Journal of Systems Architecture 138 (2023) 102870

Contents lists available at ScienceDirect

Journal of Systems Architecture

journal homepage: www.elsevier.com/locate/sysarc

A survey on cybersecurity attacks and defenses for unmanned aerial systems ☆

Zhaoxuan Wang [a], Yang Li [b,*], Shihao Wu [b], Yuan Zhou [c], Libin Yang [a], Yuan Xu [c], Tianwei Zhang [c], Quan Pan [b]

[a] School of Cybersecurity, Northwestern Polytechnical University, Xi'an 710129, China
[b] School of Automation, Northwestern Polytechnical University, Xi'an 710129, China
[c] School of Computer Science and Engineering, Nanyang Technological University, Singapore, 639798, Singapore

ARTICLE INFO

Keywords:
UAS
Cybersecurity
Threat assessment
Software security
Artificial intelligence

ABSTRACT

In recent years, unmanned aerial systems (UAS) have been widely used in both military and civilian fields. However, their open-source software and protocols have made their security vulnerable, resulting in a growing number of cybersecurity issues. This paper provides a comprehensive review of UAS cybersecurity research, with a focus on attack and defense technologies. Regarding UAS being a system that integrates software and hardware and can work independently with complex tasks, this paper analyzes the UAS architecture and classifies security threats into four categories: communication network security, software security, payload security, and intelligent security. Additionally, it provides an overview of existing threat assessment methods. This paper also highlights representative research progress in UAS cyberattacks and defense technologies in the four identified categories. Finally, this paper examines the current research status and future prospects of UAS cybersecurity.

1. Introduction

With the rapid development of electronic information and autonomous driving, the application scale of UAVs in the military, civil, industrial, and consumer fields has continued to expand. For example, UAVs have been widely used in aerial photography, agricultural plant protection [1], express delivery [2], and remote sensing mapping [3] etc., which further unleashes their application value and market prospects. Based on parameters such as flight range, flight altitude, and load capacity, UAVs can be divided into five types: high-altitude long-endurance (HALE) UAVs, medium-altitude long-endurance (MALE) UAVs, tactical UAVs (TUAV), small UAVs (SUAV) and miniature UAVs (MAV). Table 1 [4] describes the performance parameters of various types of UAV platforms.

Since Iran successfully captured the U.S. RQ-170 drone through global positioning system (GPS) spoofing technology in 2011 [5], more and more UAS attacks have emerged, and the issue of UAV cybersecurity has become increasingly prominent. From the perspective of system architecture, The vulnerability of UAS extends beyond the UAV itself and encompasses its supporting systems, such as communication networks and ground-based stations, etc. Therefore, securing UAS involves not only protecting the UAV but also safeguarding its entire system against potential attacks. The potential threats of UAS include attacks on communication networks [6], software systems [7], payload systems [8], and intelligent applications and algorithms [9]. These attacks can undermine the confidentiality, integrity, and availability of UAS, leading to data loss in minor cases, crashing in major cases, and even threatening the lives and property on the ground, a.k.a., an attacked drone can be compared vividly to a "flying incendiary bomb".

More specifically, cybersecurity threats to UAS primarily involve their software and hardware devices, such as flight control software, communication protocols, sensors, and operating systems. Since most of these devices are developed with common chips, open-source operating systems, universal protocols, and software architectures, and are designed on the principles of user-friendly and affordability, their security is often overlooked. As a result, UAS have obvious security vulnerabilities, making them susceptible to malicious attacks, which will inevitably pose a major threat to the security of the UAS and seriously hinder the healthy development of the UAS industry. Hence, it is crucial to detect and prevent any potential threats from causing damage.

Although progress has been made in cybersecurity, providing some technical support for UAS to deal with security threats. However, these

☆ This research is supported by the National Natural Science Foundation of China (No. 62103330, No. 62233014, No. 62203358), and the Fundamental Research Funds for the Central Universities of China (3102021ZDHQD09).

* Corresponding author.
E-mail addresses: zxwang@mail.nwpu.edu.cn (Z. Wang), liyangnpu@nwpu.edu.cn (Y. Li), wshnpu@mail.nwpu.edu.cn (S. Wu), y.zhou@ntu.edu.sg (Y. Zhou), libiny@nwpu.edu.cn (L. Yang), xu.yuan@ntu.edu.sg (Y. Xu), tianwei.zhang@ntu.edu.sg (T. Zhang), quanpan@nwpu.edu.cn (Q. Pan).

https://doi.org/10.1016/j.sysarc.2023.102870
Received 18 December 2022; Received in revised form 12 March 2023; Accepted 29 March 2023
Available online 3 April 2023

Table 1
Classification and performance parameters of UAV that cited from [4].

Type of UAV	Flight altitude (m)	Flight range (km)	Load capacity (kg)
HALE	>9100	NA	400–2000
MALE	<9100	<200	60–400
TUAV	<5500	<160	5–150
SUAV	<3000	<50	5–50
MAV	<1500	<10	0–5

works are mainly designed for static computer systems with relatively fixed locations. This makes it difficult to meet the high-security demands of dynamic, complex, real-time, and intelligent UAS. As the UAS not only involves Ethernet communication, but also satellite communication, bus communication, and electromagnetic communication. Furthermore, UAS are not only on-board operating systems but also equipped with ground station operating systems and various sensors and payloads. More importantly, the discovery of artificial intelligence (AI) algorithms vulnerabilities brings unique security threats to UAS, particularly in mission execution and navigation control while enhancing its autonomy. Therefore, to better understand the current research status of UAS cybersecurity and improve the security protection system, this paper reviews the attack and defense (including detection, identification, and mitigation of attacks) technologies in the UAS cybersecurity research. To the best of our knowledge, this work should be the first Comprehensive and systematic review article on UAS in attack and defense research.

This paper is organized as follows: in Section 2, an overview of UAS architecture, security vulnerabilities, and threat assessment methods are presented. Then we outline the cyberattacks and defense technologies of the UAS in four aspects: communication network security in Section 3, software security in Section 4, payload security in Section 5 and machine-learning-based security in Section 6 respectively. Then we discuss the current development technique, and recommendations for future research directions in Section 7. Finally, we conclude our work in Section 8. The outline of this paper is shown in Fig. 1.

Comparisons with existing surveys. A number of excellent works also conduct surveys related to robotic vehicles (RV) or UAVs [10–21]. However, they are significantly different from this paper. Some papers focus on malicious drone detection [10], privacy, security policies and regulations [11,12], while only a small amount of space is devoted to describing attack and defense technologies, especially without focusing on the role of AI in UAS attack and defense. Some papers outline UAS cybersecurity threats mainly from an engineering perspective while neglecting academic approaches [13–15]. Some papers focus on component security issues of UAS (e.g. communication networks), [16–19] or general security and safety issues in autonomous driving systems, especially autonomous vehicles [20,21], and lack analysis of the specific unmanned aerial system. Differently, we explicitly target UAS and review attack and defense methods proposed by academia and industry. The main presentation details the threat assessment methods and analyzes the security problems at various levels from the perspective of UAS architecture. It gives a comprehensive view of the relationship between attacks and system vulnerabilities using a threat model. In particular, we explore the threats to UAS security from the application of artificial intelligence and their use in security protection. For general attack methods, we also analyze their implementation on UAS and the possible impact on them.

2. UAS basics

In this section, we begin by presenting the classification and architecture of UAS, and then proceed to examine the cybersecurity threats at various levels by analyzing the UAS architecture. Lastly, we outline the threat assessment methods for UAS cybersecurity.

2.1. UAS architecture

The commonly used UAS architecture is shown in Fig. 2. From the perspective of information systems, a standard UAS consists of five parts: sensor system, flight control and navigation system, communication network, ground control station (GCS), and command and control system. Its system architecture model is shown in Fig. 3.

The Sensor System is a device that senses the flight environment and converts the detected information into a specific form of an electrical signal or another specific signal for output, usually including external sensors and built-in sensors for flight control and navigation. Built-in sensing devices usually referred to as Inertial Measurement Units (IMU), including accelerometers, gyroscopes, magnetometers, barometers, etc., ensure the normal operation of the flight control and navigation system. External sensing devices include vision sensors, optical flow sensors, GPS, Lidar, and Automatic Dependent Surveillance-Broadcast (ADS-B) sensors, etc., providing a closer guarantee for the flight safety of UAVs. The external sensors are important parts of the UAV's Sense and Avoidance (SAA) function that is used for ensuring flight safety.

The Flight Control and Navigation System of UAS controls the sensors, navigation, and communication systems of the UAV, and is a key part for communication between components. Functioning as the "operating system", it typically employs an ARM-based, MIPS-based, or Performance Optimization With Enhanced RISC - Performance Computing (PowerPC) CPU as the main control chip. In terms of software operating systems, consumer UAVs mostly use embedded operating systems such as Linux, Open WRT, Android, and Microsoft IoT. Some medium and large UAVs use the VxWorks operating system for flight control. Most motherboards of flight control and navigation systems reserve development interfaces such as USB, JTAG, and UART for manufacturers and users to develop or debug.

Communication Networks can be divided into two components: the external communication network and the internal communication network. As shown in Fig. 4, the external communication network typically encompasses networks for data transmission between UAVs and ground stations (①) or satellites (②), mobile Ad Hoc networks (③), and application networks such as cellular networks and auxiliary communication networks (④). The basic component of these communication networks is the data link. The direction is divided into uplink for sending control signals and downlink for telemetry data return. According to the connection object, it can be divided into control links (e.g., ground control system data link, remote control data link)and data links (e.g., global positioning system data link, inter-machine data link, ADS-B data link). For internal communication networks, UAVs typically employ a Bus architecture to physically connect Electronic Control Units (ECU) for distributed real-time control and multi-way transmission of onboard data. ECUs on UAVs usually include steering gear, engine, controller, power supply, sensors, etc.

GCS is a channel for ground operators to directly exchange information with the UAV. It integrates control, communication, and data processing, and mainly completes the data collection and monitoring of the UAV's flight status. GCS is generally composed of one or more portable computers, mainly equipped with operating software developed based on Windows or Linux. Ground operators can complete mission planning, flight playback, and real-time monitoring through the ground station. At present, the common open source GCS are MissionPlanner [22] and QGroundControl [23].

The Command and Control System is generally used in strategic-level HALE and MALE UAVs and is mainly used to control, operate and manage the flight of UAVs. The specific contents include: monitoring the flight process and flight track of the aircraft, ensuring the normal operation of the communication link, launching and recovering the aircraft, completing the combat mission, and collecting the information of the GCS.

However, more devices means more risk points. Section 2.2 will give a systematic analysis of UAS based on these devices.

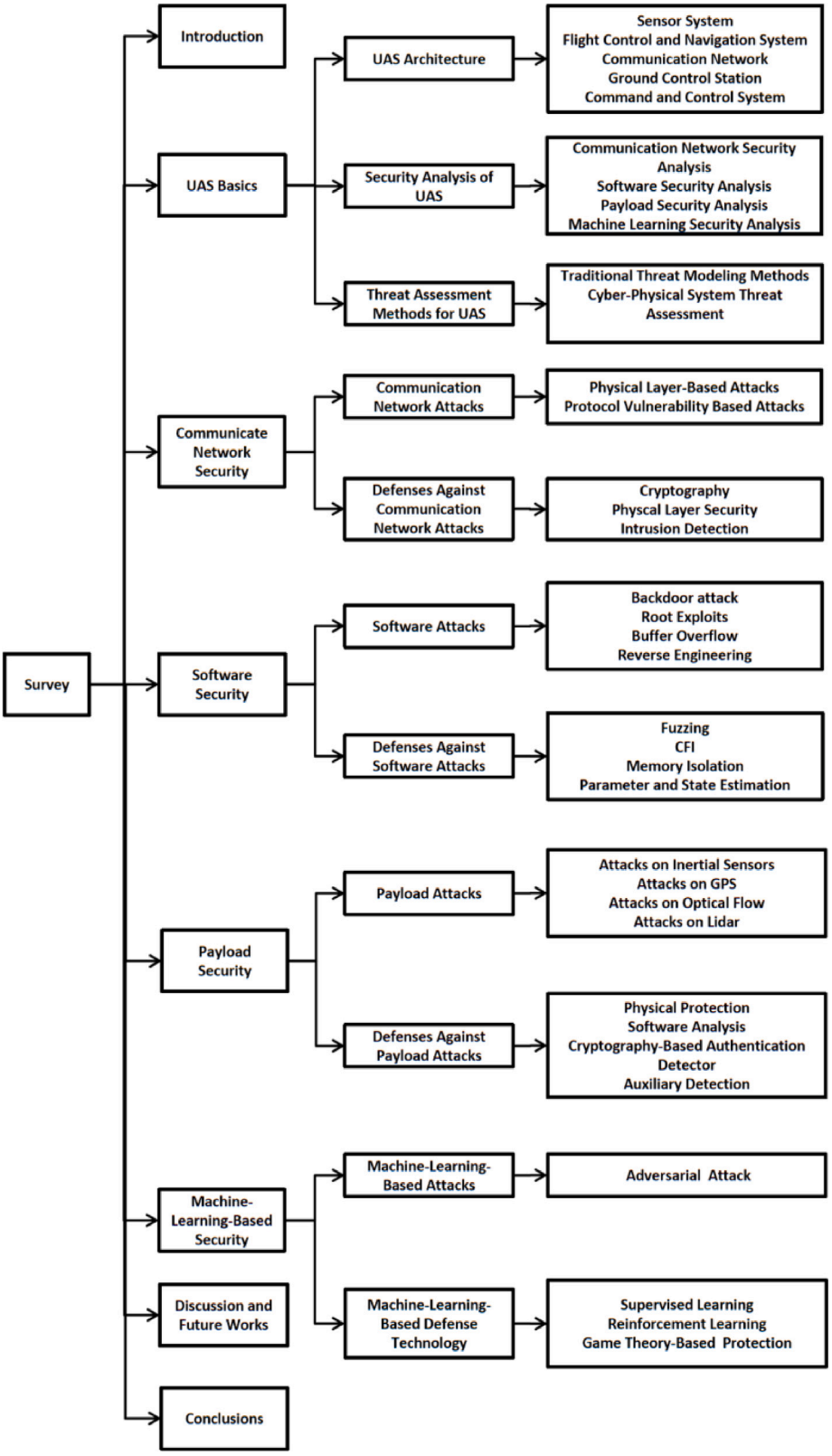


Fig. 1. Outline of the paper.

2.2. Security analysis of UAS

A typical UAS is a complex information system that integrates hardware and software, capable of functioning independently, and supports a wide range of applications, such as environmental information fusion, collaborative control, and intelligent decision-making. Due to the system's complexity, the vulnerabilities that may occur within it can often be intricate, involving multiple components of the UAS. Therefore, it is important to give a clear perspective of its security issues. We conduct a systematic security analysis of the UAS, which

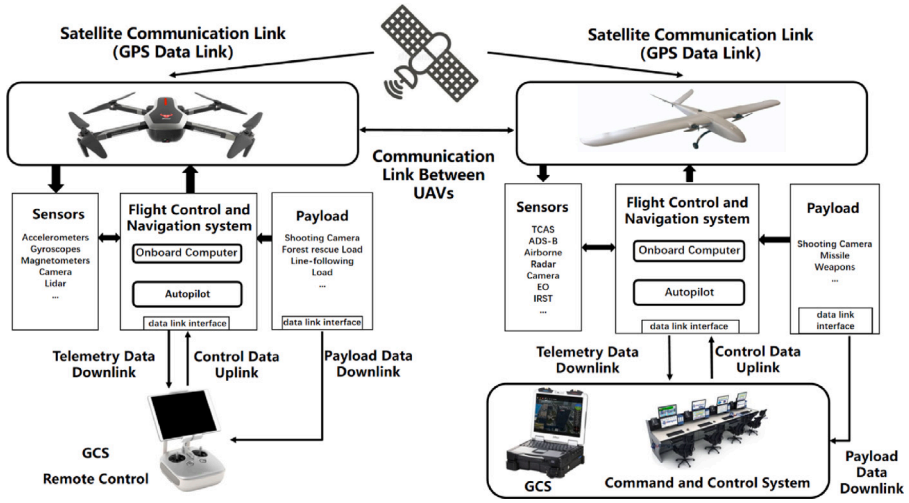


Fig. 2. UAS architecture.

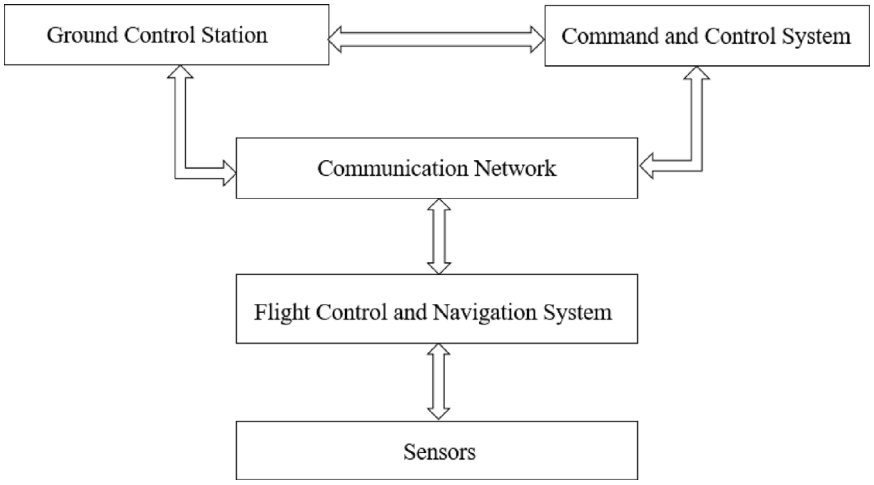


Fig. 3. UAS system architecture model.

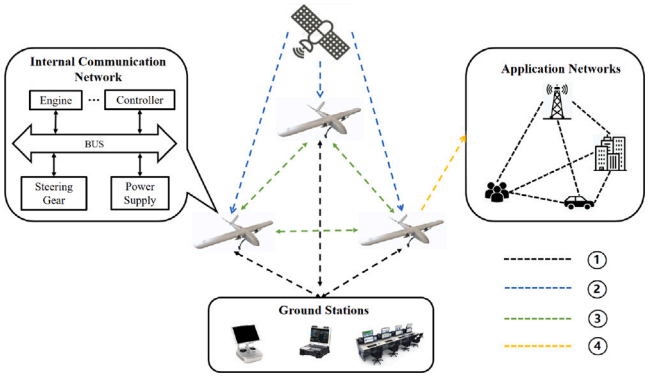


Fig. 4. Communication network architecture.

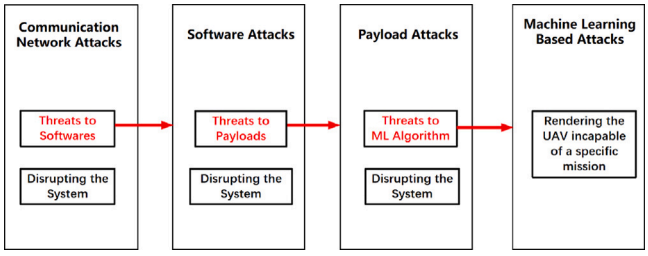
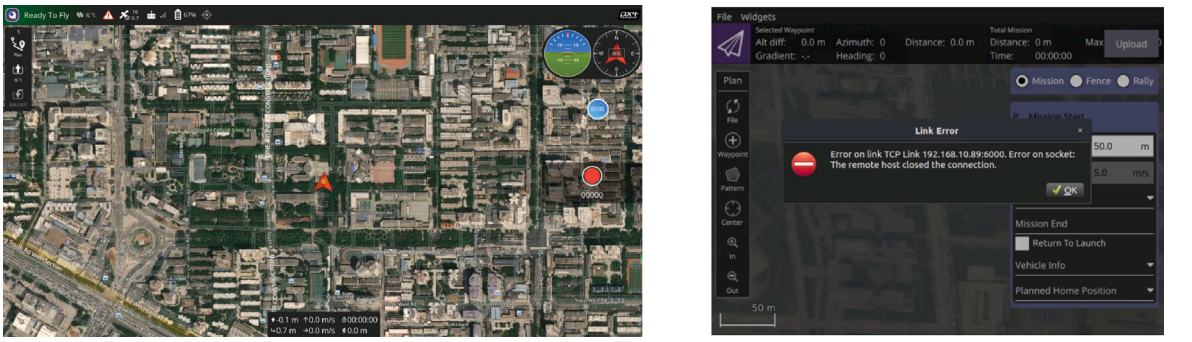


Fig. 5. Interactions in four security threats.

enables us to gain a clear understanding of the most dangerous and potentially intrusive vulnerabilities in such a complex cyber–physical system. It helps to understand the causes of attacks and the relationship between the attacks and the various layers of UAS, and thus to avoid potential risks. More specifically, we sort out the security threats in four aspects of communication network security, software security, payload security, and machine learning-based security. These methods are both distinctive and interactive. The first three attacks are primarily aimed at disrupting the UAS itself, whereas the last one is more focused on rendering the UAV incapable of a specific mission. Fig. 5 shows the interactions in these four security threats. Further details regarding the threat models will be presented in Sections 3 to 6.

2.2.1. *Communication network security analysis*

The main security threats in the communication network of the UAS are data security and application security. First of all, the communication network uses electromagnetic signals as the data transmission medium. This communication environment is generally open and has



(a) An Example of Normal QGC Interface (b) An Example of QGC Interface under DOS Attack

Fig. 6. An example of DOS attack.

different standards (e.g., IEEE 802.11, Radio Frequency, Bluetooth, Cellular Network et al.), which are designed at the beginning considering only transmission efficiency and lacking effective data encryption and authentication methods. Even if some UAVs use encryption or authentication strategies, most of them are unreliable private cryptographic algorithms and authentication protocols. These algorithms and protocols have not been verified for long-term security, and there are often security vulnerabilities in logic and implementation. The above problems make the communication network vulnerable to eavesdropping [24], tampering [25], replaying [6] and other attacks, which make the information transmitted in the network easy to be intercepted, resulting in the data leakage of images, videos, and even control information [6].

Secondly, there are various transmission protocols (e.g., Mavlink, WiFi, Xbee, CAN, etc.) used in the UAS communication network, which lacks unified security transmission standards. The vulnerabilities in the protocols will also cause the leakage of control information. For example, the authenticate data packages can be used to authenticate the communication between the controller and UAV. The leak of these packages can result in the UAS be vulnerable to attacks such as spoofing, Denial-of-Service (DOS), and control hijacking [26], causing the loss of communication, or the illegal takeover by the attacker. We conducted DOS attack experiment on a UAV and demonstrated the effect of communication loss on QGC (shown in Fig. 6). Moreover, as shown in Fig. 5, the attackers may exploit vulnerabilities to launch software attacks.

2.2.2. Software security analysis

The command and control system, flight control, navigation system, and GCS all rely on software platforms to ensure the proper operation of the UAV flight, mission execution, information acquisition, and data return. As such, these software platforms constitute a crucial aspect of the overall UAS. However, these systems also encounter serious software security challenges. Firstly, the software is an executable program, and most UAV software is either off-the-shelf products or developed based on open-source frameworks, which inevitably leads to some vulnerabilities [27] or backdoors [28]. Secondly, the majority of the software operating environments are either Windows or Linux, both of which are known to have system vulnerabilities [29]. Therefore, attackers can analyze and exploit to attack the system, such as overflow attacks [28], unauthorized access attacks, illegal function execution [30], etc., leading to problems such as system freezes, crashes, leakage of key files, and even the seizure of control.

In addition to the security threats of the system and the software itself, there are also plenty of communication interactions and human–computer interaction behaviors in the process of using this software. As a result, problems such as untrustworthy data and authentication flaws may arise. More realistically, due to the relative closure and independence of UAS platforms (e.g., GCS and command and control

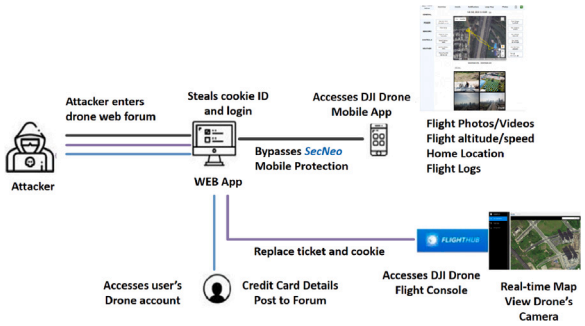


Fig. 7. Attacking drones through social engineering that cited from [33].

systems), their updates and maintenance generally lag behind, which leads to inadequate access control means and weak configuration [31]. These problems increase the possibility of software vulnerabilities being discovered and exploited. For example, malicious attackers can use social engineering methods such as email phishing, psychological exploitation, information mining, and supply chain attacks to gain access to UAV-sensitive information [32]. Authentication flaws are then exploited to bypass authentication mechanisms in order to gain advanced privileges. Fig. 7 [33] shows the attack flow of an attacker using social engineering to steal data from a DJI drone through a drone network forum. All of these possible attacks increase the security risks faced by UAS. What is more, these vulnerabilities can also be exploited to launch attacks on the sensor system.

2.2.3. Payload security analysis

From the perspective of aircraft structure design, a UAV can be divided into three parts: the engine, the aircraft body, and the flight payload. Among them, the flight payload is the equipment that is equipped on the UAV, independent of the aircraft body, and to complete a specific task, such as flight steering gear, motor, sensor equipment, etc. As an important part of the UAV payload, the sensor system faces serious data security problems. These payloads lack the necessary authentication mechanism in actual operation, and coupled with technical and cost constraints, UAV payloads often face the risk of availability. At the same time, in order to emphasize the real-time nature of data transmission, payload data transmission also lacks encryption. Therefore, the UAV payload also faces the risk of data integrity and confidentiality. In addition, the UAV payload does not have the ability to actively detect and respond to abnormal attacks. For these payload vulnerabilities, attackers can send jamming signals to sensors to disable sensor functions or send intentionally constructed false data to sensors for spoofing attacks, such as GPS spoofing attacks [8], acoustic signal injection attacks [34–36], and transfer attacks [37], stealthy attacks [38], etc., leading to incorrect decisions during position calculation and flight

navigation of UAVs. Besides, as shown in Fig. 5, these vulnerabilities make payloads the entrance for machine-learning-based attacks. In conclusion, these payload attacks seriously threaten the flight safety of UAVs.

2.2.4. Machine learning security analysis

In recent years, the next-generation of artificial intelligence has developed rapidly and has been widely used for tasks such as sense and avoidance [39], autonomous navigation [40], object detection and tracking [41,42]. The application of AI has gradually made UAVs highly intelligent unmanned flight cyber systems. However, the gradual emergence of security threats such as data-based adversarial attacks [43,44], data poisoning [45], and model tampering [46,47] has made artificial intelligence, especially machine learning algorithms increasingly vulnerable. For these reasons, the increasing intelligence and autonomous capabilities of UAVs, coupled with their complex application environments and target missions, make their cyber systems more vulnerable to attacks. To make a better understanding of the vulnerabilities that exist in machine learning algorithms in UAS, this paper summarizes the application of machine learning in UAS cybersecurity as machine-learning-based security problems, which can be divided into two aspects. On the one hand, as a novel technology, machine learning can be widely used in the attack detection and mitigation of UAS, enabling it to have a more intelligent malicious attack defense capability. On the other hand, As mentioned previously, although machine learning helps in securing UAS, its own vulnerability introduces a new kind of risk to the algorithm's security. Since most of the machine learning algorithms carried by UAVs are not designed with robustness and security in mind, they are extremely vulnerable to malicious adversarial attacks such as "data poisoning" and "backdoor attacks". These attacks can use camera [48], optical flow [49], Lidar [50], and other loads as the entrance to interfere with the correct output of algorithms, so as to have a huge impact on UAS intelligent applications such as environmental perception, obstacle avoidance, and autonomous flight.

2.3. Threat assessment methods for UAS

Threat assessment refers to the process of systematically examining cyber systems, identifying existing security vulnerabilities, and evaluating the threat level of the vulnerabilities and the possibility of being exploited. In recent years, with the continuous development of UAS, the research on its cybersecurity has received extensive attention from scholars. At present, the vulnerability assessment method for UAS has not yet formed a standard research system. One analysis method is to carry out risk identification and threat assessment through traditional threat modeling methods. For example, Mansfield et al. [51] analyzed cybersecurity vulnerabilities that exist in communication networks, software programs, hardware, and insider threats. They developed a threat profile for GCS based on risks, which helped to fill a gap in the threat model approach. Katharina et al. [52] conducted a comprehensive analysis of UAV attacks, considering three key dimensions: attack surface, attack method, and attack target. Through this analysis, they proposed the attack vector of UAS. This method combines the kill chain with the STRIDE threat model.[1] Threats to UAS can be assessed from an offensive and defensive perspective. For example, Hartmann et al. [53] proposed a system architecture-based threat assessment method to achieve risk assessment of military UAVs based on factors such as communication systems, storage media, sensor systems, and fault handling mechanisms. However, the method based on threat modeling has limited specification and coverage, and can only defend information systems with clear boundaries, low real-time, dynamic, and openness.

Another mainstream UAV vulnerability assessment method is to classify UAVs as a type of cyber–physical system and use the mature cyber–physical system threat assessment theory to equivalently analyze attack behavior and assess the threat degree under different levels of UAS and attack methods.

In a single UAV scenario, some researchers have implemented threat assessment by studying attack patterns, e.g., Sun et al. [54] examined the attack patterns targeting the physical layer of drone wireless networks, such as eavesdropping attacks. They further investigated the overall threat landscape of these systems. However, some researchers implement threat assessment by quantifying attacks. For example, Fouda et al. [55] achieved the overall vulnerability assessment of UAS in a given state, by enumerating attack vectors and quantifying them into three aspects: electromagnetic attacks, cyberattacks, and physical attacks to construct the attack surface model. Leela et al. [56] classified UAV cyberattacks and conducted threat analysis based on target attack vectors. Similarly, Javaid et al. [57] proposed a network security threat model based on possible attack paths to achieve threat and vulnerability assessment of the system, which can identify high-priority threats and reduce the impact.

In multi-UAV scenarios, threat assessment is mainly carried out from the perspective of equivalent analysis. For example, Petnga et al. [58] aimed at state estimation, a typical function of UAS, and conducted vulnerability analysis based on cyber–physical attacks, and construct distributed control structure to realize the identification of potential attack behaviors. Finally, the controller is designed under the premise of considering the threat of attack behaviors to achieve effective state estimation in attack scenarios. Vyacheslav et al. [59] treated multi-UAV systems as distributed nodes in the Internet of Things (IoT) and analyzed their potential threats in IoT application scenarios. Using an analysis method based on intrusion mode and consequence criticality, they identified the potential threats of multi-UAVs in IoT environments. Ilker et al. [60] conducted a threat analysis of multi-UAV systems by treating multi-UAV collaborative perception as a novel type of Ad-Hoc network and compared it to the current Ad-Hoc network system. They analyzed the attack methods at different physical information system levels and threat levels to identify potential threats to multi-UAV systems.

3. Communication network security

3.1. Communication network attacks

Compared with terrestrial wireless networks, the UAS communication network has the remarkable characteristics of high mobility, harsh environment, dynamic changes in the communication environment, and limited communication resources. The protection measures in the transmission process are relatively weak and it is vulnerable to malicious attacks. This section summarizes the possible attacks on the UAS communication networks. Generally, as shown in Fig. 8, wireless networks are typically targeted by attackers on a hardware basis (pipeline ①). As for internal communication networks, attackers can remotely connect to the ECU via wireless means (pipeline ②), and once successful, they can compromise the bus by reprogramming or refreshing the ECU's firmware (pipeline ③). Specifically, the attacks are divided into two aspects of physical-layer-based attacks and protocol-vulnerability-based attacks. (Shown in Table 2).

3.1.1. Physical-layer-based attacks

The common attack methods in the physical layer are jamming, eavesdropping, and tampering. Jamming attack is the act of directing electromagnetic energy to a communication system to interfere with or prevent signal transmission. It is a special case of a Denial-of-Service (DOS) attack and one of the most effective means of attacking UAVs.

[1] STRIDE is a tool developed by Microsoft for threat modeling. It divides threats into the following six dimensions to examine: Spoofing, Tampering, Repudiation, Information Disclosure, Denial-of-Service, and Elevation of Privilege.

Table 2
Communication network attacks.

Attacks	References	Description	Result
Physical layer based attacks	Robinson et al. [61], Luo et al. [62], Sharma et al. [63] Fotouhi et al. [25], Sampigethay et al. [64], Wang et al. [65]	Jamming; Eavesdropping; Tampering	Lost some functions (FPV etc.) and data
Protocol vulnerability based attacks	Deligne et al. [6], Xu et al. [66], Rodday et al. [67], Westerlund et al. [26], Krishna et al. [56], Altawy et al. [68], Kamkar et al. [69], Alexandre et al. [70], Highnam et al. [71], Koscher et al. [72], Tang et al. [73], Cheng et al. [74], Miller et al. [75] Jedh et al. [76] Murvay et al. [77], Fernandez et al. [78], White et al. [79]	DOS attacks; Spoofing attacks; Data theft	Lost communication; Illegal takeover by the attacker

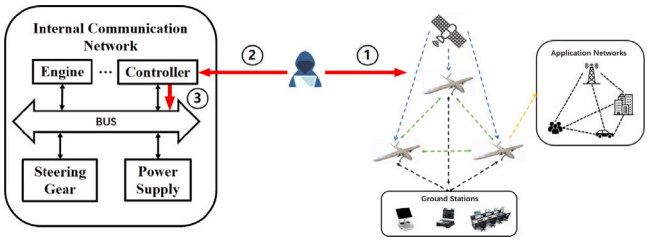


Fig. 8. Attack model of communication network attacks.

Jamming attacks have a wide range of applications in military and civilian anti-UAV fields. Robinson et al. and Luo et al. [61,62] interfered with the UAV's GPS and video link channels, respectively, resulting in the loss of its "return to home" function and the FPV functions. At present, common anti-UAV jammers are mainly divided into two types: mobile directional RF transmitters and fixed ones, both of which interfere with the ISM band. In the future, as Sharma et al. [63] pointed out, the increasing implementation of 5G communication in UAS will escalate the threat of jamming attacks and subsequently intensify the challenge posed to UAS security.

In addition, the existence of eavesdropping and tampering is also a major threat to UAS. Including the UAV-assisted communication network [25], ADS-B system [64], the 5G line-of-sight (LoS) links between UAV and ground nodes [65] etc. are all facing the risk of eavesdropping and tampering attacks.

3.1.2. Protocol-vulnerability-based attacks

The physical attack is caused by the vulnerability of the hardware. At the software level, due to the limited computing power and memory resources of UAS, its communication network generally uses a large number of lightweight communication protocols, such as Micro Air Vehicle Link Communication (MAVLink) protocol, XBee protocol, MavRos protocol, Controller Area Network (CAN) protocol etc. However, due to the consideration of cost and computing performance, plaintext communication is generally used in the design, and there is a lack of encryption and authentication mechanisms. In response to this vulnerability, an attacker can launch DOS attack [6,66] to disconnect legitimate communication connections, or through spoofing attacks, such as replaying XBee protocol-based control commands on the 868 MHz frequency band [67], authentication frames based on WiFi 802.11 protocol [6,26,56,68–70], and key authentication information of Mavlink protocol [71] to hijack the UAV and gain control privilege. For internal communication networks, DOS attacks and spoofing attacks are also major threats to the CAN protocol. For example, CAN's arbitration logic prioritizes frames with smaller IDs, which creates an opportunity for attackers to flood the bus by sending malicious frames with the smallest IDs at a high rate. This flood can delay or even prevent the transmission of other normal frames, disabling normal control of the bus to other devices [72]. Additionally, the CAN error handling mechanism can be exploited for a special type of DoS attack called a "Bus-Off" attack. These attacks utilize carefully crafted frames to create transmission conflicts, forcing the victim into a Bus-Off state and preventing future CAN Bus transmissions [73,74]. Furthermore, the attacker can launch spoofing attacks by initially infiltrating and seizing control of ordinary nodes or implanting malicious nodes into the bus, subsequently utilizing these malicious Electronic Control Units (ECUs) to transmit counterfeit frames to the CAN bus. Such attacks may include attempts to transmit frames with forbidden IDs [75] or deceiving legitimate ECUs by injecting counterfeit data [76] or replaying outdated frames [77].

In addition to the above attacks, data theft can also be carried out by exploiting the vulnerabilities of lack of encryption and authentication, such as obtaining videos and images captured by UAVs through an unauthenticated FTP service port [6], or intercepting topics and services in the security protection design lacked Robot Operating System (ROS) [78,79], and pose threat to the data security of UAVs.

Both physical-layer-based attacks and protocol-vulnerability-based attacks are primarily executed on a hardware basis. Their success rate depends on the cost and capabilities of the hardware. Consequently, larger UAVs often possess better containment and protection capabilities for their system, leading to higher hardware requirements.

3.2. Defenses against communication network attacks

Defending communication networks from cyber attacks is essential in protecting sensitive information and ensuring the normal operation of UAS. Specifically, The defense methods involve cryptography, physical layer security, and intrusion detection (shown in Table 3). These defense methods are suitable for all types of UAVs. However, Whether these methods can be deployed depends on the arithmetic power.

Cryptography is a crucial and commonly used technology for wireless network security. It enables the encryption and authentication of UAS communication networks. The application of cryptography can be categorized into two types: symmetric cryptosystem and asymmetric cryptosystem. Symmetric cryptosystems are generally used to encrypt data, such as using traditional ciphers [80], block ciphers (AES [81,82], RC5 [83]), lightweight sequence ciphers (ChaCha20 [84]), and so on to encrypt the communication link between the UAV and the GCS or CAN bus. These methods can reduce the probability of malicious attackers intercepting communication data, and improve fault tolerance. In asymmetric cryptosystems, researchers use lattice cipher methods [85] to encrypt swarm communication networks, or use digital signatures to authenticate data between UAVs and ground stations [78], and the information transmitted between the UAVs [86], to prevent them from being controlled by unauthorized intruders. For ROS, White et al. [79]

added a new set of security features called Secure ROS (SROS) to the core codebase of ROS, using modern cryptography and security measures to solve the existing communication vulnerabilities in ROS.

The influences on energy consumption and computation overhead are essential evaluation metrics for cryptography methods. However, cryptography needs additional computational overhead and requires hardware modifications, making it limited in scope for small UAVs with limited computing resources and energy. In addition, for multi-UAV systems, the increase in the number of drones will also bring problems to the management and transmission of keys.

In recent years, the research on the security of wireless communication from the perspective of the physical layer has gradually become a research hot spot. Different from the upper layer cryptography-based communication security technology, physical layer security is based on the concept of security capacity, which refers to the maximum transfer rate that can be achieved between the sender and receiver when the reliability and confidentiality of information transmission are satisfied at the same time. For multi-user eavesdrop system with J users, its security capacity C_s is defined as:

$$C_s = \max\{0, R_D - \max_{1\le j\le J} R_E^j\} \tag{1}$$

where R_D is the information received by the receiver, R_E^j is the jth eavesdropping node's information rate. More specifically, we assume that h_D and h_E^j denote the channel gain from the source to the legitimate receiver and from the source to the jth eavesdropping end, respectively. δ_D^2 and δ_E^2 refer to the Additive White Gaussian Noise (AWGN). When giving the average transmission power P, R_D and R_E^j are defined as [87]:

$$R_D = log_2(1 + \frac{P|h_D|^2}{\delta_D^2}) \tag{2}$$

$$R_E^j = log_2(1 + \frac{P|h_E^j|^2}{\delta_E^2}) \tag{3}$$

Physical layer security aims to establish a channel security model based on the actual physical environment, and enhance security capacity through optimization methods. This helps to prevent the system from jamming attacks and eavesdropping. Unlike encryption technology applied to higher layers, physical layer security for wireless communication does not require keys or complex algorithms, making it more suitable for large-scale distributed wireless networks. As a result, it can effectively protect wireless data transmission without the need for keys and complex algorithms.

Some researchers give solutions to the UAS communication network security based on physical layer security. For example, adding artificial noise [24] to the transmission information to confuse the attacker, or verifying by comparing the control command format [88], which can reduce the influence of eavesdropping and malicious interference on the UAS communication system.

In the field of information-theoretic security, research on UAS security mainly focuses on two scenarios: UAV-assisted direct secure communication and UAV-assisted secure collaboration [89]. In the first scenario, the drone is a legitimate communication node in the air. Researchers usually study issues such as improving the security capacity of communication systems, the average secure transmission rate, and the probability of secure communication interruption under the multi-user eavesdropping channel and mixed eavesdropping channel models [90–94]. In the second scenario, researchers use UAVs as mobile relays to enhance effective information transmission between the source and receiver [95,96], or as an aerial interference source [95,97] and study methods to reduce the attacker's eavesdropping effectiveness by sending artificial noise.

However, physical layer security remains limited to theoretical research, with the channel model used for research often requiring some limitations or assumptions. These assumptions, such as the legal communication channels being stronger than eavesdropping channels, and the need for accurate, knowable channel information, can impact the results of the research. While the feasibility of physical layer security has been demonstrated through theoretical research, a generalized channel coding scheme that achieves the guaranteed transmission rate according to information theory is not yet available for practical use.

Intrusion detection involves identifying attempted, ongoing, or already occurred intrusions. Currently, a rule-based intrusion detection strategy has been applied in the field of UAS wireless network protection. For example, Strohmeier et al. [98] developed an anomaly detection method based on physical layer information to protect the communication between UAV and ground stations, which can effectively detect erroneous data injection attacks and detect attackers within 40 s. Mitchell et al. [99] proposed a UAV intrusion detection system based on adaptive behavior rules to detect whether a single UAV in a multi-UAV system is maliciously attacked. Some researchers extract distinct features, such as transmission frequency [100], electrical signals [101], and ID [102], from the typical bus transmission process. These features are then analyzed to ascertain if the frames conform to established normal rules, which can help in identifying potential bus invasions. However, the rule-based intrusion detection system (IDS) has the problem of complicated management, which needs to be preconfigured. To this end, some studies also use signature-based intrusion detection techniques as an improvement, such as Kacem et al. [103] proposed an ADS-B intrusion detection framework to protect aircraft from network attacks targeting ADS-B messages. The framework is based on a feature detection strategy that analyzes the position of an aircraft's GPS. Casals et al. [104] developed a biologically inspired detection scheme to detect cyberattacks against aerial networks. For this method, a detection rate is usually adopted to evaluate the performance as well as the missing report rate and false alarm rate. However, the above two intrusion detection systems are essentially misused detection. Neither of them can detect unknown attacks since both of them need to know the characteristics of the attack in advance.

4. Software security

4.1. Software attacks

Software attacks refer to the method of attacking the target software or system by exploiting vulnerabilities. For UAS, the flight control and navigation system, GCS, and command and control system are all composed of one or more computers. These computer systems have certain particularity and closeness. They may have weak configuration and relative lag in update and maintenance. Also, they lack unified management standards and vulnerability libraries, once attacked by software, the loss will be more serious than traditional computers. Generally, The attack model (shown in Fig. 9) can be divided into three ways: ① The attacker directly invades the communication network (e.g. Man-in-the-middle attack) to inject attack payloads into the UAV's on-board software system. ② The attacker gain access and attack ground equipment. (social engineering, vulnerability exploitation, etc.). ③ The attacker obtains the UAS software authority or injects attack payloads into it based on pipeline ②, this way is often achieved based on the data transmission of the communication network. Classified from a technical point of view, the software attacks of UAS include backdoor attack [7], root exploit attack [105], buffer overflow attack [28,106], reverse cracking [62], etc. (Shown in Table 4).

The backdoor attack is a method of bypassing security controls to gain access to a program or system. For example, Rahul [7] installed the malware Maldrone on the drone's flight control firmware to set up a backdoor, and then secretly entered or controlled the system and seized the control of the drone. Rahul also noted that the combination of Maldrone and replaying attacks can make the UAVs disconnect from the legitimate controller without enabling emergency protection measures

Table 3
Defenses against communication network attacks.

Method	References	Strengths	Weaknesses
Cryptography	Rajatha et al. [80], Shoufan et al. [81], Woo et al. [82] Butcher et al. [83], Allouch et.al [84], Abdallah et al. [85], Fernandez et al. [78], Bian et al. [86], White et al. [79]	Encrypting and authenticating the communication network	Needs additional computational overhead; Requires hardware modifications; Bringing problems to key management and transmission
Physical layer security	Liu et al. [24], Rubin et al. [88] Wang et al. [89], Zhang et al. [90] Zhang et al. [91], Cui et al. [92], Yang et al. [93], Zhao et al. [95], Bastami et al. [96], Lee et al. [97] Khan et al. [94]	Protecting wireless data transmission without the need for keys and complex algorithms	No practically available generalized channel coding scheme to achieve the transmission rate; Need limitations or assumptions for channel model
Intrusion detection	Mitchell et al. [99]	Identifying attempted, ongoing or already occurred intrusions	Cannot detect unknown attacks; Safety specifications are not adaptive
	Strohmeier et al. [98] Taylor et al. [100], Choi et al. [101], Cho et al. [102] Kacem et al. [103], Casals et al. [104]		Cannot detect unknown attacks

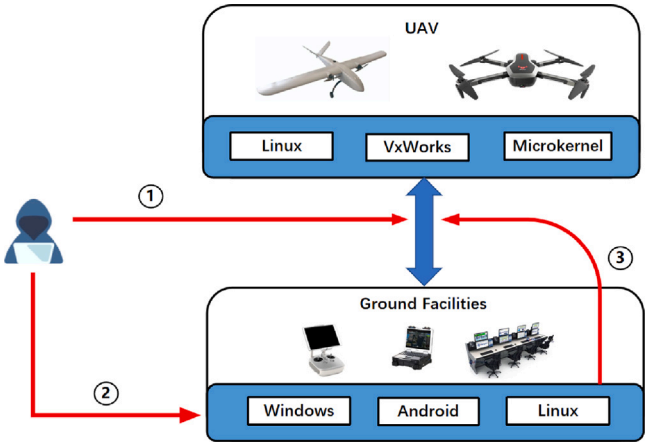


Fig. 9. Attack model of software attacks.

and still be controlled by malicious programs. This attack follows the pipeline ①.

Koo et al. [105] pointed out that Linux-based UAV operating systems are vulnerable to root exploits. In response to this problem, some drones use microkernel-based operating systems, but such systems are less scalable and vulnerable to buffer overflow attacks [28,106], that is, the program attempts to write data outside the area. This attack method can invade the flight control program, and then force the drone to shut down and fall. They often follow pipeline ③.

Reverse engineering is a technology that explores the internal structure and working principle of software, which can be used to analyze and crack the related software of UAS. For example, the attackers can reverse the Android-based UAV control application to obtain the format of the control command; or reverse the secondary development tool and elevate the authority to bypass the authentication to control the UAV [62]. Also, it demonstrates the ability to write an attacker-defined file into the UAV [107] Reverse engineering can save a tremendous amount of time, manpower, and material resources, and can be used to launch attacks on drones beyond visual range. It often follows pipeline ② and ③.

In general, due to the ubiquity of WiFi protocols and interfaces, most of the software attacks target MAV or SUAV since they use WiFi as the protocol for communication networks. Furthermore, most attacks are essentially one-time static attacks since they target on static UAVs. For UAVs that are in a dynamic flight state and use special protocols for communication (especially TUAV, HALE, and MALE), their attack channels are limited, and they can only start from the ground station or command and control system (pipeline ② in Fig. 9). These characteristics make it very difficult to exploit the vulnerabilities and deliver attack payloads.

4.2. Defenses against software attacks

As UAS software security becomes an imperative challenge, its mitigation has received attention, especially in the military field. For example, the US Defense Advanced Research Projects Agency is conducting research called High Assurance Cyber Military Systems (HACMS). The project aims to develop security software based on a formal method to defend against malicious attacks on UAS by hackers. Software defense techniques generally include fuzzing, memory isolation, Control Flow Integrity (CFI), and parameter and state estimation (Shown in Table 5). These defense methods are suitable for all types of UAVs.

Fuzzing is an automated or semi-automated software testing methodology, which finds vulnerabilities by inputting a large amount of malformed data into the tested target and observing and analyzing the abnormal operation of the program. For UAS software attack mitigation, Alhawi et al. [108] applied fuzzing and bounded model checking techniques to predict where unknown software vulnerabilities in UAS may appear. Ye [109] used fuzzing technology to test file transfer programs and flight control programs for denial-of-service vulnerabilities, and found an unknown denial-of-service vulnerability in a certain type of UAS. Kim et al. [110] utilized the UAV control model to provide helpful semantic guidance for improving bug-discovery accuracy and efficiency. They proposed RVFUZZER, a vetting system for finding input validation bugs in RV control programs through control-guided input mutation. The performance of fuzzing can be evaluated by the amount and categories of vulnerabilities it uncovers.

CFI is a framework that against control flow hijacking attacks based on jump instructions. Pike et al. [30] and Clements et al. [111] proposed a CFI-based method to detect attacks on software. When implemented on the operating system of UAV, it is proved that the method can detect attacks such as buffer overflow and illegal function execution.

Memory isolation is a method of isolating the virtual memory space of a process from the actual physical memory space, making it difficult for attackers to conduct memory corruption attacks. For example, Koo et al. [105] adopted a virtualized microkernel to isolate the wireless communication module on a Linux-based UAV operating system, which can effectively prevent root exploit attacks.

Parameter and state Estimation is a method to realize real-time estimation and tracking of UAS by comparing controller parameters with known normal parameters. This method can be used to detect

Table 4
Software attacks.

Attacks	References	Description	Result
Backdoor attack	Rahul [7]	Bypassing security controls and set backdoors	Malicious control the UAV
Root exploits	Koo et al. [105]	Elevating to root privileges	Invading the flight control program
Buffer overflow	Hooper et al. [28], Elley [106]	Attempting to write program data in illegal area	Causing the drone to shut down and fall
Reverse engineering	Luo [62], Li [107]	Exploring internal application structure and working principle	Obtaining control command format; Bypassing authentication to control UAV; Writing attacker-defined file into UAV

Table 5
Defenses against software attacks.

Method	References	Strengths	Weaknesses
Fuzzing	Alhawi et al. [108] Ye [109] Kim et al. [110]	Observing and analyzing the abnormal operation of the program	Lacking standard UAV vulnerability libraries Limited in defending attacks against physical features of control systems; The type of vulnerability identified through the excavation is relatively limited in scope.
CFI	Pike et al. [30], Clements et al. [111]	Effectively detect buffer overflow and illegal function execution	Cannot address the resteering problem
Memory isolation	Koo et al. [105]	Making it difficult for attackers to conduct memory corruption attacks	The network communication performance gets deteriorated
Parameter and State estimation	Birnbaum et al. [112], Fei et al. [113]	Detecting software-oriented attacks and malicious code attacks	/

software-oriented attacks against drones [112] and malicious code attacks [113].

Software defense methods can effectively defend the attacks for software vulnerabilities. However, due to the strong coupling between UAS cyber and physical systems, such methods are still limited in defending against attacks on the physical features of control systems. In future research, we need to focus more on such "control-semantic" vulnerabilities rather than just protecting against or mitigating code vulnerabilities [114]. In addition, although researchers have begun to focus on the standardization of vulnerabilities in robotic systems and the construction of vulnerability libraries [115], there is still a lack of standard UAV vulnerability libraries to provide standardized vulnerability information and data for their software security research.

5. Payload security

5.1. Payload attacks

Payload attacks aim to destroy or manipulate the load readings by means of electromagnetic, sound waves, software, etc., so that it outputs wrong data to the back-end software for processing, thereby affecting the decision-making of the flight system. Generally, The attack model (shown in Fig. 10) can be divided into two ways: (1) Physical Attacks: The attacker exploits the physical vulnerabilities of payloads and use hardware (Laser, SDR, Sound card, etc.) to launch sensor spoofing attacks. (2) Cyber attacks: The attacker exploits software vulnerabilities to get access to UAS software and tamper the payloads' readings. Specific attack strategies include jamming attacks and spoof attacks. Attack objects include inertial sensors, GPS, Optical Flow, Lidar, etc. (shown in Table 6). This kind of attack comprehensively utilizes the vulnerability of payload hardware and system control software to tamper with data. It is a typical cyber–physical composite attack technology. And its protection is difficult since the attack surface is wide.

Micro-Electro-Mechanical System (MEMS) has a wide range of applications in UAV inertial sensors. However, inertial sensors have obvious vulnerabilities to spoofing attacks, such as acoustic signal spoofing attacks [34–36], out-of-band signal injection attack [116], transfer attack [37] etc. These attacks can erroneously output values from inertial sensors or establish implicit control channels that force a drone to land or even crash without triggering a security response mechanism.

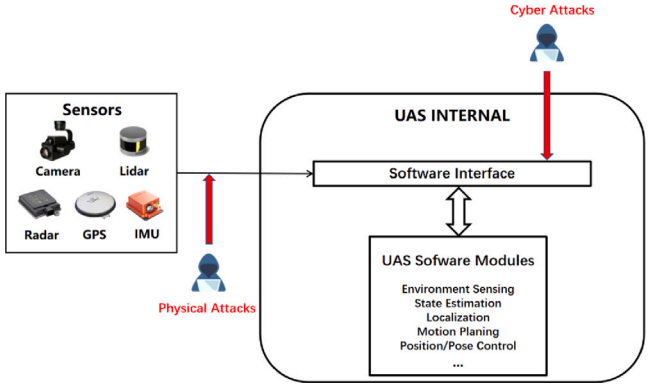
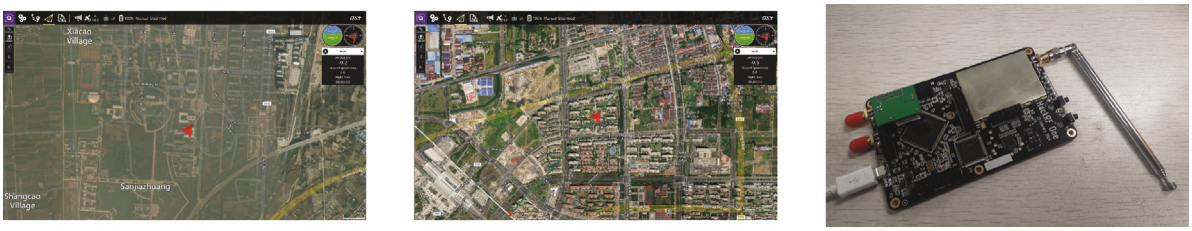


Fig. 10. Attack model of payload attacks.

The main attack for UAV GPS sensors is spoofing attack [8], that is, sending false location coordinates to the GPS receiver, and the receiver processes these false data as real data, thus effectively masking the UAV's real location. The navigation system can easily receive the camouflaged signal, and then calculate the wrong position information (shown in Figs. 11(a) and 11(b)), causing the UAV to crash or be captured by the attacker.

GPS spoofing attacks can be easily launched using Software Defined Radio (SDR) [117] (Fig. 11(c)). It has become a serious threat to UAS security. Specifically, the attack may cause GPS jamming by setting a no-fly zone in the autonomous flight mode or even hijack and disable the UAV [118–120]. Based on the injection of false location coordinates, the researchers take the detection threshold as the constraint condition of the attack payload and propose an optimization-based stealth attack strategy [38,121]. Specifically, For a fixed time horizon T_a, the attacker aims to look for an attack sequence $\delta = \{\delta(1), \delta(2), \ldots, \delta(T_a)\}$ to maximizes the residual vector $\|r(k)\|_2 = E[r(k)^T r(k)]$ measured by the sensor without being detected. This is formulated as the following



(a) Actual Location of UAV (b) Spoofed Location of UAV (c) Software Defined Radio

Fig. 11. GPS spoofing attacks.

Table 6
Payload attacks.

Attacks	References	Description	Result
Attacks on inertial sensors	Tripple et al. [34], Farshteindiker et al. [35], Son et al. [36], Tu et al. [37,116]	Acoustic signal spoofing attacks; Out-of-band signal injection attacks; Transfer attacks	Causing a drone to land; Crashing without triggering security response mechanism
Attacks on GPS	Hermans et al. [8], Kerns et al. [118], Vervisch et al. [119], He et al. [120], Quinonez et al. [38]	GPS spoofing attacks; Stealthy attacks	Hijacking and disabling the UAV; Capture the UAV
Attacks on optical flow	Davidson et al. [49]	Deceiving the optical flow sensing algorithm	Causing potential threats to the navigation and control process
Attacks on Lidar	Yan et al. [122], Shin et al. [123]	Making the Lidar unable to perceive a certain direction	

constrained optimization problem:

$$\begin{aligned} &arg\max_{\delta} \quad \sum_{i=0}^{T_a} E[r^T(k)r(k)] \\ &s.t. \quad E[r^{'}(k)] \leq \tau \quad \forall k \in \{1, ..., T_a - 1\} \end{aligned} \tag{4}$$

where $r'(k)$ and τ are defined in Eq. (5) in Section 5.2. Compared with the former, this attack can force the UAV to enter a preset location without triggering a specific security detection mechanism, achieving the induction and capture of the UAV in a more stealthy way [121].

In addition to IMU and GPS, sensors such as Lidar and Optical Flow are also at risk of being attacked. Such as constructing a mesh laser image to deceive the optical flow sensing algorithm [49], blinding the camera to make it unable to recognize the image [122], and making the Lidar unable to perceive a certain direction [123]. These attacks will cause potential threats to the navigation and control process of UAS. However, the corresponding defense technology still lacks relatively systematic research progress.

The problems existing in the research of payload attacks are similar to those of communication network attacks. Since the attacks need high hardware requirements, and can only be launched at close range, it is difficult to attack payloads in large UAVs (especially TUAV, HALE, and MALE) except for GPS. Therefore, most researchers have only designed and verified their methods in a simulated environment or on small UAVs in some limited scenarios. There is still a gap in verifying most attacks on practical UAVs in real physical scenarios.

5.2. Defenses against payload attacks

The mitigation against payload attacks can be divided into two categories: hardware protection and software protection. Specifically, it includes physical protection, software analysis, Cryptography authentication, detector, and auxiliary positioning detection (shown in Table 7). They are theoretically suitable for all types of UAVs.

Physical protection methods are frequently applied for inertial sensors. Physical isolation, such as the use of acoustic foam and sound enclosures, is one such method. Another approach is to enhance the redundancy of the system, such as utilizing dual gyroscopes for active defense of differential measurement. [124,125]. These methods can effectively reduce the resonance effect of the noise frequency on the sensor and reduce the possibility of spoofing attacks.

Software analysis methods are primarily utilized to ensure the integrity and availability of payload data, They are commonly applied to detect spoofing attacks on GPS and IMU. Its core idea is to model the flight state of the UAV by extracting some system features of the UAV itself. When the flight state of the UAV deviates from the calculation result of the model (exceeds a determined threshold) during the flight process, it is considered to be attacked. For example, extracting system control invariant modeling to detect inertial sensor attacks [126], using system physical constant modeling to detect inertial sensor stealth attacks [38], using IMU data to build machine learning models to detect GPS spoofing attacks [127,128] and etc.

Cryptography-based authentication methods are mostly used to protect GPS sensors, mainly to ensure the confidentiality of payload data. For example, researchers authenticated GPS signal based on quantum key distribution [129], symmetric cryptography [130,131] and statistical hypothesis testing [132]. Although these methods can effectively defend against fake GPS signals. However, they usually require changing the physical structure of the existing satellite infrastructure, which increases the communication overhead and has a certain impact on the real-time performance of the UAS. Simultaneously, cryptography-based authentication methods are still vulnerable to replay attacks [133].

Detector method [134,135] uses the differences between measured values and filter estimates to calculate the residual vector $r(k)$ [136] and construct a random variable $r' = f(r(k), \Sigma_r)$. Then it achieve the attack detection by comparing the difference in the probability distribution of single or multiple samples in the normal and attacked cases. It assumes that r' follows a zero-mean Gaussian distribution with a constant covariance matrix Σ_r, and abrupt changes in data can be detected by testing the following two incompatible statistical hypotheses,

$$H_0 : r(k) \sim N(0, \Sigma_r) \quad and \quad H_1 : r(k) \nsim N(0, \Sigma_r) \tag{5}$$

where $N(0, \Sigma_r)$ represents the Gaussian distribution with mean 0 and covariance Σ_r. This is realized by comparing r' with a threshold τ. If the estimated r' is above τ, H_1 is accepted and the algorithm detects the fault in the system, which may be introduced by spoofing attacks. The Detector can effectively detect spoofing attacks in MEMS and GPS sensors since most of the attacks can cause abrupt changes. However,

Table 7
Defenses against payload attacks.

Method	References	Strengths	Weaknesses
Physical protection	Roth et al. [124], Soobramaney et al. [125]	Reducing the probability of spoof attacks	Physical isolation will cause poor heat dissipation
Software analysis	Choi et al. [126], Quinonez et al. [38], Liang et al. [127], Feng et al. [128]	Effectively detecting spoofing attacks on GPS and IMU	Cannot respond to attacks; Have false detections
Cryptography-based authentication	Bonior et al. [129], Hanlon [130], Kerns et al. [131], Wesson et al. [132], Papadimitratos et al. [133]	Effectively defending against fake GPS signals	Require physical structure changing; Reduce real-time performance; Vulnerable to replay attack
Detector	Yang et al. [134], Ju et al. [135], Ceccato et al. [137]	Effectively detecting spoofing attacks on GPS and MEMS	Its accuracy depends heavily on the choice of threshold; Vulnerable to stealth attacks
Auxiliary detection	Tippenhauer et al. [138], Jansen et al. [139], Magiera et al. [140], Kwon et al. [141], Davidovich et al. [142]	Improving the detection accuracy	Cannot respond to attacks

it has obvious drawbacks for either single or multiple samples. If only a single sample is used, the detection accuracy depends heavily on the choice of the threshold value. Although detection accuracy can be improved by using multiple samples, the relatively large window causes time delays, e.g., the General Likelihood Ratio Test (GLRT) [137]. Such methods may expose the system to attack for a short period of time before detection is complete. Furthermore, as described in Section 5.1, detector techniques are vulnerable to stealth attacks since it is based on the hypotheses that r follows a zero-mean Gaussian distribution.

Auxiliary detection methods mainly detect and protect GPS attacks by positioning signals or related characteristics of other sensors. For the utilization of positioning signals, including multi-receiver detection [138], crowd-sourced cross-validation [139], phase delay estimation and signal spatial filtering [140], state change analysis [141] and other methods. For the utilization of sensor characteristics, Davidovich et al. [142] used the correlation between frames in the video stream captured by the camera to establish a motion representation model of the UAV, and compared the model with GPS measurements to detect spoofing attacks.

In general, the research on payload defenses, especially software methods, mostly focuses on the detection of malicious attacks, while ignoring protection and response. In cybersecurity research, protection or emergency response technologies such as patching and disconnecting the network can generally achieve "medicine to cure the disease" and get immediate results. Still, it is often aimed at static systems or even offline systems, which is more like a kind of after-loss remedy. For a highly dynamic real-time information system like UAS, these passive defense technologies cannot cope with complex and highly concealed payload attacks. In the future, the research of load protection should focus on protection and emergency response technology, comprehensively consider information systems, physical characteristics, flight decision-making, and other factors integrate network security, optimization theory, and control theory, etc., to form a dynamic real-time and efficient active defense strategy.

6. Machine-learning-based security

6.1. Machine-learning-based attacks

In this chapter, we discuss the machine-learning-based attack against the algorithms, that is, attackers usually artificially create noise to change the data distribution, or generate malicious adversarial examples to carry out "poisoning attacks" to interfere with the classification process of the model and cause the model to classify incorrectly. The attack can be defined as Eq. (6).

$$\begin{cases} x_i' = x_i + \Delta x_i \\ f(x_i) = y_i \\ f(x_i') \neq y_i \end{cases} \tag{6}$$

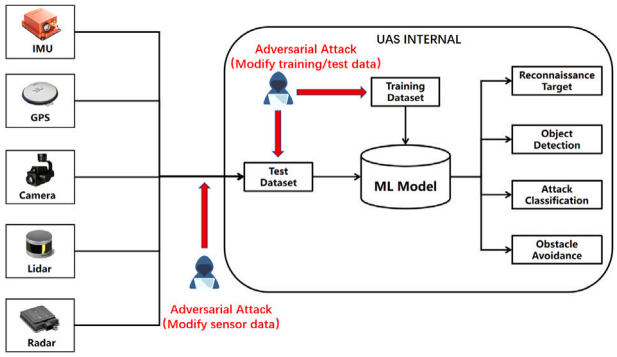


Fig. 12. Attack model of machine-learning-based attacks.

where x_i and y_i refer to the benign input and output respectively. Δx_i refers to the adversarial perturbation the attacker inject to x_i and x_i' refers to the adversarial example.

The vulnerability of machine learning algorithms generally include two aspects, firstly, activation functions in neural networks like Rectified Linear Unit (RELU) and Sigmoid often have the effect of compression, linearizing nonlinear neural networks. Therefore, several studies have shown that adversarial example attacks result from the lack of resistance to perturbations of linearized networks [43,44,143]. Second, there are vulnerabilities in some generic operations of the machine learning algorithm itself that can be exploited by attackers, such as convolution operations [144] and image scaling operations [145]. The effect of intelligent attacks is generally evaluated from the following aspects.

Adversarial Effectiveness. The effectiveness of the attacks is determined by the reduction of the target model's task performance on the adversarial examples compared to its original performance.

Adversarial Stealthiness. The stealthiness means that the Δx_i should be indistinguishable from humans or well hid in the environment.

Adversarial Transferability. The transferability means that an adversarial example can be successfully attacked on one model and can have a similar impact on other models.

In recent years, as we concluded in Table 8, adversarial attacks have also been gradually applied in actual physical scenarios to attack intelligent algorithms deployed on UAS. As shown in Fig. 12, the attacker can construct an adversarial sample by modifying the sensor data. Through investigation, we found that modifying camera [48] and Lidar [50,146] data to attack object detection and tracking tasks is one of the most popular attack methods. In addition, related works have shown that attackers may cause some task failures for Autonomous Driving (AD)

Table 8
Machine-learning-based attacks.

Method	Vulnerabilities of linear	Vulnerabilities of general operations
Modify sensor data	Johnson et al. [9] Cao et al. [50], Zhu et al. [146]	Han et al. [48], Sun et al. [148]
Modify training/testing data	Kim et al. [149], Xie et al. [150], Chen et al. [151], Wei et al. [152], Yan et al. [153], Athalye et al. [154], Held et al. [155]	/

systems by attacking other payloads like GPS [147] and Radar [148]. Although they did not directly attack the intelligent algorithms on UAS, since the AD system is a crucial part of UAS, the methods proposed in the field of AD systems have a good reference value. they demonstrated that these sensors run the risk of becoming an entrance for adversarial examples to attack intelligent algorithms.

Except for sensor attacks, the attacker can also gain internal access to the UAS and directly modify the training/testing data. In this way, they can defraud UAVs to find enemy activities in reconnaissance missions [9], or use Fast Gradient Sign Method (FGSM) algorithm to construct adversarial samples to interfere with attack detection models [149]. In addition, some attacks may also pose potential threats to UAVs. For example, for object detection and tracking models, Researches [150–155] proposed attack methods such as Dense Adversary Generation (DAG) and Unified and Efficient Adversary (UEA) to significantly reduce the accuracy of the classifier. As described in Section 5.1, machine learning-based attacks pose similar challenges as payload attacks for different types of UAVs since some attacks rely on the payloads. Additionally, UAVs with strong containment present a challenge for attacks that require internal access.

6.2. Machine-learning-based defense technology

Machine learning can also be applied to the protection of UAS. From a technical point of view, traditional security protection measures can defend against many known security threats. However, as the application fields of UAS continue to expand, application scenarios and tasks are becoming more and more diverse, and various attack methods are being introduced. Defense technology has struggled to cope. AI has strong automatic feature extraction and analysis capabilities, which is suitable for multi-level security protection in different kinds of UAS, and become a feasible technical direction for protecting new types of attacks. This section summarizes some applications of machine learning in UAS cybersecurity protection, including supervised learning, reinforcement learning, and game theory (shown in Table 9).

Supervised learning is the process of using a set of samples of known classes to adjust the parameters of a classifier to achieve the required performance. For the cybersecurity of UAS, supervised learning is widely used, such as using LSTM to identify the legitimate ADS-B message sequence and calculate the flight deviation [156], using LSTM, SVM, and other algorithms to detect sensor spoofing attacks [157–159], Detecting malicious replay attacks by authenticating drone operators based on random forest algorithm [160]. In multi-UAV systems, supervised learning algorithms can learn from abnormal states to protect UAVs from DOS attacks [161]. Like intrusion detection methods, detection rate, missing report rate, and false alarm rate are adopted to evaluate the performance. Moreover, as these tasks belong to deep learning-based classification, the evaluation metrics commonly used for such tasks as accuracy and recall are also employed to assess the model's performance.

Reinforcement learning is a learning method in which the agent aims to maximize the cumulative reward and learns by interacting with the environment in a "trial and error" way to obtain a strategy [162,163]. It also has a wide range of application scenarios in UAV cybersecurity. For example, Johansson et al. [164] used reinforcement learning to learn policy functions to help UAVs accurately find the flight path when they lost control, and ensure that UAVs can cruise correctly when attacked by interference. Lu et al. [165] proposed a reinforcement learning-based method for abnormal temperature detection of UAV motors, which prevents them from operating at abnormal temperatures by learning the temperature thresholds of the motors and executing corresponding flight strategies under different thresholds. It can make a forced landing when the motor is overheated to ensure flight safety. Lin et al. [166] designed a joint control scheme of UAV trajectory and communication transmission power for the communication network of UAS. The user-perceived channel trajectory and transmission power were selected by the reinforcement learning method to counteract the malicious interference attack.

Intelligent attacks generally have complex attack intentions, and there is a certain antagonism between them and defenders. Game theory-based prediction methods can infer attack intentions according to attack "actions" by establishing game theory models, and making targeted defense "actions" so that the defender's reward can be maximized. For example, Yang et al. [167] established a connection game between a pair of communication drones and an attacker, and optimized the game using generative adversarial networks (GAN) to adjust the connection policy while improving the defense against malicious attacks and the attacker's ability to jam the drones. However, this work is employed with the assumption of full rationality, but in actual confrontation scenarios, it is difficult for attackers and defenders to satisfy the requirement of complete rationality. For this reason, Sanjab et al. [168] introduced prospect theory to describe the bounded rationality of both attackers and defenders, and calculated the optimal path strategy for UAVs to avoid malicious attacks by combining prospect theory and traditional game models. Xiao et al. [169] introduced prospect theory to study the static game of information transmission between attackers and UAVs, and on this basis, introduced reinforcement learning methods such as Q-learning, WoLF-PHC, and DQN to carry out power allocation strategies. These methods can effectively resist deception and jamming attacks.

The machine-learning-based defense methodology should consider not only the model accuracy but also the detection granularity, response time, and other factors to ensure that the detection model meets the real-time safety needs of UAS. At the same time, the design of machine-learning-based defenses for different types of UAVs should consider the constraints of computing power, as the UAVs have limited load capacity and hardware computing power. Therefore, the model should be optimized and compressed reasonably.

7. Discussion and future works

This paper introduces the UAS cybersecurity problems and the corresponding protective measures from four aspects: communication network security, software security, payload security, and intelligent security. On the whole, UAS cybersecurity research has made many breakthroughs and has become an important part of the UAS security protection architecture; on the other hand, there are still many problems in UAS cybersecurity research.

First, compared with the IoT, UAS generally uses private communication protocols for data communication. It generally does not need to connect to the Internet cloud and dynamically interact with a large amount of data, and is more like an independent and closed local area network. In addition, UAS has physical constraints such as volume, weight, and power consumption, as resource constraints such as load, computing power, and real-time requirements. These problems lead to the fact that some Internet cybersecurity protection technologies

Table 9
Machine-learning-based defense technology.

Method	References	Strengths	Weaknesses
Supervised learning	Habler et al. [156], Panice et al. [157], Abbaspour et al. [158], Sun et al. [159], Shoufan et al. [160], Rani et al. [161]	Can detect malicious attacks	Lack of labeled training data for UAS; Has constraints of computing power; The training of these models is a time-consuming process
Reinforcement learning	Johansson et al. [164], Lu et al. [165], Lin et al. [166]	Can respond to malicious attacks	The convergence of policy networks depend on the design of scenario rewards.
Game theory-based protection	Yang et al. [167], Sanjab et al. [168], Xiao et al. [169]	Infering attack intentions according to attack "actions" and make targeted defense	The model need good timeliness and quickly, accurate response

with rich research and excellent effects but too large computational complexity cannot be directly applied to UAS. For small and medium UAVs, it is mainly due to the severe limitation of computing resources and energy, while for large UAVs, it is more reflected in the strong closure of the system itself. In the future, under the development trend of the Internet of Everything, UAVs will be used more as the terminal of the IOT system to perform complex tasks. The autonomous intelligence degree will be further improved, and the application scenarios and system architecture will be more complex and diverse. This trend will expose more and more UAS to the Internet environment, which will bring more severe challenges to their security. Hence, it is crucial to explore the practical implementation and adoption of internet information security technology within the constraints of limited resources, tailored to the unique features of diverse UAV types. This will ensure seamless interconnectivity, secure information exchange, and productive collaboration within a trustworthy environment, thereby holding significant engineering significance.

Secondly, medium and large UAVs, especially strategic and tactical UAVs are usually used to perform military operations or confidential missions in hostile environments, and often carry a large amount of sensitive data (such as flight operation data, log data, mission-related data, reconnaissance data, etc.), once captured by malicious people, the OS needs to ensure that the data cannot be leaked and that any modifications to the hardware/software can be detected. However, these data are often stored in plaintext, with the read and write of the data usually lacking integrity verification, which makes the data easily obtained by attackers or illegally tampered with. In addition, the cross-domain transmission also increases the risk of critical data leaking in more open communication networks. Furthermore, the attacker could perform an attack on the side channel of the AD hardware (CPU, Cache, etc.) and thus steal private data [170]. At present, most of the research on data security focuses on the communication transmission level, while there is a lack of systematic security research on data acquisition, storage, reading, and writing. Thus there is an urgent need to address the issue of data security both in software and hardware. Therefore, it is of great significance to study the storage encryption, operational integrity verification, hardware security, and illegal operation auditing of key data in UAS. These measures can ensure the security and control of core data, reduce property losses, and improve overall UAS security.

Finally, the rapid development of a new generation of AI and the rapid improvement of cluster networking capabilities make UAVs need to be used to perform more diverse and complex flight missions. The degree of coupling and interaction between aircraft and the flight environment is deepening. The complexity and diversity of these environments and tasks increase the attack surface of the system and bring more severe security threats to UAS. Therefore, it is far from enough to rely solely on traditional airworthiness safety or cybersecurity technical specifications to ensure the safety of UAS. At present, the UAS security research mainly focuses on the security of physical systems and information systems, while ignoring the security issues under the constraint of mission orientation. For example, in some scenarios, the UAV chooses to return or change the flight route in order to avoid electromagnetic interference. Although the UAS itself is protected, it leads to the failure of the mission, which is also unacceptable. In the future, it is essential to redefine the scope and boundaries of UAS security in conjunction with specific tasks and establish a comprehensive security framework, technical systems, and evaluation standards to address emerging threats. This represents a crucial research direction that aligns with the strategic needs of the drone industry's sustainable growth.

8. Conclusions

In this paper, we first introduce the classification and architecture of UAS. Then We systematically analyze the security threats and summarize a systematic approach to vulnerability assessment from the perspective of UAS architecture. Based on security analysis, we detail the attack and defense research from four aspects of communication network security, software security, payload security, and intelligent security. Finally, we discuss three future research directions and conclude our work. We expect this work can inspire researchers to design the corresponding defense technology and provide solutions for UAS cybersecurity.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Yang Li reports financial support was provided by National Natural Science Foundation of China. Quan Pan reports financial support was provided by National Natural Science Foundation of China.

Data availability

No data was used for the research described in the article.

References

[1] Yu Liu, Jianzhong Sun, Hang Li, Supervision and norm discussion on civil unmanned aerial vehicle, J. Nanjing Univ. Aeronaut. Astronaut. 49 (S) (2017) 152–157.
[2] K.W. Chan, U. Nirmal, W.G. Cheaw, Progress on drone technology and their applications: A comprehensive review, in: AIP Conference Proceedings, Vol. 2030, AIP Publishing LLC, 2018, 020308.
[3] Deren Li, Ming Li, Research advance and application prospect of unmanned aerial vehicle remote sensing system, Geom. Inform. Sci. Wuhan Univ. 39 (2014) 505–513.
[4] Lyu Yang, UAV Environment Sensing and Collision Avoidance (Ph.D. thesis), Northwestern Polytechnical University, 2019.
[5] Y.S. Lee, Y.J. Kang, S.G. Lee, H.J. Lee, Y.J. Ryu, An overview of unmanned aerial vehicle: Cyber security perspective, in: IT Convergence Technology 2016, 2016.
[6] Eddy Deligne, Ardrone corruption, J. Comput. Virol. 8 (1–2) (2012) 15–27.
[7] Sasi Rahul, Drone attacks: How I hijacked a drone, 2015.
[8] Bart Hermans, Luc Gommans, Targeted GPS spoofing, Res. Project Rep. (2018) 1–16.
[9] James Johnson, Artificial intelligence, drone swarming and escalation risks in future warfare, RUSI J. 165 (2) (2020) 26–36.
[10] Georgia Lykou, Dimitrios Moustakas, Dimitris Gritzalis, Defending airports from UAS: A survey on cyber-attacks and counter-drone sensing technologies, Sensors 20 (12) (2020) 3537.

[11] Ben Nassi, Ron Bitton, Ryusuke Masuoka, Asaf Shabtai, Yuval Elovici, Sok: Security and privacy in the age of commercial drones, in: 2021 IEEE Symposium on Security and Privacy, SP, IEEE, 2021, pp. 1434–1451.

[12] Ghulam E Mustafa Abro, Saiful Azrin BM Zulkifli, Rana Javed Masood, Vijanth Sagayan Asirvadam, Anis Laouti, Comprehensive review of UAV detection, security, and communication advancements to prevent threats, Drones 6 (10) (2022) 284.

[13] Daojing He, Du Xiao, Yinrong Qiao, Yaokang Zhu, Qiang Fan, Luo Wang, A survey on cyber security of unmanned aerial vehicles, Chinese J. Comput. 42 (5) (2019) 1076–1296.

[14] Yueyan Zhi, Zhangjie Fu, Xingming Sun, Jingnan Yu, Security and privacy issues of UAV: a survey, Mob. Netw. Appl. 25 (1) (2020) 95–101.

[15] Rongxiao Guo, Buhong Wang, Jiang Weng, Vulnerabilities and attacks of UAV cyber physical systems, in: Proceedings of the 2020 International Conference on Computing, Networks and Internet of Things, 2020, pp. 8–12.

[16] Kai-Yun Tsao, Thomas Girdler, Vassilios G. Vassilakis, A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks, Ad Hoc Netw. 133 (2022) 102894.

[17] Gaurav K Pandey, Devendra S Gurjar, Ha H Nguyen, Suneel Yadav, Security threats and mitigation techniques in UAV communications: A comprehensive survey, IEEE Access (2022).

[18] James McCoy, Danda B. Rawat, Software-defined networking for unmanned aerial vehicular networking and security: A survey, Electronics 8 (12) (2019) 1468.

[19] Arslan Shafique, Abid Mehmood, Mourad Elhadef, Survey of security protocols and vulnerabilities in unmanned aerial vehicles, IEEE Access 9 (2021) 46927–46948.

[20] Simon Parkinson, Paul Ward, Kyle Wilson, Jonathan Miller, Cyber threats facing autonomous and connected vehicles: Future challenges, IEEE Trans. Intell. Transp. Syst. 18 (11) (2017) 2898–2915.

[21] Kyounggon Kim, Jun Seok Kim, Seonghoon Jeong, Jo-Hee Park, Huy Kang Kim, Cybersecurity for autonomous vehicles: Review of attacks and defense, Comput. Secur. 103 (2021) 102150.

[22] Mission planner. https://ardupilot.org/planner/.

[23] QGroundControl. http://qgroundcontrol.com/.

[24] Chenxi Liu, Tony Q.S. Quek, Jemin Lee, Secure UAV communication in the presence of active eavesdropper, in: 2017 9th International Conference on Wireless Communications and Signal Processing, WCSP, IEEE, 2017, pp. 1–6.

[25] Azade Fotouhi, Haoran Qiang, Ming Ding, Mahbub Hassan, Lorenzo Galati Giordano, Adrian Garcia-Rodriguez, Jinhong Yuan, Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges, IEEE Commun. Surv. Tutor. 21 (4) (2019) 3417–3442.

[26] Ottilia Westerlund, Rameez Asif, Drone hacking with raspberry-pi 3 and WiFi pineapple: Security and privacy threats for the internet-of-things, in: 2019 1st International Conference on Unmanned Vehicle Systems-Oman, UVS, 2019.

[27] Shahrear Iqbal, A study on UAV operating system security and future research challenges, in: 2021 IEEE 11th Annual Computing and Communication Workshop and Conference, CCWC, 2021, pp. 0759–0765.

[28] Michael Hooper, Yifan Tian, Runxuan Zhou, Bin Cao, Adrian P Lauf, Lanier Watkins, William H Robinson, Wlajimir Alexis, Securing commercial WiFi-based UAVs from common security attacks, in: Military Communications Conference, 2016, pp. 1213–1218.

[29] Common vulnerabilities & exposures (CVE). https://cve.mitre.org/.

[30] Lee Pike, Pat Hickey, Trevor Elliott, Eric Mertens, Aaron Tomb, Trackos: A security-aware real-time operating system, in: International Conference on Runtime Verification, Springer, 2016, pp. 302–317.

[31] Randall K Nichols, Hans C Mumm, Wayne D Lonstein, Julie JCH Ryan, Candice Carter, John-Paul Hood, Unmanned Aircraft Systems in the Cyber Domain, New Prairie Press, 2019.

[32] Sofia Belikovetsky, Mark Yampolskiy, Jinghui Toh, Jacob Gatlin, Yuval Elovici, dr0wned–{cyber-physical} attack with additive manufacturing, in: 11th USENIX Workshop on Offensive Technologies (WOOT 17), 2017.

[33] Ionut Ilascu, DJI drone flight logs, photos and videos exposed to unauthorized access. https://www.bleepingcomputer.com/news/security/dji-drone-flight-logs-photos-and-videos-exposed-to-unauthorized-access/.

[34] Timothy Trippel, Ofir Weisse, Wenyuan Xu, Peter Honeyman, Kevin Fu, WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks, in: 2017 IEEE European Symposium on Security and Privacy (EuroS&P), IEEE, 2017, pp. 3–18.

[35] Benyamin Farshteindiker, Nir Hasidim, Asaf Grosz, Yossi Oren, How to phone home with someone else's phone: Information exfiltration using intentional sound noise on gyroscopic sensors, in: 10th {USENIX} Workshop on Offensive Technologies ({WOOT} 16), 2016.

[36] Yunmok Son, Hocheol Shin, Dongkwan Kim, Youngseok Park, Juhwan Noh, Kibum Choi, Jungwoo Choi, Yongdae Kim, Rocking drones with intentional sound noise on gyroscopic sensors, in: 24th {USENIX} Security Symposium ({USENIX} Security 15), 2015, pp. 881–896.

[37] Kevin Fu, Wenyuan Xu, Risks of trusting the physics of sensors, Commun. ACM 61 (2) (2018) 20–23.

[38] Raul Quinonez, Jairo Giraldo, Luis Salazar, Erick Bauman, Alvaro Cardenas, Zhiqiang Lin, {SAVIOR}: Securing autonomous vehicles with robust physical invariants, in: 29th {USENIX} Security Symposium ({USENIX} Security 20), 2020, pp. 895–912.

[39] Hung Manh La, Ronny Lim, Weihua Sheng, Multirobot cooperative learning for predator avoidance, IEEE Trans. Control Syst. Technol. 23 (1) (2014) 52–63.

[40] Sitong Zhang, Yibing Li, Qianhui Dong, Autonomous navigation of UAV in multi-obstacle environments based on a deep reinforcement learning approach, Appl. Soft Comput. 115 (2022) 108194.

[41] Gan Liu, Ying Tan, Lingfeng Chen, Wenchuan Kuang, Binghua Li, Feng Duan, Chi Zhu, The development of a UAV target tracking system based on YOLOv3-tiny object detection algorithm, in: 2021 IEEE International Conference on Robotics and Biomimetics, ROBIO, 2021, pp. 1636–1641.

[42] Danilo Avola, Luigi Cinque, Anxhelo Diko, Alessio Fagioli, Gian Luca Foresti, Alessio Mecca, Daniele Pannone, Claudio Piciarelli, MS-faster R-CNN: Multi-stream backbone for improved faster R-CNN object detection and aerial tracking from UAV images, Remote Sens. 13 (9) (2021) 1670.

[43] Nicolas Papernot, Patrick McDaniel, Somesh Jha, Matt Fredrikson, Z Berkay Celik, Ananthram Swami, The limitations of deep learning in adversarial settings, in: 2016 IEEE European Symposium on Security and Privacy (EuroS&P), IEEE, 2016, pp. 372–387.

[44] Christian Szegedy, Wojciech Zaremba, Ilya Sutskever, Joan Bruna, Dumitru Erhan, Ian Goodfellow, Rob Fergus, Intriguing properties of neural networks, in: 2nd International Conference on Learning Representations, ICLR 2014, 2014.

[45] Antonio Emanuele Cinà, Kathrin Grosse, Ambra Demontis, Sebastiano Vascon, Werner Zellinger, Bernhard A Moser, Alina Oprea, Battista Biggio, Marcello Pelillo, Fabio Roli, Wild patterns reloaded: A survey of machine learning security against training data poisoning, 2022, arXiv preprint arXiv:2205.01992.

[46] Hengrui Jia, Christopher A Choquette-Choo, Varun Chandrasekaran, Nicolas Papernot, Entangled watermarks as a defense against model extraction, in: 30th USENIX Security Symposium (USENIX Security 21), 2021, pp. 1937–1954.

[47] Yingqi Liu, Shiqing Ma, Yousra Aafer, Wen-Chuan Lee, Juan Zhai, Weihang Wang, Xiangyu Zhang, Trojaning attack on neural networks, 2017, Purdue E-Pubs.

[48] Xingshuo Han, Guowen Xu, Yuan Zhou, Xuehuan Yang, Jiwei Li, Tianwei Zhang, Clean-annotation backdoor attack against lane detection systems in the wild, 2022, arXiv preprint arXiv:2203.00858.

[49] Drew Davidson, Hao Wu, Rob Jellinek, Vikas Singh, Thomas Ristenpart, Controlling UAVs with sensor input spoofing attacks, in: 10th {USENIX} Workshop on Offensive Technologies ({WOOT} 16), 2016.

[50] Yulong Cao, Chaowei Xiao, Benjamin Cyr, Yimeng Zhou, Won Park, Sara Rampazzi, Qi Alfred Chen, Kevin Fu, Z Morley Mao, Adversarial sensor attack on lidar-based perception in autonomous driving, in: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, 2019, pp. 2267–2281.

[51] Katrina M Mansfield, Timothy J Eveleigh, Thomas H Holzer, Shahryar Sarkani, DoD Comprehensive Military Unmanned Aerial Vehicle Smart Device Ground Control Station Threat Model, Technical Report, Defense Acquisition Univ Ft Belvoir Va, 2015.

[52] Katharina L Best, Jon Schmid, Shane Tierney, Jalal Awan, Nahom M Beyene, Maynard A Holliday, Raza Khan, Karen Lee, How to Analyze the Cyber Threat from Drones: Background, Analysis Frameworks, and Analysis Tools, Technical Report, Rand Arroyo Center Santa Monica Ca, 2020.

[53] Kim Hartmann, Christoph Steup, The vulnerability of UAVs to cyber attacks-an approach to the risk assessment, in: 2013 5th International Conference on Cyber Conflict (CYCON 2013), IEEE, 2013, pp. 1–23.

[54] Xiaofang Sun, Derrick Wing Kwan Ng, Zhiguo Ding, Yanqing Xu, Zhangdui Zhong, Physical layer security in UAV systems: Challenges and opportunities, IEEE Wirel. Commun. 26 (5) (2019) 40–47.

[55] Reham M. Fouda, Security vulnerabilities of cyberphysical unmanned aircraft systems, IEEE Aerosp. Electron. Syst. Mag. 33 (9) (2018) 4–17.

[56] C.G. Leela Krishna, Robin R. Murphy, A review on cybersecurity vulnerabilities for unmanned aerial vehicles, in: 2017 IEEE International Symposium on Safety, Security and Rescue Robotics, SSRR, IEEE, 2017, pp. 194–199.

[57] Ahmad Y Javaid, Weiqing Sun, Vijay K Devabhaktuni, Mansoor Alam, Cyber security threat analysis and modeling of an unmanned aerial vehicle system, in: 2012 IEEE Conference on Technologies for Homeland Security, HST, IEEE, 2012, pp. 585–590.

[58] Leonard Petnga, Huan Xu, Security of unmanned aerial vehicles: Dynamic state estimation under cyber-physical attacks, in: 2016 International Conference on Unmanned Aircraft Systems, ICUAS, 2016.

[59] Vyacheslav Kharchenko, Volodymyr Torianyk, Cybersecurity of the internet of drones: Vulnerabilities analysis and imeca based assessment, in: 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies, DESSERT, IEEE, 2018, pp. 364–369.

[60] İlker Bekmezci, Eren Şentürk, Tolgahan Türker, Security issues in flying ad-hoc networks (FANETS), J. Aeronaut. Space Technol. 9 (2) (2016) 13–21.

[61] Michael Robinson, Knocking My Neighbor's Kid's Cruddy Drone Offline, Vol. 23, DEF CON, 2016.

[62] Aaron Luo, Drones Hijacking, Tech. Rep, DEF CON, Paris, France, 2016.

[63] Himanshu Sharma, Neeraj Kumar, Raj Kumar Tekchandani, Nazeeruddin Mohammad, Deep learning enabled channel secrecy codes for physical layer security of UAVs in 5G and beyond networks, in: ICC 2022-IEEE International Conference on Communications, IEEE, 2022, pp. 1–6.

[64] Krishna Sampigethaya, Aircraft cyber security risk assessment: Bringing air traffic control and cyber-physical security to the forefront, in: AIAA Scitech 2019 Forum, 2019, p. 0061.

[65] Jue Wang, Xuanxuan Wang, Ruifeng Gao, Chengleyang Lei, Wei Feng, Ning Ge, Shi Jin, Tony QS Quek, Physical layer security for UAV communications in 5G and beyond networks, 2021, arXiv preprint arXiv:2105.11332.

[66] Yuan Xu, G Deng, Tianwei Zhang, Qiu Han, Yungang Bao, Novel denial-of-service attacks against cloud-based multi-robot systems, Inform. Sci. 576 (2021) 329–344.

[67] Nils Rodday, Hacking a professional drone, Black Hat Asia 2016 (2016).

[68] Riham Altawy, Amr M. Youssef, Security, privacy, and safety aspects of civilian drones: A survey, ACM Trans. Cyber-Phys. Syst. 1 (2) (2016) 1–25.

[69] Samy Kamkar, SkyJack: autonomous drone hacking, 2013, Online. http://samy.pl/skyjack.

[70] D'Hondt Alexandre, Pasquazzo Yannick, Hacking drones with dronesploit, Black Hat Arsenal 2019 (2019).

[71] Kate Highnam, Kevin Angstadt, Kevin Leach, Westley Weimer, Aaron Paulos, Patrick Hurley, An uncrewed aerial vehicle attack scenario and trustworthy repair architecture, in: 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop (DSN-W), IEEE, 2016, pp. 222–225.

[72] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, et al., Experimental security analysis of a modern automobile, in: 2010 IEEE Symposium on Security and Privacy, IEEE, 2010, pp. 447–462.

[73] Jiacheng Tang, Shiping Shao, Jiguo Song, Abhishek Gupta, Nash equilibrium control policy against bus-off attacks in CAN networks, IEEE Trans. Inf. Forensics Secur. (2022).

[74] Kun Cheng, Yuebin Bai, Yuan Zhou, Yun Tang, David Sanan, Yang Liu, CANeleon: Protecting CAN bus with frame ID chameleon, IEEE Trans. Veh. Technol. 69 (7) (2020) 7116–7130.

[75] Charlie Miller, Chris Valasek, Remote exploitation of an unaltered passenger vehicle, Black Hat USA 2015 (S 91) (2015) 1–91.

[76] Mubark Jedh, Lotfi Ben Othmane, Noor Ahmed, Bharat Bhargava, Detection of message injection attacks onto the can bus using similarities of successive messages-sequence graphs, IEEE Trans. Inf. Forensics Secur. 16 (2021) 4133–4146.

[77] Pal-Stefan Murvay, Bogdan Groza, Security shortcomings and countermeasures for the SAE J1939 commercial vehicle bus protocol, IEEE Trans. Veh. Technol. 67 (5) (2018) 4325–4339.

[78] Manuel J Fernandez, Pedro J Sanchez-Cuevas, Guillermo Heredia, Anibal Ollero, Securing UAV communications using ROS with custom ECIES-based method, in: 2019 Workshop on Research, Education and Development of Unmanned Aerial Systems (RED UAS), IEEE, 2019, pp. 237–246.

[79] Ruffin White, Dr Christensen, I Henrik, Dr Quigley, et al., SROS: Securing ROS over the wire, in the graph, and through the kernel, 2016, arXiv preprint arXiv:1611.07060.

[80] B.S. Rajatha, C.M. Ananda, S. Nagaraj, Authentication of mav communication using caesar cipher cryptography, in: 2015 International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials, ICSTM, IEEE, 2015, pp. 58–63.

[81] Abdulhadi Shoufan, Hassan AlNoon, Joonsang Baek, Secure communication in civil drones, in: International Conference on Information Systems Security and Privacy, Springer, 2015, pp. 177–195.

[82] Samuel Woo, Hyo Jin Jo, Dong Hoon Lee, A practical wireless attack on the connected car and security protocol for in-vehicle CAN, IEEE Trans. Intell. Transp. Syst. 16 (2) (2014) 993–1006.

[83] Neil Butcher, Angela Stewart, Saad Biaz, Securing the Mavlink Communication Protocol for Unmanned Aircraft Systems, Appalachian State University, Auburn University, USA, 2013.

[84] Azza Allouch, Omar Cheikhrouhou, Anis Koubâa, Mohamed Khalgui, Tarek Abbes, MAVSec: Securing the mavlink protocol for ardupilot/PX4 unmanned aerial systems, in: 2019 15th International Wireless Communications & Mobile Computing Conference, IWCMC, IEEE, 2019, pp. 621–628.

[85] Asmaa Abdallah, M. Zulfiker Ali, Jelena Mišić, Vojislav B Mišić, Efficient security scheme for disaster surveillance UAV communication networks, Information 10 (2) (2019) 43.

[86] Jiang Bian, Remzi Seker, Mengjun Xie, A secure communication framework for large-scale unmanned aircraft systems, in: 2013 Integrated Communications, Navigation and Surveillance Conference, ICNS, IEEE, 2013, pp. 1–12.

[87] S. Leung-Yan-Cheong, M. Hellman, The Gaussian wire-tap channel, IEEE Trans. Inform. Theory 24 (4) (1978) 451–456.

[88] Stuart H Rubin, William K Grefe, Thouraya Bouabana-Tebibel, Shu-Ching Chen, Mei-Ling Shyu, Kenneth S Simonsen, Cyber-secure UAV communications using heuristically inferred stochastic grammars and hard real-time adaptive waveform synthesis and evolution, in: 2017 IEEE International Conference on Information Reuse and Integration, IRI, IEEE, 2017, pp. 9–15.

[89] Huiming Wang, Xu Zhang, Jia-Cheng Jiang, UAV-involved wireless physical-layer secure communications: Overview and research directions, IEEE Wirel. Commun. 26 (5) (2019) 32–39.

[90] Guangchi Zhang, Qingqing Wu, Miao Cui, Rui Zhang, Securing UAV communications via trajectory optimization, in: GLOBECOM 2017-2017 IEEE Global Communications Conference, IEEE, 2017, pp. 1–6.

[91] Guangchi Zhang, Qingqing Wu, Miao Cui, Rui Zhang, Securing UAV communications via joint trajectory and power control, IEEE Trans. Wireless Commun. 18 (2) (2019) 1376–1389.

[92] Miao Cui, Guangchi Zhang, Qingqing Wu, Derrick Wing Kwan Ng, Robust trajectory and transmit power design for secure UAV communications, IEEE Trans. Veh. Technol. 67 (9) (2018) 9042–9046.

[93] Peng Yang, Kun Guo, Xing Xi, Tony Q.S. Quek, Xianbin Cao, Chenxi Liu, Fresh, fair and energy-efficient content provision in a private and cache-enabled UAV network, IEEE J. Sel. Top. Sign. Proces. 16 (1) (2022) 97–112.

[94] Wali Ullah Khan, Eva Lagunas, Zain Ali, Muhammad Awais Javed, Manzoor Ahmed, Symeon Chatzinotas, Björn Ottersten, Petar Popovski, Opportunities for physical layer security in UAV communication enhanced with intelligent reflective surfaces, IEEE Wirel. Commun. 29 (6) (2022) 22–28.

[95] Nan Zhao, Fen Cheng, F Richard Yu, Jie Tang, Yunfei Chen, Guan Gui, Hikmet Sari, Caching UAV assisted secure transmission in hyper-dense networks based on interference alignment, IEEE Trans. Commun. 66 (5) (2018) 2281–2294.

[96] Hamed Bastami, Mehdi Letafati, Majid Moradikia, Ahmed Abdelhadi, Hamid Behroozi, Lajos Hanzo, On the physical layer security of the cooperative rate-splitting-aided downlink in UAV networks, IEEE Trans. Inf. Forensics Secur. 16 (2021) 5018–5033.

[97] Hoon Lee, Subin Eom, Junhee Park, Inkyu Lee, UAV-aided secure communications with cooperative jamming, IEEE Trans. Veh. Technol. 67 (10) (2018) 9385–9392.

[98] Martin Strohmeier, Vincent Lenders, Ivan Martinovic, Intrusion detection for airborne communication using PHY-layer information, in: International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Springer, 2015, pp. 67–77.

[99] Robert Mitchell, Ray Chen, Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications, IEEE Trans. Syst. Man Cybern. 44 (5) (2013) 593–604.

[100] Adrian Taylor, Nathalie Japkowicz, Sylvain Leblanc, Frequency-based anomaly detection for the automotive CAN bus, in: 2015 World Congress on Industrial Control Systems Security, WCICSS, IEEE, 2015, pp. 45–49.

[101] Wonsuk Choi, Hyo Jin Jo, Samuel Woo, Ji Young Chun, Jooyoung Park, Dong Hoon Lee, Identifying ecus using inimitable characteristics of signals in controller area networks, IEEE Trans. Veh. Technol. 67 (6) (2018) 4757–4770.

[102] Kyong-Tak Cho, Kang G. Shin, Fingerprinting electronic control units for vehicle intrusion detection., in: USENIX Security Symposium, Vol. 40, 2016, pp. 911–927.

[103] Thabet Kacem, Duminda Wijesekera, Paulo Costa, Alexandre Barreto, An ADS-B intrusion detection system, in: 2016 IEEE Trustcom/BigDataSE/ISPA, IEEE, 2016, pp. 544–551.

[104] Silvia Gil Casals, Philippe Owezarski, Gilles Descargues, Generic and autonomous system for airborne networks cyber-threat detection, in: 2013 IEEE/AIAA 32nd Digital Avionics Systems Conference, DASC, IEEE, 2013, pp. 4A4–1.

[105] KwangMin Koo, Woo-yeob Lee, Sung-Ryung Cho, Inwhee Joe, A secure operating system architecture based on linux against communication offense with root exploit for unmanned aerial vehicles, J. Inf. Process. Syst. 16 (1) (2020) 42–48.

[106] Elley, Amazon IoT operating system freertos has serious vulnerabilities, 2018, https://blog.360totalsecurity.com/en/amazon-iot-operating-system-freertos-has-serious-vulnerabilities/.

[107] Bai Li, Brief reverse engineering work on FIMI-A3. https://www.4hou.com/posts/7XwA.

[108] Omar M. Alhawi, Mustafa A. Mustafa, Lucas C. Cordiro, Finding security vulnerabilities in unmanned aerial vehicles using software verification, in: 2019 International Workshop on Secure Internet of Things, SIOT, IEEE, 2019, pp. 1–9.

[109] Xianghao Ye, Research on UAV System Security Vulnerability Discovering Based on Fuzzing (Ph.D. thesis), Xidian University, 2020.

[110] Taegyu Kim, Chung Hwan Kim, Junghwan Rhee, Fan Fei, Zhan Tu, Gregory Walkup, Xiangyu Zhang, Xinyan Deng, Dongyan Xu, RVFuzzer: Finding input validation bugs in robotic vehicles through control-guided testing, in: USENIX security symposium, 2019, pp. 425–442.

[111] Abraham A Clements, Naif Saleh Almakhdhub, Khaled S Saab, Prashast Srivastava, Jinkyu Koo, Saurabh Bagchi, Mathias Payer, Protecting bare-metal embedded systems with privilege overlays, in: 2017 IEEE Symposium on Security and Privacy, SP, IEEE, 2017, pp. 289–303.

[112] Zachary Birnbaum, Andrey Dolgikh, Victor Skormin, Edward O'Brien, Daniel Muller, Christina Stracquodaine, Unmanned aerial vehicle security using recursive parameter estimation, J. Intell. Robot. Syst. 84 (1) (2016) 107–120.

[113] Fan Fei, Zhan Tu, Ruikun Yu, Taegyu Kim, Xiangyu Zhang, Dongyan Xu, Xinyan Deng, Cross-layer retrofitting of UAVs against cyber-physical attacks, in: 2018 IEEE International Conference on Robotics and Automation, ICRA, IEEE, 2018, pp. 550–557.

[114] Hyungsub Kim, Muslum Ozgur Ozmen, Z Berkay Celik, Antonio Bianchi, Dongyan Xu, PGPATCH: Policy-guided logic bug patching for robotic vehicles, in: 2022 IEEE Symposium on Security and Privacy, SP, IEEE, 2022, pp. 1826–1844.

[115] V'ıctor Mayoral, Lander Usategui San Juan, Bernhard Dieber, Unai Ayucar Carbajo, Endika Gil-Uriarte, Introducing the robot vulnerability database (rvd), 2019, arXiv preprint arXiv:1912.11299.

[116] Yazhou Tu, Zhiqiang Lin, Insup Lee, Xiali Hei, Injected and delivered: Fabricating implicit control over actuation systems by spoofing inertial sensors, in: 27th {USENIX} Security Symposium ({USENIX} Security 18), 2018, pp. 1545–1562.

[117] Woohyun Kim, Jiwon Seo, Low-cost software-defined GPS simulator with the capability of time synchronization, in: 2018 18th International Conference on Control, Automation and Systems, ICCAS, IEEE, 2018, pp. 1087–1090.

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

[119] Alexandre Vervisch-Picois, Nel Samama, Thierry Taillandier-Loize, Influence of gnss spoofing on drone in automatic flight mode, in: ITSNT 2017: 4th International Symposium of Navigation and Timing, Ecole nationale de l'aviation civile, 2017, pp. 1–9.

[120] Daojing He, Yinrong Qiao, Shiqing Chen, Xiao Du, Wenjie Chen, Sencun Zhu, Mohsen Guizani, A friendly and low-cost technique for capturing non-cooperative civilian unmanned aerial vehicles, IEEE Netw. 33 (2) (2018) 146–151.

[121] Jie Su, Jianping He, Peng Cheng, Jiming Chen, A stealthy gps spoofing strategy for manipulating the trajectory of an unmanned aerial vehicle, IFAC-PapersOnLine 49 (22) (2016) 291–296.

[122] Chen Yan, Wenyuan Xu, Jianhao Liu, Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle, Def Con 24 (8) (2016) 109.

[123] Hocheol Shin, Dohyun Kim, Yujin Kwon, Yongdae Kim, Illusion and dazzle: Adversarial optical channel exploits against lidars for automotive applications, in: International Conference on Cryptographic Hardware and Embedded Systems, Springer, 2017, pp. 445–467.

[124] Grant Roth, Simulation of the Effects of Acoustic Noise on Mems Gyroscopes (Ph.D. thesis), Auburn University, 2009.

[125] Pregassen Soobramaney, Mitigation of the Effects of High Levels of High-Frequency Noise on Mems Gyroscopes (Ph.D. thesis), Auburn University, 2013.

[126] Hongjun Choi, Wen-Chuan Lee, Yousra Aafer, Fan Fei, Zhan Tu, Xiangyu Zhang, Dongyan Xu, Xinyan Deng, Detecting attacks against robotic vehicles: A control invariant approach, in: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, 2018, pp. 801–816.

[127] Chen Liang, Meixia Miao, Jianfeng Ma, Hongyan Yan, Qun Zhang, Xinghua Li, Teng Li, Detection of GPS spoofing attack on unmanned aerial vehicle system, in: International Conference on Machine Learning for Cyber Security, Springer, 2019, pp. 123–139.

[128] Zhiwei Feng, Nan Guan, Mingsong Lv, Weichen Liu, Qingxu Deng, Xue Liu, Wang Yi, An efficient uav hijacking detection method using onboard inertial measurement unit, ACM Trans. Embedded Comput. Syst. (TECS) 17 (6) (2018) 1–19.

[129] Jason Bonior, Philip Evans, Greg Sheets, John Paul Jones, Toby Flynn, Lori Ross O'Neil, William Hutton, Richard Pratt, Thomas Carroll, Implementation of a wireless time distribution testbed protected with quantum key distribution, in: 2017 IEEE Wireless Communications and Networking Conference, WCNC, IEEE, 2017, pp. 1–6.

[130] Brady W O'Hanlon, Mark L Psiaki, Jahshan A Bhatti, Daniel P Shepard, Todd E Humphreys, Real-time GPS spoofing detection via correlation of encrypted signals, Navig. J. Inst. Navig. 60 (4) (2013) 267–278.

[131] Andrew J. Kerns, Kyle D. Wesson, Todd E. Humphreys, A blueprint for civil GPS navigation message authentication, in: 2014 IEEE/ION Position, Location and Navigation Symposium-PLANS 2014, IEEE, 2014, pp. 262–269.

[132] Kyle Wesson, Mark Rothlisberger, Todd Humphreys, Practical cryptographic civil GPS signal authentication, Navig. J. Inst. Navig. 59 (3) (2012) 177–193.

[133] Panagiotis Papadimitratos, Aleksandar Jovanovic, GNSS-based positioning: Attacks and countermeasures, in: MILCOM 2008-2008 IEEE Military Communications Conference, IEEE, 2008, pp. 1–7.

[134] Tianci Yang, Chen Lv, A secure sensor fusion framework for connected and automated vehicles under sensor attacks, IEEE Internet Things J. (2021).

[135] Zhiyang Ju, Hui Zhang, Ying Tan, Deception attack detection and estimation for a local vehicle in vehicle platooning based on a modified UFIR estimator, IEEE Internet Things J. 7 (5) (2020) 3693–3705.

[136] Cheolhyeon Kwon, Inseok Hwang, Reachability analysis for safety assurance of cyber-physical systems against cyber attacks, IEEE Trans. Automat. Control 63 (7) (2017) 2272–2279.

[137] Marco Ceccato, Francesco Formaggio, Nicola Laurenti, Stefano Tomasin, Generalized likelihood ratio test for GNSS spoofing detection in devices with IMU, IEEE Trans. Inf. Forensics Secur. 16 (2021) 3496–3509.

[138] Nils Ole Tippenhauer, Christina Pöpper, Kasper Bonne Rasmussen, Srdjan Capkun, On the requirements for successful GPS spoofing attacks, in: Proceedings of the 18th ACM Conference on Computer and Communications Security, 2011, pp. 75–86.

[139] Kai Jansen, Matthias Schäfer, Daniel Moser, Vincent Lenders, Christina Pöpper, Jens Schmitt, Crowd-gps-sec: Leveraging crowdsourcing to detect and localize gps spoofing attacks, in: 2018 IEEE Symposium on Security and Privacy, SP, IEEE, 2018, pp. 1018–1031.

[140] Jaroslaw Magiera, Ryszard Katulski, Detection and mitigation of GPS spoofing based on antenna array processing, J. Appl. Res. Technol. 13 (1) (2015) 45–57.

[141] Keum-Cheol Kwon, Duk-Sun Shim, Performance analysis of direct GPS spoofing detection method with AHRS/accelerometer, Sensors 20 (4) (2020) 954.

[142] Barak Davidovich, Ben Nassi, Yuval Elovici, VISAS–detecting GPS spoofing attacks against drones by analyzing camera's video stream, 2022, arXiv preprint arXiv:2201.00419.

[143] Ian J. Goodfellow, Jonathon Shlens, Christian Szegedy, Explaining and harnessing adversarial examples, 2014, arXiv preprint arXiv:1412.6572.

[144] Jiachen Sun Sun, Yulong Cao Cao, Qi Alfred Chen, Z Morley Mao, Towards robust lidar-based perception in autonomous driving: General black-box adversarial sensor attack and countermeasures, in: USENIX Security Symposium (Usenix Security'20), 2020.

[145] Qixue Xiao, Yufei Chen, Chao Shen, Yu Chen, Kang Li, Seeing is not believing: Camouflage attacks on image scaling algorithms., in: USENIX Security Symposium, 2019, pp. 443–460.

[146] Yi Zhu, Chenglin Miao, Tianhang Zheng, Foad Hajiaghajani, Lu Su, Chunming Qiao, Can we use arbitrary objects to attack LiDAR perception in autonomous driving? in: Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, CCS '21, Association for Computing Machinery, New York, NY, USA, 2021, pp. 1945–1960.

[147] Junjie Shen, Jun Yeon Won, Zeyuan Chen, Qi Alfred Chen, Drift with devil: Security of multi-sensor fusion based localization in high-level autonomous driving under GPS spoofing, in: Proceedings of the 29th USENIX Conference on Security Symposium, 2020, pp. 931–948.

[148] Zhi Sun, Sarankumar Balakrishnan, Lu Su, Arupjyoti Bhuyan, Pu Wang, Chunming Qiao, Who is in control? Practical physical layer attack and defense for mmwave-based sensing in autonomous vehicles, IEEE Trans. Inf. Forensics Secur. 16 (2021) 3199–3214.

[149] Kyo Kim, Siddhartha Nalluri, Ashish Kashinath, Yu Wang, Sibin Mohan, Miroslav Pajic, Bo Li, Security analysis against spoofing attacks for distributed UAVs, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security(CCS'16), Association for Computing Machinery, New York, NY, 2020, http://dx.doi.org/10.1145/2976749.2978388.

[150] Cihang Xie, Jianyu Wang, Zhishuai Zhang, Yuyin Zhou, Lingxi Xie, Alan Yuille, Adversarial examples for semantic segmentation and object detection, in: Proceedings of the IEEE International Conference on Computer Vision, 2017, pp. 1369–1378.

[151] Shang-Tse Chen, Cory Cornelius, Jason Martin, Duen Horng Polo Chau, Shapeshifter: Robust physical adversarial attack on faster r-cnn object detector, in: Joint European Conference on Machine Learning and Knowledge Discovery in Databases, Springer, 2018, pp. 52–68.

[152] Xingxing Wei, Siyuan Liang, Ning Chen, Xiaochun Cao, Transferable adversarial attacks for image and video object detection, in: Proceedings of the 28th International Joint Conference on Artificial Intelligence, 2019, pp. 954–960.

[153] Bin Yan, Dong Wang, Huchuan Lu, Xiaoyun Yang, Cooling-shrinking attack: Blinding the tracker with imperceptible noises, in: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2020, pp. 990–999.

[154] Anish Athalye, Logan Engstrom, Andrew Ilyas, Kevin Kwok, Synthesizing robust adversarial examples, in: International Conference on Machine Learning, PMLR, 2018, pp. 284–293.

[155] David Held, Sebastian Thrun, Silvio Savarese, Learning to track at 100 fps with deep regression networks, in: European Conference on Computer Vision, Springer, 2016, pp. 749–765.

[156] Edan Habler, Asaf Shabtai, Using LSTM encoder-decoder algorithm for detecting anomalous ADS-B messages, Comput. Secur. 78 (2018) 155–173.

[157] G Panice, Salvatore Luongo, Gabriella Gigante, Domenico Pascarella, Carlo Di Benedetto, Angela Vozella, Antonio Pescapè, A SVM-based detection approach for GPS spoofing attacks to UAV, in: 2017 23rd International Conference on Automation and Computing, ICAC, 2017.

[158] Alireza Abbaspour, Kang K Yen, Shirin Noei, Arman Sargolzaei, Detection of fault data injection attack on uav using adaptive neural network, Procedia Comput. Sci. 95 (2016) 193–200.

[159] Yang Sun, Chunjie Cao, Junxiao Lai, Tianjiao Yu, Anti GPS spoofing method for UAV based on LSTM-KF model, Chin. J. Netw. Inf. Secur. 6 (5) (2020) 80.

[160] Abdulhadi Shoufan, Continuous authentication of uav flight command data using behaviometrics, in: 2017 IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC), IEEE, 2017, pp. 1–6.

[161] Chaitanya Rani, Hamidreza Modares, Raghavendra Sriram, Dariusz Mikulski, Frank L Lewis, Security of unmanned aerial vehicle systems against cyber-physical attacks, J. Defense Model. Simul. 13 (3) (2016) 331–342.

[162] Richard S. Sutton, Andrew G. Barto, Reinforcement Learning: An Introduction, MIT Press, 2018.
[163] David Silver, Aja Huang, Chris J Maddison, Arthur Guez, Laurent Sifre, George Van Den Driessche, Julian Schrittwieser, Ioannis Antonoglou, Veda Panneershelvam, Marc Lanctot, et al., Mastering the game of go with deep neural networks and tree search, Nature 529 (7587) (2016) 484–489.
[164] Ronnie Johansson, Peter Hammar, Patrik Thorén, On simulation-based adaptive UAS behavior during jamming, in: 2017 Workshop on Research, Education and Development of Unmanned Aerial Systems (RED-UAS), IEEE, 2017, pp. 78–83.
[165] Huimin Lu, Yujie Li, Shenglin Mu, Dong Wang, Hyoungseop Kim, Seiichi Serikawa, Motor anomaly detection for unmanned aerial vehicles using reinforcement learning, IEEE Internet Things J. 5 (4) (2017) 2315–2322.
[166] Zihan Lin, Xiaozhen Lu, Canhuang Dai, Geyi Sheng, Liang Xiao, Reinforcement learning based UAV trajectory and power control against jamming, in: International Conference on Machine Learning for Cyber Security, Springer, 2019, pp. 336–347.
[167] Bo Yang, Min Liu, Attack-resilient connectivity game for UAV networks using generative adversarial learning, in: Proceedings of the 18th International Conference on Autonomous Agents and MultiAgent Systems, 2019, pp. 1743–1751.
[168] Anibal Sanjab, Walid Saad, Tamer Başar, A game of drones: Cyber-physical security of time-critical UAV applications with cumulative prospect theory perceptions and valuations, IEEE Trans. Commun. 68 (11) (2020) 6990–7006.
[169] Liang Xiao, Caixia Xie, Minghui Min, Weihua Zhuang, User-centric view of unmanned aerial vehicle transmission against smart attacks, IEEE Trans. Veh. Technol. 67 (4) (2017) 3420–3430.
[170] Mulong Luo, Andrew C. Myers, G. Edward Suh, Stealthy tracking of autonomous vehicles with cache side channels, in: 29th USENIX Security Symposium (USENIX Security 20), 2020, pp. 859–876.