A Design Scheme and Security Analysis of Unmanned Aerial Vehicle

Dongyu Yang[1,2,3(✉)], Yue Zhao[1,2,3], Kaijun Wu[1,2,3], Zhongqiang Yi[1,2,3], and Haiyang Peng[1,2,3]

[1] Science and Technology on Communication Security Laboratory, Chengdu 610041, China
[2] No. 30 Research Institute of China Electronics Technology Group Corporation, Chengdu 610041, China
[3] China Electronics Technology Cyber Security Co., Ltd., Chengdu 610041, China

Abstract. Since the 21st century, informatization, modernization and intellectualization have become an important direction of national science and technology development. Especially in recent years, with the continuous improvement and perfection of artificial intelligence, 5G, edge computing and autonomous unmanned technology, the UAV industry has made unprecedented development and has been applied to many fields of military and civil, such as: information collection, investigation and combat integration, geological mapping, border defense inspection, emergency rescue, power inspection, traffic supervision, intelligent logistics, pesticide spraying, meteorological monitoring, etc. However, with the continuous development of UAV business, more and more researchers realize that UAV depends on security and effective information system and network connection, and the cyber security problem of UAV is becoming increasingly prominent. The cyber security research of UAV has become a new subject. This paper first elaborates the development of UAV through a large number of researches. Secondly, according to the current development status of UAV, the future development trend of UAV is analyzed. Then, focusing on the communication, network and system of UAV, the security threats faced by UAV are elaborated and analyzed in detail. After that, the new cyber security problems caused by UAV are analyzed from three aspects of important infrastructure security, public security and privacy security. Finally, the paper gives suggestions on the future development of UAV from the perspective of cyber security, which provides a strong support for solving the cyber security problems of UAV.

Keywords: UAV · Cyber security · Communication security · Privacy security

1 Introduction

UAV is the abbreviation of unmanned aerial vehicle, which refers to the unmanned aircraft controlled by radio remote control or self-contained program. It can fly autonomously or remotely, carry a variety of mission equipment, perform a variety of tasks, and can be used once or repeatedly [1].

Q. Guo et al. (Eds.): WiSATS 2021, LNICST 410, pp. 554–567, 2022.
https://doi.org/10.1007/978-3-030-93398-2_50

With the development of unmanned technology, the concept of UAV is constantly enriched and evolved. In the 1920s, the newly emerging UAV was known as pilotless aircraft. In the 1930s, UAV was more used as target aircraft, known as drone. In the early 1950s, UAV controlled by radio signal, known as radio controlled aerial target (RCAT). In the mid-1950s, unmanned aerial vehicle (UAV) was equipped with reconnaissance function, known as surveillance drone. In the 1960s, UAV was equipped with remote control function, known as remote piloted vehicle (RPV). In the 1980s, unmanned aerial vehicle (UAV) can perform autonomous or preset tasks, which is called unmanned aircraft (UMA),unmanned aerial vehicle (UAV) has been widely used since 1990s [2].

With the rapid development of information technology, UAV related technology is becoming more and more mature. According to report [3], in recent years, the scale of UAV market has maintained a rapid growth trend of 50% every year, and the annual sales volume of UAV is expected to reach 4.33 million by 2020. It is estimated that sales of UAVs will exceed $12 billion by 2021. With the continuous development of UAV business, UAV is more and more advanced, and the cyber security problem of UAV is very prominent. Due to the characteristics of UAV and its communication structure, when the attacker intercepts the communication information or hijacks the UAV itself, it will bring serious consequences to the user and the surrounding environment. Furthermore, in addition to being vulnerable to attack, UAV itself can also be used as a new means of cyber attack.

This paper is divided into six sections, the second section introduces the development of UAV in detail. The third section analyzes the development trend of UAV. In the fourth section, the cyber security threats of UAV are described in detail from three aspects of communication, network and system. In the fifth section, the cyber security problems caused by UAV as a new means of cyber attack are analyzed in detail from three aspects of important infrastructure, public security and privacy security. The sixth section summarizes the full text and some suggestions are put forward for the development of UAV from the perspective of cyber security.

2 Overview of UAV Development

The global UAV industry is in the stage of vigorous development, and all countries in the world are aware of the huge application potential and broad application prospects of UAV in military and civil fields.

The development of UAV has gone through the following stages: 1920–1960 is the initial stage, and UAV was often used as target aircraft. 1960–1980 is the practical stage, and UAV was used in the battlefield. Since 1990 is the high-speed development stage, and a large number of modern and intelligent UAVs have emerged.

2.1 Initial Stage

The development of UAV can be traced back to 1917, when the Royal Aircraft Establishment (RAE) developed the world's first unmanned aircraft. In 1918, France's first radio controlled aircraft was successfully tested. In 1921, Britain developed the

world's first practical unmanned target aircraft, which can fly at a speed of 160km/h at an altitude of nearly 2 km. In September 1931, Fairey Company refitted the "Queen" manned biplane into a "Fairey Queen" target aircraft, as shown in Fig. 1. In 1933, Britain developed the famous "Queen Bee" drone, which produced 420 drones from 1934 to 1943. In 1948, the American Ryan Aeronautical Company began to develop a high subsonic, jet propelled target aircraft, which was later known as the "Fire Bee" target aircraft. Due to the successful design, mass production began in 1953, and soon 1280 early "Fire Bee" Q-2A and KDA were in service in the US armed forces and the Royal Canadian air force.

At this stage, in addition to the United Kingdom and the United States, France, Italy, Australia, Canada, Israel, Japan and Germany have also developed many target aircraft. The development of unmanned target aircraft drives the development of key technologies of UAV, such as remote control and telemetry technology, flight control and guidance technology, small engine technology, launch and recovery technology and special equipment for UAV. In the development process of UAV, UAV technology has broken through the speed limits of low speed, high subsonic speed and supersonic speed, as well as the airspace flight limits of ultra-low altitude, low altitude, medium altitude and high altitude, laying a foundation for the comprehensive development of UAV in the future [4].

Fig. 1. Fire bee

2.2 Practical Stage

In 1960, the American Ryan Aeronautical Company began to try to transform "Fire Bee" into a kind of unmanned reconnaissance aircraft 147A with low radar

detectability, longer voyage and better maneuverability. Later, it quickly improved and completed the 147B with longer voyage, and then developed the famous 147D "Firefly" unmanned reconnaissance aircraft.

Military UAV is the first large-scale application in Vietnam battlefield. During the Vietnam War, the "Fire Bee" series of unmanned high altitude reconnaissance aircraft were used for as many as 3435, and had carried out such tasks as high altitude and ultra-low altitude photo reconnaissance, electronic eavesdropping, jamming the communication of Vietnam radio station, scattering metal chaff in the air corridor to escort the bombers, of which 2873 sorties returned safely, with a battle damage rate of only 16%.

The outstanding performance of "Fire Bee" reconnaissance UAV in Vietnam battlefield makes people realize the new value of UAV, and also makes UAV used in actual combat for the first time as combat equipment, opening up a new stage of UAV application and development. During the Middle East War, Israel successively developed two kinds of unmanned reconnaissance aircraft: "Scout" and "Mastiffs", which are used to collect radar signals and conduct photoelectric composite reconnaissance. These two kinds of unmanned reconnaissance aircraft can be deployed flexibly and have all-weather working ability. Since then, Pakistan, India, Singapore, Iraq, Iran and other countries have carried out the development of unmanned reconnaissance aircraft, and made great progress.

2.3 High-Speed Development Stage

Since the 1980s, the military value of UAV has been gradually valued by the military of all countries. After the 1990s, several high-tech local wars have provided a broader stage for UAV to show its combat capability. Guided by the needs of war, UAV has entered a stage of rapid rise and rapid development.

Since the 1990s, many countries have placed UAV development in an important strategic position, and the investment has increased year by year. At present, there are nearly 1000 kinds of UAV systems developed by 57 countries in the world, among which nearly 400 have become UAV products. The United States has occupied the technological commanding height of UAV development. Israel started early and has characteristics and advantages in Tactical UAV and long endurance UAV. Russia has never relaxed the development and application of advanced technology. European countries and Asian countries have also accelerated the pace of UAV development and set off a climax of UAV development in the world.

In the civil field, UAV is more and more used in all walks of life. The agricultural UAV uses the high-precision camera to realize the real-time monitoring of crop growth and the surrounding soil moisture, and accordingly sowing, watering, fertilizing and spraying pesticides. Through the aerial survey and aerial exploration of UAV, mineral deposits and other resources can be found, and the local geological conditions can be monitored at any time to guide the development of resources. In daily use, UAVs can patrol important public facilities such as roads, railways, high-voltage wires and oil and gas pipelines to reduce accidents. The application of UAV in many industries in the civil field has promoted social progress and gradually become an important growth point to promote social and economic development.

3 UAV Development Trend

Looking forward to the future, UAV technology will continue to improve, mission will continue to expand, the number of equipment will continue to grow. At the same time, UAVs will continue to develop in the direction of diversification, intelligence and swarming, so as to better adapt to various complex environments.

3.1 System Performance Level

With the development of new power and energy, diversified detection, identification technology, advanced communication and control technology, the capability of UAV system such as mission duration, situation awareness, information transmission and autonomous control will be greatly increased in the future, and higher, farther, larger, smaller and faster UAV Systems will continue to be applied.

3.2 Application Fields

In the military aspect, it will continue to improve the application scope, flexibility, efficiency and adaptability of the unmanned system, and ultimately cover all mission fields such as ground, sea, air, missile defense and network power attack and defense. In the civil aspect, it will have broad market development prospects in the fields of Agriculture, forestry, animal husbandry and sideline fishing, entertainment, logistics, emergency rescue, public services and other industries.

3.3 The Level of Intelligent Autonomy

Mastering autonomous ability is the ultimate goal of unmanned system development. With the gradual improvement of the autonomy of the unmanned system, the human intervention required by the unmanned system in the process of completing the task will be greatly reduced in the future. Finally, the unmanned system will have the ability of autonomous learning and adapting to the environment, and be able to make decisions independently and provide suggestions to human beings, so as to achieve a higher level of more autonomous “man-in-the-loop” or even “man out of the loop”. In addition, the intelligent technology of unmanned system will develop rapidly in the direction of aggregating many single agents to realize swarm intelligence, robust architecture and more efficient cost ratio.

3.4 Human Machine Cooperation

It is an important development direction for all kinds of unmanned systems to realize the cooperative combat capability between manned and unmanned systems. The U.S. military has further emphasized the coordinated development and joint application of unmanned equipment in its latest unmanned system roadmap. The U.S. Army plans to build a modern force composed of manned unmanned system teams. The U.S. Air Force has verified the ability of manned and UAV formation to independently attack targets. The U.S. Navy is vigorously promoting the coordinated development of air,

surface and underwater unmanned systems. With the development of human-computer force, the cross domain cooperative combat capability of underwater, surface and air man-machine formation has been verified, trying to build a new maritime combat system with high efficiency and cooperation.

3.5 Swarm

Unmanned system swarm is a kind of low-cost unmanned system with an index of 10 or 100. It is like a bee colony performing tasks in groups and rapidly assembling in local areas to form large-scale equipment advantages. It has the characteristics of swarm substitution mobility, quantity improvement ability and cost creation advantages. It is an important development direction of unmanned system. The United States has carried out swarm research of unmanned systems, conducted dozens of swarm tests of UAVs and unmanned boats, and conducted grouping and maneuvering flight tests. In the past two years, China and the United States have refreshed the scale record of UAV swarm flight for four times. In 2017, China completed 119 UAV swarm flight tests, which broke the world record of UAV swarm test again. The competition between China and the United States in this field is becoming increasingly fierce.

4 UAV: The Target of Cyber Attacks

UAV is mainly includes the following parts: UAV system, ground control station and communication link to transmit information, as shown in Fig. 2. The UAV system includes power system, main controller, communication link module, sensor and task execution unit. The ground control station includes remote controller, intelligent terminal and communication link module [5]. The control command is transmitted to the UAV platform through the ground control station, and the data collected by the UAV platform and its operation data are also transmitted to the ground control station [6]. UAV relies on security and effective information system and network connection, which makes UAV become a new network attack target. These network attacks may destroy the control system of UAV, hijack UAV or sneak into the data collected by UAV and take it away. With the continuous development of UAV business, the cyber security problems of UAV become increasingly prominent [7, 8]. At present, the cyber security problems of UAV mainly focus on communication security, cyber security and system security.

4.1 Security Threats of UAV Communication

The UAV completes the flight mission under the guidance and control of the ground control station. The communication link between the UAV and the ground control station is used to exchange control commands and data. Generally, Ku band tactical communication data link (TCDL) is used in satellite communication, and C-band radio signal, 2.4 GHz wireless signal or wireless data transmission are used in communication between UAV and ground control station [9]. Because wireless signal is the main communication mode between UAV and controller, UAV receives command or

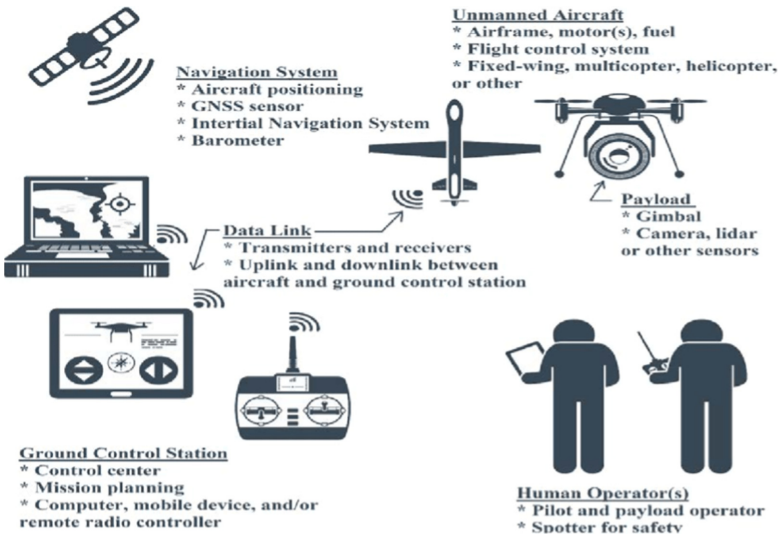

Fig. 2. UAV components

transmits information through communication link. Once the communication link is attacked, it is like closing the "ears" of UAV.

The attack mode of UAV communication link can be divided into three layers: signal layer, protocol layer and system layer. Signal layer attack is mainly against the tracking of transmission channel and the cracking of signal receiving and sending. Protocol layer attack is against the communication protocol by identifying and analyzing the protocol itself and the loopholes existing in the implementation. System layer attack is mainly about the attack methods against the operating system and various application software. The countermeasure of signal layer needs accurate communication protocol, while the countermeasure of protocol layer needs the modulation of signal layer and the control of system layer. The system layer needs the other two layers to provide physical access. At present, the main attacks on UAV communication link are as follows:

1. Eavesdropping attack
   Due to the lack of encryption and other protection mechanisms, UAV information interacting in an open environment can be directly accessed by the enemy.
2. Information injection attack
   If there is no proper authentication scheme, the opponent can disguise as a legal entity to inject false information or commands. One of them is man in the middle attack. As the intermediary between UAV and remote control, attacker can steal and tamper with communication information.
3. Denial of service attack (DOS)/Distributed denial of service attack (DDoS)
   If there is no proper DOS/DDoS Defense mechanism, single or many hijacked systems attack the target UAV, resulting in the UAV refusing to provide services to its legitimate users.

4. Flooding attack
   Usually send a large number of SYN, UDP, ICMP and Ping packets, causing network congestion. Buffer overflow attack forces the buffer overflow of network devices, making the network card unable to accept new requests.
5. Interference attack
   Transmit high-power multi band radio to interfere with the communication of UAV, or use the vulnerability of WIFI communication to remove the communication connection between UAV and ground control station.

The attack on UAV communication link can directly affect the normal operation of UAV, and even gain control of the UAV. Successfully invade the UAV and obtain full authority, not only can control the flight function of the UAV, but also browse, copy, and tamper with the data stored on the UAV at will.

4.2 Security Threats of UAV Network

In some application scenarios, multiple UAVs or cooperation between UAVs and other facilities may be required to complete a task. UAV network can be seen as a flying wireless network [10]. Each UAV can be a network data transceiver node or a network relay The UAV network can be self-organized or based on ground or satellite infrastructure support [11]. The air communication network composed of multiple UAVs is called Mobile ad hoc Network (MANET), which mostly adopts ad hoc mode architecture [12]. According to the topology type, Manet can be divided into planar topology and hierarchical topology. In the planar topology, each node in the network plays an equal role in routing calculation, message sending and receiving. Planar Topology Routing Protocols generally include AODV, DSR and OLSR [13]. In the hierarchical topology, the UAV nodes in the network are divided into multiple groups, each group has a group head, which is responsible for the topology management and communication between groups. The group heads of multiple groups can form a higher level network, and the higher level group heads are selected to form a multi-level network. The group head in each group is selected by the group members, which is dynamic and self-organized. Hierarchical Topology Routing Protocols generally include ZRP, LANMAR and CGSR.

As the UAV network is a subclass of mobile ad hoc network, the existing attacks of traditional mobile ad hoc network will also threaten the UAV ad hoc network, such as denial of service attack, black hole attack and so on. However, there are some special cyber security requirements in UAV ad hoc network.

1. Denial of service attack
   The traditional denial of service attack is that the attacker makes the network service abnormal by occupying a large number of system resources, so as to make the legitimate users unable to use the service normally. Similarly, the same idea can be adopted for UAV, but it has a greater impact on UAV ad hoc network, and even leads to the fall and destruction of UAV, threatening ground facilities and the masses. For example, Vasconcelos [14] and others used tools such as hping3 to implement a denial of service attack on drone 2.0, which made the legitimate operators unable to control the UAV and eventually led to the UAV crash.

2. Black hole attack
   The attack mode of black hole attack is that the malicious node disguises itself as the best path node by using the defects of routing protocol, so when forwarding packets, it will give priority to the malicious node as a relay node, that is, change the routing table. However, when the normal node in the UAV network forwards the packet to the malicious node, the malicious node will not transmit the packet to the next node in the routing table, but directly discard it, which leads to the failure of control command transmission. When the UAV at the edge of UAV group wants to receive the command sent by the controller, it needs the relay forwarding of the middle UAV. When the malicious UAV enters the UAV network, the malicious UAV will not continue to forward the data, which makes the edge UAV unable to receive the control command.

4.3 Security Threats of UAV System

UAV system refers to the sum of the various parts that make up the UAV system, which is usually composed of aircraft subsystem, remote control and navigation subsystem, mission equipment subsystem, data communication subsystem and support equipment. The security threats of UAV system mainly focus on sensors, positioning system and system software.

1. Sensor security threats
   The sensors of UAV collect environment data from physical domain and feed back to UAV control system to assist UAV to issue control instructions. When the sensor is attacked, the wrong data will be collected, making the control system unable to give correct instructions, resulting in the UAV flying out of control and even crashing.
2. Positioning system security threat
   GPS is an important sensor of UAV, which is responsible for providing accurate position information for UAV. When the attacker collects some public information of GPS system, such as signal definition, communication link, communication protocol. They can calculate the location, time and other information of each GPS transmission according to the attack target, and through high-power transmission of forged GPS signal with specific direction, they can cheat the UAV to choose the false signal with higher receiving strength, so as to achieve the purpose of deceptive attack. For example, the attacker can send the jamming signal with the same frequency as GPS, so that the GPS receiver cannot receive the normal signal, and can also send the high-power forged GPS signal, so that the UAV GPS can receive the forged GPS signal and get the wrong location information.
3. Software security threats
   Both the underlying software and the flight control software of the UAV have certain security vulnerabilities, and hackers can use these security vulnerabilities to launch attacks on the UAV. For example, the UAV flight control software Maldrone has a security loophole. Attackers can enter the UAV system through this loophole, or install a backdoor program on the control end to steal UAV data or perform

remote control. In addition, ZigBee chip threat and keyboard Trojan horse threat are also the means of attack against UAV software.

5 UAV: A New Means of Cyber Attack

From the perspective of cyber security, UAV has two sides. On the one hand, UAV becomes a new target of network attack, which causes data leakage and hijacking by means of UAV equipment vulnerability or network attack. On the other hand, UAV has become a new way of network attack. UAV may provide a new way for network attack. By injecting worms into the target's data and network, UAV can carry out data penetration attack or other attacks, thus destroying its key infrastructure. In addition, as shown in Table 1, the widespread use of UAV also brings new problems to public security and data privacy.

Table 1. Part of the UAV security events

NO.	Event description
1	On February 24, 2015, five UAVs of unknown origin hovered over the US consulate in Paris
2	On September 15, 2013, German President Angela Merkel was at a campaign rally when a drone crashed in front of a number of senior executives and Merkel herself
3	In April 2015, a drone carrying radioactive material fell on the Japanese Prime Minister's residence
4	On June 30, 2013, a man used a remote-controlled UAV to take aerial photos of letoria hospital
5	From 1995 to 2014, there were hundreds of terrorist attacks against politicians' UAVs carrying explosives, chemical or biological weapons, of which only 16 were cracked
6	In November 2014, 20 UAVs flew over many nuclear facilities in France
7	At the end of 2014, after a damaged nuclear reactor in Belgium was reopened, it was visited by a micro UAV the next day
8	On January 28, 2015, some light UAVs flew to the anchorage of Brest military port, which is a French nuclear military base with four nuclear submarines capable of submarine launched nuclear missiles
9	On January 26, 2015, a UAV broke into the no fly zone of the White House and fell in the zone. In this process, the air defense radar system did not find the whereabouts of the aircraft
10	On August 14, 2015, a drone crashed while flying near HMP Pentonville prison in the United States. Police intercepted a large number of drugs and mobile phones it was carrying
11	On January 22, 2015, an unmanned aerial vehicle (UAV) on the U.S. - Mexico border crashed due to overloading and tried to transport drugs and weapons
12	Mike Tassey and rich Perkins, former members of the U.S. air force, have successfully built an unmanned reconnaissance plane, which can perform Wi-Fi password cracking, phone tapping, SMS interception, etc

5.1 Cyber Attack Performance of UAV

In addition to being vulnerable to attack, UAV itself can also be used as a weapon to launch network attacks. According to its network attack performance, UAV can be divided into jamming UAV, eavesdropping UAV and defensive UAV.

1. Jamming UAV
   Selex Glileo, a US Italian technology military contractor, has designed a small UAV for electronic warfare and cyber attacks. The main purpose of its design is to interfere with the surface to air missile system. UAV can interfere with the communication system of the target, such as Bluetooth or Wi-Fi signal. It can also control suicide missiles, electronic warfare equipment will automatically delete its stored data before it is destroyed.
2. Eavesdropping UAV
   Septier Communications, an Israeli company, launched its first drone in 2017 to eavesdrop on phone calls and transmit data from smart phones. The UAV is equipped with a network listener, which can monitor the data of 2G, 3G and 4G networks. The maximum monitoring range of the UAV is one kilometer, which means that it cannot be physically detected by its monitoring target. This UAV is very likely to use proximity degradation attack to force devices in high security network to reduce the security level, such as from 4G to 2G. At this time, the UAV is not an unmanned vehicle, but a high-end camera for physical monitoring or attack.
3. Defensive UAV
   With the rise of the military UAV market, the anti UAV market, as a balancing force, also rises. The Cyber-Box UAV sold by Israel company in 2015 can detect and control the UAVs around the equipment boundary. By maintaining a kind of radio frequency jamming weapon, DoS attack or zero day vulnerability attack can be carried out on the UAV until the enemy UAV is completely controlled.

5.2 The Threat of UAV to Important Infrastructure

The vulnerability of UAV can make physical access to the network and equipment of important infrastructure. Extract information from systems that are not otherwise accessible due to scope constraints. UAVs can also cover up the identity of intruders to some extent. In addition, in their recent report, the researchers highlighted the risk of UAVs penetrating critical infrastructure with high security. Researchers have shown that UAVs can be used for wireless intrusion access points, insecure networks and devices. In 2016, for example, Israeli researchers manipulated a drone near an office building and used a flaw in a radio protocol called Zigbee to invade a smart light bulb inside the building.

5.3 The Threat of UAV to Public Security

For different application scenarios, different types of UAVs play their own strengths. Military UAVs are used in battlefield and enemy intelligence collection, while civilian UAVs are used in some illegal espionage and criminal activities. For example, in 2015,

drones broke into the White House and made headlines in major media. The literature describes that UAVs may be used by criminals in terrorism, drug smuggling, unconventional weapons (such as biological and chemical weapons) attacks, etc. All of these pose a great threat to public security and cause irreparable losses to people's property security and national interests.

5.4 The Threat of UAV to Privacy

Flexible mobility makes the UAV like a "thief" can intrude into the forbidden or private airspace, equipped with high-definition cameras may pry into other people's privacy [15, 16]. Unmanned aerial vehicles (UAVs) with cameras fly to the house above the courtyard or near the window, and become "voyeurism" in the high-tech field. Even if UAVs are used for monitoring on specific occasions, there are privacy violations, such as video monitoring of parking lots, roads, parks, and so on. The privacy issues are also mentioned in [17–20] of the literature. Another example: hackers use dedicated Wi-Fi similar to fake base stations to attack passersby's mobile phones and steal personal privacy. Even the U.S. government uses spy planes with fake base stations to monitor millions of U.S. smartphones.

6 Summary

UAV brings convenience to people's life, but also faces increasingly serious cyber security problems. As a complete physical information system, UAV is used in the uncontrolled environment. UAV itself is constantly changing, and its security threats are also constantly changing. Therefore, the security protection measures of UAV must be updated. It is necessary to continuously evaluate the cyber security of UAV and find new countermeasures. Aiming at the cyber security problem of UAV, this paper gives the following suggestions:

1. From the top-level design of UAV, a complete UAV cyber security protection system should be established.
2. Researchers should pay more attention to the cyber security related topics of large UAV, and constantly pay attention to the latest technological achievements in related fields.
3. UAV, like unmanned vehicle, unmanned ship and other unmanned systems, need security systems such as firewall, and become a part of product safety standards.

Acknowledgements. This work was supported by Sichuan Science and Technology Program 2021JDRC0072.

References

1. Department of Defense (DoD). U.S. Army "Unmanned Aircraft Systems Roadmap 2010–2035". Office of the Secretary of Defense. US Fort Rucker, Alabama (2010)
2. Suraj, G., Mangesh, M., Jawandhiya, M.: Review of unmanned aircraft system (UAS). Int. J. Adv. Res. Comput. Eng. Technol. (IJARCET) **4**(2) (2013). ISSN 2278–1323
3. Schmidt, M., Shear, M.: A drone too small for radar to detect rattles the White House. http://www.suasnews.com/2015/01/a-drone-too-small-for-radar-to-detect-rattles-the-white-house/
4. Villasenor, J.: Drones and the future of domestic aviation. Proc. IEEE **102**(3), 235–238 (2014)
5. Abhishek, S., Pankhuri, V., Nikhil, P., et al.: Communication and networking technologies for UAVs: a survey. J. Netw. Comput. Appl. **168** (2020)
6. Imad, J., Nader, M., Jameela, A., et al.: Communication and networking of UAV-based systems: classification and associated architectures. J. Netw. Comput. Appl. **84**, 93–108 (2017)
7. Rodday, N., Schmidt, R., Pras, A.: Exploring security vulnerabilities of unmanned aerial vehicles. In: Network Operations & Management Symposium, pp. 993–994 (2016)
8. Javaid, Y., Sun, W., Devabhaktuni, K., et al.: Cyber security threat analysis and modeling of an unmanned aerial vehicle system. In: 2012 IEEE Conference on Technologies for Homeland Security (HST), Waltham, MA, pp. 585–590 (2012)
9. Hartmann, K., Steup, C.: The vulnerability of UAVs to cyber attacks: an approach to the risk assessment. In: 2013 5th International Conference on the Cyber Conflict (CyCon), Tallinn, Estonia, pp. 1–23 (2013)
10. Mansfield, K., Eveleigh, T., Holzer, T., et al.: Unmanned aerial vehicle smart device ground control station cyber security threat model. In: The IEEE International Conference on the Technologies for Homeland Security (HST), Waltham, USA, pp. 722–728 (2013)
11. He, D., Chan, S., Guizani, M.: Communication security of unmanned aerial vehicles. IEEE Wirel. Commun. 2–7 (2017)
12. Muhammad, A., Alamgir, S., Ijaz, M., et al.: Flying ad-hoc networks (FANETs): a review of communication architectures, and routing protocols. In: 2017 First International Conference on Latest trends in Electrical Engineering and Computing Technologies (INTELLECT), Karachi, Pakistan (2017)
13. Deng, H., Li, W., Agrawal, D.: Routing security in wireless ad hoc networks. IEEE Commun. Mag. **40**(10), 70–75 (2002)
14. Vasconcelos, G., Carrijo, G., Miani, R., et al.: The impact of DoS attacks on the AR. Drone 2.0. In: 2016 XIII Latin American Robotics Symposium and IV Brazilian Robotics Symposium (LARS/SBR), Recife, pp. 127–132 (2016)
15. Korshunov, P., Ebrahimi, T.: Using warping for privacy protection in video surveillance. In: The 18th IEEE International Conference on Digital Signal Processing (DSP), Fira, pp. 1–6 (2013)
16. Korshunov, P., Ebrahimi, T.: Using face morphing to protect privacy. In: The 10th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), Krakow, pp. 208–213 (2013)
17. Pitt, J., Perailslis, C., Michael, H.: Drones humans introduction to the special issue. Technol. Soc. Mag. **33**(2), 38–39 (2014)

18. Wilson, R.L.: Ethical issues with use of drone aircraft. In: The 2014 IEEE International Symposium on Ethics in Science, Technology and Engineering, Chicago, pp. 1–4 (2014)
19. Finn, R.L., Wright, D.: Unmanned aircraft systems: surveillance, ethics and privacy in civil applications. Comput. Law Secur. Rev. **28**(2), 184–194 (2012)
20. Villasenor, J.: Observations from above: unmanned aircraft systems and privacy. Harv. J. Law Public Policy **36**, 457 (2013)