intentionally landing it at a location other than the originally intended one. This attack can be coupled with a GPS spoofing attack to completely take control of an autonomous or even a human operated drone.

- Injecting Falsified Sensor Data. The goal of this attack is to destabilize the UAV by compromising a set of sensors through injecting fabricated readings in the flight controller [Mo and Sinopoli 2010], thus undermining the secure control [Alvaro A. Cardenas 2008] of the drone. All externally influenced sensors such as radar, infrared, and electro-optical sensors can be manipulated. As part of the electronic warfare [Robinson et al. 2015], directed energy can be used to control the electromagnetic spectrum which is not limited to radio and radar frequencies but also includes infrared, visible, and ultraviolet signals. A demonstration where an external source of audio energy was used to alter the output of a UAV Microelectromechanical gyroscope by interfering with its resonance frequency was performed in [Son et al. 2015], which led the drone to lose control and crash. Moreover, assuming an attacker with capabilities that enable access to the onboard flight controller procedures, sensors relying on an onboard reference such as the barometer and gyroscope can also be attacked by altering their reported values when requested through system calls by the onboard flight controller.

- Malicious Hardware/Software. Both the flight controller and ground control unit are vulnerable to hardware and software trojans. Such trojans can be either discretely designed in the system or transfered to it. A discovered instance of a software trojan was demonstrated in 2011 when the exposure of the ground control unit in the Creech U.S. Air Force base to a keylogging virus was revealed [Hartmann and Steup 2013]. The software back door was discovered on the computers in the base even though they are not used on the Internet. The keylogger tracked keyboard strokes made by UAV operators to manage the drone fleet over Iraq and Afghanistan. Although there were no reported consequences of the incident, possible ones range from loss of sensitive data to loss of control of the concerned UAVs. An example of a virus that infects civilian drones is a software known as Maldrone [Paganini 2015a], which once installed on the drone, enables the attacker to take control of the UAV. The malware opens a backdoored connection with its botmaster to receive its commands. Maldrone then acts as a proxy for the drone's flight controller and sensor communications, thus enabling the injection of the desired values for both communications. In other words, Maldrone can be used to land any infected drone at the location chosen by the attacker.

On the other hand, hardware trojans can be intentionally designed in the UAV's chips to disable some security mechanisms and when triggered can have catastrophic consequences. An example of such backdoor is the Actel ProASIC chip [Casals et al. 2013] in the new Boeing 787 passenger jet that was designed to allow the chip to be accessed through the Internet. This trojan was discovered by two Cambridge security

experts and it allows passengers using the entertainment system in the aircraft to take over the avionics and control the aircraft. Such trojans can be mitigated by managing the security of the supply chain [Waller et al. 2008] to avoid the use of corrupted components which grants financially capable criminal groups or adversarial nations physical access to the hardware used in the drone.

- Attacking the Mission Assignment System. Companies such as Amazon are planning to employ a low-altitude flying fleet of drones in their Prime Air service [Amazon 2015]. As stated in their proposal, the deployed UAV fleet will consist of a multitude of drones with different cargo weight limits to cope with various packages. Such a delivery system is going to rely on an effective dispatching backbone system [Bethke et al. 2008] to efficiently assign different packages to the right drones that can support the assigned packages and endure the required flight time to destinations. Attacking the dispatching system software so that it does not follow the right logic in the assignments of packages to drones can bring down the whole system and possibly lead to loss of the drones and/or other financial losses. Particularly, if for example a low endurance drone was assigned to deliver a package to a destination that requires flight time more than it can endure, both the drone and possibly its payload will land or even crash somewhere where it is not supposed to be. Another possible motivation for a third party for breaking into the GCS network can be the desire to collect customers' personal information.

4.1.2. ***Attacks on the Data Link***. An important class of attacks is the one aiming to violate the confidentiality and integrity of the communication between the UAV and the ground control station on the data link. Usually, sophisticated attacks aiming to take control of the drone combine one or more of the presented attacks on both the flight controller and the data link. For example, the Iranian acquisition cyber attack carried out on the U.S. Lockheed Martin RQ-170 Sentinel drone allegedly started by attacking the communication on the data link and then carried on with an attack on the flight controller by spoofing the GPS signals. In what follows, we list the possible attacks on the data link.

- Unauthorized Disclosure of Communication. Information exchanged between the UAV and GCS include the telemetry feeds and GCS issued commands. Such information must be protected against unauthorized disclosure when intercepted. A reported example of such attacks is the passive interception attack that was carried out on the U.S. Reapers and Predators drone fleet operating in Iraq. During this attack, the captured live video feeds sent by the UAVs to the GCS were intercepted by Iraqi militants [Hartmann and Steup 2013], who used a cheap off-the-shelf product called SkyGrabber which is mainly used to capture satellite feeds of music and TV. The attack was possible because encryption of the video feeds was disabled for performance reasons. In the context of civilian drones, experiments carried out on an AR drone Parrot quadcopter [Krajník et al. 2011] have shown that the data link communication is not encrypted [Deligne 2012] and hence, interception attacks are also valid. Given that only GCS is the entity receiving information from the drone, key management will not be complicated in the context of civilian drones. Accordingly, authenticated encryption [Bellare and Namprempre 2000] is the first step in guaranteeing the confidentiality and integrity of the exchanged data on the communication link.

- GCS Control Signals Jamming. An adversary who is trying to take control of the drone will first attempt to disable the reception of control signals from the ground control by the drone. The loss of control signals forces the aircraft to go into a *lost link* state. Drones are often designed to enable their operators to upload a lost link protocol [Marshall et al. 2015], which once the ground control communication is lost for a spe-

cific period of time, the drone is supposed to follow a fail-safe autonomous procedure that can, for example, instruct the UAV to return to its base. However, this fail-safe protocol assumes that the lost link state is the result of a malfunction in the data link and that the drone is able to navigate itself autonomously using GPS signals to return to its base. Usually, this is not the case if the drone is under attack, because the adversary is also likely to jam the GPS signals as well, which leads the UAV to fly aimlessly with no control. A case when the fail-safe protocol did not function as predicted was shown in 2010 when the military Fire Scout unmanned helicopter wondered into the no fly zone of the U.S. capital Washington DC [Wesson and Humphreys 2013]. The drone had lost communication with the ground control station and its control system failed due to a software glitch which inhibited its ability to autonomously navigate itself to its home base. After half an hour, the operators were able to re-established control over the helicopter by shifting the operation to another ground control station, thus landing it safely at its home base.

- Denial of Service. One of the main functional requirements of parcelcopters is the delivery of goods and services. Also, such drones would probably belong to the mini drone category and are planned to fly below 200ft with a relatively short flight endurance. A denial of service attack can be launched on such small drones given that the adversary can access the flight controller parameters and therefore is able to disrupt the UAV system. In other words, such an attacker is able to manipulate the flight control commands including the shutdown command which can be illegitimately invoked while the drone is in operation. Moreover, because some models of this category of drones are relatively small, they encompass moderately powered processors. Accordingly, flooding their network cards with random commands via the data link can force such drones to go into an unexpected state and possibly halt their operation.

- GCS Control Signals Spoofing. Injecting false wireless control commands using the data link can be accomplished by a man in the middle attack. During this attack, the adversary blocks the legitimate communication between the UAV and the ground control station, and begins commanding the drone herself. A covert wireless injection is also possible if the adversary acts in both directions to trick both the drone and the ground control into believing they are communicating with each other. In other words, the attacker intercepts the genuine commands generated by the ground control station, sends her desired instructions to the drone, and then communicates the expected responses to the ground control. Confidentiality, integrity and authentication mechanisms can be used to mitigate such attacks but they are not usually implemented in mini UAVs as has been shown in [Deligne 2012]. Also, since the GCS is usually stationary, location-based authentication [Denning and MacDoran 1996] can be used by the drone to determine the origin of the received control signals, and accordingly, possibly detect spoofed signals.

Software such as SkyJack [Crook 2013] can be installed on a malicious drone that takes a predator role to take control of civilian WiFi operated drones. In this case, the predator drone flies setting its WiFi card on monitor mode and sniffs for wireless communications between drones and their operators by scanning for certain MAC addresses published by specific drone companies. Then, SkyJack forcefully deauthenticates the operators from their perspective drones and finally authenticates itself as a new operator for the drone, thus having the drone under its control. The SkyJack software has been updated by adding a malicious firewall feature so that the original operator cannot regain control of its own drone.

4.2. Physical Challenges and Vulnerabilities

Civilian drones and particularly if operating within the perimeter of metropolitan areas are expected to fly at a low altitude. Other than the cyber attacks investigated above, such drones are vulnerable to a multitude of physical threats that can complicate their operation and further prevent the accomplishment of their missions. This section presents some of the possible physical threats that face the integration of civilian UAVs in the low altitude airspace.

- Theft and Vandalism. Drones flying at a visual distance are attractive targets for vandalism and theft which can be accomplished using various methods that vary from using a simple dart gun to an anti-drone rifle [Hodgkins 2015]. Specifically, anti-drone rifles are being used by the police for catching snoopy drones, and are likely to be available to regular civilians in the near future. Such rifles are designed to disable drones within a distance of 1300ft, without damaging them, using radio pulses which disrupt the data link communication and in turns force the drone to execute the fail-safe protocol which makes the drone hover near the ground as it prepares to land. Another technique that can be used to sabotage drones is to infect them with a software virus such as Maldrone [Paganini 2015a]. On the other hand, to protect the delivered goods from being stolen, the legitimate recipient can authenticate herself to the drone using information supplied by the operating company through an auxiliary channel (e.g., through the use of Short Message Service (SMS)) so that the drone can release the delivered parcel. Such a mechanism does not prevent a determined thief from stealing the whole drone but we argue that, since the goods being delivered are lighter and easier to hide, they will be more attractive targets in this context.

A different approach for grounding drones is the adoption of hostile drones. Such a drone acts as a predator UAV which can be built by attaching a fishing net to it to physically catch other drones. This approach has been demonstrated by the Japanese police to catch drones in response to the incident where a drone carrying a small amount of radioactive sand was landed on the roof of the Japanese prime minister's home. An electronic immobilizer can also be used to reduce the attractiveness of stealing drones. Such an immobilizer should only allow the starting of the drone engine when it is physically present at or near the GCS. While the idea is adopted in cars using ignition keys or key fobs, the drone immobilizer can rely on location-based information broadcasted by their respective GCSs to activate the aircraft. Accordingly, stolen drones shall remain useless to novice adversaries.

- Weather and Civic Challenges. Deploying a fleet of mini drones for the purpose of delivery of goods requires that these drones overcome a number of physical challenges. Different weather conditions and the drone's ability to maneuver and navigate itself through different kinds of objects are important examples of such challenges. The effect of weather conditions on a drone is similar to that on a manned aircraft as it depends on the size, design, and power of the aircraft. The effect of some weather conditions depends on the flight time that the drone is going to endure in such conditions. As with manned aircraft, harsh weather conditions such as thunderstorms, turbulence, or freezing rain can be a critical factor during flights and may ultimately cause accidents. Mini drones are more vulnerable to such conditions including extremely low or high temperatures. Parcelcopters are light weight and moderately powered drones which suggests that they are going to be exceptionally vulnerable to crashes. Also, such weather conditions can be detrimental to cyber performance which can be manifested in GPS outage or lost link state. Examples of weather related incidents in strategic drones include the loss of a *Predator* UAV in Afghanistan due to an ice storm and the loss of NASA's Helios experimental UAV due to air turbulence [NASA 2013].

Another challenge facing civilian drones is their need to avoid colliding with different civic constituents such as trees, electric cables, and buildings. Such drones must possess a minimum level of situational awareness and artificial intelligence (AI) capabilities in order to deal with different situations. For example, it is reasonable to think that a firefighting drone might get entangled in heavy tree bushes while attempting its operation procedures. However, approaches that enable the drone to free itself from this situation remain unclear.

- Friendly Drones Collision. Having multiple fleets with many drones belonging to the same fleet operating together at the same time can certainly raise the chances of friendly unintentional collisions. Sense and avoid mechanisms [Angelov 2012] must be enforced among UAVs flying at low altitude within the national airspace. However, such mechanisms alone do not necessarily imply collision avoidance. In fact, they might be abused to launch a denial of service attack by flying another drone close by and forcing the parcelcopter to go in loops until its battery is drained. For that reason, a complementary inter-drone communication protocol is essential between friendly drones in order to better determine the best course to follow in such scenarios. Also, in addition to the (ADS-B)-like system, adopting mechanisms similar to manned aircraft where most midair collisions are mitigated by relying on onboard navigational systems, such as Traffic Collision Avoidance System (TCAS) transceiver can be beneficial. TCAS communicates with corresponding transceivers from neighboring aircraft and warns pilots of their presence when they pose a threat of midair collision.

Other threats include software or hardware malfunctioning which can affect any component of the UAV system. Faulty sensor readings can be endured by adopting a fault-tolerant control system which allows the degradation of control by adopting fewer sensor configurations to achieve the desired functionality [Zhai et al. 2010]. Based on the possible cyber threats and physical vulnerabilities, in what follows, we identify the security properties required from a UAV system and give a brief outline of a security architecture that provides various security services to meet the overall security requirements.

4.3. Security Requirements

In this section, we provide the security features required from a UAV system in order to protect the confidentiality and integrity of its acquired and communicated information, and to ensure its ability to adhere to its operational requirements. Securing the information of the system refers to protecting it from disclosure, disruption, modification, and destruction. According to the FAA [George 2015], security requirements can be derived based on the perspective of the stakeholders which include the FAA, agencies for national security, aviation authorities, UAV operators and manufacturers, users of the national airspace, society, and privacy advocates.

For a secure UAV operation, we identify the following security requirements:

- **Authorized access**: The UAV system must provide means to ensure that only authorized operators are granted access to its resources including both the ground control station and the aircraft. More precisely, authentication mechanisms and mandatory access control policies must be implemented to mitigate unauthorized personnel from accessing the GCS and consequently commanding the vehicle in a malicious manner. Also, continuous mutual authentication between the operator and the UAV is essential during their communication. Authentication mechanisms may incorporate operation specific distance bounding protocols [Boureanu et al. 2014] to further authenticate the distance between the communicating entities. Such measure can reduce the success of spoofing attacks where the spoofer is unlikely to be at close proximity to the impersonated party.

- **Availability**: All the elements of the UAV system should be guaranteed to perform their required functions under defined spatial and temporal circumstances such that the system sustains its availability without disruption during its operational period. For instance, the UAV must adopt measures such as anomaly-based intrusion detection systems [Han et al. 2014] to distinguish normal communications from those resulting from denial of service attacks. Additionally, the utilization of alternative operational procedures such as using different set of sensors to crosscheck readings can allow the flight control system to tolerate specific components malfunctioning or alteration. Also, managing the patching and updating processes in a way that does not compromise the availability of the UAV system during its operation is of paramount importance.
- **Information confidentiality**: the UAV system should employ mechanisms to mitigate unauthorized disclosure of the telemetric and control information. Different encryption standards such as AES [Daemen and Rijmen 2013] can be used for encryption of the data link.
- **Information integrity**: the UAV system should be able to ensure that the telemetric information, and the GPS and control signals are genuine and have not been intentionally or unintentionally altered. Authenticated encryption cryptographic primitives may be used to ensure both the integrity and confidentiality of such information.
- **System integrity**: the UAV system should be able to guarantee the authenticity of its software and hardware components. Techniques from trusted computing such as memory curtaining, sealed storage, and remote attestation can be used to ensure the authenticity of the system's firmware and sensitive data [Dietrich and Winter 2009]. The deployment of intrusion detection system, anti virus software, firewall, and strict policies regarding the use of external storage media can aid in the detection and prevention of malware. Also, regular side-channel analysis, including timing and power analysis, may be used for the detection of the activation of hardware trojans [Tehranipoor and Koushanfar 2010] because such trojans usually alter the system's parametric characteristics such as its expected performance and power consumption.
- **Accountability of actions**: the UAV system should employ mechanisms that enforce non-repudiation to ensure that operators are held responsible for their actions. Digital signature algorithms may be used to both authenticate the operators and to bind them to an issued action. Moreover, logging procedures which are used to chronologically track the sequence of actions and changes in the system should be implemented.

Figure 3 summarizes the identified security threats against UAVs, the corresponding violated security properties, and possible mitigation techniques.

A UAV distributed security architecture [Wolf 2009] is a structured collaboration between sets of security services implemented on various components of the UAV system to provide the overall security functionality. These services defend against and detect identified and previously unknown threats. Such architecture categorizes security services based on how they are implemented or what components of the UAV system they protect such that when these services are utilized, they enable the UAV system to meet the overall security requirements. Inspired by [Brown et al. 2015], we present a three-layer architecture of security services which is depicted in Figure 4. These services include software-based services, hardware-based services, and physical security services. The physical security services protect the physical operating components such as control modules, busses, and computer systems from intentional and accidental damage. These services include securely managing the UAV systems supply

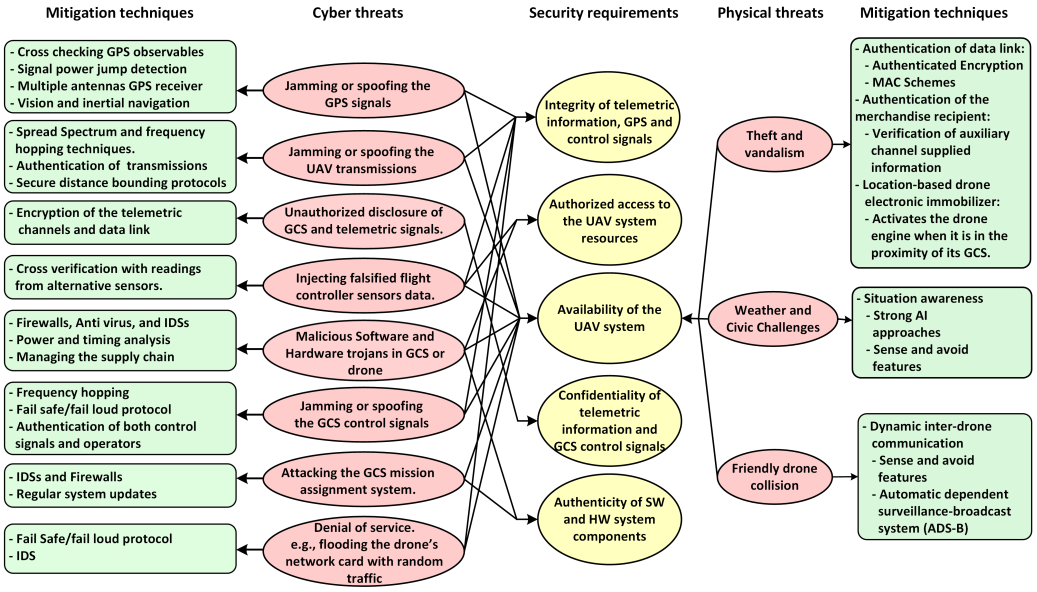

Fig. 3. Cyber and physical security threats against UAV systems. (IDS: Intrusion Detection System)

chain, using tamper-protected devices, and running trojan detection tests. Hardware-based security services are used to provide fast cryptographic performance and other efficient solutions to spoofing attacks such as the use of redundant or alternative set of sensors, and the utilization of GPS receivers with multiple antennas. Software-based solutions work on top of hardware solutions to provide a wide range of security services such as anti-malware, access authorization to the systems resources, software isolation for secure updates, firewall and intrusion detection systems, and defenses against the fabrication of sensors readings.

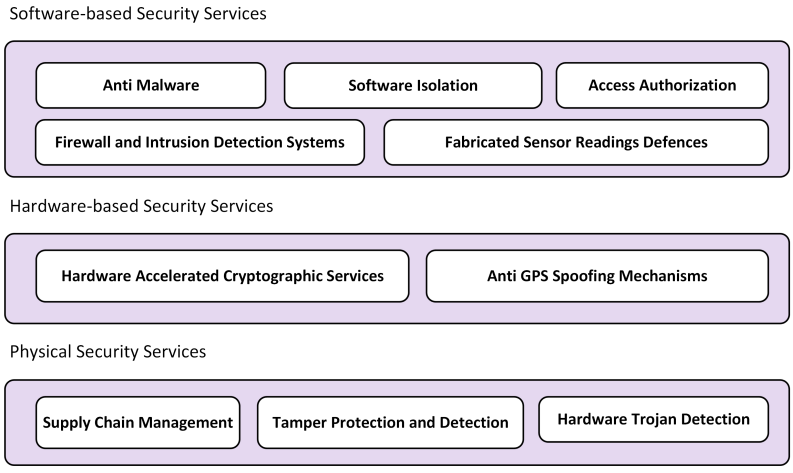

Fig. 4. Proposed security architecture for UAV systems.

It is crucial when adopting security solutions to investigate the effect of the solution implementation on the functionality and performance of the UAV system. Most of the identified security solutions implicitly assume that the processing and transfer of the secured information require no time. Accordingly, the dynamics of the adopted security mechanism are assumed to have no effect on the behavior of the UAV system. However, computation and communication introduce delays, consequently, it is important to investigate the effect of adopting different security models on the real time constraints required for the safe functionality of the UAV system.

The impact of implementing various security features such as the effect of adding cryptographic primitives on the performance of civilian drones is not well documented in the literature. However, one can expect that slight delays associated with encryption can be tolerated by the UAV system because the civilian operation environment is not as critical as the military environment. As indicated in an unclassified report published by the Dutch ministry of defense (cf. Table 4 in [de Vries 2005]), encryption constitutes only 0.24% of the maximum allowable delay [Kim et al. 2003] to maintain a stable control of the UAV system. Also, unlike resource constrained systems such as those that employ RFID technology, and nano and micro drones, civilian drones which are covered by this survey can accommodate cryptographic algorithms that require reasonable chip area, computational, and memory requirements.

Practically, the cryptographic primitives required for establishing secure channels between the UAV and GCS include symmetric block or stream ciphers, hash functions, and message authentication codes (MACs), all of which are very fast and are often hardware accelerated. Also, symmetric ciphers and hash functions have almost no overhead on the communication bandwidth. More precisely, for symmetric ciphers, the ciphertext size is equal to the plaintext size, and hash functions compress the input message to a fixed size output which usual varies between 128 to 512 bits, so unless the input message size is less than that of the hash function's output, there is no communication overhead. MACs generate fixed size tags (usually between 128 to 512 bits in size) which are transmitted along with the authenticated messages, and the overhead of the tag is inversely proportional to the size of the authenticated message. Establishing secure channels also requires public key infrastructure where elliptic curve cryptography (ECC) solutions can be used instead of RSA because they work with shorter keys and hence, for the same security level, they require less computation for key generation and signature operations. While public key cryptography is characterized by its slow running time, it is often used during the initial session setup stage and infrequently afterwards which suggests its limited overhead on the communication bandwidth. Cryptographic performance benchmarks of various processors are available in [Bench.crypto 2016]. For example, one of the most popular civilian drones is Parrot's AR Drone 2.0 which runs a 1 GHz 32-bit ARM cortex A8 processor and has a 1 GB DDR2 Ram. Encrypting long messages on this ARM CPU using AES-128 operating in cipher block chaining mode (CBC) has a throughput of 32702.46 KB/sec. Also, SHA1 compresses an average of 84317.03 KB/sec and for ECDSA signature scheme, using the standard NIST B-163 elliptic curve, generating a key pair, signing, and signature verification requires an average of 3.6138 msec, 3.775.4 msec, and 7.2332 msec, respectively [Bench.crypto 2016]. Although it is not used as frequent as symmetric key algorithms during communications, public key algorithms are computationally expensive and would introduce substantial delays that may be unacceptable to safely control the drone. Accordingly, it is important that a dedicated cryptoprocessor is utilized to carry out such computationally expensive operations. It should also be noted that parcelcopters and other task specific drones are expected to be equipped with more advanced processors where if cryptographic primitives are implemented efficiently, they would have minimal impact on their resource requirements. However, the expected im-

pact on the performance and functionality of the drone is dependent on the criticality of the mission and the tolerability of the UAV control system.

5. PRIVACY ISSUES RELATED TO CIVILIAN DRONES

An important concern about civilian drones is the ease of their use in violating personal privacy and the difficulty of capturing the intruding ones. UAVs possess a unique range of agile access techniques which distinguish them from other privacy infiltrating devices. In fact, currently, drones with high precision cameras can be remotely controlled to perform surveillance tasks with better accuracy and maneuverability than mounting static cameras. The use of drones in surveillance has been acknowledged by the FBI director Robert Mueller in 2013 [Cratty 2013]. An FBI issued report stated that the agency has no knowledge about any guidelines related to using drones in surveillance and that they try to keep their use to a minimum. The Fourth Amendment of the U.S. Constitution is consistent in protecting the privacy of people. However, it does not define precisely the scope of such privacy [Legal Information Institute 2016].

5.1. Drones and the Harvesting of Information and Resources

Building a profile of a person's behavior and preferences can be a profitable business as it is hugely valuable to marketers. One can often notice this concept on the web in the form of targeted advertisement based on individual browsing history. Despite being unconsciously tolerated by many, such monitoring in the real world is unlikely to be tolerated. Drones are certainly going to be deployed to gather data about our lifestyles and interests as a part of the physical targeted market scan. With the added feature of visual evidence, the information gathered by drones is expected to be more valuable to marketing entities than that collected online by a botnet [Rosen 2013]. In fact, given that both online and physical behaviors are concurrently watched without people even noticing, one can expect that a nearly complete picture of a person's movements, social circle, and preferences can be reconstructed. In what follows, we give examples of drones used maliciously to harvest information and resources.

- *Snoopy*. Malicious software [Gittleson 2014] that can be installed on a drone to harvest personal information, and to track and profile individuals using wireless localization of their WiFi enabled smart phones. Snoopy can also sniff Radio Frequency Identification (RFID), Bluetooth, and IEEE 802.15. A Snoopy equipped drone exploits the WiFi feature of smart phones that makes them always looking for a network to join including previously known networks. The software first picks a given signal emitted by the victim's phone and identifies a network that is already known and trusted by the device. Then, Snoopy impersonates the identified network to trick the smart phone into joining it. After this, Snoopy can collect all the information entered while on this disguised network including the MAC address of the smart phone which can be used to later track the phone in real time.
- *SkyNet*. A stealth network [Reed et al. 2011] that uses drones to forcefully recruit and command host computers for a botmaster. The drones are used to scan a given area and compromise home WiFi networks and eventually the connected computers. Afterwards, the drones are regularly used to issue the botmaster's commands for the compromised computers. SkyNet exploits the weak security nature of personal networks which are considered the most unsecured networks on the Internet. Such networks usually include unpatched machines, and also they do not implement auditing features and are known for their poor wireless security and bad password choices. Once the home computers are compromised, the botmaster can access personal files and acquire sensitive account credentials. SkyNet toughens the botnet through bypassing the use of the Internet for communicating with the host bots,

thus avoiding known security mechanisms such as firewalls and intrusion detection systems.

- *IoT drone*: In [Paganini 2015b], a drone that can communicate with smart devices [Won et al. 2015], including smart appliances and smart lighting, using ZigBee on the Internet of Things (IoT) is proposed. The drone is stocked with multiple ZigBee radios for interacting with devices using the same protocol. IoT drone is also equipped with a GPS functionality to determine the location of each device. The drone is fully autonomous and operates by capturing and recording the locations and information of all smart devices within a range of 330ft. The collection of information about the type and possibly usage status of devices in individuals' homes can be used to predict their living standards and the times where they are out of their homes. Such information does not only violate the privacy of the affected persons but also can be used for theft and vandalism purposes.

5.2. Defense Approaches Against Intruding Drones

As a response for the malicious use of drones for surveillance, information and resource harvesting, several proposals and products have emerged to defend against the presence of drones in a given airspace. Most of the techniques used to steal or damage drones (discussed in section 4) can also be used for protection against them. In what follows, we provide an overview of other proposals that offer a more forgiving solution.

- *Access policies*: Currently, some drone manufacturers include a list of no fly GPS coordinates that cover sensitive areas such as airports, stadiums, and government facilities. New entries to this no fly list are included in the drone's mandatory firmware update. Also, regular individuals can register their home address in the NoFlyZone database [NoFlyZone 2016], which is used by various drone manufacturers as a source for their no fly lists. Similarly, in [Vaidya and Sherr 2015], a location access-control framework is proposed, which allows individuals to determine rules regarding the operation of drones in their specified geographical areas. For example, homeowners can specify the desired access policy for their controlled airspace including keep away distances for each day/time of the week. Their home wireless access point periodically broadcasts the chosen access policy using the home WiFi as a beacon. Passing drones listen to policies from neighboring WiFi beacons and verifies that its location and the rest of its route does not violate the advertised access policies. However, there is no definite way to ensure that obeying this policy can be enforced and that all drones will be programmed to apply it. Furthermore, intruders are unlikely to buy such privacy abiding drones.
- *Drone tracking*: Techniques that fall under this category aim to detect and possibly track drones within a given perimeter, and then alert the owner of the tracking system. Systems such as Nippon Electric Company (NEC) surveillance system [Williams 2015] employ a combination of different acoustic and thermal sensors, infrared cameras, and radio communication detectors to sense the presence of an intruding drone by either its sound, shape, or communication with its operator. Once identified, triangulation is used to determine the location of the drone and further actions, such as dropping or acquiring the drone, are determined by the owner of the tracking system.

6. FUTURE RESEARCH DIRECTIONS

With all the security, safety, and privacy risks associated with deploying civilian drones in the national airspace, a comprehensive solution that integrates important features for their safe operation is required. Some of these solutions are proposed in the literature such as privacy preserving and collision avoidance approaches. However, because

the field of cyber-physical security in civilian UAVs is relatively new as the security community is just starting to identify its emerging threat spectrum, some areas are left untouched or barely looked at. For example, a promising research direction is to venture the application of formal verification techniques on the adopted security solutions so that engineers can formally prove that they satisfy the identified security requirements simultaneously and at the same time do not compromise any of the UAV's safety measures. In what follows, we identify some challenging areas in the hope of having our discussion serve as first steps for possible research avenues.

6.1. UAV Forensic Investigations

For UAVs, security incidents include invasion of privacy, flying over controlled airspace, crashing and consequently damaging property and possibly injuring or killing people. Trying to catch the operator of an unregistered violating drone is nearly impossible, if the drone was not physically caught, due to the lack of evidence. Even if one catches a crashing unregistered drone, the process of extracting evidence from the aircraft that can lead to its operator is not clear. Particularly, because while drones encompass a multitude of sensors for different events, not all of them carry logging capabilities. In some drones, the captured sensor values are transfered to the ground control station where logs can be kept. Additionally, the main part of data related to the flight course is likely to reside in a random access memory which makes it very hard to recover once power has been shut off. Accordingly, reconstructing the actions of the drone before it crashed, probing the sensors for their captured events and the GPS for locations remains an essentially open problem.One can predict that civilian drones will be equipped with event data recorders that record a wide variety of information about the drone's subsystems and flight course which can be used for diagnostic purposes. However, the protection of the authenticity and integrity of the recorded and stored data is not a simple task and may be considered an open problem as well. Additionally, the adoption of electronic license plates which wirelessly broadcast drone identification information can be used so that law enforcement representatives can remotely extract such information from violating drones. Also, to uniquely identify drones, device fingerprinting using wireless communication where persistent device features are used to generate device-specific signatures [Xu et al. 2016] can be employed. Device fingerprinting can also be used for authenticating drones to their respective GCSs.

Previous work in the area of forensic investigation includes a practical implementation of an investigative tool by David Kovar [Kovar 2015] that was used to retrieve partial GPS coordinates and the purchase account information from the configuration file of a DJI Phantom 2 quadcopter. During this analysis, the launch location of the drone and the shipping address used when the drone was bought from the manufacturer were identified. Another demonstration has been shown by Graeme Horsman [Horsman 2016], where the challenges of evidence extraction were identified and an analysis of the onboard flight data and ground controllers was presented.

6.2. Intrusion Detection

An intrusion detection system (IDS) is deployed to monitor the incoming communication and perform some intelligent analysis based on either anomaly or signature identification. An anomaly-based IDS contrasts the protected system behavior against an established pattern for the normal behavior of the system. Such a pattern is often constructed by the IDS during a training phase. On the contrary, a signature-based IDS identifies malicious behavior if a known threat signature is stored in its database. In computer systems, the two types of IDSs are usually deployed for intrusion detection due to the fact that each of them detects different forms of intrusion. In UAVs, intrusion detection should be an integral part of the AI approach embedded in the flight

controller. Indeed, cyber attacks, especially those aiming for hostile takeover [Dulo 2015], would definitely cause the aircraft to deviate unexpectedly from its intended behavior. Upon the detection of such unexpected behavior, a drone under attack should follow a fail-loud strategy where it alerts the operator with the intrusion using an auxiliary channel in the case that its communication may be jammed. Also, the majority of external communication should be shut down including the GPS, and autonomous navigation may rely on other sensors. An example of a non-GPS relying navigation systems has been proposed by Wu *et al.* [Wu et al. 2013] where a vision-aided inertial navigation system employing vision sensors and measurements from the aircraft's inertial measurement unit are used to bound how far and in which direction the drone has drifted from the last known location.

There are only a few works covering the area of intrusion detection in UAVs. Existing proposals include the work done by Mitchell and Chen [Mitchell and Chen 2014] which provides the details of an adaptive IDS that detects deviations with various degrees from a set of seven specified behavioral rules. Another IDS has been presented by Birnbaum *et al.* [Birnbaum et al. 2014] where they proposed a system that monitors both the avionics and flight controller, and using the recursive least squares method, the IDS is able to estimate immediate values of the system parameters and detect deviations from their expected values. Birnbaum *et al.* [Birnbaum et al. 2015] proposed an IDS, based on behavior profiling, that is capable of alerting the operator of unplanned flight deviations which may indicate either a cyber attack, spoofed sensor, or malfunctioning.

6.3. Drone Fleet Communication

Avoiding midair collisions among friendly drones is essential for guaranteeing the safe operation of civilian UAVs in the national airspace. In addition to the adaptation of ADS-B and TCAS systems for drones, inter-drone communication is even more beneficial for the safe operation as it enforces collaboration among UAVs. While combat drones have the ability to communicate sensor parameters and video feeds among each other, the technology is not deployed among mini drones. For modeling a fleet of friendly drones that need to communicate when they encounter each other, a Flying Ad hoc Network (FANET) model is proposed in [Bekmezci et al. 2013; Lilien et al. 2014]. Due to the highly dynamic and mobile nature of the UAVs operation, FANETs suffer from frequent inter-node link outages and traffic loss. Also, FANETs are highly susceptible to many attacks that target ad hoc networks. Therefore, efficient methods for establishing secure communications between drones within a fleet remains an open problem.

According to Amazon's proposal, parcelcopters are going to be operated below 400ft which is an uncontrolled part of the national airspace. However, an air traffic control system may be deployed once multiple fleets occupy this part of the airspace. A communication protocol similar to the Internet-Protocol-based Aeronautical Telecommunication Network (IP ATN) protocol may be required (IP ATN is utilized in the civil aviation system to communicate voice and text between pilots, air traffic controllers, and airlines for status updates [Sampigethaya et al. 2011]). To this end, we argue that there is an urgent need for standards that support secure drone communication, otherwise, we will end up with numerous incompatible devices with proprietary technologies that may not be able to securely communicate with each other.

Figure 5 summarizes the proposed research directions and the corresponding approaches that are presented in the literature and identified in our survey.

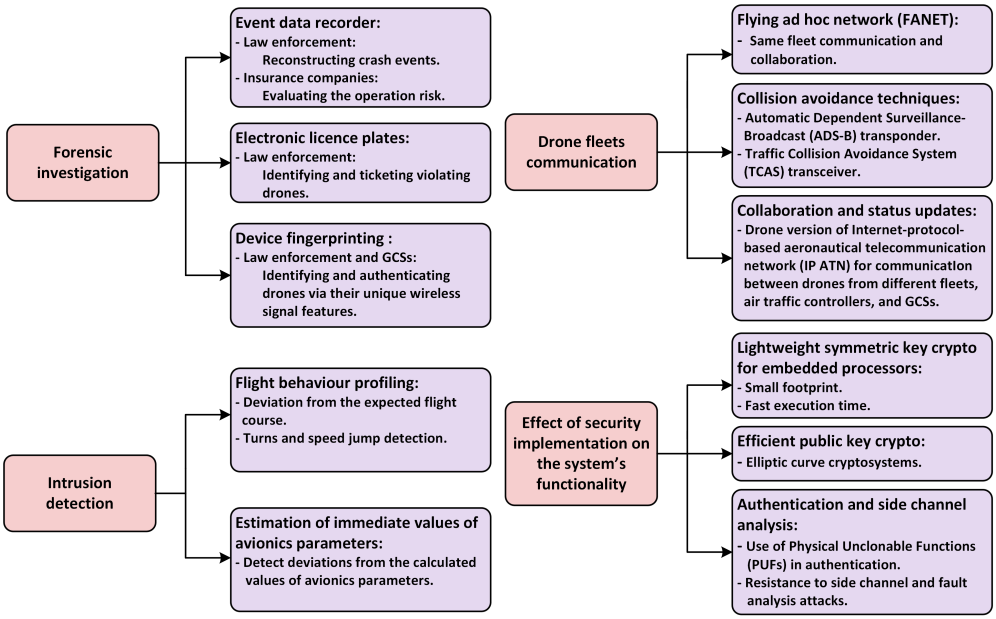

Fig. 5. UAV security, privacy and safety research directions and their existing and proposed approaches

7. CONCLUSION

The integration of civilian UAVs into the national airspace is approaching fast. However, prior to having these aerial machines flying above us, certain security, safety and privacy measures should be enforced. In this paper, we presented a survey that identifies the various security, safety and privacy aspects of civilian drone operation. We particularly identified the UAV system properties required for its secure operation. Also, we have classified the possible cyber attacks according to its targeted UAV components. Moreover, we pinpointed the physical threats associated with the use of drones to perform civilian tasks. Furthermore, we investigated the possible consequences of using drones on the privacy of humans. Finally, we identified possible research directions and discussed the work that has been proposed in each area.

REFERENCES

Michal Addady. 2015. The number of drones expected to sell during the holiday seasons is caring the government. (2015). http://fortune.com/2015/09/29/drones-holiday-sales/

Riham AlTawy and Amr M Youssef. 2016. Security Tradeoffs in Cyber Physical Systems: A Case Study Survey on Implantable Medical Devices. *IEEE Access* 4 (2016), 959–979.

Shankar Sastry Alvaro A. Cardenas, Saurabh Amin. 2008. Secure control: towards survivable cyber-physical systems. In *The 28th International Conference on Distributed Computing Systems Workshops*. 495–500.

Amazon. 2015. Amazon revising the airspace model for the safe integration of small Unmanned Aircraft Systems. (2015). http://utm.arc.nasa.gov/docs/Amazon_RevisingtheAirspaceModelfortheSafeIntegrationofUAS[6].pdf

Plamen Angelov. 2012. *Sense and avoid in UAS: research and applications*. John Wiley & Sons.

Ilker Bekmezci, Ozgur Koray Sahingoz, and Şamil Temel. 2013. Flying ad-hoc networks (FANETs): A survey. *Ad Hoc Networks* 11, 3 (2013), 1254–1270.

Mihir Bellare and Chanathip Namprempre. 2000. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. In *Advances in Cryptology-ASIACRYPT*, Tatsuaki Okamoto (Ed.), Vol. 1976. Springer, 531–545.

Bench.crypto. 2016. Computers used for benchmarking cryptographic systems. (2016). https://bench.cr.yp.to/computers.html

Brett Bethke, Mario Valenti, and Jonathan P How. 2008. UAV task assignment. *IEEE Robotics & Automation Magazine* 15, 1 (2008), 39–44.

Zachary Birnbaum, Andrey Dolgikh, Victor Skormin, Edward O'Brien, and Dirk Muller. 2014. Unmanned Aerial Vehicle security using recursive parameter estimation. In *the International Conference on Unmanned Aircraft Systems*. IEEE, 692–702.

Zachary Birnbaum, Andrey Dolgikh, Victor Skormin, Edward O'Brien, Daniel Muller, and Christina Stracquodaine. 2015. Unmanned Aerial Vehicle security using behavioral profiling. In *International Conference on Unmanned Aircraft Systems*. 1310–1319.

Ioana Boureanu, Aikaterini Mitrokotsa, and Serge Vaudenay. 2014. Towards Secure Distance Bounding. In *Fast Software Encryption (Lecture Notes in Computer Science)*, Shiho Moriai (Ed.), Vol. 8424. Springer, 55–67.

Michael J Boyle. 2015. The Race for Drones. *Orbis* 59, 1 (2015), 76–94.

David A Brown, Geoffrey Cooper, Ian Gilvarry, Anand Rajan, Alan Tatourian, Ramnath Venugopalan, David Wheeler, and Meiyuan Zhao. 2015. Automotive security best practices. (2015). www.mcafee.com/ca/resources/white.../wp-automotive-security.pdf

Guowei Cai, Jorge Dias, and Lakmal Seneviratne. 2014. A survey of small-scale Unmanned Aerial Vehicles: Recent advances and future development trends. *Unmanned Systems* 2, 02 (2014), 175–199.

Silvia Gil Casals, Philippe Owezarski, and Gilles Descargues. 2013. Generic and autonomous system for airborne networks cyber-threat detection. In *IEEE/AIAA 32nd Digital Avionics Systems Conference*. 4A4–1–4A4–14.

Rohan Chabukswar. 2014. Secure Detection in Cyberphysical Control Systems. (2014).

Laurent Ciarletta, Loïc Fejoz, Adrien Guenard, and Nicolas Navet. 2016. Development of a safe CPS component: the hybrid parachute, a remote termination add-on improving safety of UAS. In *Embedded Real-Time Software and Systems*. (to appear).

Roger Clarke. 2014. Understanding the drone epidemic. *Computer Law & Security Review* 30, 3 (2014), 230–246.

Chris Constantinides and Paul Parkinson. 2008. Security challenges in UAV development. In *IEEE/AIAA Digital Avionics Systems Conference*. IEEE, 1–C.

Carol Cratty. 2013. FBI uses drones for surveillance in U.S. (2013). http://www.cnn.com/2013/06/19/politics/fbi-drones/

Jordan Crook. 2013. Infamous hacker creates SkyJack to hunt, hack, and control otherdrones. (2013). http://techcrunch.com/2013/12/04/infamous-hacker-creates-skyjack-to-hunt-hack-and-control-other-drones/

Joan Daemen and Vincent Rijmen. 2013. *The design of Rijndael: AES - the Advanced Encryption Standard*. Springer Science & Business Media.

Sacco de Vries. 2005. UAV and Control Delays. (2005). http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA454251

Eddy Deligne. 2012. ARDrone corruption. *Journal of Computer Virology* 8, 1-2 (2012), 15–27.

Dorothy E Denning and Peter F MacDoran. 1996. Location-based authentication: Grounding cyberspace for better security. *Computer Fraud & Security* 1996, 2 (1996), 12–16.

Kurt Dietrich and Johannes Winter. 2009. Implementation aspects of mobile and embedded trusted computing. In *proceedings of Trusted Computing*, Liqun Chen, Chris J. Mitchell, and Andrew Martin (Eds.). Springer, 29–44.

Donna A Dulo. 2015. Unmanned aircraft: the rising risk of hostile takeover. *IEEE Technology and Society Magazine* 34, 3 (2015), 17–19.

Noam Eshel. 2015. A mini UAV becomes a suicide drone. (2015). http://aviationweek.com/paris-air-show-2015/mini-uav-becomes-suicide-drone-0

FAA.gov. 2015. Next Generation Air Transportation System (NextGen). (2015). https://www.faa.gov/nextgen/

FAA.gov. 2016. FAA special airworthiness certificate. (2016). https://www.faa.gov/aircraft/air_cert/airworthiness_certification/sp_awcert/

Michelle S Faughnan, Brian J Hourican, G Collins MacDonald, Megha Srivastava, JA Wright, Yacov Y Haimes, Eva Andrijcic, Zhenyu Guo, and James C White. 2013. Risk analysis of Unmanned Aerial Vehicle hijacking and methods of its detection. In *IEEE Systems and Information Engineering Design Symposium*. IEEE, 145–150.

Stephen George. 2015. FAA Unmanned Aircraft Systems (UAS): cyber security initiatives. (2015). http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2015-02/2015-feb_george-ispab.pdf

Kim Gittleson. 2014. Data-stealing Snoopy drone unveiled at Black Hat - BBC News. (2014). http://www.bbc.com/news/technology-26762198

Song Han, Miao Xie, Hsiao-Hwa Chen, and Yun Ling. 2014. Intrusion detection in cyber-physical systems: techniques and challenges. *IEEE Systems Journal* 8, 4 (2014), 1049–1059.

Klaus Hartmann and Christoph Steup. 2013. The vulnerability of UAVs to cyber attacks-An approach to the risk assessment. In *the 5th International Conference on Cyber Conflict*. IEEE, 1–23.

Kelly Hodgkins. 2015. Anti-drone shoulder rifle lets police take control of UAVs with radio pulses. (2015). http://www.digitaltrends.com/cool-tech/battle-innovations-anti-drone-gun/

Graeme Horsman. 2016. Unmanned Aerial Vehicles: A preliminary analysis of forensic challenges. *Digital Investigation* 16 (2016), 1–11.

Andrew J Kerns, Daniel P Shepard, Jahshan A Bhatti, and Todd E Humphreys. 2014. Unmanned aircraft capture and control via GPS spoofing. *Journal of Field Robotics* 31, 4 (2014), 617–636.

Siddhartha Khaitan and James D. McCalley. 2015. Design Techniques and Applications of Cyberphysical Systems: A Survey. *IEEE Systems Journal* 9, 2 (June 2015), 350–365.

Dong-Sung Kim, Young Sam Lee, Wook Hyun Kwon, and Hong Seong Park. 2003. Maximum allowable delay bounds of networked control systems. *Control Engineering Practice* 11, 11 (2003), 1301–1313.

David Kovar. 2015. Forensic analysis of sUAS (aka) drones. In *Digital Forensics and Incident Response Summit* (1ˆst ed.). https://files.sans.org/summit/Digital_Forensics_and_Incident_Response_Summit_2015/PDFs/ForensicAnalysisofsUASakaDronesDavidKovar.pdf

Tomáš Krajník, Vojtěch Vonásek, Daniel Fišer, and Jan Faigl. 2011. AR-drone as a platform for robotic research and education. In *Research and Education in Robotics-EUROBOT*. Springer, 172–186.

Legal Information Institute. 2016. Fourth Amendment. (2016). https://www.law.cornell.edu/wex/fourth_amendment

Leszek T Lilien, Lotfi Ben Othmane, Pelin Angin, Andrew DeCarlo, Raed M Salih, and Bharat Bhargava. 2014. A simulation study of ad hoc networking of UAVs with opportunistic resource utilization networks. *Journal of Network and Computer Applications* 38 (2014), 3–15.

Sharon Lozano. 2016. First steps toward drone traffic management. (2016). http://www.nasa.gov/feature/ames/first-steps-toward-drone-traffic-management

Katrina Mansfield, Timothy Eveleigh, Thomas H Holzer, and Shahryar Sarkani. 2013. Unmanned Aerial Vehicle smart device ground control station cyber security threat model. In *IEEE International Conference on Technologies for Homeland Security*. IEEE, 722–728.

Douglas M Marshall, Richard K Barnhart, Eric Shappee, and Michael Thomas Most. 2015. *Introduction to Unmanned Aircraft Systems*. CRC Press.

Donald McCallie, Jonathan Butts, and Robert Mills. 2011. Security analysis of the ADS-B implementation in the next generation air transportation system. *International Journal of Critical Infrastructure Protection* 4, 2 (2011), 78–87.

Nils Melzer. 2013. *Human Rights implications of the usage of drones and unmanned robots in warfare*. European Parliament's Subcommittee on Human Rights.

Alfred J. Menezes, Scott A. Vanstone, and Paul C. Van Oorschot. 1996. *Handbook of applied cryptography* (1st ed.). CRC Press, Inc., Boca Raton, FL, USA.

Robert Mitchell and Ray Chen. 2014. Adaptive intrusion detection of malicious Unmanned Air Vehicles using behavior rule specifications. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 44, 5 (2014), 593–604.

Yilin Mo and Bruno Sinopoli. 2010. False data injection attacks in control systems. In *First Workshop on Secure Control Systems*.

Fihri Mohammed, Ahmed Idries, Nader Mohamed, Jameela Al-Jaroodi, and Imad Jawhar. 2014. UAVs for smart cities: Opportunities and challenges. In *the international conference on Unmanned Aircraft Systems*. IEEE, 267–273.

Dieter Moormann. 2015. DHL Parcelcopter research flight campaign 2014 for emergency delivery of medication. In *ICAO RPAS Symposium*.

NASA. 2013. NASA - Helios. (2013). http://www.nasa.gov/centers/dryden/news/ResearchUpdate/Helios/

BBC News. 2014. Pentagon to use drones to create remote wi-fi hotspots. (2014). http://www.bbc.com/news/technology-27019389

NoFlyZone. 2016. NoFlyZone.org. (2016). https://www.noflyzone.org/about

Pierluigi Paganini. 2015a. A hacker developed Maldrone, the first malware for drones. (2015). http://securityaffairs.co/wordpress/32767/hacking/maldrone-malware-for-drones.html

Pierluigi Paganini. 2015b. ZigBee-sniffing drone used to map online Internet of Things. (2015). http://securityaffairs.co/wordpress/39143/security/drone-internet-of-things.html

Albert Rango, Andrea Laliberte, Caiti Steele, Jeffrey E Herrick, Brandon Bestelmeyer, Thomas Schmugge, Abigail Roanhorse, and Vince Jenkins. 2006. Using unmanned aerial vehicles for rangelands: current applications and future potentials. *Environmental Practice* 8, 03 (2006), 159–168.

Theodore Reed, Joseph Geis, and Sven Dietrich. 2011. SkyNET: A 3G-enabled mobile attack drone and stealth botmaster. In *Proceedings of the 5th USENIX conference on Offensive technologies*. 28–36.

J.E. Reich. 2015. Guards are battling contraband-smuggling drones at US prisons. (2015). http://www.techtimes.com/articles/104020/20151106/drones-prisons-guards.htm

Michael Robinson, Kevin Jones, and Helge Janicke. 2015. Cyber warfare: Issues and challenges. *Computers & Security* 49 (2015), 70–94.

Lea Rosen. 2013. Drones and the Digital Panopticon. *XRDS: Crossroads, The ACM magazine for students - scientific computing* 19, 3 (March 2013), 10–10.

Krishna Sampigethaya, Radha Poovendran, Sudhakar Shetty, Terry Davis, and Chuck Royalty. 2011. Future e-enabled aircraft communications and security: the next 20 years and beyond. *Proc. IEEE* 99, 11 (Nov 2011), 2040–2055.

Daniel P Shepard, Jahshan A Bhatti, Todd E Humphreys, and Aaron A Fansler. 2012. Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks. In *Proceedings of the Institute of Navigation GNSS Meeting*, Vol. 3.

Yunmok Son, Hocheol Shin, Dongkwan Kim, Youngseok Park, Juhwan Noh, Kibum Choi, Jungwoo Choi, Yongdae Kim, and others. 2015. Rocking drones with intentional sound noise on gyroscopic sensors. In *Proceedings of the 24th USENIX Conference on Security Symposium*. USENIX Association, 881–896.

Mohammad Tehranipoor and Farinaz Koushanfar. 2010. A survey of hardware trojan taxonomy and detection. *Design Test of Computers* 27, 1 (Jan 2010), 10–25.

TU Delft. 2014. TU Delft's ambulance drone drastically increases chances of survival of cardiac arrest patients. (2014). http://www.tudelft.nl/en/current/latest-news/article/detail/ambulance-drone-tu-delft-vergroot-overlevingskans-bij-hartstilstand-drastisch/

Tavish Vaidya and Micah Sherr. 2015. Mind Your (R,Φ)s: Location-Based Privacy Controls for Consumer Drones. In *Security Protocols XXIII (LNCS)*, Bruce Christianson, Petr Švenda, Vashek Matyáš, James Malcolm, Frank Stajano, and Jonathan Anderson (Eds.), Vol. 9379. Springer International Publishing, 80–90.

Nick Valencia and Michael Martinez. 2015. Drone carrying drugs crashes south of U.S. border. (2015). http://www.cnn.com/2015/01/22/world/drug-drone-crashes-us-mexico-border/

Peter VAN Blyenburgh. 2003. *Furthering the introduction of UAVs/ROA into civil managed airspace*. Technical Report. DTIC Document.

John Villasenor. 2014. Drones and the future of domestic aviation [Point of View]. *Proc. IEEE* 102, 3 (2014), 235–238.

Matthew Waller, Zachary Williams, Jason E Lueg, and Stephen A LeMay. 2008. Supply chain security: an overview and research agenda. *the International Journal of Logistics Management* 19, 2 (2008), 254–281.

Hengqing Wen, Peter Yih-Ru Huang, John Dyer, Andy Archinal, and John Fagan. 2005. Countermeasures for GPS signal spoofing. In *Proceedings of the Institute of Navigation GNSS Meeting*. 13–16.

Kyle Wesson and Todd Humphreys. 2013. Hacking drones. *Scientific American* 309, 5 (2013), 54–59.

Martyn Williams. 2015. NEC's surveillance system will detect, track drones. (2015). http://www.pcworld.com/article/2990525/necs-surveillance-system-will-detect-track-drones.html

Marko Wolf. 2009. *Security engineering for vehicular IT systems*. Vieweg+Teubner Research.

Jongho Won, Seung-Hyun Seo, and Elisa Bertino. 2015. A Secure Communication Protocol for Drones and Smart Objects. In *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*. ACM, 249–260.

Allen D Wu, Eric N Johnson, Michael Kaess, Frank Dellaert, and Girish Chowdhary. 2013. Autonomous flight in GPS-denied environments using monocular vision and inertial sensors. *Journal of Aerospace Information Systems* 10, 4 (2013), 172–186.

Qiang Xu, Rong Zheng, Walid Saad, and Zhu Han. 2016. Device fingerprinting in wireless networks: challenges and opportunities. *IEEE Communications Surveys Tutorials* 18, 1 (2016), 94–104.

Xiaohua Zhai, Jian'an Liu, Zhengzai Qian, and Gongcai Xin. 2010. Research on UAV degrade control system under sensor fault state. In *the 2nd WRI Global Congress on Intelligent Systems*, Vol. 2. IEEE, 20–23.