A Design Scheme of Data Security for Unmanned Aerial Vehicles

Dongyu Yang[1,2,3](✉), Yue Zhao[1,2,3], Zhongqiang Yi[1,2,3], Dandan Yang[4], and Shanxiang He[5]

[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
jobjob2019@163.com
[3] China Electronics Technology Cyber Security Co., Ltd., Chengdu 610041, China
[4] Shanghai Tunnel Engineering & Rail Transit Design and Research Institute, Shanghai, China
[5] Chengdu Luxingtong Information Technology Co., Ltd., Chengdu, China

Abstract. Since the 21st century, informatization, modernization and intellectualization have become an important direction of 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 social life. However, with the development and popularity of UAVs, the development of emerging technologies such as autonomous analysis, unmanned traffic control, UAV swarms, and artificial intelligence continue to increase the complexity of the unmanned systems domain, making cyber attacks against UAVs more and more frequent, and the chances of security threats and potential hazards are increasing. Currently, UAV cyber security has become a very important issue, especially UAV data security, but there are few papers that give systematic solutions for UAV data security. This paper first provides a systematic analysis of UAV security threats from a data security perspective. Next, the existing UAV security protection strategies are analyzed from three aspects: UAV platform security, communication network security, and ground station security. Then, the proposed UAV data security design scheme is introduced in detail. Finally, the full paper is summarized and suggestions for the development of UAV security are given.

Keywords: UAV · Data security · Network security

1 Introduction

Compared with traditional manned aircraft, UAVs (Unmanned Aerial Vehicles) are inexpensive and flexible in use, and in recent years, with the development of UAV swarm technology, they have effectively made up for the shortcomings of smaller individual UAV loads and weaker information sensing and processing capabilities, and have seen

W. Fu and L. Yun (Eds.): ADHIP 2022, LNICST 468, pp. 165–178, 2023.
https://doi.org/10.1007/978-3-031-28787-9_13

explosive development in multiple industry sectors. However, UAVs, as an integrated system with information technology as the traction, face high-intensity information security risks and challenges, especially in complex electromagnetic environments that are more vulnerable to various types of attacks [1], such as information spoofing, false data injection, counterfeit control, signal interference, denial of service, etc.

The traditional UAV security program adopts a divide and conquer approach, mainly focusing on four aspects: sensor security, communication security, software security and network security [2], such as: sensor physical isolation technology, GPS anti-spoofing technology, malware identification technology based on feature codes [3–7], etc. This divide and conquer security scheme can only guarantee the local security of UAVs, while there are many drawbacks, specifically in the following aspects.

1. In terms of application methods, traditional security protection technologies only target individual UAVs and are not applicable to new scenarios such as UAV swarms and manned/unmanned aircraft coordination.
2. In terms of application environments, UAVs and UAV swarm are often required to perform specific tasks in complex electromagnetic environments.
3. In terms of data processing, traditional security solutions focus on security at the communication level, while new scenarios such as swarm and manned/unmanned collaboration are more concerned with the security of multi-source heterogeneous data.
4. In terms of technical means, the traditional "stacked" security protection technology is inefficient and increases the arithmetic and energy overhead of unmanned systems, which is against the principle of lightweighting.

Therefore, this paper proposes a data security service scheme for UAVs, centering on the whole lifecycle process of data collection, data transmission, data storage, data processing, data sharing and data destruction of UAVs, with data security as the core, and proposes a systematic and global security service scheme to realize sensitive information security exchange and sharing, unified authority control, security protocol provisioning and cryptographic algorithm service. The main contributions of this paper are as follows.

1. This paper provides a systematic analysis of the security threats faced by UAVs from the perspective of data security, providing a new approach to the study of UAV cyber security.
2. This paper analyzes the existing UAV security protection strategies in detail and puts forward new suggestions for UAV network security protection.
3. In this paper, a new design scheme for UAV data security is proposed, which can systematically implement UAV data security protection.

This paper is divided into five sections, the second section focuses on systematic analysis of UAV security threats from the perspective of data security. The third section analyzes the current UAV security protection strategies from three aspects: UAV platform security, communication network security, and ground station security. In the fourth section, details the proposed data security service scheme for UAVs. The fifth section summarizes the full text and some suggestions are put forward for the data security of UAVs.

2 UAV Security Threats

UAVs are not designed at the top level with much consideration for security protection, for example, in the design of security protocols, there is only simple link encryption and point-to-point authentication, leading to numerous risks and threats in network information security for UAVs, the main security threats are as follows.

2.1 System Vulnerability

Most UAVs and ground stations are using open source operating systems, and most of the various payloads of UAVs are also standalone operating systems, which may have unknown vulnerabilities that attackers can easily exploit to compromise the UAV or ground station to attack, hijack or steal data [8].

2.2 Malicious Software

Communication protocols in UAVs allow users to control UAVs via wireless remote means (e.g. tablets, laptops and cell phones). However, this approach poses a significant security risk, as an attacker could create a TCP payload of a reverse shell and inject it into the UAV's memory, which could silently install malware on the UAV's ground station system.

2.3 Interference Spoofing

Hijacking of UAV is one of the most important security threats faced by UAV. The most common ways are GPS spoofing, hardware implantation and control signal interference [9–11], among which GPS spoofing includes no-fly zone location spoofing, trajectory spoofing and return point spoofing.

1. GPS Spoofing

   The UAV receives GPS signals with this characteristic: whoever's signal is strong listens to whoever's signal is strong. GPS satellites are so far away that the signal attenuation is very much, so the signal strength will be inferior to the GPS signal faked nearby. No-fly zone location spoofing is by replaying the GPS signal in the no-fly zone near the UAV, so that the UAV will mistakenly think that it has entered the no-fly zone and thus automatically land. The UAV will fly along the selected waypoint, and when the UAV flies towards the next selected location, the trajectory

spoofing makes the UAV fly in the direction of the line connecting the spoofed location and the next scheduled location by spoofing the GPS location signal until it reaches the selected point. When the ground station and the UAV lose contact, the UAV will automatically fly toward the return point and eventually return to the return point. Return point spoofing is to control the UAV by tricking it into setting the current position as the return point and continuously changing the return direction.

2. Hardware Implantation

   The UAV determines its own position by using the GPS module. Since some of the GPS modules do not do any encryption processing on the data, the communication between the master control MCU of the UAV and the GPS module can also be effectively changed by hijacking the UAV's position information, thus achieving the effect of deception.

3. Signal Interference

   The control signal commonly used by UAVs is in the 2.4G band, and the graphics transmission is in the 5.8G band. Wi-Fi, ZigBee, Bluetooth, etc. also use the 2.4G band, and the co-channel interference is very serious and unavoidable.

In addition, attackers use jammers to create flight control jamming signals and satellite positioning jamming signals, by blocking the uplink flight control channel and satellite positioning channel of the UAV, so that it loses flight control instructions and satellite positioning information, making it unable to fly normally, and for different types of UAVs will produce the control effect of returning, landing and crashing. An attacker can also hijack a UAV by sending a de-authentication process between the access point and the device controlling the UAV, which can be performed temporarily or permanently, such as jamming the intended UAV frequency and inducing it to connect to the hacker's Wi-Fi, an attack that can be accomplished with a simple Raspberry Pi development configuration.

2.4 Data Security

UAVs are vulnerable to various attacks during data exchange and sharing, for example, data interception, malicious data injection and even installation and insertion of many infected digital files (videos, images) into ground stations.

UAV data security can be divided into three main levels [12] (see Fig. 1), the first level considers the interaction between the UAV and the user, the second and third levels involve wireless data transmission and cloud storage. The main security threats at the first level include: Malicious code/malware virus, Brute force attack, Rootkit booting, Removal of storage media for data theft, etc. At the second level include: Man-in-the-middle, Hacked/no encryption, No ecosystem access control, No network segmentation, etc. And at the third level include: Ransomware, Unverified platform access, Plaintext username & passwords, Insecure admin interface, Insecure cloud backend APIs, etc.

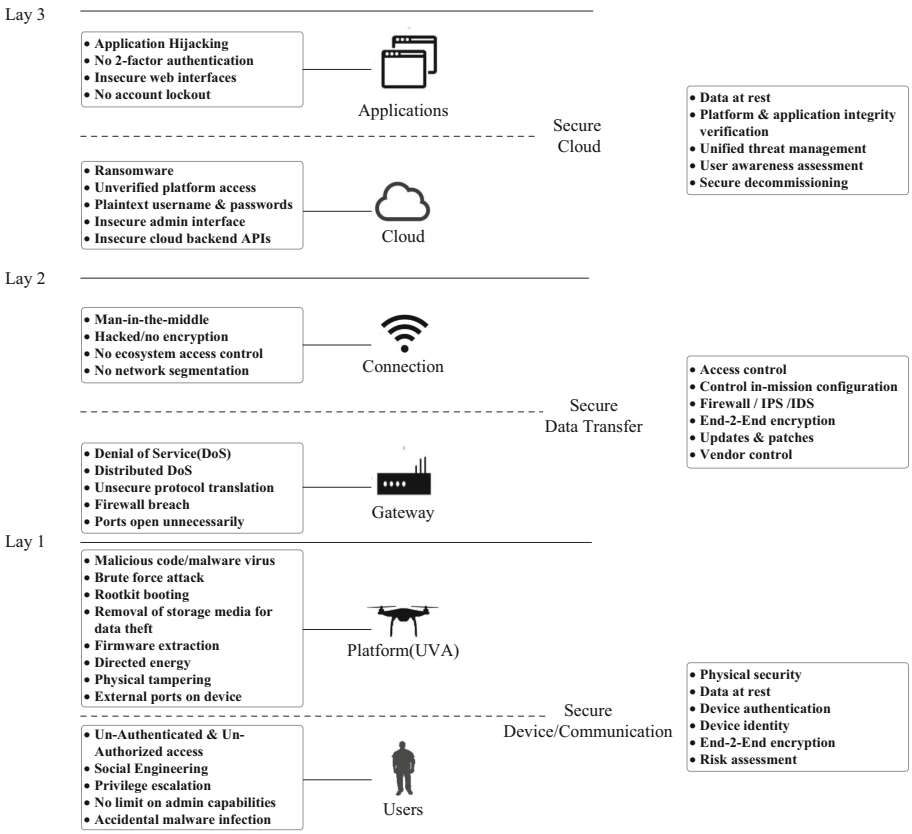

Fig. 1. The data security of UAVs

3 UAV Security Protection Strategy

UAVs are mainly composed of three parts: UAV platforms, ground stations and communication networks [13]. At present, the UAV security protection strategy involves UAV platform security, ground station security and communication network security and other aspects (see Fig. 2).

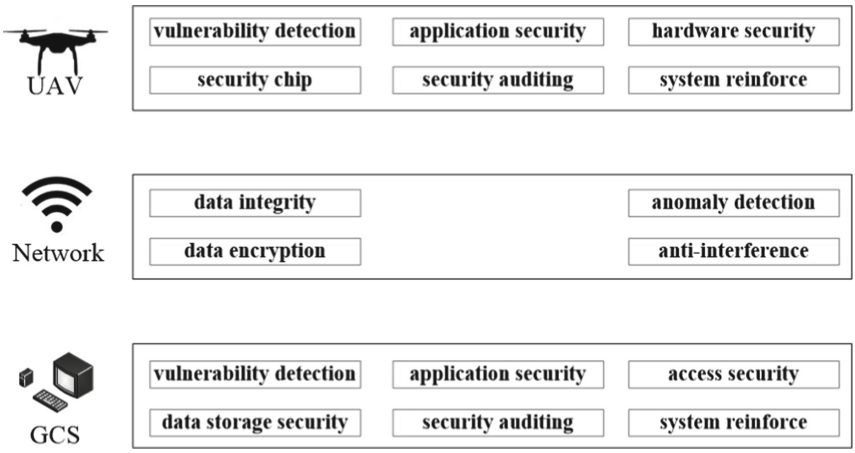

Fig. 2. UAVs security protection strategy framework

3.1 UAV Platform Security Protection Strategy

The UAV platform itself and the external terminal face numerous security threats, including viruses, malware, hijacking attacks, phishing networks, etc. Considering the characteristics of the security threats faced by the UAV itself and the external terminal, appropriate security protection measures need to be taken from hardware, access, operating system, vulnerability, application and audit to ensure the overall security of the UAV and the external terminal.

1. Hardware Security
   A security chip can be added to the main UAV control device to achieve secure external access to the main UAV control system and provide a trusted computing environment. The security chip can also provide a globally unique identity ID and an independent high-speed encryption unit without taking up system resources, which can ensure that system programs, terminal parameters, security data and user data within the chip are not tampered with or illegally accessed [14].
2. Vulnerability Detection and Repair
   By conducting security testing activities such as vulnerability scanning and penetration testing on UAVs and external terminals beforehand or on a regular basis, system vulnerabilities and risks in the system are found in a timely manner, repaired and patched, and then system upgrades are performed on UAVs and external terminals to effectively reduce the security risks of system vulnerabilities in UAVs and ensure that UAV systems are safe and controllable [15].
3. Access Security
   Because the UAV will have multiple external terminals, these terminals may become the entry point to hack the UAV to control hijack or damage the UAV. A network relationship whitelist can be established based on the network connection relationship between the UAV and the external terminal, which can be checked based on source address, destination address, source port, destination port and protocol to allow/deny packets in and out.

At the same time, a lightweight access authentication mechanism is developed for external terminals to enhance the ability of the UAV master control system to analyze the abnormal behavior of external terminals, which can prevent illegal terminal access as well as timely discovery of abnormal terminal intrusion behavior [16].

4. Application Security

   To prevent malicious program implantation by attackers on UAVs, UAVs can identify and authenticate the application software to be installed, for example, by using application signatures [17]. The UAV can use a trusted verification mechanism to verify the trusted execution of applications and important configuration files/parameters. The UAV should control the sensitive behavior of installed applications, build a system-level security protection policy, establish an internal data relationship analysis model, unify control over UAV applications, and "end" malicious applications according to the discovered "operation to prevent malicious program infection, illegal access and other attacks.

5. System Reinforcement

   As an embedded terminal, coupled with the fact that many vendors do not have security development capabilities, UAVs can be security hardened by embedding security modules, security SDKs, and other kits in the UAVs [18]. These security kits can make the UAV have the ability to receive and execute security policies, which include network access policies (black and white lists), process operation policies, etc. The kits can also perform security analysis and policy restrictions on some access, data reporting and other behaviors.

6. Security Auditing

UAVs need to conduct security audits of their own system behavior and audit important behaviors and important security events for behavioral analysis or post-event traceability of security events. Important security audits include:

- Inspection and audit of key file directories and files, including file additions, modifications, changes, etc.
- Audit protection of system process behavior to prevent unauthorized interruptions
- Monitoring of various network behaviors to detect abnormal access, system intrusion, abnormal traffic attacks, etc.
- Monitoring of system resources, including monitoring the use of CPU, memory and other resources, and timely alerts for overruns
- Audit and record system behavior, including the date and time of events, users, event types and other audit-related information

3.2 Communication Network Security Protection Strategy

At present, a variety of network communication technologies can be used among UAVs and ground stations, which include radio, Wi-Fi (2.4G or 5.8G), cellular mobile communication networks, satellite communication and other heterogeneous networks, all of which are air-port communication technologies. Also UAVs use technologies such as GPS /GLONAS in order to pinpoint the location. Hackers or attackers usually attack

and invade through these open air-ports as attack entrances [19]. So it is very important to protect the communication network security of UAVs.

The communication network security protection can be taken mainly in the following aspects.

1. Network Access Authentication
   For the UAVs communication network, access to the network must be controlled by authority, especially the Wi-Fi communication method. Access to the UAVs communication network access before the need for identity verification and authorization to ensure the legitimacy [20]. Weak passwords cannot be used for access authentication, while strict access control permissions are set for devices accessing the UAVs communication network. For the UAVs communication network, a black and white list of network access can be set, while the ports are open for control and non-essential access ports are closed.
2. Data Integrity Protection
   By establishing a data security channel between the UAV and the ground station and guaranteeing the communication quality, digital signature technology is used to provide a reliability guarantee mechanism for information transmission, guarantee the authenticity and integrity of important data, solve the credibility problem of evidence, and effectively prevent data leakage, communication content from being eavesdropped and tampered.
3. Data Transmission Encryption
   The sensitive data transmitted by the air-port is encrypted, including the use of encryption algorithms and end-to-end encryption between the UAV and the ground station to guarantee the security of data transmission. At the same time, multi-dimensional checks such as device fingerprint, time stamp, identity verification and message integrity can be performed to ensure the security of data transmission to the maximum extent [21].
4. Anti-signal Interference
   At present, the main anti-jamming technologies are divided into three categories: technologies related to improving system reliability and effectiveness, collaborative communication-based technologies, cognitive radio-based anti-jamming technologies, including technologies related to improving system reliability and effectiveness include coding anti-jamming technology, spread spectrum anti-jamming technology, multiple input and output anti-jamming technology, array antenna anti-jamming technology.

3.3 UAV Ground Station Security Protection Strategy

More advanced UAV ground station equipment typically consists of a remote control, computer, video monitor, power system, radio, and other equipment. A simple UAV ground station may only have a remote control or a computer (phone, tablet, laptop) with control software.

The security protection strategy for UAV ground stations is generally similar to that of UAV platform, but since ground stations are control terminals as well as storage terminals, they need to be strengthened in the following aspects.

1. Data Security Protection

   The ground station will store a large amount of UAV flight data, including important data such as aerial photography data. Security protection must be carried out for these data, including identity verification, data encryption, data backup and recovery, etc.
2. System Protection

   UAV ground stations need system security protection in the following aspects, including applications security, system reinforcement, vulnerability detection and repair, security baseline check, anti-DDoS attack, anti-buffer overflow, abnormal behavior detection, security audit and other security construction, which can effectively prevent ground stations from being invaded and causing system damage, data leakage, data tampering and other security problems [22].

4 UAV Data Security Scheme

Due to the numerous types of UAVs and ground stations, large business differences and weak computing power, especially consumer-grade UAVs, traditional security protection means such as firewalls and anti-virus software are not applicable. Aiming at the security threats faced by UAVs and the shortcomings of existing security protection technologies, a data security service solution for UAVs with data security as the core is designed. It realizes sensitive information security exchange and sharing, unified authority control, security protocol provisioning and cryptographic algorithm services in the whole lifecycle process of data collection, data transmission, data storage, data processing, data sharing and data destruction of UAVs, covering all links of UAV data flow, realizing security protection for the whole lifecycle of UAV platform data, and providing guarantee for the safe operation of UAVs.

4.1 UAV Data Security Service System

The UAV data security service solution designs a UAV data security service system (see Fig. 3), which consists of an runtime component, a data security component and a basic security component.

The runtime component includes a runtime library and a resource manager. The runtime library is used to provide the necessary procedures for the security service function of the unmanned platform, and the resource manager automatically configures the system environment required for the security function and manages the runtime resources according to the system properties of the unmanned platform.

Data security components are security functional components used to provide security functions including data source detection, integrity verification, tamper-proof, dense state transmission, distributed storage, data traceability, data access policy, fine-grained level data access authority control and permanent deletion during the whole life cycle of data collection, transmission, storage, exchange and sharing, processing and destruction.

The basic security components include security protocol swarms and cryptographic algorithm library, including efficient dynamic batch authentication protocol, attribute policy control protocol, lightweight group key management protocol, security protocol

negotiation protocol and base protocol, which can adapt to different mission scenarios and usage scale of UAV swarms; cryptographic algorithm library is used to provide the required cryptographic algorithms.

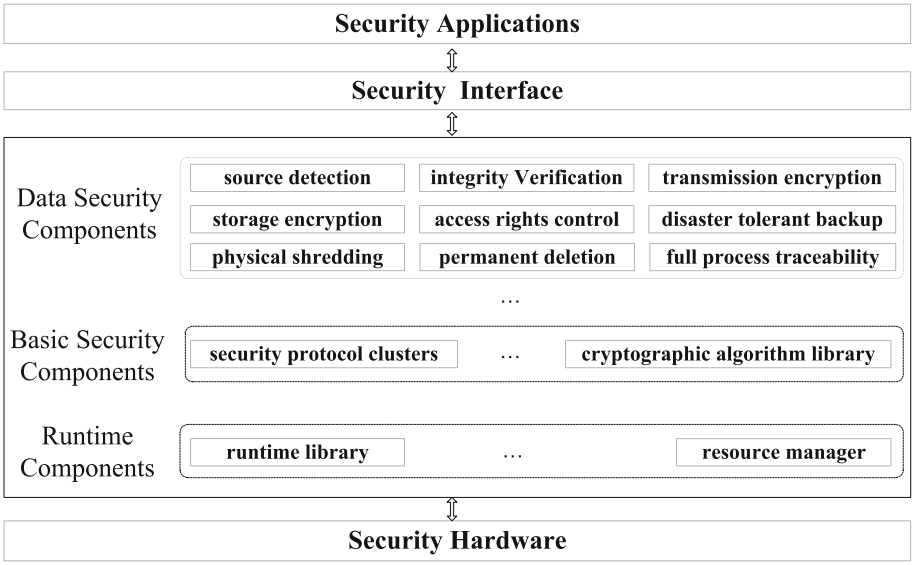

Fig. 3. The framework of UAV data security service system

4.2 System Workflow

The workflow of the UAV data security service system proposed in this paper mainly includes the following steps (see Fig. 4).

Step 1, after the security service system is transplanted to the unmanned platform, a local installation procedure is performed, and if the installation fails, the reason for the error is fed back and the installation is performed again; if the installation is successful, a connection is established with the unmanned platform's own system.
Step 2, run the basic security component to detect the unmanned platform's own system properties and security status, if the security status is abnormal, then feedback abnormal information and alarm; if the security status is normal, then automatically configure the system environment required for the security service function, while the background supervision of the system operating resources.
Step 3, after the system environment is configured, the data security component sets the initial policy for unmanned platform data access.
Step 4, when the unmanned platform task scenario or scale quantity and other circumstances change, the basic security component completes the selection of security protocols such as batch authentication protocol, data transmission protocol, attribute

policy control protocol, and key management protocol, and determines the data encryption algorithm used. At the same time, the data access policy is dynamically adjusted to achieve fine-grained level data access permission control.
Step 5, When the data access policy, security protocol and encryption algorithm are determined, the data security component carries out security protection in the processes of data collection, data transmission, data storage, data exchange and sharing, data processing and data destruction according to the access policy and protocol requirements to ensure the information security of the unmanned platform.

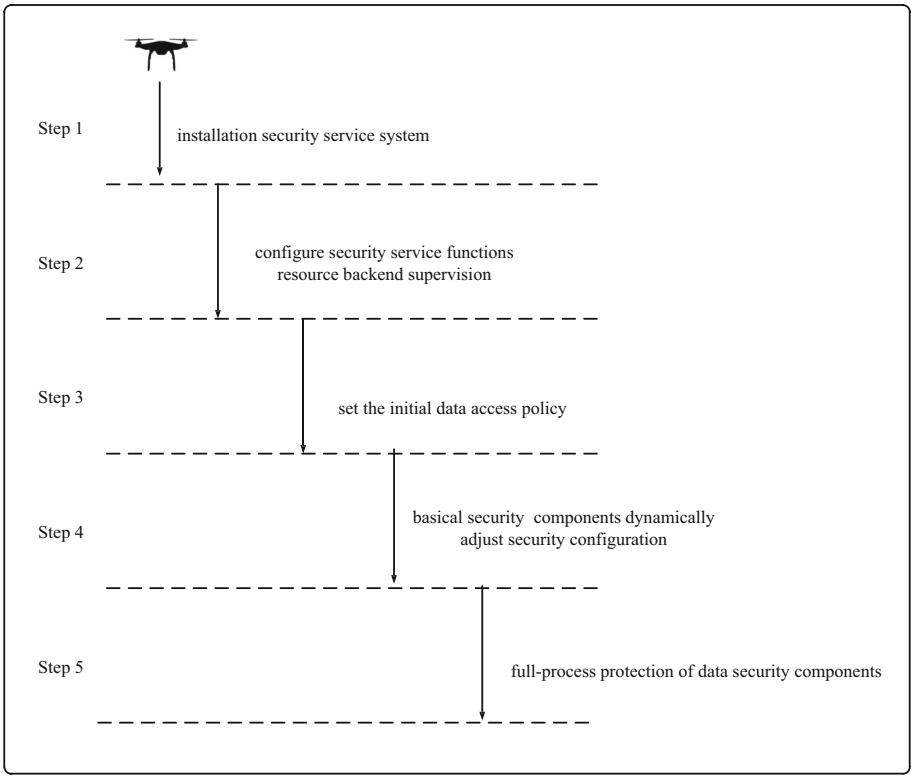

Fig. 4. The workflow of UAV data security service system

4.3 Application Scenarios

One application example of the data security solution between UAV U_1 and U_2 is shown in Fig. 5 and the specific description is as follows.

1. U_1 and U_2 travel to a predetermined target area to collect mission-related information, and the security service system mainly provides security functions such as data source identification, anti-tampering, logging and risk assessment.

2. During the information collection process, U_1 and U_2 respectively store the collected information locally and, at the same time, exchange information with each other for backup. The security service system mainly provides security functions such as data encryption transmission, dense state distributed storage and disaster-tolerant backup.
3. When the information collection is completed, U_1 and U_2 transmit the information back to the ground control center. The ground control center issues task instructions to U_1 and U_2. The security service system mainly provides security functions such as data encryption, highly reliable dense state transmission, and unified authority control.
4. U_1 and U_2 share intelligence information and collaborate to execute tasks. The security service system mainly provides security functions such as unified authority control, data integrity verification, group key management, security protocol deployment, data anti-tampering, and data traceability throughout the process.
5. When U_1 or U_2 finds a target, it immediately establishes a connection with the other party, shares this information, and makes a decision on the most optimal execution plan to complete the mission by comparing and evaluating its location, its own status and the nature of the target. The security service system mainly provides security functions such as security protocol provisioning, group key management, data security calculation, security edge calculation, integrity checking, data tampering prevention, etc.
6. After the mission, U_1 and U_2 destroy all information. The security service system mainly provides security functions such as data desensitization, key destruction, data permanent deletion, and anti-reversal.

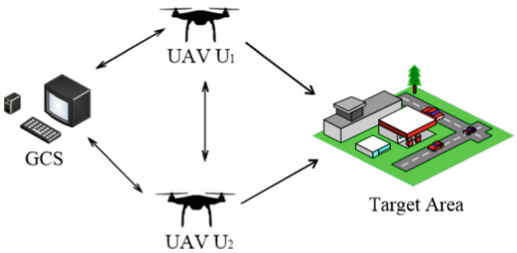

Fig. 5. One application scenarios of the UAV data security scheme

5 Summary

The continuous development of unmanned system technology has also brought new challenges to the security protection technology of unmanned system. On the one hand, the current technology only focuses on point-to-point entity authentication, link level data encryption, anti-electromagnetic interference of communication links, and safe and reliable software operation, without forming a systematic security plan. On the other hand, the safety protection means of the existing system are mostly "stacked", which

is inefficient and may affect the system itself. How to prove the safety needs to be considered from many aspects, such as verification and safety confirmation, meeting the specifications and meeting the application requirements.

Therefore, the future unmanned system security technology should focus on the following aspects:

1. Based on the information security theory of "data security as the core", supported by "artificial intelligence", "edge computing" and other emerging technologies, the cryptosystem is constructed around all links of the whole life cycle of data from generation to destruction, rather than simple channel encryption.
2. It is necessary to design a new cryptographic protocol to adapt to the high real-time, high reliability, dynamic changes of network topology and other communication characteristics faced by unmanned systems in various complex task scenarios, rather than a simple modification of the traditional Internet protocol.
3. Realize security protection for the internal data of unmanned system and the data flow between unmanned swarms, and strengthen the endogenous security of unmanned system, rather than the simple superposition of multiple security technologies.
4. With the deepening of the intelligence of unmanned systems, security configuration also needs to have a high degree of autonomy to realize the functions of key independent negotiation and dynamic adjustment of security policies.

References

1. Javaid, Y., Sun, W., Devabhaktuni, K.: 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)
2. He, D., Du, X., Qiao, Y.: A survey on cyber security of unmanned aerial vehicles. Chin. J. Comput. **42**(5), 1076–1094 (2019)
3. Roth, G.: Simulation of the effects of acoustic noise on MEMS gyroscopes (M.S. dissertation), Auburn University, Alabama, USA (2009)
4. Soobramaney P.: Mitigation of the effects of high levels of high-frequency noise on MEMS gyroscopes (Ph. D. dissertation). Auburn University, Alabama, USA (2013)
5. Lee, J.-H., Kwon, K.-C., An, D.-S., Shim, D.-S.: GPS spoofing detection using accelerometers and performance analysis with probability of detection. Int. J. Control Autom. Syst. **13**(4), 951–959 (2015). https://doi.org/10.1007/s12555-014-0347-2
6. Daneshmand, S., Jafarnia-Jahromi, A., Broumandan, A.: A low-complexity GPS anti-spoofing method using a multi-antenna array. In: Proceedings of the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation. Nashville, USA, pp. 1233–1243 (2012)
7. Shabtai A.: Malware detection on mobile devices. In: Proceedings of the 11th International Conference on Mobile Data Management. Kansas City, USA, pp. 289–290 (2010)
8. Shahrear, I.: A Study on UAV Operating System Security and Future Research Challenges. 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC). IEEE, pp. 759–765 (2021)
9. Gaspar, J., Ferreira, R., Sebastiao, P.: Capture of UAVs through GPS spoofing. In: 2018 Global Wireless Summit (GWS), pp. 21–26 (2018)

10. Riahi, M., Kenney, J.: Detection of GPS spoofing attacks on unmanned aerial systems. In: Proceedings of the 2019 16th IEEE Annual Consumer Communications and Networking Conference (CCNC), pp. 1–6 (2019)
11. Kamkar, S.: Skyjack. https://samy.pl/skyjack/. Accessed 20 Jan 2019
12. Drones and data security: a progressive look into the future. https://droneii.com/drone-data-security. Accessed 23 May 2018
13. UAV Security White Paper 2021. https://www.dbappsecurity.com.cn/. Accessed 24 Apr 2021
14. Gaurang, B., Biplab, S.: S-MAPS: scalable mutual authentication protocol for dynamic UAV swarms. IEEE Trans. Veh. Technol. **70**(11), 12088–12100 (2021)
15. How to analyze the cyber threat from drones. https://www.rand.org/pubs/research_reports/RR2972.html. Accessed 5 May 2020
16. Srinivas, J., Das, A.K., Kumar, N.: TCALAS: temporal credential-based anonymous lightweight authentication scheme for internet of drones environment. IEEE Trans. Veh. Technol. **68**(7), 6903–6916 (2019)
17. Ana, H., Alejandro, Z., Jorge, B.: Security orchestration and enforcement in NFV/SDN-aware UAV deployments. IEEE Access **8**, 131779–131795 (2020)
18. Dominic, P., Thomas, F., Christian, L.: Global and secured UAV authentication system based on hardware-security. In: 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), pp. 84–89. IEEE (2020)
19. Zhang, J., Cui, J., Zhong, H.: Intelligent drone-assisted anonymous authentication and key agreement for 5G/B5G vehicular ad-hoc networks. IEEE Trans. Netw. Sci. Eng. **8**(4), 2982–2994 (2020)
20. Abhishek, S., Pankhuri, V., Nikhil, P., et al.: Communication and networking technologies for UAVs: a survey. J. Netw. Comput. Appl. **168**, 102739 (2020)
21. Keonwoo, K., Yousung, K.: Drone security module for UAV data encryption. In: 2020 International Conference on Information and Communication Technology Convergence (ICTC), IEEE (2020)
22. Arslan, S., Abid, M., Mourad, E.: Survey of security protocols and vulnerabilities in unmanned aerial vehicles. IEEE Access **9**, 46927–46948 (2021)