Wireless secure communication involving UAV: an overview of physical layer security

Jiawei Li[1], *Ruixia* Cheng[1], *Junwen* Zhu[1], *Yu* Tian[1]and *Yiwen* Zhang[2,*]

[1]Graduate Group, Engineering University of PAP, Xi 'an 710086, China
[2]College of Information Engineering, Engineering University of PAP, Xi 'an 710086, China

Keywords: UAV, Physical layer security, Secrecy capacity.

Abstract. Unmanned aerial vehicle (UAV) is a flight device with power and energy based on computer program control, which has the characteristics of small size, light weight, high maneuverability and low cost. With its characteristics, UAV can play an important role in military and civil fields. However, due to the broadcast nature of wireless communication and inherent air-to-ground line-of-sight channel, UAV wireless communication system is more vulnerable to security threats. On the basis of traditional encryption technology, the secrecy capacity of the UAV communication system can be improved by introducing physical layer security. This article aims to study the security of the physical layer in the UAV communication system, and summarizes the latest research results on the safety communication involving UAVs on the physical layer, such as trajectory optimization, power allocation, user scheduling and cooperative UAVs. Further, some potential research directions and challenges in physical layer security of UAV system are discussed.

1 Introduction

At present, with the reduction of cost and the miniaturization of equipment, from the exclusive equipment in the military field to the popularization in the civil and commercial fields, the UAV market is gradually opening up, bringing new valuable opportunities for the future wireless communication industry. The World Radio Conference clearly defined the 5030-5091Mhz band as the legal communication band of UAV[1]. Since UAVs are at high altitude when carrying out communication missions, the air-to-ground (A2G) line-of-sight (LoS) channel can provide a powerful channel advantage compared with the ground communication channel which is seriously affected by fading and shadow. Due to its on-demand mobility, UAVs can be deployed flexibly, thus introducing new degrees of freedom. The arrival of the fifth-generation mobile communication (5G) network era in 2019 has accelerated the rapid development of UAV communication network. After obtaining the authorization of The Federal Aviation Administration (FAA), Qualcomm and American Telephone and Telegraph Company (AT&T) are also considering using UAV to provide large-scale wireless access in 5G network[2].

* Corresponding author: 28703637@qq.com

Despite the encouraging achievements of UAVs, the openness of A2G wireless channels makes secure information transmission even more challenging. The management and distribution of keys is more difficult due to the rapid mobility of UAVs. And relying on computational complexity does not guarantee complete secrecy, which would be ineffective if the enemy had powerful computing facilities. In this case, physical layer security (PLS) was proposed and developed as a key supplementary technology for secure wireless communication[3]. The basic idea of PLS is to take advantage of the random nature of wireless channels, which are keyless and thus hopefully overcome these shortcomings for secure UAV communications. Figure 1 shows the Comparison between traditional cryptology-based methods and PLS technology.

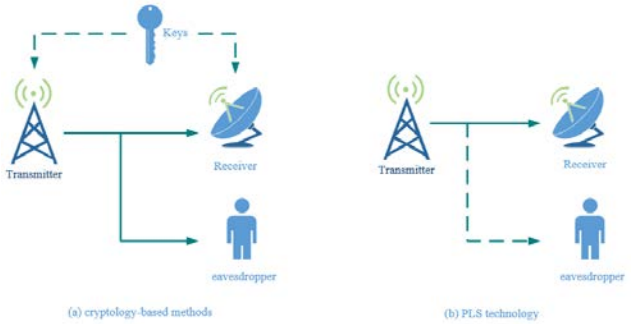

Fig. 1. Comparison between traditional cryptology-based methods and PLS technology.

The performance of PLS depends on the channel characteristics. On the one hand, the programmed mobility of the UAV can be used to adjust its trajectory to enhance communication security. On the other hand, LoS channel conditions may make UAV communications systems more vulnerable to eavesdropping. Therefore, introducing UAV into wireless communication system has both opportunities and challenges, which require careful system design and in-depth study.

Due to the opportunities and challenges brought by the UAV communication system, this article provides an important overview of the PLS issues based on UAV communication, and discusses the potential security attacks of UAV communication systems from two aspects: passive eavesdropping and active interference, providing corresponding emerging technologies. This paper mainly introduces the latest research results of UAV security communication in various typical application scenarios. Finally, the future research direction of this topic is put forward.

2 Security attack scenarios

There are many indicators to measure the security performance of a communication system, and the most common one is secrecy capacity. American mathematician Wyner first mentioned the concept of PLS and gave the definition of secrecy capacity, which played an important role in the subsequent research on PLS[4]. The secrecy capacity is determined by the quality of the main channel and the eavesdropping channel, which is equal to the difference between the capacities of the two channels, which can be expressed as:

$$C_s = C_m - C_w \tag{1}$$

In the above formula, $C_m = 1 + \log_2(1 + P / N_m)$ is the main channel capacity, and $C_W = \log_2(1 + P / N_W)$ is the eavesdropping channel capacity, variable P , N_m

and N_w respectively represent the transmission power, main channel noise power and eavesdropping channel noise power. When the signal-to-noise ratio of the main channel is better than that of the eavesdropping channel ($P / N_m > P / N_w$), secure communication is possible. In the following, we will discuss potential security attacks in UAV communication systems from the perspectives of passive eavesdropping and active jamming.

2.1 Terrestrial eavesdropping scene in A2G communication

In A2G communication, due to the influence of LoS channel, the signal received on the ground is very strong, so it becomes particularly difficult to prevent ground eavesdropping. Because eavesdroppers work passively, intending to intercept only confidential messages, they are usually silent, and UAVs do not have easy access to their location. There are three possible scenarios for eavesdropper location information:

2.1.1 Known eavesdropper complete location information

What is known about the eavesdropper's location is often difficult to obtain. If the eavesdropper is stationary, the UAV can be equipped with an optical camera or synthetic aperture radar to detect the eavesdropper's location. But the additional equipment adds extra burden to the UAV, and the cost of obtaining accurate location information is high hardware cost and excessive energy consumption.

2.1.2 Known eavesdroppers part location information

It is rare for eavesdroppers to be completely stationary. In fact, eavesdroppers are not completely stationary, but are likely to move within a certain range, making it more difficult for UAVs to obtain the precise location of eavesdroppers. By means of an optical camera or synthetic aperture radar, the UAV can be tracked to obtain some information about the eavesdropper's position. This kind of circumstance usually requires a robust analysis method, and the main performance indicators is the worst-case secrecy capability or the confidentiality interrupt probability.

2.1.3 Unknown eavesdropper location information

When the eavesdropper deliberately hides its location, it is difficult for the UAV to track and detect the hidden eavesdropper, and the UAV communication system without the eavesdropper's location information is extremely vulnerable to eavesdropping. In this case, it is difficult to ensure secure communication.

2.2 Terrestrial interference scenario in G2A communication

The legitimate ground receiver in A2G communication is easier to hide its position with the help of terrain advantages and is not vulnerable to interference. In contrast, when the legitimate UAV in G2A communication is used as the receiver, it is more vulnerable to interference attack by ground enemy nodes due to its exposure in the air. Enemy nodes on the ground send jamming signals to confuse the UAV, in order to reduce its received signal jamming noise ratio (SINR), that is, reduce the capacity of the main channel (C_m).

Therefore, active jamming is more likely to destroy the security of uav communication system than passive eavesdropping. There are two types of ground jamming nodes. One is full-duplex eavesdropper, which can send jamming signals while intercepting confidential messages[5]. The other are half-duplex eavesdroppers, which are usually deployed collaboratively to eavesdrop. Some eavesdroppers send messages that interfere with legitimate recipients, while others intercept confidential signals[6]. In this case, the UAV communication system would be extremely vulnerable because eavesdroppers could choose the right distribution based on their location.

3 PLS Strategy to Ensure the Security of UAV Communication System

In order to enhance the security performance of UAV communication system, the high mobility and flexibility of UAVs can be utilized to ensure better secure communication by adopting the strategies of physical security.

3.1 PLS strategy to protect A2G from Terrestrial eavesdropping

3.1.1 Joint optimization of trajectory and UAV communication resources

Resources in UAV communication system are limited, such as transmission power, cruise speed, user scheduling slot and frequency bandwidth. How to allocate the restricted resources reasonably is an issue to be considered, which will affect the system security performance. For example, joint optimization of UAV flight trajectory and transmission power distribution improves the safety rate of the system. However, the joint optimization problem is non-convex, so it is difficult to solve. In order to solve the problem, the alternating optimization technique is used to transform the problem into two subproblems: power allocation and trajectory optimization. Then the two subproblems are solved respectively by means of Convex optimization theory and Successive Convex Approximation (SCA), and the local optimal solutions to the original problems are obtained by means of iterative optimization[7]. Similarly, there is joint optimization of joint trajectory and user scheduling, considering a UAV security data distribution system that uses unconventional TDMA protocols to transmit confidential information to a legitimate user in each slot. In order to ensure that the information is not stolen by eavesdroppers in the system, another jamming UAV is introduced to interfere with eavesdropping, and the flight trajectory and ground user scheduling of the UAV are jointly optimized within a limited flight cycle to maximize the minimum average safety rate[8].

3.1.2 Robust trajectory optimization

When eavesdropper's partial or statistical location information is available, robust analysis can be considered to enhance the security of UAV communication systems by analyzing worst-case performance indicators. An appropriate method can be adopted to model the location uncertainty area of the eavesdropper. For example, a certain point can be used as the center of the circle to select a radius to draw a circle, and the circle area can be taken as the potential location uncertainty area of the eavesdropper. The selection of radius is related to the uncertainty of the eavesdropper's position. The greater the uncertainty, the larger the radius selected. The robust design of UAV communication system is to ensure the quality of communication service in the worst case when the eavesdropper is located in an uncertain area[9]. As shown in the figure 2, in the case of defined uncertain area, trajectory

optimization can be used to make the UAV close to the legal receiver and away from the uncertain area where the eavesdropper is located. In addition, when the UAV is close to the legal receiver, the transmitting power can be increased, and when it is closer to the uncertain area of the eavesdropper, the transmitting power can be reduced or turned off. Finally, the purpose of improving the confidentiality performance can be achieved.

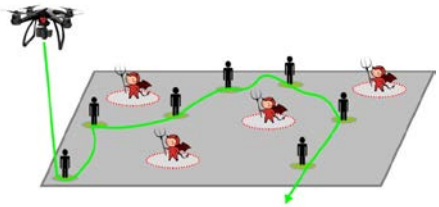

Fig. 2. Robust trajectory optimization.

3.1.3 3D beamforming

While 2D beamforming from traditional ground base stations can control the beam pattern in the azimuth plane, 3D beamforming can achieve more spatial reuse for users due to its finer beam resolution and the ability to adjust the elevation Angle and beam pattern in the azimuth plane. Although beamforming technology has a huge advantage in the physical layer security of the terrestrial communication system, the UAV communication scene usually has a LoS propagation path, which is different from the rich scattering path of terrestrial communication and limits the advantage of beamforming technology in multiplexing gain[10]. As shown in the figure 3, if the two nodes of the legitimate user on the ground and the eavesdropper are located in the same direction at the same time, even if the UAV is equipped with 3D beamforming capability and the horizontal distance is different, the lack of enough elevation Angle to distinguish between them and the rich scattering environment on the ground make the channel have more multipath effect, which cannot avoid leaking confidential messages to the eavesdropper. In addition, Distributed Collaborative Beamforming (DCBF) is a technology in Collaborative multi-point communication. Independent and randomly distributed nodes cooperate to form a virtual antenna array, and send or receive information directly with the target by means of joint beamforming. Similar to traditional array beamforming, distributed cooperative beamforming can gain the receiver SNR in communication. When multiple users on the ground receive signals from UAV at the same time, a virtual multi-antenna array will be formed, and diversity gain can also be obtained at this time[11]. Due to the mobility of UAVs, it is difficult to obtain directional beam of transmission and receiving. Therefore, the application of beamforming technology in future UAV communication is still quite challenging.

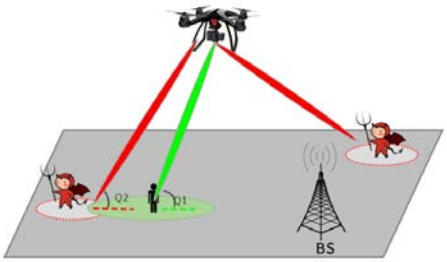

Fig. 3. 3D beamforming.

3.1.4 Artificial noise

The security problem is especially serious when the location information of eavesdropper is unknown. An effective method is to use UAV to transmit artificial noise to the null space of the legal channel and transmit confidential messages only when it is close to the legal ground receiving node. In this way, the capacity of the legal channel can be increased and the capacity of the eavesdropping channel can be reduced. Due to the need to split a portion of the power to send artificial noise, this will result in the power of sending confidential messages being weakened, because the energy carried by the UAV is very limited, so power allocation is an important issue. The optimal power allocation scheme is often difficult to find, and suboptimal solutions can usually be proposed[12]. However, in the UAV communication scenario, the UAV communication channel is more complicated due to the time-varying nature of the UAV communication network topology. Therefore, in the future UAV swarm communication network, how to effectively estimate the channel state information of high-dynamic UAV swarm becomes particularly difficult, which undoubtedly increases the difficulty in the study of artificial noise in the UAV PLS communication.

3.1.5 Multi-UAV coordination

The maneuverability and throughput of a single UAV is limited, so if there are multiple eavesdroppers in a large area, secure communication performance may not be achieved. Therefore, to achieve more effective and secure communication requires the coordinated deployment of multiple UAVs. According to the location of eavesdroppers, ground users can be divided into areas according to the actual situation, and the ground users in each area will be served by a single UAV. If a single UAV needs to avoid each eavesdropper, it will result in higher computational complexity and more energy consumption. As shown in the figure 4, if there are multiple UAVs, tasks can be assigned according to requirements and areas. Some UAVs can act as air jammers[10,13] and be deployed over nearby eavesdroppers to reduce the performance of eavesdroppers[10,13] by sending jamming signals. This in turn provides greater flexibility and convenience for the deployment or trajectory design of other UAVs to achieve better secure communication performance.

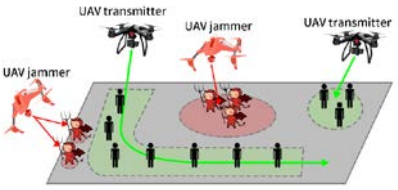

Fig. 4. Multi-UAV coordination.

3.2 PLS strategy to protect G2A from Terrestrial interference

In [14], the author discusses the G2A secure communication of hovering UAV as a legal terminal under the condition that terrestrial eavesdropping and jamming exist simultaneously. Since only the statistical channel state information (CSI) of the eavesdropper is known, the artificial noise is designed to aim at the null space of the legal channel to reduce the quality of the eavesdropping channel. Taking hybrid outage probability (combination of transmission outage probability and confidentiality outage probability) as the performance index, based on analytical expressions, the optimal power allocation strategy is obtained through Binary Search.

In order to further consider the maneuverability of UAV, the author studied the trajectory planning of UAV legal terminals against malicious interference to improve the quality of G2A secure communication in [15]. It is assumed that the position of the ground attacker and the jamming power are fixed during flight, and empirical estimates are made based on a large number of statistical values. The 3D trajectory is optimized and SCA method is used to overcome the non-convexity of the optimization problem to maximize the throughput that can be achieved throughout the flight cycle.

4 Opportunities and challenges

In fact, UAVs have irreplaceable advantages in the field of wireless communication, and there is still a long way to go in the research of their safety. With the coverage of 5G network and the development of wireless communication technology, the system and architecture of UAV auxiliary communication may appear in many new forms. Combined with new application fields and scenarios, the security related research will also have more abundant forms.

UAV channel modeling: Research on UAV channel modeling is still ongoing, and there is no unified summary. In reality, the link and channel of UAV communication will vary according to different applications and scenarios. Therefore, it will be a great challenge and of great significance to further consider the more practical channel model, analyze its impact on the PLS of UAV communication, and based on this, give a more practical algorithm to improve the PLS of the system.

Dynamic beamforming: Different from 2D beamforming in traditional ground communication, UAVs perform 3D beamforming with elevation adjustment. It can effectively enhance the strength of confidential signals received by legitimate users and reduce the strength of confidential signals received by eavesdroppers. In addition, 3D beamforming can also be used to transmit signals that interfere with eavesdroppers and thereby achieve stronger interference and better communication security.

Joint optimization technology: The existing research mainly uses alternate optimization and successive convex approximation technology to obtain the safety rate of joint UAV flight trajectory and wireless resource allocation optimization in UAV communication system. However, these problems can only get local optimal solutions, and there is a lack of deeper inference and analysis results for the optimal flight path and hovering point of UAV.

Limited on-board energy: Due to the limited power storage capacity of UAVs, it is particularly critical to simultaneously improve confidentiality and energy performance. The energy issues associated with UAVs depend on its motion characteristics, such as average speed, maximum speed, and acceleration. Therefore, the final trajectory design is very complicated. In addition, the durability of UAVs can be supplemented by Wireless Power Transmission technology. The energy-carrying signal is designed as an interference signal, so it can not only recharge the energy, but also reduce the quality of the eavesdropping channel. Therefore, the security performance can be further improved.

5 Conclusions

In this paper, we provide an overview of the latest research achievements in secure wireless communications involving UAVs from the perspective of PLS. First, we introduce two security attack scenarios and two new and challenging issues arising from them, namely, protecting A2G communications from ground eavesdropping and protecting G2A from ground interference. Secondly, in the eavesdropping or jamming activities against UAV,

the technology and method based on PLS are proposed. Finally, some potential opportunities and challenges are prospected.

References

1. Colomina I , Molina P . Unmanned aerial systems for photogrammetry and remote sensing: A review - ScienceDirect[J]. ISPRS Journal of Photogrammetry and Remote Sensing, 2014, 92(2):79-97.
2. Patzold M . Toward Realizing the Full Potential of a 5G-Empowered World [Mobile Radio][J]. IEEE Vehicular Technology Magazine, 2020, 15(1):5-11.
3. Yuan, Jinhong, Yang, et al. Safeguarding 5G Wireless Communication Networks Using Physical Layer Security[J]. IEEE Communications Magazine Articles News & Events of Interest to Communications Engineers, 2015.
4. Wyner A D. "The wire-tap channel," [J]. Bell System Technical Journal, 1975, 54(8): 1355-1387.
5. Li Q , Xu D . Secure Communication with a Wireless Powered Full-Duplex Eavesdropper[C]// 2019 IEEE 19th International Conference on Communication Technology (ICCT). IEEE, 2020.
6. Thanh P D , Hoan T N K , Koo I . Joint Resource Allocation and Transmission Mode Selection Using a POMDP-Based Hybrid Half-Duplex/Full-Duplex Scheme for Secrecy Rate Maximization in Multi-Channel Cognitive Radio Networks[J]. IEEE Sensors Journal, 2020, 20(7):3930-3945.
7. Zhang G , Wu Q , Cui M , et al. Securing UAV Communications via Joint Trajectory and Power Control[J]. IEEE Transactions on Wireless Communications, 2018.
8. Li A , Zhang W , Dou S T . UAV-enabled Secure Data Dissemination via Artificial Noise: Joint Trajectory and Communication Optimization[J]. IEEE Access, 2020, PP(99):1-1.
9. Yi Z , Lep Y P , He C , et al. Improving Physical Layer Security via a UAV Friendly Jammer for Unknown Eavesdropper Location[J]. IEEE Transactions on Vehicular Technology, 2018:1-1.
10. Li A , Wu Q , Zhang R . UAV-Enabled Cooperative Jamming for Improving Secrecy of Ground Wiretap Channel[J]. 2018.
11. Liang S , Fang Z , Sun G , et al. A joint optimization approach for distributed collaborative beamforming in mobile wireless sensor networks[J]. Ad Hoc Networks, 2020, 106:102216.
12. Li A , Zhang W , Dou S T . UAV-enabled Secure Data Dissemination via Artificial Noise: Joint Trajectory and Communication Optimization[J]. IEEE Access, 2020, PP(99):1-1.
13. Zhong C , Yao J , Xu J . Secure UAV Communication With Cooperative Jamming and Trajectory Control[J]. IEEE Communications Letters, 2019, 23(2):286-289.
14. Liu C , Lee J , Quek T Q S . Secure UAV communication in the presence of active eavesdropper[J]. 2017:1-6.
15. Wang H , Chen J , Ding G , et al. Trajectory Planning in UAV Communication with Jamming[C]// 2018 10th International Conference on Wireless Communications and Signal Processing (WCSP). 2018.
16. Hoon L , Subin E , Junhee P , et al. UAV-Aided Secure Communications With Cooperative Jamming[J]. IEEE Transactions on Vehicular Technology, 2018, PP:1-1.