IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 3, 2021, accepted October 28, 2021, date of publication November 2, 2021, date of current version November 8, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3124996

A Survey of Cyberattack Countermeasures for Unmanned Aerial Vehicles

PENG-YONG KONG, (Senior Member, IEEE)
Electrical Engineering and Computer Science Department, Khalifa University, Abu Dhabi, United Arab Emirates
e-mail: pengyong.kong@ku.ac.ae

ABSTRACT Unmanned aerial vehicle (UAV) has been increasingly used in a wide range of commercial and civilian applications. As an advanced cyber-physical system, UAVs are exposed to a wide range of cyberattacks. This paper first surveys existing literature for different cyberattacks. Then, we classify these attacks based on their attack entry points, which can be radio channels, messages or on-board systems. There are six classes of UAV cyberattacks, namely channel jamming, message interception, message deletion, message injection, message spoofing and on-board system attack. In the existing literature, there is no survey focusing on UAV cyberattack countermeasures. To close this gap, we survey existing countermeasures for the six attack classes. A comprehensive review of countermeasures is important because countermeasure may not be exclusive to an attack. Knowing a wide range of existing countermeasures can prepare us against existing and new cyberattacks. We classify countermeasure into three classes, namely prevention, detection and mitigation. Prevention countermeasures stop a cyberattack from starting. When prevention countermeasures fail, detection countermeasures alert UAV operator of an attack. After detecting an attack, mitigation countermeasures limits the damage. Following the survey, we further discuss the open challenges in developing countermeasures and propose some potential future research works.

INDEX TERMS Cybersecurity, cyberattack, countermeasure, unmanned aerial vehicle, UAV, drone.

I. INTRODUCTION

An unmanned aerial vehicle (UAV) is an aircraft without any human pilot, crew or passenger on-board. As such, UAVs are technically robots that can fly autonomously or must be controlled remotely by a human operator. UAVs have been invented originally for military purposes [1], such as practicing anti-aircraft strategies, gathering intelligence, killing enemies, destroying hostile targets, etc. With rapid technology advancement in the past two to three decades, the use of UAVs has been extended beyond military, to many civilian and commercial applications. In Germany, the logistic company DHL has used UAVs to deliver medicine twice a day to the car-free island of Juist over a 12 km distance. Since 2017, Amazon Air Prime has used UAVs to pickup and deliver packages. In 2019, Google's parent company, Alphabet has received from the United State Federal Aviation Administration an approval, to deliver food using UAVs.

In addition to package and food delivery, UAVs are used in wildlife monitoring, disaster response, search and rescue operation, ambulance service, public surveillance, traffic monitoring, firefighting, journalism, panoramic photography, aerial videography, etc. There is an increasing interest in using UAVs as mobile base stations and relays that can be rapidly deployed to improve service coverage and quality for wireless communication networks [2]–[4]. The combination of UAVs and internet of things (IoT) technology has created numerous innovative use cases [5]. For example, working with IoT sensors on the ground, UAVs can help agricultural companies in surveying land and crops, energy companies in monitoring power lines and operational equipment, as well as insurance companies in inspecting properties and assets.

The widespread adoption of UAVs is probably due to their reasonable cost, ease of maneuver, simple maintenance, flexibility of flight route, and ability to serve hard-to-reach locations. A comprehensive survey has been presented in [6], highlighting a rich set of UAV civilian applications and related technical challenges. All the popular applications demand that each UAV be a highly sensor-driven cyber-physical system. Such system consists of firmware and software components, capable of performing advanced communication and computation functions to acquire, transmit and process sensor data. As presented in [7]–[9], the increasing popularity has attracted much attention to

The associate editor coordinating the review of this manuscript and approving it for publication was Jiankang Zhang.

UAV cybersecurity issues. Cybersecurity is a major concern because UAVs may handle critical data with serious security implication and UAVs communicate through wireless channels which are not secure by default [10].

In the context of cybersecurity, we need to ensure confidentiality, integrity and authenticity of information handled by UAVs. In addition, we must ensure availability of service used by or offered by UAVs. Such availability of service, when combined with confidentiality, integrity and authenticity of information, are collectively called the UAV cybersecurity requirements. Cybersecurity threats, risks and vulnerabilities are terms which are often used to refer to weaknesses in the firmware, software and wireless communication channels, that may result in a UAV's failures in satisfying the cybersecurity requirements. Cybersecurity weaknesses are located on an attack surface, which include all potential entry points for a cyberattack. Cyberattacks are malicious acts of exploiting the weaknesses to cause failures in fulfilling the cybersecurity requirements. For simplicity, we use the terms "cyberattack" and "attack" interchangeably hereafter in this paper. In face of cyberattacks, various countermeasures may be deployed as defense against the malicious acts.

In the literature, [11] has identified the different threats, risks and vulnerabilities with respect to security, privacy and safety within a UAV operating environment. These threats include unregulated co-existence of a large number of UAVs in national airspace with commercial aircraft, unauthorized aerial video capturing over private space, and material smuggling into prison. In the work, cybersecurity is only one, but not the main focus. In [12], the authors have investigated the use of UAVs as attack agents in launching cyberattacks in civilian, military and terrorism domains. In some of these attacks scenarios, a UAV must first be an attack target for hijacking, before the hijacked UAV can be turned into an attack agent. In the investigation, the attack may not be strictly in the cyber space, but can also be a physical attack in the sense that the hijacked UAV is used to deliver harmful material or to enable kinetic impact. The work has also presented a number of countermeasures to thwart the investigated attacks. Some of these countermeasures involve physical mechanisms, such as firing a bullet to shot down or deploying a net to capture a hijacked UAV.

With a clear focus on cyber space and cybersecurity, [13] has used an attack tree to formalize how a cyberattack can be carried out as a sequence of atomic attacks, where each atomic attack focuses only on breaking one of three security aspects, which are information confidentiality, information integrity and service availability. In an attack tree, the root node is the ultimate attack objective, and all other node represents a compromised state. An arc from a child node towards a parent node models a transition to a more compromised state after the success of an atomic attack, that exploits some cybersecurity weaknesses. By enumerating all possible weaknesses, a complex attack tree can identify all possible attacks. There may be too many potential attacks and dealing with each attack incurs a cost. For cost effectiveness, the work has further proposed to priority efforts to deal with only a subset of the most critical attacks. Similar to [13], the work [14] has used a tree structure to formalize potential attack pathways, which are also known as attack vectors in the literature and each vector has an ultimate goal of breaking information confidentiality, information integrity or service availability. However, for the tree structure in [14], each node can represent an attack vector, attack agent, attack entry point, etc. The lack of consistency in tree node definition has made it harder to understand. Also, [14] has dealt with only attacks on wireless communication channels. These channels can be between UAV and satellite, UAV and ground control station, or two neighboring UAVs.

The work [15] has analyzed three potential UAV cyberattacks, namely denial-of-service, controller hijacking and man-in-the-middle. According to [15], denial-of-service is caused by limited on-board resources, controller hijacking is caused by inadequate access control and man-in-the-middle attack is caused by weak information confidentiality. For each of the three attacks, the work has ranked its occurrence probability and impact severity in a range of 1 to 5. Given such ranking, the paper has proposed a method to identify the most critical attack to focus on. Following the method, man-in-the-middle attack should be given a higher priority, compared to the other two attacks. While such ranking and prioritization is useful, assigning quantitative values to occurrence probability and impact severity can be subjective and may vary significantly among different application scenarios.

TABLE 1. Comparison with existing surveys.

Reference	Remark
[12]	Strong focus on military applications and criminal use of UAVs. Cover cyberattacks as well as physical attacks. Include UAV as attacks target as well as tool. No classification of countermeasures.
[16]	Classify cyberattacks on large and small UAVs, using taxonomy modified from that of autonomous terrestrial vehicles. Conclude attacks on data communication channels can cause severe damage but have not been given much attention.
[17]	Classify UAV cyberattacks into three classes, namely data interception attack, data manipulation attack and denial-of-service attack. Include a significant number of references which have not been developed within the context of UAV.
This paper	Focus on countermeasures of cyberattacks. Classify countermeasures into three classes, namely prevention, detection and mitigation. Analyze countermeasures and apply them commonly across six types of attacks, namely channel jamming, message interception, message deletion, message injection, message spoofing, and on-board system attack.

There are a few exiting surveys on UAV cyberattacks as summarized in Table. 1. The work [16] has surveyed different types of cyberattacks and classified them using a taxonomy which is modified from that of autonomous terrestrial vehicles. Also, [16] has concluded that cyberattacks on data communication channels can cause significant damage, but have not been given sufficient attention by the research community. Therefore, data channel attack should deserve a higher priority compared to other attacks. In another survey, [17] has classified existing cyberattacks into three classes, namely data interception attack, data manipulation attack and denial-of-service attack. However, in [17], the reference list includes a significant number of existing works which have not been developed in the context of UAVs.

Compared to cyberattacks, we find it more useful to survey the countermeasures for these attacks. This is because countermeasures may not be cyberattack specific, in the sense that a countermeasure may be effective against more than one kind of attacks. As such, having a comprehensive understanding of the state-of-the-art in countermeasures, can prepare us against any current or newly created cyberattack. Unfortunately, no existing work has provided a comprehensive survey of cyberattacks with a focus on countermeasures. This paper aims to close this gap in the existing literature.

While surveying for cyberattack countermeasures, this paper focuses on attacks which are launched on UAVs, but not using UAVs as attack agents on other UAV or non-UAV targets. We focus on cyberattacks but not physical attacks, which must use some forms of mechanical contact or physical tool to seize, trap or catch a targeted UAV. We first classify UAV cyberattacks, based on the type of their attack entry point, which can be either radio channel, message or on-board system. Following this classification, there are six categories of attack, namely channel jamming, message interception, message deletion, message injection, message spoofing, and on-board system attack. Given the classification, we survey the existing literature for their countermeasures. We organize the countermeasures into three categories, namely prevention, detection and mitigation. We identify some countermeasures which are commonly applicable to multiple types of cyberattacks. The main contributions of this paper are summarized as follows:

- A systematic classification of different types of UAV cyberattacks, based on the types of attack entry point. There are six attack categories, namely channel jamming, message interception, message deletion, message injection, message spoofing, and on-board system attack.
- A comprehensive and concise review of countermeasures against UAV cyberattack. We organize these countermeasures into three categories, namely prevention, detection and mitigation. We emphasize that some countermeasures are not exclusive to a particular cyberattack and thus, can be effective against more than one malicious acts.
- A detailed discussion of open research challenges and potential future works.

The rest of this paper is organized as follows. Section II describes the UAV system and operation model. In Section III, we first present the basis of cyberattack classification and group the attacks into six classes. For these attack classes, in Section IV, we survey their countermeasures, and organize them into three categories. Section V highlights open research challenges and present potential future works. This paper ends with concluding remarks in Section VI.

II. UAV SYSTEM AND OPERATION MODEL

Based on the operating altitude and flying range, UAVs can be classified into three classes as follows:

- *Small UAV:* Operates at an altitude up to 300 m, and a range of up to 3 km. Weight for small UAV should not exceed 24 kg.
- *Medium UAV:* Operates at an altitude above 300 m but below 5,500 m, and a range above 3 km but below 200 km.
- *Large UAV:* Operates at an altitude above 5,500 m, and a range above 200 km.

We focus on civilian and commercial applications. Hence, we consider only small and medium UAVs that fly at an altitude of less than 0.5 km for non-tactical operations.

Small and medium UAVs can be further classified based the level of operational autonomy, into two categories as follows:

- *Remotely controlled UAV:* This type of UAVs are controlled by a human operator from a remote location. The remote operator sends control commands over a wireless communication channel to control the UAV. On-board the UAV, the received command is delivered to an embedded controller. The controller is aware of the UAV's internal and external states through various measurements from on-board sensors. Given the state information, the controller translates a command into a set of executable maneuver instructions. In addition to movement control, a command may simply request the UAV to send to the human operator, its state information and sensor measurements. In this type of UAVs, the human control can be direct or indirect. Under direct control, the UAV can change its movement only if there is a specific command to do so. On the other hand, with indirect control, the human operator may only specify some high level details of a mission such as altitude, speed, direction, etc., and does not provide continuous commands. In this case, the on-board controller is responsible of translating such a high level mission specification into a sequence of control commands.
- *Fully autonomous UAV:* This type of UAVs requires human operator to provide only mission objective and possibly also way-points. They can make control decisions, react to events and perform flight maneuvers without any human involvement. Such capability requires the UAV to independently and continuously perceive its internal and external states using on-board sensors. Based on the perceived states, the embedded controller will issue intelligent control commands and maneuver instructions to various parts of the UAV. While autonomous UAVs are capable of self-control, there may be a provision for human intervention in some exceptional cases. For example, the UAV may request

for confirmation from a human operator before making a detour from its original flight mission to avoid an unexpected event.

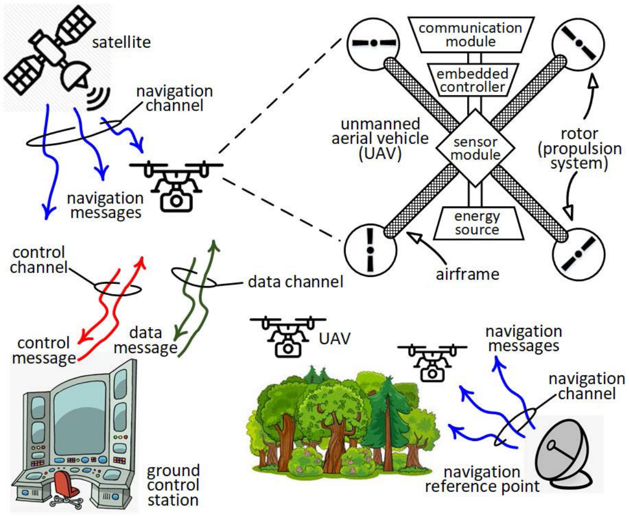

FIGURE 1. Unmanned area vehicle (UAV) system and operation model. Navigation messages are broadcast in the navigation channel, from external navigation reference points which can be earth-orbiting satellite or a static ground facility.

Following the description above, we have generalized the remotely controlled and the fully autonomous UAV into a single system model as illustrated in Figure 1. In summary, each UAV is a cyber-physical system, which other than the unmanned aircraft itself, needs supports from several external elements, such as a wireless communication network, a few navigation reference points, and a ground control station. Despite the fact that UAV is a system, consisting of several components other than the UAV itself, we continue to use the term "UAV" to refer to both the whole system as well as the aircraft alone, for simplicity hereafter. For a UAV, its payload includes all cargo and equipment that it carries. For brevity in the system model, we intentionally do not describe a UAV's payload, because its characteristics can vary significantly depending on applications. Although it is not explicitly illustrated in Figure 1, the system model does not exclude UAV-to-UAV communications. In such a case, the peer-to-peer communication link between two neighboring UAVs is the same as the one between a UAV and the ground control station.

The navigation reference points are nodes that know their own position coordinates and are equipped with communication capability. These nodes periodically broadcast their coordinates through navigation message to other nodes, such as UAVs. The radio channel used for such navigation message broadcast is called the navigation channel. With the navigation messages received from multiple reference points, a UAV can determine its own position coordinate using localization techniques, such as triangulation or multilateration. These navigation reference points can be static infrastructures on the ground, or earth-orbiting satellites in the space. Typically, these satellites are part of a global navigation satellite system (GNSS), such as the global positioning system (GPS), GLONASS, Galileo and Beidou. A brief characteristic summary of several GNSS is presented in Table. 2. Our system model does not demand a specific type of navigation reference points, but most existing literature has assumed GPS. On the other hand, Beidou as the newest GNSS, has attracted increasing interest. Hereafter, navigation reference point mean an earth-orbiting satellite of a GNSS.

TABLE 2. Comparison of several global navigation satellite systems.

	GPS	GLONASS	Galileo	Beidou
Owner	United States	Russia	European Union	China
Altitude	20,180 km	19,130 km	23,222 km	21,150 km
Number of operational satellites	24	24	24 + 6 backups	28
Signal transmission frequency (GHz)	1.563–1.587 1.215–1.239 1.164–1.189	1.593–1.610 1.237–1.254 1.189–1.214	1.559–1.592 1.164–1.215 1.260–1.300	1.561098 1.589742 1.20714 1.26852
Localization precision (meter)	0.3 - 5	2 - 4	0.01 - 1.0	0.1 - 3.6

In the system model, the ground control station is a facility for human operators to monitor and control a UAV during its operation. The control station may exist in different forms. For small-size recreational UAVs, the control station is a small hand-held device, such as a smart phone, etc. For commercial cargo-ferrying UAVs, the control center is a self-contained room with multiple workstations and real-time data feed, functioning like a virtual cockpit. The ground control station can be directly connected to a UAV through a wireless communication link, such as Wi-Fi, Zigbee, Bluetooth, proprietary telemetry, or remote controller link, if the UAV's operation range is within the communication range. Otherwise, a satellite communication network or other wide-area wireless communication network, such as 5G cellular network is required to connect the control station with UAVs. As depicted in Figure 1, each communication link may contain a control channel, a data channel or both a control and a data channel. The control channel is used to transmit control commands and other control-related messages. On the hand, the data channel is used to deliver data, which may include video, images, sensor measurements, position coordinates, etc. Through these communication channels, the ground control station can monitor and dictate the behavior of a UAV, as well as exchanging data with the UAV.

As shown in Figure 1, each unmanned aircraft consists of a few modules, namely airframe, propulsion system, energy source, sensor module, communication module and embedded controller. The sensor module consists of various sensors and is equipped with capability to pre-process sensor data. The sensors may include pressure sensor, attitude sensor, inertia measurement unit, gyroscope and accelerometer, which are essential to safely fly a UAV at a steady speed and altitude. Depending on applications, some UAVs may be installed with radar, infrared scanner and camera. The communication module is responsible of receiving navigation messages from the external reference points, as well as connecting UAVs to the ground control station and to other neighboring UAVs. Through this communication module, UAVs can receive control commands from and send collected data to the ground control station. The embedded controller is the central processing unit, that forms the foundation and hosts the operating system of the UAV. It links different modules together by supporting inter-module communications. This controller processes the received navigation messages to determine the UAV's own coordinates, velocity and timing, which can be provided to the ground control station for tracking. As the central processing unit, the controller also collects and processes real-time data from on-board sensors, to determine its internal and external state, to stabilize the aircraft and to perform maneuvers according to commands from the ground control station.

III. CYBERATTACKS

A cyberattack is an offensive act with malicious intents that affect computation and communication functions. While an attacks can result in some incremental failures in cybersecurity requirements, such failures may not be the ultimate goal of an adversary. As illustrated in Figure 2, through a series of incremental cybersecurity failures, the adversary may aim to ultimately destroy or hijack the UAV, to jeopardize a flight mission, or to simply steal the collected information. As such, cyberattack may be a complex multi-stage process. For example, a cyberattack may consist of three stages, to first feed a UAV with fake navigation messages leading to a wrong calculation of its coordinate. Then, the adversary will jam the control channel to prevent the UAV from receiving commands from the ground control station. Finally, with fake navigation messages and without control command, the UAV may be disoriented and eventually crash to ground.

In each of the multiple stages, an atomic attack adds a further cybersecurity failure and bring the UAV to more compromised state, which is closer to the malicious ultimate goal. We treat the atomic attack at each stage as an independent cyberattack, and classify these attacks based on their attack entry points. As depicted in Figure 2, there are three types of attack entry points, namely radio channel, message, and on-board system. Based on these entry points, with reference to Figure 3, we have grouped cyberattacks into the following six categories: channel jamming, message interception, message deletion, message injection, message spoofing, and on-board system attack.

A. CHANNEL JAMMING

Channel jamming is a carried out by producing an interfering radio signal with a power which is significantly higher than the power of legitimate signals in a targeted channel. As a result, the legitimate signals are overpowered and will appear only as noise at the receivers. By causing such message reception failures, this attack aims to make a communication channel unavailable to a receiver. Hence, channel jamming is a form of denial-of-service attack in the physical layer.

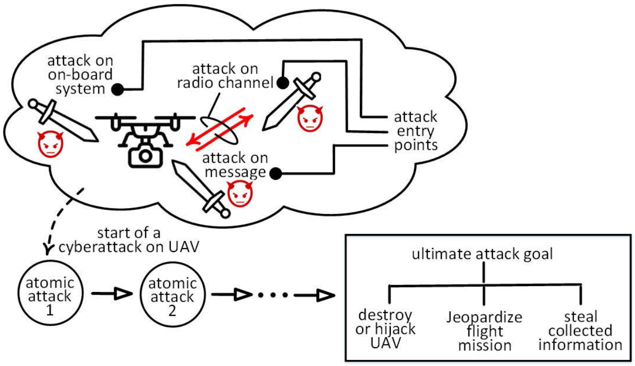

FIGURE 2. Illustration of a cyberattack on a UAV.

Channel jamming is not sophisticated and is probably the simplest among all UAV cyberattacks. As illustrated in Figure 4, it can be launched in the navigation channel, control channel and data channel. For attacks on navigation channel, the impact is often the loss of navigation messages at a targeted UAV. Without navigation messages from GNSS satellites, the UAV will not be able to accurately determine its own position, and probably also times. As a result, the UAV cannot follow a desired flight path and may crash to ground.

For attacks on control and data channel, the attack target can be both a UAV and the ground control station. Jamming control channel can lead to failure in receiving control commands from the ground control station and system state updates from the UAV. Jamming data channel can disrupt images, video and data exchange between UAV and the ground control station.

B. MESSAGE INTERCEPTION

Message interception is a passive attack, where an eavesdropper simply receives through sniffing capture, the messages transmitted in a communication channel. In this attack, the adversary needs to interpret and understand the intercepted messages. The aims may be as simply as to see what the targeted UAV is seeing. On top of this, the adversary may be able to derive other secondary information from the intercepted messages. For example, a leaked video streaming from a UAV may allow the adversary to determine the concerns or interests of the UAV operator.

Message interception is a serious breach of information confidentiality. As illustrated in Figure 4, this attack is typically applicable only to both control and data channel, but not to navigation channel. This is because the navigation messages are openly broadcast with intention to be received by everyone.

C. MESSAGE DELETION

Message deletion is a malicious act that discards a message, which should have been transmitted to its intended receiver.

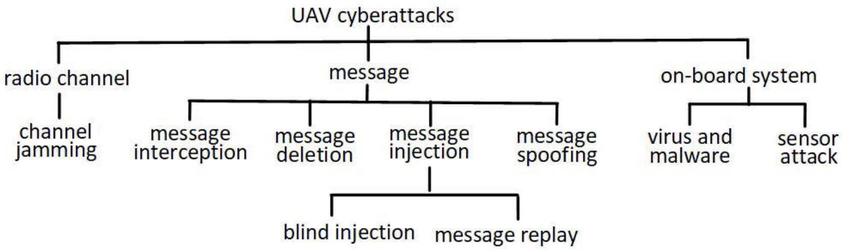

FIGURE 3. Unmanned aerial vehicle (UAV) cyberattack classification.

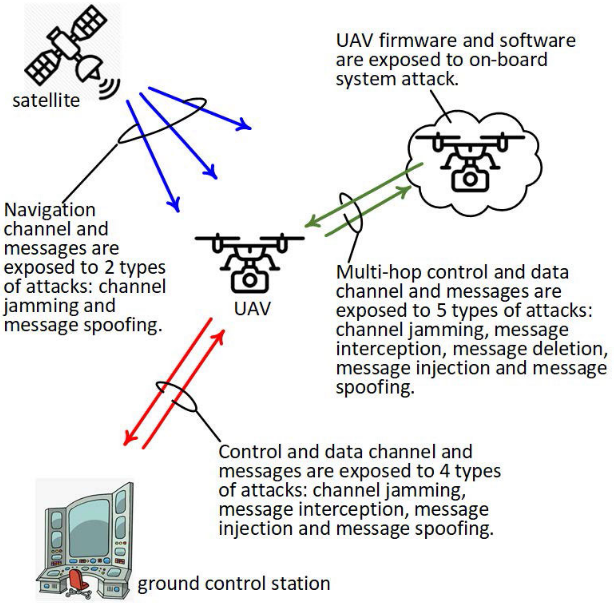
satellite
UAV firmware and software are exposed to on-board system attack.
Navigation channel and messages are exposed to 2 types of attacks: channel jamming and message spoofing.
UAV
Multi-hop control and data channel and messages are exposed to 5 types of attacks: channel jamming, message interception, message deletion, message injection and message spoofing.
Control and data channel and messages are exposed to 4 types of attacks: channel jamming, message interception, message injection and message spoofing.
ground control station

FIGURE 4. Exposure of different attack entry points to different attack classes.

This attack is carried out by an adversary which supposes to relay the message, where the sender and intended receiver are not within the communication range of each. Compared to message interception, message deletion may be less complicated because it does not require the adversary to understand the message, but to simply discard it.

As illustrated in Figure 4, this attack is usually not applicable to navigation channel, because the navigation reference points, i.e., satellites can broadcast directly to UAVs. As a result of message deletion in control and data channel, a UAV may not receive commands from the ground control station and the control station may not receive video streams from a UAV. By discarding a large number of messages, this attack has the effect of disconnecting UAV and the ground control station in both control and data channel.

D. MESSAGE INJECTION

Message injection is a form of cyberattack in which illegitimate messages are created and then, transmitted through control or data channel. As illustrated in Figure 4, this attack is not normally launched in navigation channel.

Message injection can be further divided into blind injection and message replay. In blind injection, the illegitimate messages are independently created by the attacker without any consideration of the targeted UAV and its operating environment. In message replay attack, the illegitimate messages are created as duplicates of some intercepted messages. However, message replay attack is different from message interception attack in the sense that such message replay attack may not require the adversary to understand an intercepted message before retransmitting the message.

Blind injection is less sophisticated than message replay attack. Blind injection attack aims to generate addition message traffic to overload control and data channel. As a result of blind injection, legitimate messages are squeezed out of the communication channel by illegitimate messages [18]. Blind injection can also be used to send excessive requests to overload a server at the ground control station or the embedded controller on-board a UAV. Overloading on-board controller can quickly deplete the UAV's battery. Therefore, blind injection attacks is a form of denial-of-service attack which is performed above the physical layer. In a computer simulation developed by [19], such a denial-of-service attack has been carried out by using up to 30 hostile UAVs, which collectively transmit a large number of control messages to a targeted UAV or a ground control station.

Video replay attack is a specific form of message replay attack when the replayed messages are produced from a captured video stream. A video replay attack can be used by an adversary to hide the actual condition of a critical infrastructure or facility under surveillance by substituting the actual live feed of a camera with a previously recorded video. Keep replaying a recorded video which shows a satisfactory condition, may create an all-good illusion while the infrastructure has already been intruded. According to [20], VideoJak is a free video security assessment tool which can be used to launch video replay attack on internet protocol (IP) cameras, that are similar to the video systems used in many commercially available UAVs.

E. MESSAGE SPOOFING

Message spoofing is the malicious act of producing and transmitting a fake version of a message, and making them appear as they are transmitted from a legitimate sender. In this context, the attacker is the illegitimate fake message sender and it is called the spoofer. As illustrated in Figure 4, this attack can be launched in navigation channel, control channel and data channel. For navigation channel, the spoofer mimics only the actual navigation reference points, which are the earth-orbiting satellites of GNSS. For control and data channel, the spoofer may mimic a UAV as well as the ground control station.

For message spoofing attacks on navigation channel, the aim is to make a UAV believes that it is at a location other than where it actually is, or it is at the actual location but at a wrong time. A spoofer performs the attack by first receiving the original navigation message and then, either modifying it or simply holding it for a delay, before retransmitting the message at the current or another location. Due to the popularity of GPS, message spoofing is widely known as GPS spoofing in the literature. According to [21], the spoofed GPS message should be transmitted at a power as much as 3 times the expected received power of a legitimate navigation message to suppress it at the targeted UAV. This should not a problem to most attackers because legitimate navigation messages from satellites often have a weak power on earth. For example, GPS signals are normally -160 dBW at a ground-level receiver. The falsified or delayed navigation messages will result in errors when they are used by a UAV in determining its own position coordinates. The work [22] describes the use of GPS spoofing in an effort to hijack a UAV. Examples of navigation message spoofing attack have been presented in [23] and [24], where fake GPS messages have successfully induced an upward drift in the UAV's perceived locations, and caused the UAV diving in to the ground.

Navigation message (GPS) spoofing attack needs to imitates the true messages, rather than just destroying the message. As suggested in [25], depending on the level of details in such imitation, GPS spoofing itself can be further divided into three classes, namely basic, intermediate and advanced. Basic attacks produce a fake message without paying attention to consistency with the legitimate messages. Intermediate attacks synchronize the physical signal characteristics of a fake message with that of the legitimate messages, taking into account signal power, signal arrival angle, etc. Advanced attacks not only synchronize a fake message with the legitimate messages, but also work in coordination with multiple other spoofers to mimic the presence of multiple external reference points of an actual GNSS. Compared to the basic and intermediate attacks, the advanced attacks are meticulous and ambitious with significant attacking resources.

For message spoofing attacks on control channel, the aim is to use falsified control messages to mislead a UAV or the control center into performing some acts in favor of an adversary. For example, a falsified command may instruct a UAV to alter its flight path or to land in a hostile location. In addition to these attacks over generic wireless links, there is a specific type of control message spoofing attack for the case of Wi-Fi being used to inter-connect UAV and ground control station. This attack over Wi-Fi is called the de-authentication attack [26]. In a UAV Wi-Fi network, the aircraft is an access point and the ground control station is its client. The access point periodically broadcasts its identifier. Upon discovering an access point based on the identifier, a client can request to connect to the access point by sending an authentication request followed by an association request. Later, the client can request to be disconnected from the access point by sending a disassociation or de-authentication message to the UAV, i.e., the access point. A de-authentication attack is performed on a UAV by first discovering the UAV's access point identifier from its broadcast. Then, the attacker finds out the medium access control (MAC) address of the ground control station through wireless sniffing. Subsequently, the attacker sends a spoofed de-authentication message to the UAV on behalf of the control station. As a result, the UAV is disconnected from the ground control station pre-maturely. The detailed steps of such a de-authentication attack using a free software tool, called aircrack-ng [27] have been described in [28].

After a successful de-authentication attack, the adversary can launch further attacks to mimic the actual ground control station to hijack the UAV. One example of such further attack is the man-in-the-middle attack, where the adversary pretends to be both a UAV and the ground control center [29]. In such attack, the adversary intercepts the genuine commands generated by the control station, replaces the command with a falsified one before sending it to the UAV, and transmits a fake response as if is generated by the UAV to the control station. As such, the adversary may directly command the UAV without being noticed. The elaborated de-authentication and man-in-the-middle attack has been automated in SkyJack, which is a UAV that has been engineered to autonomously seek out and then, to take control over any other UAVs within its Wi-Fi range. The source codes of SkyJack implementation are publicly available at [30].

Data message spoofing attack may exist in various forms depending on the types of data being falsified. Falsifying images taken by a UAV may hide the existence of an object under surveillance. A falsified coordinate broadcast from a UAV may cause the UAV becomes untrackable by the ground control station. In the literature, an example of such data message spoofing attacks on coordinate broadcast can occur in the Automatic Dependent Surveillance Broadcast (ADS-B) system [31]. In ADS-B, an aircraft derives its position coordinates based on navigation messages received from a GNSS, such as GPS. Then, the aircraft is required to broadcast its coordinates once per second. Based on the position information, the ground control station and other aircraft can precisely track the aircraft without the need of using radar. Compared to radar which sweeps for position information every 5 to 12 seconds, ADS-B is more responsive. Through ADS-B, a UAV can achieve situational awareness and perform self-separation to avoid mid-air collision. The occurrence of ADS-B message spoofing attack has been studied in [32]. In this attack, an adversary first acquires the precise position and velocity information of a targeted UAV through its ADS-B messages. Then, the adversary falsifies similar ADS-B messages from other neighboring UAVs to impose on the targeted UAV, an impression of an upcoming mid-air collision. This impression will trigger a collision avoidance procedure in the targeted UAV and forces it to alter its flight path into a pre-determined trajectory. A sequence of such alterations in flight path can force the targeted UAV into a position as dictated by the adversary.

F. ON-BOARD SYSTEM ATTACKS

As illustrated in Figure 4, this class of attacks target on-board firmware and software systems, such as the embedded controller, sensor modules, operating system, etc., but not radio signals, communication channels or transmitted messages, which are off-board. These attacks can be carried out in diverse forms, with different objectives. In some cases, on-board system attacks are launched to build foundation or to provide covert to subsequent attacks.

An attack may exist in the form of a malicious computer program, such as a virus or malware implanted in the on-board software and operating system. Such a virus may introduce without being notice, a sequence of small changes in rotor speed, that will eventually cause the UAV to lose its lift and then, crash to ground. In [33], the authors have raised the concern of malware attacks when off-the-shelf Apple and Android hand-held devices are prevalently used to control UAV. However, this concern is slightly different from ours, because it deals with the risk of malware invading the hand-held devices, but not the UAV. Nevertheless, building on [33], a malware may invade a UAV from the infested hand-held devices, where the hand-held devices are just stepping stones. A malware may perform as a ransomware when it is capable of blocking access to a UAV unless a random is paid.

If an attacker knows exactly how the UAV's sensor algorithm works, then the attacker can manipulate the UAV's environment to generate a certain input to the UAV's sensor. Such generated sensor input aims to induce a certain UAV behaviors in favor of the attacker. This kind of attack is called on-board sensor attack, which exploits predictable responses of a UAV with respect to a sensor input. As an example, [34] has first noted that the accuracy of a micro-electro-mechanical (MEM) gyroscope can deteriorate significantly at its resonance frequencies. Given such an exploitable vulnerability, the authors have used simple consumer-grade speakers to generate interfering audio signals at the MEM's resonant frequencies, to alter the outputs of a UAV's gyroscopes, causing the UAV to lose control and crash to ground. Another example of sensor attack is called sensor input spoofing attack in [35]. The attack targets optical flow sensor which measures a UAV's drift by observing changes in its ground plane images. An adversary can influence the ground plane image from a distance by projecting light onto the ground surface. As a result, the UAV will calculate wrongly its drift or may not obverse the existence of a ground underneath.

IV. COUNTERMEASURES

In the literature, a number of countermeasures have been proposed against various cyberattacks on UAVs. Some of these countermeasures require mechanical systems, such as one that deploys a physical net to catch a straying UAV or fires a bullet to shoot down a hijacked UAV, etc. We focus on the countermeasures that do not require such mechanical systems. We notice that some countermeasures may not be exclusive to a particular cyberattack in the sense that each countermeasure may be applicable to more than one type of attacks. This is because different attacks may differ in their attack targets and attack vectors, but may lead to a same consequence. For example, a control message spoofing attack and a virus attack are from different categories, but may lead to a same result of a misbehaving UAV.

As illustrated in Figure 5, countermeasures can be classified based on their functional scopes into three categories, namely prevention, detection, and mitigation. Prevention countermeasures try to stop a cyberattack from starting. When the prevention countermeasures have failed and an attack has been successfully started, detection countermeasures become important in alerting the UAV operator of such attack. After detecting the presence of an attack, mitigation countermeasures help in reducing the negative impacts and limiting the damage. The functional scopes of different countermeasures are illustrated in Figure 6.

A. PREVENTION

In general, prevention countermeasures work in the following three methods:

- Impose strict system access control such that only authorized personnel and software agent may establish contact with a UAV.
- Protect information confidentiality, integrity and authenticity such that no fake or erroneous data and command will be accepted.
- Use only system firmware and software components without exploitable vulnerabilities.

As shown in Table. 3, not all the three prevention methods are applicable to all cyberattacks. For example, as a countermeasure against the sensor attack in [34] and [35], we need to design and implement the UAV by using only sensors with acceptable characteristic within an expected operating range. Specifically, in the case of [34], we need to select a suitable gyroscope which is not affected by the surrounding acoustic noise in its typical operating range. But, such a countermeasure is not useful for other attacks. Furthermore, on-board system components must be equipped with anti-tampering features, to guard against the opening up of more attack entry points. Another example is the use of jamming resilient transmission schemes, such as direct sequence spread spectrum and frequency hopping spread spectrum, to prevent channel jamming attacks. Such countermeasure is not generally useful for other attacks, which are not launched in the physical layer.

Despite being grouped within a same class, different prevention countermeasures may have significantly

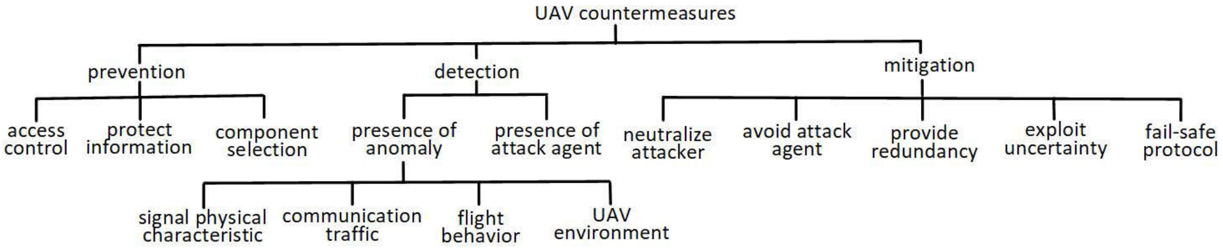

FIGURE 5. Unmanned aerial vehicle (UAV) cyberattack countermeasure classification.

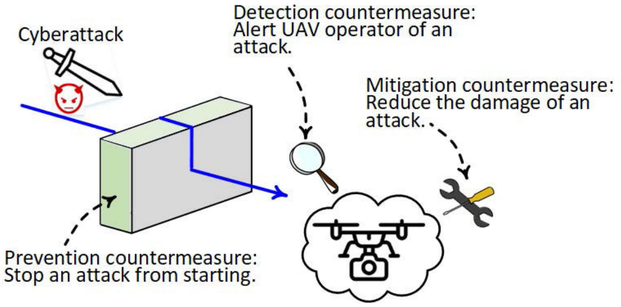
Cyberattack
Detection countermeasure: Alert UAV operator of an attack.
Mitigation countermeasure: Reduce the damage of an attack.
Prevention countermeasure: Stop an attack from starting.

FIGURE 6. Functional scopes of different cyberattack countermeasures.

different realizations. The access control to prevent message deletion and virus attacks can be some password-based node authentication schemes over generic wireless links. When the wireless link is Wi-Fi as in the case of de-authentication attack described earlier in Section III.E, access control can be done in the form of allowing only devices with pre-registered MAC addresses to establish connection with the UAV, which is a Wi-Fi access point. According to [28], this is a reliable countermeasure because MAC address is a unique hardware identifier assigned to each Wi-Fi interface card. By checking the MAC address, the UAV can accurately filter out an adversary and deny its chance in submitting a fake de-authentication message. In addition to access control via MAC address filter, [28] has suggested to prevent de-authentication attacks by not broadcasting, but hiding a UAV's access point identifier. Also, the authentication and association messages which are transmitted in clear text by default, should be encrypted to prevent wireless sniffing, which precedes the attack.

In Table 3, cryptography appears as useful in preventing several cyberattacks. With reference to Figure 3, encrypting a message can protect its confidentiality and thus, can prevent message interception attack [36]. Compared to asymmetric cryptography, symmetric cryptography is less computationally demanding and thus, is more suitable for low-cost UAVs with limited on-board resources. A challenge in implementing symmetric encryption is secret key distribution. A symmetric key distribution scheme has been proposed in [37] for implementation on the radio control channel. The scheme is unique in the sense that it can be implemented on commonly available radio modules and does not require any hardware modification. The key distribution scheme has adopted Galois Embedded Crypto, and has modified it for implementation using ArduinoLibs Crypto library on resource-limited Arduino Uno. In the implementation, both the control station and UAV have a commonly known permanent secret key K_p, which is pre-programmed in ROM at the factory. At the start of a new communication session, the control station first generates a session key K_c and a random initialization number I_c. The control station encrypts K_c using K_p and then, pre-appends the generated cypher text with I_c to produce an encrypted message m_c. The control station transmits m_c to the UAV. The UAV extract I_c from m_c and decrypts the received cypher text to obtain K_c. Then, the UAV generates its own session key K_u and sets its initialization number $I_u = 0$. The UAV encrypts K_u using K_c and then, pre-appends the generated cypher text with I_u to produce an encrypted message m_u. The UAV sends m_u to the control center. The control center decrypts the received cipher text using K_c to obtain K_u. After exchange of acknowledgments, the control center encrypts all messages to the UAV using K_u and I_u, and the UAV encrypts all messages to the control center using K_c and I_c. The values of I_c and I_u are increased by a fixed number after each message.

Apart from cryptographic encryption, information confidentiality can also be achieved using physical layer security techniques. In the context of a UAV-aided communication system, [38] has proposed to guard against a full-duplex eavesdropper by transmitting in the physical layer, artificial noise signals together with information signals. A scheme has been derived to determine the optimal power allocation factor between artificial noise and information signals, such that a combination of transmission outage probability and secrecy outage probability is minimized. Also, the scheme can control the height of a UAV to achieve a desire information secrecy rate. By exploiting the mobility of a UAV, the work [39] has proposed to maximize the information secrecy rate against an eavesdropper on the ground, by jointly optimizing the UAV's trajectory and transmit power over a finite horizon. While physical layer security techniques are promising, when the eavesdropper is located close to the transmitter, which can be the ground control station or UAV, there is still a challenge in achieving a high enough information secrecy rate for meaningful communications.

TABLE 3. Applicability of prevention countermeasures to cyberattacks.

Cyberattacks	Prevention Countermeasures		
	Access control	Protect information	System component selection
Channel Jamming		Jamming resilient transmission schemes, such as direct sequence spread spectrum, frequency hopping spread spectrum, etc.	
Message Interception		Protect information confidentiality through cryptographic encryption [36], [37], physical layer security scheme [38], [39], etc.	
Message Deletion	Stringent node authentication to admit only trusted neighbor as message relay when the intended receiver is not within communication range.		
Message Injection		Verify message authenticity through cryptographic encryption, to confirm that the message is indeed originated from a sender.	
Message Spoofing	Stringent node authentication to admit control station using MAC address filter and to avoid broadcast of access point identifier, to prevent de-authentication over Wi-Fi wireless link [28].	Confirm message integrity through cryptographic encryption [40], Blockchain [41]–[44], etc.	
On-board System Attack	Stringent node authentication to admit only trusted programs to prevent virus and malware attack.		Design and implement a system that uses only firmware, software and sensors which have no exploitable characteristics or vulnerabilities. Equip on-board systems with anti-tampering technology to guard against opening up of attack entry points.

Protecting information confidentiality can also prevent message spoofing, which requires first to understand a message before modifying it. In [40], message encryption has been proposed to prevent control message spoofing which appears in the form of man-in-the-middle attack. In another example, in navigation message spoofing, cryptography can prevent the attack by encrypting all broadcast messages. However, such a method is normally expensive and has been done only for military applications, where the intended receivers are knows *a priori*. In the context of GPS, the encrypted Precise(P)-Code messages can be assessed only by the military while the Coarse/Acquisition(C/A)-Code messages for civilian application are not encrypted. After information confidentiality is breached, encryption can still offer a second line of defense in preventing message spoofing with an ability to check for message integrity. Cryptographic encryption is also useful in preventing message injection attack through message authentication, which can verify if a message is indeed transmitted from a legitimate sender.

In addition to message encryption, cryptography is also the foundation for Blockchain technology. In the literature, Blockchain that depends heavily on one-way hash function has been used to provide UAVs with secure communication [41]–[43]. A Blockchain-based communication scheme has been proposed in [44], where a group of UAVs collectively build a Blockchain as a verifiable record of past communication activities. All UAVs in the group has a fair chance to add a block to the chain. As a record of activities that have happened, the Blockchain may be useful for forensic purposes, but not to protect confidentiality of a current message transmission. In the scheme, a sender UAV must first encrypt its message using a one-time symmetric encryption key, transmit the encrypted packet to all UAVs in the Blockchain group, and seek consensus from the group in confirming the integrity of message. The confirmation is consensus-based and is done through simple majority voting. Only after such confirmation, the sender UAV will deliver the message to its intended receiver, which can be another UAV or the ground control station. While the work has highlighted the use of Blockchain, message confidentiality is actually achieved through the symmetric encryption. In a separate work, [45] has proposed to use Blockchain for distributed storage of machine learning data to be used in intelligent decision making among multiple UAVs.

B. DETECTION

Cyberattacks can be detected through the following two methods:

- Detect the presence of an attack agent. An attack agent is an element that actually performs the attack or creates an impact, on behalf of an attacker. Such agent may appear in different forms depending on the type of attacks. For example, the attack agent for a channel jamming is a strong interfering radio signal, while the attack agent for a virus attack is a malicious computer program.
- Detect the presence of anomalies, which may exist in on-board resource usage pattern, radio signal, communication traffic, flight movement, etc.

Due to the passive nature of an eavesdropper, the attack agent of message interception is the attacker itself. Such a passive eavesdropper may not be easily detectable. Nevertheless, an eavesdropper may still be detected indirectly using secondary information, such as the heat generated by the eavesdropper's electronic circuits. Through a heat seeking infra-red camera, a UAV may scan its ground coverage area for any hidden data interceptor.

With reference to Table 4, virus and malware attacks can be detected through up-to-date anti-virus scanning software. Therefore, it is crucial to have the latest virus signature database uploaded to a UAV before its flight mission. Message replay attack and message spoofing can be detected by observing the presence of replayed and spoofed messages, respectively. Detecting such malicious messages can be done through cryptographic algorithms.

Channel jamming attacks can be detected by observing the presence of an attack agent, i.e. jamming signals in the same radio channel. A simple method to detect the jamming signal's presence is by monitoring the total received power in the frequency channel of interest. A jamming signal is considered presence if the received signal power to noise power ratio (SNR) is above a threshold. This method requires proper selection of the detection threshold, which can affect the detection accuracy. Compared to this simple threshold method, [46] has suggested to use sum-of-squares of the power ratio as the decision statistic. This is because, compared to non-jamming signals, jamming signals can cause correlated changes in all measured values of the ratio.

A cyberattack often leads to changes in on-board resource usage pattern, radio signal, communication traffic, flight movement, etc. As summarized in Table 4, by observing abnormal variation in these characteristics, we may detect the occurrence of an attack. Since different attack may target different aspect of a UAV, the anomalies may appear in diverse forms.

Message deletion and blind injection attack can lead to anomalies in network performance and traffic. Message deletion can cause the packet delivery ratio to drop significantly. Consider a disruption tolerant network with UAVs functioning as relay nodes, [47] has proposed to detect message deletion by monitoring the packet delivery ratio. The work has defined a parameter, called message dropping rate (MDR). Each UAV may monitor other UAVs within its neighborhood and increase the monitored UAV's MDR value in the following three conditions: (a) A UAV claims to be a relay and reports that it has forwarded a message, but the intended receiver has not received the message, (b) A UAV claims to be a source node, but another verified source has reported to have forward a message to it, (c) A UAV claims to be a relay and reports that it has not received a message from a verified source node. After a number of increments, the MDR value will exceed a threshold, which indicate the occurs of an attack. For high detection accuracy, the detection threshold is determined based on the posterior belief probability distribution given the observations and updated using a learning algorithm. However, this method does not allow a UAV to play multiple roles, such as a data source and a message relay, at a same time. In addition to message deletion, [47] has proposed another method to detect data message spoofing, by verifying data consistency from multiple transmitters. Here, the assumption is that in a surveillance applications, multiple UAVs may be deployed to observe a same events. Therefore, a message spoofing attack can be detected when the data received from multiple UAVs are not consistent with each other.

Building on [47] and with a similar disruption tolerant network, the same authors have worked on detecting blind injection attacks in [48]. As a result of blind injection, the number of incoming messages or service requests can suddenly surge to a high value. In [48], blind injection is detected by checking the statistical characteristics of number of packets and packet delay jitter. The work assumes the statistics follow a Gaussian distribution. Then. an attack is detected when the packet count or delay jitter exceeds a threshold. The threshold is originally set at 3 times standard deviation, and is subsequently updated using a support vector machine.

Without targeting a specific attack type, [49] has proposed to detect anomalies in network traffic using different machine learning algorithms. The algorithm inputs are different network traffic features, which include flow duration, number of packets, maximum and minimum packet sizes, average and total packet sizes, standard deviation of packet sizes, etc. It has been found that decision tree algorithm performs the best as compared to logistic regression, linear discriminant analysis, K-nearest neighbors algorithm, Gaussian naive Bayes algorithm, stochastic gradient descent and K-mean algorithm.

Control message spoofing can cause a UAV to move unexpectedly as dictated by a hijacker. On the other hand, navigation message spoofing can cause a UAV to be disoriented in an aimless flight. Hence, we can detect both control and navigation message spoofing by finding anomalies in a UAV's flight behaviors and statistics. The work [50] has proposed a recursive least square algorithm to compute several flight control statistics, such as roll, pitch, yaw, drag, thrust and lift, to characterize the control dynamics of a flight mission. Then, by tracking the real-time values of these statistics, an attack can detected when there is a significant deviation from the statistics' typical values. However, this scheme is applicable only for cases where the UAV are repeatedly flying a same flight mission. This is because different flight missions will yield different statistics, and require a separate characterization effort. Instead of control statistics, [51] has proposed to detect flight anomaly by using movement statistics. Through statistical analysis of flight data, the scheme first establishes a flight profile baseline. Then, this baseline is compared against a set of simulated hijacking scenarios, where a match in the comparison indicates an attack. In the paper, the proposed scheme is capable of detecting all hijackings where the targeted UAV has been fully compromised and the flight path has been randomly changed. For other scenarios where control over hijacked UAV is not consistently asserted by the attacker, the detection may not be successful. The work [52]

TABLE 4. Applicability of detection countermeasures to cyberattacks.

Cyberattacks	Countermeasures				
	Presence of attack agent	Presence of anomaly			
		Signal characteristic	Communication traffic	Flight behavior	UAV environment
Channel Jamming	Detect presence of jamming signals through excessive SNR, sum-of-square of SNR [46], etc.				
Message Interception	Detect the presence of eavesdropper using infrared camera to seek out heat generating electronic circuits.				
Message Deletion			Detect abrupt or unexpected drop in message delivery ratio [47], [49].		
Message Injection	Detect the presence of replayed message through cryptographic encryption.		Detect blind injection through surge in incoming messages, service requests, etc [48], [49].		Detect video replay through time and solar shadow inconsistency in video stream [54].
Message Spoofing	Detect the presence of spoofed message through failures of message integrity and/or authenticity checks.	Detect GPS spoofing by observing anomaly in received signal's physical characteristics, such as signal strength, noise level, automatic gain control value [57], signal arrival angle [58], signal phase-delay [59], etc. Detect GPS spoofing by comparing received signal against reference model [62]–[64]. Detect GPS spoofing by observing general anomaly in raw received signals using fuzzy logic and Kalman filter [65]. Detect GPS spoofing by finding discrepancy between between the received GPS signals against a secondary on-board systems [66].	Detect inconsistency in data from multiple UAVs deployed in a same operation [47].	Detect deviation in flight control statistics [50], movement statistics [51], location statistics [52], etc. Detect abnormal behaviors using a set of rules which checks on internal system states [53].	Detect inconsistency in location using solar shadow [55], aerial images [56], neighbor UAVs' coordinates [67], etc.
On-board System Attacks	Detect the presence of virus and malware using anti-virus scanning software with up-to-date virus signature.				

has proposed an idea to detect flight behavior anomaly through deviation in UAV location statistics. Here, location statistics are in the form of UAV's elevation angle and horizontal angle with respect to the ground control station. The work first builds a standard model for normal UAV behavior as a regression function of angles. In order to account for variation in location statistics caused by wind, the standard model is established using recurrent neural network. At each time instance, the standard model is used to predict a UAV location. The error between the predicted and the actual UAV location is recorded. When the normalized root mean square of the errors is larger than a threshold, the flight behavior is considered abnormal.

Instead of detailed statistics, [53] has proposed to detect abnormal flight behaviors at a higher level of abstract using a rule-based method. The work has defined a set of seven potential attack vectors (threats). Each attack vector has been transformed into a set of internal system states, where conjunctive and disjunctive predicates of the state can indicate the occurrence of an attack. These predicates form the rules and the work has proposed to check these rule following a priority list, where protecting integrity has a higher priority than protecting confidential, which has a higher priority than protecting availability. In [53], the rule checking can be done on a UAV by its neighbor UAV, or solely on-board where a system component checks on another component. The work has defined three types of attackers, namely reckless, random and opportunistic. Evaluation results have shown that the proposed method can effectively trade higher false positives for lower false negatives in detecting more sophisticated random and opportunistic attackers.

As a form of message injection, video replay attack can be detected by finding environmental inconsistency in the video stream. For example, solar shadow of a UAV depends on the UAV's location, the sun position and the current time. According to [54], an expected solar shadow at a given time and UAV location can be determined using an analemmatic sundial model. Then, a video replay attack is detected if the shadows in the video do not match the expected shadow. Such video analytic approach can also be used to detect navigation message spoofing, which is popular known as GPS spoofing in the literature [55]. This is because a mismatch in the solar shadow also implies an inconsistency in location. Specifically, a GPS spoofing is detected if the solar shadow in a received video does not match the expected shadow at a UAV location which is calculated from navigation messages.

Other than solar shadow, location consistency for GPS spoofing detection can also be verified using other environmental features. More specification, the surrounding environment of a UAV must be consistent with the location derived using the received navigation messages. For example, if the GPS messages determine that the UAV is flying above a sea, a picture taken from the UAV must not show it flying above a forest. In [56], a method has been proposed to detect GPS spoofing by using the a camera and a terrain elevation map. The method determines an expected video image based the UAV's position which is derived from the GPS messages, and compare that image against the actual image captured by the camera.

In addition to visual based location consistency method described above, there is a rich literature on GPS spoofing detection by checking anomalies in GPS's radio signal characteristics. These anomalies are in the form of unusually strong received signal strength and excessively low noise floor levels. Abnormal values may also be observed in automatic gain control values of GPS receivers [57], arrival angle of GPS signals [58], signal phase-delay [59], etc. Instead of focusing on a single physical characteristic, [60] has proposed to consider multiple signal characteristics collectively using a feedforward artificial neural network (ANN). The ANN input vector consists of signal-to-noise ratio, pseudo range, Doppler shift and carrier phase shift of the GPS signals from a number of satellites. The set of training input vectors contain both genuine and spoofed messages, which are generated based on actual GPS signal traces at two locations. Despite such a simple ANN, a detection accuracy of 98% can be achieved with just 2 hidden layers and 3 neurons in each hidden layer. However, these signal's physical characteristic detection methods are effective only against basic GPS spoofing with UAV remains stationary, but not intermediate and advanced attack. Also, these methods are generally not reliable in a multipath rich environment, and may require multiple antennas. Typically, a legitimate GPS signal may be overpowered by the fake GPS signal, but the legitimate signal still exists. Given this observation, a standalone method that does not require multiple antennas has been proposed in [61]. This method detects and tracks any signal correlation peak, in addition to the strongest one. The existence of such a weaker correlation peak indicates a GPS spoofing.

Apart from radio signal characteristics, GPS spoofing can also be detected by finding anomalies in calculated position coordinates. Generally, these methods calculate a UAV coordinate from the received navigation messages, and compare the calculated coordinates against the coordinates estimated by a reference model. Then, a GPS spoofing is detected when the difference between the two coordinates are large. In [62], the reference model is a kinematics state estimator, which takes into account control command and readings from an inertial measurement unit. The method detects a GPS spoofing if the error between the two coordinates is larger than a threshold. Instead of a threshold, [63] has a similar idea but to detect GPS spoofing by examining the statistical distribution of position errors. This is because while such errors exist with or without GPS spoofing, the error distribution changes in the presence of an attack. The work has used a support vector machine to learn the abnormality in such error distributions for accurate detection. However, with the use of online learning, the detection become inaccurate when the attack lasts for a long duration.

The idea of [62] has been adopted by [64], but with a different state estimator. Compared to a linear transfer function used in [62], the estimator in [64] has applied a combination of two extended Kalman filters. The benefit of using Kalman filter is that the uncertainty in UAV movements and reference signals can be incorporated into the decision process. Kalman filter has been used for GPS spoofing detection in [65] but in a different way. In [65], Kalman filter is not used to track uncertainty in the outputs of an estimator because no estimator is used in this work. Instead of an estimator, [65] has used a multi-layer tree-structure fuzzy inference process to detect spoofing based on raw navigation signals and inertial measurements. Here, Kalman filer is used to account for uncertainty in the raw measurements; and fuzzy logic is adopted to deal with the complex interactions between these measurements without the need of nonlinear equations.

Instead of finding anomalies in GPS signals by comparing against a reference model, [66] has proposed to find such discrepancies by comparing signals from two redundant physical systems on-board a UAV. The primary system is GPS-based which has a high accuracy, but also has a higher cost and is potentially more vulnerable to attack. The secondary system may have a lower positioning accuracy, but it will provide greater security than that of the GPS-based system. A GPS spoofing is detected when the difference between the two systems exceeds a certain threshold for a certain duration. However, [66] has not clearly stated what the secondary system can be.

With reference to Table 4, [55] and [56] described above can detect GPS spoofing by checking consistency of visual images captured by a UAV against the UAV's supposed environment based on its coordinates which are calculated from received reference messages. Apart from visual images, such environmental consistency can also be verified by checking a UAV's calculated position against its neighbor UAVs' coordinates. More specifically, a GPS spoofing is detected when a UAV's calculated position is not within an acceptable range from its immediate UAV neighbors, or as observed by a group of ground sensors. According to [67], this verification of coordinate consistency can be implemented through crowdsourcing to monitor advertisement messages from ADS-B system. As described earlier, ADS-B can be used by an aircraft to periodically announce its coordinates. However, to achieve a position accuracy of around 150 meters, this method needs 15 minutes of monitoring time, which is long enough for an attacker to hijack a UAV.

C. MITIGATION

As summarized in Table 5, the impacts and damage incurred by a cyberattack can be reduced through the following five mitigation methods:

- Neutralize the attacker.
- Avoid the attack agent.
- Provide redundancy.
- Exploit uncertainty.
- Fail-safe protocol.

Neutralizing attacker is a unique countermeasure which disables a passive eavesdropper by jamming its receiver. This is like a channel jamming attack which is launched by an attack target on the attacker. By overpowering the eavesdropper's radio receiver, it will not be able to sniff the communication channel for a message. As shown in Table 5, this countermeasure is applicable to message interception, message replay attack and message spoofing. This countermeasure is effective against message replay attack and message spoofing because both attacks require the attacker to first acquire some legitimate messages, to be used in the attacks. However, a straightforward channel jamming on the attacker may not be very effective when the attacker is located close to the intended receiver, i.e., the targeted UAV. This is because the jamming signals may also affect the targeted UAV at the same time of interfering the eavesdropper. The work [68] has proposed the idea of cooperative jamming, where a friendly UAV is deployed as a jammer close to the location of an eavesdropper. With such cooperative jamming, a scheme has been developed to determine the optimal flight path and transmit power of the friendly UAV jammer, taking into account the locations of both the eavesdropper and targeted UAV. This work is built on the physical security technique, and information secrecy rate is one of the main performance metrics. While [68] is indeed interesting, it relies on the ability to pinpoint the exact location of an eavesdropper, which may be difficult to know in practice.

Instead of actively transmitting jamming signals, an attacker can also be neutralized by luring it to attack a honeypot, which is a system whose only value lies in being attacked. The work [69] has proposed the idea of a HoneyDrone, which is a portable UAV honeypot to emulate a number of UAV-specific and UAV-tailored protocols, making it possible to lure adversaries into attacking it, instead of the original target UAV. The work has argued that such redirection of an attack is possible as long as the honeypot has a stronger signal than the targeted UAV and has been placed in a strategic location. In [69], the UAV honeypot operates on low-cost Raspberry Pi. By attacking and recording attacks, the honeypot can shed light into adversaries' techniques.

It can be an effective countermeasure to reduce the influence of an attack agent by avoiding it. For example, in channel jamming attack, a UAV may escape from the strong interfering signals by dynamically switching to another radio channel. In [70] and [71], a cognitive radio system has been developed using software-defined radio blocks. The system performs spectrum sensing to detect jamming signals. Upon a positive detection result, given the agility of software-defined radio, the system can switch all communicating UAVs out from the attacked channel, to another available channel.

In addition to radio channel switching, we can also avoid an attacker by exploring alternatives in spatial domain because each attacker has only a limited coverage area. Consider a UAV performing territorial surveillance and facing physical-layer control channel jamming attack. The work [72] has proposed a scheme that helps the targeted UAV in autonomously finding a new flight path to avoid the coverage areas of a group of jammers. The authors have assumed that

TABLE 5. Applicability of mitigation countermeasures to cyberattacks.

Cyberattacks	Countermeasures				
	Neutralize attacker	Avoid attack agent	Provide redundancy	Exploit uncertainty	Fail-safe protocol
Channel Jamming		Use cognitive radio to dynamically switch out from the attacked channels [70], [71]. Change flight path to avoid the coverage area of an attacker [72].	Against navigation channel jamming, equip each UAV with multiple receivers, each for a different GNSS.	Against mobile aerial jamming attack, add uncertainty to UAV flight movement and find optimal spatial reconfiguration of a multiple UAVs formation through formulation of multi-player pursuit-evasion game [75].	Pre-determined procedure which controls UAV to autonomously fly to a safe location [76], to self-destruct, etc.
Message Interception	Launch a channel jamming attack on the malicious eavesdropper. Deploy friendly UAV as cooperative jammer close to the location of eavesdropper, control fly path and transmit power of the friendly UAV to guarantee a minimum secrecy rate [68]. Redirect attacker to a fake target by luring it to a honeypot [69].	Change flight path to avoid the coverage area of an attacker.			
Message Deletion					Pre-determined procedure which controls UAV to autonomously fly to a safe location, to self-destruct, etc.
Message Injection	Launch a channel jamming attack on the malicious eavesdropper to prevent it from acquiring new messages for message replay attack.	Change flight path to avoid the coverage area of an attacker.			
Message Spoofing	Launch a channel jamming attack on the malicious eavesdropper to stop the spoofer from getting source messages for spoofing attack.	Change flight path to avoid the coverage area of an attacker.		Against navigation message spoofing, add uncertainty to UAV's behavior through game theory [73], [74].	Pre-determined procedure which controls UAV to autonomously fly to a safe location, to self-destruct, etc.
On-board System Attacks			Against sensor attack, using more than type of sensors for each critical measurement.		Pre-determined procedure which controls UAV to autonomously fly to a safe location, to self-destruct, etc.

the UAV can locate the jammers, and know the transmission strength of the jammers. Also, the UAV is capable of identifying the boundary between the jammed and non-jammed area. The proposed scheme first identifies all candidate flight paths, which are selected from all quadratic Bezier curves connecting the UAV's current position and a candidate end point within the non-jammed area. Among the candidate flight paths, an optimal path is selected using a reinforcement learning scheme with stochastic approximation. In addition to channel jamming, this flight path rerouting can be effective against message interception, message injection and message spoofing. More specifically, we can change a UAV's flight path to avoid getting close to eavesdropping attackers.

Another countermeasure against navigation channel jamming is to provide redundancy by installing multiple receivers, each for a different GNSS. As such, when navigation messages from one GNSS are jammed, the targeted UAV can still receive navigation messages from another GNSS. For example, when GPS is jammed, a UAV may receive navigation messages from GLONASS, Galileo, or Beidou. Such redundancy approach can be effective and cost-efficient because there are existing off-the-shelf commercial receiver systems capable of receiving multiple types of GNSS signals. Also, it will probably be too expensive for an adversary to simultaneously jam all the different GNSS. Providing redundancy is also an effective mitigation countermeasure against the sensor attack in [34], especially when its prevention countermeasure has failed. With reference to Table 3, the component selection approach may not prevent the attack because, due to physical limitation, there may be no other choice for a certain type of sensors. In such a case, the impacts of such sensor attack can be mitigated by using a multi-sensor system, where each critical measurement is obtained from more than one type of sensors. For example, in addition to MEM gyroscope, a UAV can install a mechanical gyroscope and a laser gyroscope. Also, in addition to gyroscope, a UAV can measure its angular velocity using an accelerometer and inertia measurement unit.

A UAV will receive the full blown impact only if its behavior is perfectly predictable by the attacker. As such, we may reduce the attack impact by adding uncertainty into a UAV's behavior, making it less predictable. In the literature, game theory provides a framework to model the effects of uncertainty in the behaviors of multiple actors, on each other. The work [73] has enlisted a combination of game theory and cooperative localization to mitigate the impact of navigation message spoofing attack. Generally, cooperative location allows a UAV to determine its own position by using only location information from three other UAVs within its vicinity. For such cooperative localization to work, the UAV must know its relative distances to the three cooperative UAVs and these cooperative UAVs must know accurately their own position coordinates. As such, cooperative localization will fail if one of the cooperative neighbors has suffered from navigation message spoofing. In [73], the authors assume that the spoofer can only attack one UAV each time. From the UAV operator's perspective, it is desirable for the spoofer to attack the UAV, but none of its three cooperative neighbors. As such, the attack can be nullified because the attacked UAV can get its location accurately determined through cooperative localization, while other UAVs will still get their location determined using navigation messages. Here, cooperative localization is applied only on a UAV, because it is significantly more computationally expensive as compared to localization using navigation messages. A problem arises if the attacker chooses to spoof a UAV which has not been selected to determine its coordinate using cooperative localization. The work [73] has suggested to form a group of five UAVs, where each UAV has four cooperative neighbors. Then, a dynamic Stackelberg game has been formulated to model the interactions between the spoofer and a UAV. In the game, the spoofer randomly chooses which UAV as the attack target and modifies accordingly the radio signal characteristics to avoid being detected. Solution of the game helps the UAV operator to optimally choose a UAV from its 5-member cooperative group, to get its coordinate determined through cooperative localization.

In another game theory based scheme, [74] has modeled the strategic behavior of a UAV in response to attacker's attempt to mislead it with a fraudulent and purposefully crafted navigation message. The work has characterized the necessary and sufficient conditions of a perfect Bayesian equilibrium of the game. Based on the equilibrium, the UAV can either infer its true position, or decide rationally its position that minimizes the deviation from its true position. In addition to defending against navigation message spoofing as in [73] and [74], game theory has been used in [75] against channel jamming attack. In [75], the jammer is a UAV trying to attack the radio channel between two communicating UAVs. A multi-player pursuit-evasion game has been formulated to find the optimal spatial reconfiguration of the pair of UAVs to minimize the jamming duration. The game formulation takes into account uncertainty in the jammer's flight direction, in deciding the angular velocities for the pairs of communicating UAVs.

Recall that control channel jamming will result in a targeted UAV no longer able to receive commands from the ground control station. In the absence of control commands, a UAV may fly aimlessly or crash to ground. As a mitigation countermeasure, after losing control signals for a specific period of time, a UAV will go into a lost link state and execute a fail-safe protocol. This protocol is a pre-determined procedure which controls a UAV to autonomously perform a set of instruction to achieve a desired state. A fail-safe procedure may guide a UAV to return to its home base, to fly to a pre-determined location, to self-destruct avoiding capture, etc. Practically, a fail-safe protocol is the last resort when all other mitigation countermeasures have failed. In [76], this fail-safe protocol is called roll-back or roll-forward, which returns or forwards the UAV to a safe state.

V. RESEARCH CHALLENGES AND FUTURE WORKS

Based on the survey above, a lot of works have been done in proposing countermeasures against UAV cyberattacks. In the following, we highlight the main research challenges in developing such countermeasures:

- **Limited on-board computation resources:** Due to size and weight constraints, UAVs are typically not equipped with powerful computer. The on-board central processing unit has limited computation power. Therefore, it is not reasonable to expect a UAV to perform any complex algorithm or real-time optimization, as part of a countermeasure against cyberattacks.
- **High dependence on reliable communications:** Regardless of fully autonomous or remotely controlled, UAVs are highly dependent on the availability of reliable communication channels and networks. A UAV needs the communication systems to receive commands or feedback, as well as to transmit its collected data, to its neighbor UAVs and the ground control station. These feedback and collected data may include environmental information, flight statistic, received signal characteristics, etc, which are essential to attack detection by the UAV itself or its neighbor UAVs and control station. Hence, it is not feasible to have a highly effective countermeasure without the support of reliable communications.
- **Information security is necessity:** Ensuring information confidentiality, integrity and authenticity is not an option, but a necessity against UAV cyberattacks. Strong information security can prevent almost all cyberattacks which are launched above physical layer, except some forms of denial-of-service attacks. However, most commercially available off-the-shelf UAVs for civilian applications make use of self-organize private networks, such as Wi-Fi, Bluetooth, Zigbee, etc. Compared to 5G cellular networks, these private networks do not have a strong security protection against illegal connections, malicious control, unauthorized access, and others. Thus, it is a challenge to protect information security of low-cost UAVs operating in private networks.

In the literature, not all the critical research challenges presented above which have been fully addressed. To close the research gap, we suggest a few potential future research works as follows:

- **Real-time flight mission registry and tracking:** Develop an efficient system for a UAV to register and update its flight path in real-time. As such, we can detect UAV misbehavior by tracking its movement and comparing that against the registered flight path. This detection method requires only a simple comparison and thus, is not computationally demanding while compared to various existing methods that detect flight misbehavior through flight control statistics, movement statistics or location statistics (see Table 4).
- **Computationally efficient countermeasures:** Develop prevention, detection and mitigation countermeasures that require only minimal on-board computation resources. This can be achieved by using machine learning or artificial intelligent techniques, which are computationally intensive only during the training stage. For example, after deployment, a trained neural network is a simple mapping function. In this context, the training process must be performed off-board, and the training outcomes can be uploaded to a UAV at its base just before the start of a flight mission. Here, the training process may include the use of adversarial machine learning to model the behaviors of some sophisticated attackers, so that a more robust countermeasure can be developed. When the flight mission takes a long time and is complex, the neural network may be re-trained during the mission. In such a case, the new training outcomes must be remotely uploaded to the UAV through wireless communication channels. This implies a dependence between communication requirement and on-board computation requirement. A lower on-board computation requirement through off-board training, may lead to a higher communication requirement to upload the training outcomes. Thus, there is a need to develop a framework to optimally trade-off computation and communication requirement for a robust countermeasure.
- **Lightweight cryptography:** Develop lightweight cryptographic encryption algorithm for resource limited UAVs. As summarized in Table 3, cryptographic encryption is effective in preventing UAV cyberattacks. Compared to asymmetric cryptography, symmetric cryptography, such as the simple one-time padding algorithm is less computationally complex. However, symmetric cryptography requires a secure and reliable method to distribute the encryption key, which can be known only by the pair of sender and receiver. While the symmetric encryption itself may be computationally simple, the key distribution protocol may be complex. Compared to a traditional communication scenario where the sender and receiver are separated by a distance at fixed locations, UAVs are mobile nodes. Considering communications between a UAV and the ground control station, the UAV may be co-located with the control station before flying away for a mission. We can exploit this unique scenario in developing an efficient key distribution protocol. As an example, we may use a physically secure channel, such as a quantum communication channel to transfer a sufficiently long encryption key to a UAV when it is at the control station. Then, this key will be used in one-time-padding encryption of all messages during the flight mission. The encryption key will be replenished when the UAV returns to the control station at its base.
- **Robust fail-safe protocol:** Develop a fail-safe protocol which is robust against a combination of control channel jamming and navigation message spoofing attack. It has been described earlier that after losing

control channel due to jamming, a UAV may activate its fail-safe protocol to fly autonomously to a pre-determine location. However, a navigation message spoofing may lead the autonomously flying UAV to a wrong location, as dictated by the adversary. In such an extreme case, a robust fail-safe procedure should be able to work without navigation messages. This can be achieved by making the UAV capable of orientating itself by using only information from its environment. For example, UAV can find its direction based on the orientation of sun, moon, and stars, as well as the strength of earth magnetic field.

- **Provide redundancy through swarm of uncorrelated UAVs:** Develop an efficient configuration of a UAV swarm to provide redundancy. In the literature, a UAV swarm has been used as a solution to overcome limitation in on-board resources where each UAV takes a share of computation load in collaboration with other UAVs in achieving a same objective. As an alternative to this collaborative arrangement, we propose to investigate a UAV swarm as a way to provide uncorrelated redundancy. To be uncorrelated, neighboring UAVs may operate in different communication channels, carry different messages and use different flight paths. As such, when a UAV has been compromised in an attack, not all information is leaked and not all communication links are lost.

VI. CONCLUSION

Unmanned aerial vehicle (UAV) will occupy our airspace in an increasing number to support a wide range of commercial and civilian application. As an advanced cyber-physical system, UAVs are targets of cyberattacks. We have identified existing UAV cyberattacks and classified them based on the attack entry points, into six classes, namely channel jamming, message interceptions, message deletion, message injection, message spoofing and on-board system attack. We have further surveyed existing literature for countermeasures against the attacks. We have classified the countermeasures into three classes, namely prevention, detection and mitigation. Such classification is useful because a countermeasure may not be exclusive to an attack class and thus, can be more broadly applicable against other attacks which may not be what it was originally developed for. We have noticed that navigation message (GPS) spoofing attack has the most number of proposed countermeasures. Also, cryptographic encryption is effective in preventing almost all types of attacks launched above physical layer, except some forms of denial-of-service attacks. As the last resort countermeasure, existing fail-safe protocols are important but are not fool-proof. Based on the survey, we have identified a number of remaining research challenges in developing UAV cyberattack countermeasures, and have proposed a number of potential future research works.

REFERENCES

[1] K. L. B. Cook, "The silent force multiplier: The history and role of UAVs in warfare," in *Proc. IEEE Aerosp. Conf.*, Mar. 2007, pp. 1–7.

[2] M. Mozaffari, W. Saad, M. Bennis, Y.-H. Nam, and M. Debbah, "A tutorial on UAVs for wireless networks: Applications, challenges, and open problems," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2334–2360, 3rd Quart., 2019.

[3] A. Fotouhi, H. Qiang, M. Ding, M. Hassan, L. G. Giordano, A. Garcia-Rodriguez, and J. Yuan, "Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3417–3442, 4th Quart., 2019.

[4] Y. Zeng, R. Zhang, and T. J. Lim, "Wireless communications with unmanned aerial vehicles: Opportunities and challenges," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 36–42, May 2016.

[5] N. H. Motlagh, T. Taleb, and O. Arouk, "Low-altitude unmanned aerial vehicles-based Internet of Things services: Comprehensive survey and future perspectives," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 899–922, Dec. 2016.

[6] H. Shakhatreh, A. H. Sawalmeh, A. Al-Fuqaha, Z. Dou, E. Almaita, I. Khalil, N. S. Othman, A. Khreishah, and M. Guizani, "Unmanned aerial vehicles (UAVs): A survey on civil applications and key research challenges," *IEEE Access*, vol. 7, pp. 48572–48634, 2019.

[7] K. Hartmann and K. Giles, "UAV exploitation: A new domain for cyber power," in *Proc. Int. Conf. Cyber Conflict*, May 2016, pp. 205–221.

[8] E. M. Puchaty and D. A. DeLaurentis, "A performance study of UAV-based sensor networks under cyber attack," in *Proc. Int. Conf. Syst. Syst. Eng.*, Jun. 2011, pp. 214–219.

[9] E. Shaikh, N. Mohammad, and S. Muhammad, "Model checking based unmanned aerial vehicle (UAV) security analysis," in *Proc. Int. Conf. Commun., Signal Process. Appl. (ICCSPA)*, Mar. 2021, pp. 1–6.

[10] E. Vattapparamban, I. Guvenc, A. I. Yurekli, K. Akkaya, and S. Uluagac, "Drones for smart cities: Issues in cybersecurity, privacy, and public safety," in *Proc. Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Sep. 2016, pp. 1–6.

[11] R. Altawy and A. M. Youssef, "Security, privacy, and safety aspects of civilian drones: A survey," *ACM Trans. Cyber-Phys. Syst.*, vol. 1, no. 2, pp. 1–25, Feb. 2017.

[12] J.-P. Yaacoub, H. Noura, O. Salman, and A. Chehab, "Security analysis of drones systems: Attacks, limitations, and recommendations," *Internet Things*, vol. 11, pp. 1–38, May 2020.

[13] B. B. Madan, M. Banik, and D. Bein, "Securing unmanned autonomous systems from cyber threats," *J. Defense Model. Simul., Appl., Methodol., Technol.*, pp. 1–17, Feb. 2016.

[14] A. Y. Javaid, W. Sun, V. K. Devabhaktuni, and M. Alam, "Cyber security threat analysis and modeling of an unmanned aerial vehicle system," in *Proc. IEEE Conf. Technol. Homeland Secur. (HST)*, Nov. 2012, pp. 585–590.

[15] V. Kharchenko and V. Torianyk, "Cybersecurity of the Internet of Drones: Vulnerabilities analysis and IMECA based assessment," in *Proc. IEEE 9th Int. Conf. Dependable Syst., Services Technol. (DESSERT)*, May 2018, pp. 364–369.

[16] C. G. L. Krishna and R. R. Murphy, "A review on cybersecurity vulnerabilities for unmanned aerial vehicles," in *Proc. IEEE Int. Symp. Saf., Secur. Rescue Robot. (SSRR)*, Oct. 2017, pp. 194–199.

[17] M. R. Manesh and N. Kaabouch, "Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions," *Comput. Secur.*, vol. 85, pp. 386–401, Aug. 2019.

[18] F. A. G. Muzzi, P. R. D. M. Cardoso, D. F. Pigatto, and K. R. L. J. C. Branco, "Using botnets to provide security for safety critical embedded systems—A case study focused on UAVs," *J. Phys., Conf. Ser.*, vol. 633, Sep. 2015, Art. no. 012053.

[19] A. Y. Javaid, W. Sun, and M. Alam, "UAVSim: A simulation testbed for unmanned aerial vehicle network cyber security analysis," in *Proc. IEEE Globecom Workshops*, Dec. 2013, pp. 1432–1436.

[20] *VideoJak*. Accessed: Aug. 31, 2021. [Online]. Available: http://videojak.sourceforge.net

[21] L. He, W. Li, C. Guo, and R. Niu, "Civilian unmanned aerial vehicle vulnerability to GPS spoofing attacks," in *Proc. 7th Int. Symp. Comput. Intell. Design*, Dec. 2014, pp. 212–215.

[22] S. M. Giray, "Anatomy Of unmanned aerial vehicle hijacking with signal spoofing," in *Proc. Int. Conf. Recent Adv. Space Technol. (RAST)*, Jun. 2013, pp. 795–800.

[23] T. Humphreys, ''Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil GPS spoofing,'' Submission Subcommittee Oversight, Invest., Manage. House Committee Homeland Secur., Univ. Texas, Austin, TX, USA, Tech. Rep., Jul. 2012.

[24] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, ''Unmanned aircraft capture and control via GPS spoofing,'' *J. Field Robot.*, vol. 31, no. 4, pp. 617–636, Jul. 2014.

[25] T.-H. Kim, C. S. Sin, and S. Lee, ''Analysis of effect of spoofing signal in GPS receiver,'' in *Proc. Int. Conf. Control, Automat. Syst. (ICCAS)*, Oct. 2012, pp. 2083–2087.

[26] M. Hooper, Y. Tian, R. Zhou, B. Cao, P. A. Lauf, L. Watkins, H. W. Robinson, and W. Alexis, ''Securing commercial WiFi-based UAVs from common security attacks,'' in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Nov. 2016, pp. 1213–1218.

[27] *Aircrack-ng*. Accessed: Aug. 31, 2021. [Online]. Available: https://www.aircrack-ng.org

[28] D. He, S. Chan, and M. Guizani, ''Communication security of unmanned aerial vehicles,'' *IEEE Wireless Commun.*, vol. 24, no. 4, pp. 134–139, Aug. 2017.

[29] O. Westerlund and R. Asif, ''Drone hacking with raspberry-pi 3 and WiFi pineapple: Security and privacy threats for the Internet-of-Things,'' in *Proc. 1st Int. Conf. Unmanned Vehicle Syst.-Oman (UVS)*, Feb. 2019, pp. 1–10.

[30] *SkyKack*. Accessed: Aug. 31, 2021. [Online]. Available: https://github.com/samyk/skyjack

[31] M. Strohmeier, M. Schafer, V. Lenders, and I. Martinovic, ''Realities and challenges of nextgen air traffic management: The case of ADS-B,'' *IEEE Commun. Mag.*, vol. 52, no. 5, pp. 111–118, May 2014.

[32] P. Pierpaoli, M. Egerstedt, and A. Rahmani, ''Altering UAV flight path by threatening collision,'' in *Proc. IEEE/AIAA 34th Digit. Avionics Syst. Conf. (DASC)*, Sep. 2015, pp. 1–10.

[33] K. Mansfield, T. Eveleigh, T. H. Holzer, and S. Sarkani, ''Unmanned aerial vehicle smart device ground control station cyber security threat model,'' in *Proc. IEEE Int. Conf. Technol. Homeland Secur. (HST)*, Nov. 2013, pp. 722–728.

[34] Y. Son, H. Shin, D. Kim, Y. Park, J. Noh, K. Choi, J. Choi, and Y. Kim, ''Rocking drones with intentional sound noise on gyroscopic sensors,'' in *Proc. USENIX Conf. Secur. Symp.*, Aug. 2015, pp. 881–896.

[35] D. Davidson, H. Wu, R. Jellinek, T. Ristenpart, and A. V. Singh, ''Controlling UAVs with sensor input spoofing attacks,'' in *Proc. USENIX Workshop Offensive Technol. (WOOT)*, Aug. 2016, pp. 1–11.

[36] J. A. Steinmann, R. F. Babiceanu, and R. Seker, ''UAS security: Encryption key negotiation for partitioned data,'' in *Proc. Integr. Commun. Navigat. Surveill. (ICNS)*, Apr. 2016, pp. 1–7.

[37] M. Podhradsky, C. Coopmans, and N. Hoffer, ''Improving communication security of open source UAVs: Encrypting radio control link,'' in *Proc. Int. Conf. Unmanned Aircr. Syst. (ICUAS)*, Jun. 2017, pp. 1153–1159.

[38] C. Liu, T. Q. S. Quek, and J. Lee, ''Secure UAV communication in the presence of active eavesdropper,'' in *Proc. Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Nanjing, China, Oct. 2017, pp. 1–6.

[39] G. Zhang, Q. Wu, M. Cui, and R. Zhang, ''Securing UAV communications via trajectory optimization,'' in *Proc. IEEE Global Commun. Conf. (Globecom)*, Dec. 2017, pp. 1–6.

[40] N. M. Rodday, R. D. O. Schmidt, and A. Pras, ''Exploring security vulnerabilities of unmanned aerial vehicles,'' in *Proc. IEEE/IFIP Netw. Oper. Manage. Symp. (NOMS)*, Apr. 2016, pp. 993–994.

[41] I. J. Jensen, D. F. Selvaraj, and P. Ranganathan, ''Blockchain technology for networked swarms of unmanned aerial vehicles (UAVs),'' in *Proc. IEEE 20th Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2019, pp. 1–7.

[42] P. Mehta, R. Gupta, and S. Tanwar, ''Blockchain envisioned UAV networks: Challenges, solutions, and comparisons,'' *Comput. Commun.*, vol. 151, pp. 518–538, Feb. 2020.

[43] I. García-Magariño, R. Lacuesta, M. Rajarajan, and J. Lloret, ''Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain,'' *Ad Hoc Netw.*, vol. 86, pp. 72–82, Apr. 2019.

[44] E. Ghribi, T. T. Khoei, H. T. Gorji, P. Ranganathan, and N. Kaabouch, ''A secure blockchain-based communication approach for UAV networks,'' in *Proc. IEEE Int. Conf. Electro Inf. Technol. (EIT)*, Jul. 2020, pp. 411–415.

[45] A. A. Khan, M. M. Khan, K. M. Khan, J. Arshad, and F. Ahmad, ''A blockchain-based decentralized machine learning framework for collaborative intrusion detection within UAVs,'' *Comput. Netw.*, vol. 196, Sep. 2021, Art. no. 108217.

[46] D. Borio and C. Gioia, ''Real-time jamming detection using the sum-of-squares paradigm,'' in *Proc. Int. Conf. Location GNSS (ICL-GNSS)*, Jun. 2015, pp. 1–6.

[47] H. Sedjelmaci, S. M. Senouci, and M.-A. Messous, ''How to detect cyber-attacks in unmanned aerial vehicles network?'' in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2016, pp. 1–6.

[48] H. Sedjelmaci, S. M. Senouci, and N. Ansari, ''A hierarchical detection and response system to enhance security against lethal cyber-attacks in UAV networks,'' *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 48, no. 9, pp. 1594–1606, Sep. 2018.

[49] R. Shrestha, A. Omidkar, S. A. Roudi, R. Abbas, and S. Kim, ''Machine-learning-enabled intrusion detection system for cellular connected UAV networks,'' *Electronics*, vol. 10, pp. 1–28, Jun. 2021.

[50] Z. Birnbaum, A. Dolgikh, V. Skormin, E. O'Brien, and D. Muller, ''Unmanned aerial vehicle security using recursive parameter estimation,'' in *Proc. Int. Conf. Unmanned Aircr. Syst. (ICUAS)*, May 2014, pp. 692–701.

[51] J. McNeely, M. Hatfield, A. Hasan, and N. Jahan, ''Detection of UAV hijacking and malfunctions via variations in flight data statistics,'' in *Proc. IEEE Int. Carnahan Conf. Secur. Technol. (ICCST)*, Oct. 2016, pp. 1–8.

[52] K. Xiao, J. Zhao, Y. He, C. Li, and W. Cheng, ''Abnormal behavior detection scheme of UAV using recurrent neural networks,'' *IEEE Access*, vol. 7, pp. 110292–110305, 2019.

[53] R. Mitchell and I.-R. Chen, ''Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications,'' *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 44, no. 5, pp. 503–604, May 2014.

[54] L. Wu and X. Cao, ''Geo-location estimation from two shadow trajectories,'' in *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2010, pp. 585–590.

[55] I. N. Junejo and H. Foroosh, ''GPS coordinates estimation and camera calibration from solar shadows,'' *Comput. Vis. Image Understand.*, vol. 114, no. 9, pp. 991–1003, Sep. 2010.

[56] T. Brandon Carroll, ''Using motion fields to estimate video utility and detect GPS spoofing,'' M.S. thesis, Dept. Elect. Comput. Eng., Brigham Young Univ., Provo, UT, USA, 2012.

[57] D. M. Akos, ''Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC),'' *Navigation*, vol. 59, no. 4, pp. 281–290, Oct. 2012.

[58] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, ''Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer,'' in *Proc. ION Int. Tech. Meeting*, Jan. 2009, pp. 124–130.

[59] J. Magiera and R. Katulski, ''Detection and mitigation of GPS spoofing based on antenna array processing,'' *J. Appl. Res. Technol.*, vol. 13, no. 1, pp. 45–47, Feb. 2015.

[60] M. R. Manesh, J. Kenney, W. C. Hu, V. K. Devabhaktuni, and N. Kaabouch, ''Detection of GPS spoofing attacks on unmanned aerial systems,'' in *Proc. 16th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2019, pp. 1–6.

[61] A. Ranganathan, H. Ólafsdóttir, and S. Capkun, ''SPREE: A spoofing resistant GPS receiver,'' in *Proc. ACM Conf. Mobile Comput. Netw. (MOBICOM)*, Oct. 2016, pp. 348–360.

[62] Q. Zou, S. Huang, F. Lin, and M. Cong, ''Detection of GPS spoofing based on UAV model estimation,'' in *Proc. IEEE Conf. Ind. Electron. Soc. (IECON)*, Oct. 2016, pp. 6097–6102.

[63] G. Panice, S. Luongo, G. Gigante, D. Pascarella, C. Di Benedetto, A. Vozella, and A. Pescape, ''A SVM-based detection approach for GPS spoofing attacks to UAV,'' in *Proc. 23rd Int. Conf. Autom. Comput. (ICAC)*, Sep. 2017, pp. 1–11.

[64] S. Leyuan, H. Wende, Z. Yifan, W. Yueke, and Y. Jun, ''GPS spoofing detection of unmanned aerial vehicles by dynamics identification,'' in *Proc. IEEE CSAA Guid., Navigat. Control Conf. (CGNCC)*, Aug. 2018, pp. 1–6.

[65] K. A. Kramer and S. C. Stubberud, ''Fuzzy evidence accrual for GPS navigation protection of UAVs,'' in *Proc. IEEE AESS Eur. Conf. Satell. Telecommun. (ESTEL)*, Oct. 2012, pp. 1–7.

[66] M. S. Faughnan, J. B. Hourican, G. C. MacDonald, M. Srivastava, A. J.-P. Wright, Y. Y. Haimes, E. Andrijcic, Z. Guo, and C. J. White, ''Risk analysis of unmanned aerial vehicle hijacking and methods of its detection,'' in *Proc. IEEE Syst. Inf. Eng. Design Symp.*, Apr. 2013, pp. 145–150.

[67] K. Jansen, M. Schafer, D. Moser, V. Lenders, C. Popper, and J. Schmitt, ''Crowd-GPS-Sec: Leveraging crowdsourcing to detect and localize GPS spoofing attacks,'' in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2018, pp. 1–14.

[68] H. Lee, S. Eom, J. Park, and I. Lee, ''UAV-aided secure communications with cooperative jamming,'' *IEEE Trans. Veh. Commun.*, vol. 67, no. 10, pp. 9385–9392, Oct. 2018.

[69] J. Daubert, D. Boopalan, M. Muhlhauser, and E. Vasilomanolakis, ''HoneyDrone: A medium-interaction unmanned aerial vehicle honeypot,'' in *Proc. IEEE/IFIP Netw. Oper. Manage. Symp. (NOMS)*, Apr. 2018, pp. 1–6.

[70] H. Reyes and N. Kaabouch, ''Improving the reliability of unmanned aircraft system wireless communications through cognitive radio technology,'' *Commun. Netw.*, vol. 5, no. 3, pp. 225–230, 2013.

[71] H. Reyes, N. Gellerman, and N. Kaabouch, "A cognitive radio system for improving the reliability and security of UAS/UAV networks," in *Proc. IEEE Aerosp. Conf.*, Mar. 2015, pp. 1–9.

[72] R. Johansson, P. Hammar, and P. Thoren, ''On simulation-based adaptive UAS behavior during jamming,'' in *Proc. Workshop Res., Educ. Develop. Unmanned Aerial Syst. (RED-UAS)*, Oct. 2017, pp. 78–83.

[73] A. Eldosouky, A. Ferdowsi, and W. Saad, ''Drones in distress: A game-theoretic countermeasure for protecting UAVs against GPS spoofing,'' *IEEE Internet Things J.*, vol. 7, no. 4, pp. 2840–2854, Apr. 2020.

[74] T. Zhang and Q. Zhu, ''Strategic defense against deceptive civilian GPS spoofing of unmanned aerial vehicles,'' in *Proc. Int. Conf. Decis. Game Theory Secur.*, Oct. 2017, pp. 213-233.

[75] S. Bhattacharya and T. Basar, ''Game-theoretic analysis of an aerial jamming attack on a UAV communication network,'' in *Proc. Amer. Control Conf.*, Jun. 2010, pp. 818–823.

[76] S. Hagerman, A. Andrews, and S. Oakes, ''Security testing of an unmanned aerial vehicle (UAV),'' in *Proc. Cybersec. Symp. (CYBERSEC)*, Apr. 2016, pp. 1–6.

PENG-YONG KONG (Senior Member, IEEE) received the B.Eng. degree (Hons.) in electrical and electronic engineering from Universiti Sains Malaysia and the Ph.D. degree in electrical and computer engineering from the National University of Singapore. He is currently an Associate Professor with the Electrical Engineering and Computer Science Department, Khalifa University, Abu Dhabi, United Arab Emirates. He was previously an Adjunct Assistant Professor at the Electrical and Computer Engineering Department, National University of Singapore, concurrent to the appointment of Research Scientist at the Institute for Infocomm Research, Agency for Science, Technology and Research, Singapore. He was an Engineer with Intel Malaysia. His research interests include in the broad area of computer and communication networks, as well as cyber-physical systems.