Research on Optimization of UAV Communication Network Security Protection Strategy Based on Advanced Encryption Technology

Yue Zhang

Centre for Modern Educational Technology, Henan College of Police, Zhengzhou 450000, China
E-mail: zyue@hnp.edu.cn

Received 11 July 2024; Accepted 12 September 2024

Abstract

With the wide application of UAVs in various applications, the security, spectrum, and energy efficiency of their communication networks have become increasingly prominent. This paper proposes a joint optimization strategy based on deep reinforcement learning for drone swarm communication networks. First, a model is constructed that takes into account security threats, spectrum sharing, and energy consumption. Intelligent agents are then trained through deep reinforcement learning to dynamically select the best spectrum allocation and energy strategy to improve spectrum and energy efficiency while maintaining network security. Based on encryption technology, this paper studies resource optimization strategies for UAV security communication in different scenarios. Aiming at the incomplete certainty of multiple eavesdropping positions and the problem of the no-fly zone during UAV flight, a joint optimization algorithm is proposed to optimize UAV trajectory, interference power, and transmission power of ground base stations so as to maximize the minimum average security capacity of the system in the

Journal of Cyber Security and Mobility, Vol. 13_6, 1379–1400.
doi: 10.13052/jcsm2245-1439.1367

worst case. To solve the problem of the LoS link of UAV being quickly blocked in the city and secondary users easily causing excessive interference to primary users, intelligent reflectors are introduced to assist the UAV in secure communication. IRS can be used to reconfigure channel parameters to control the propagation direction of UAV communication links, enhance the channel quality of the primary link, and weaken the channel quality of eavesdropping links and interference links. Simulation results show that the optimization scheme improves the channel quality of UAV in crowded scenarios, inhibits the eavesdropping effect of eavesdroppers on secondary security users, and reduces the spectrum multiplexing interference of primary users, thus significantly enhancing the security capacity of the system. When the interference power of UAVs is increased, the value and growth rate of the security capacity of security users are significantly increased. The increase is 20%. Through a large number of simulation experiments, it has been proved that this method has excellent performance in improving communication security, spectrum utilization, and energy efficiency and has obvious advantages over the traditional baseline and average allocation DQN-wrap method.

Keywords: UAV, network security, spectrum energy efficiency optimization, encryption technology, communication security optimization.

1 Introduction

With the gradual popularization of fifth-generation communication technology, 5G has been widely used in various commercial and civilian scenarios [1]. It is estimated that by 2025, the number of mobile terminals will increase to 2.8 billion [2], and the data traffic generated by various communication services will increase thousands of times compared with the fourth-generation communication technology, and this number will continue to grow in the next few years. Therefore, future communication systems need to have larger system capacity, higher spectral efficiency, lower delay, and stronger security [3]. However, with the deepening of communication environment and the enhancement of communication requirements, the existing communication systems still need to be strengthened and supplemented. First of all, there are certain limitations in the coverage of 5G networks. For example, when environmental monitoring, climate prediction, and military operations are carried out in remote areas such as wetlands, and mountainous

areas, the existing communication system cannot meet these needs well [4]. Secondly, most of the existing networks are heterogeneous from large ground base stations and small cellular networks. When emergencies such as natural disasters occur, the ground communication infrastructure may be damaged and rapid emergency communication cannot be carried out [5]. In the sixth-generation communication technology, it is clearly pointed out that the future network is an air-space-ground integrated network, which allows users to access the network at any time anywhere [6, 7]. The network includes not only existing terrestrial networks, but also non-terrestrial networks (such as ocean, sky, space, etc.). Among them, aerial communication nodes such as UAVs are important hubs that constitute this three-dimensional network [8]. Due to the characteristics of flexible deployment, high maneuverability, and easy establishment of line-of-sight links, UAVs are widely used in wireless communications [9, 10]. However, due to the broadcast characteristics of wireless channels, line-of-sight transmission will also increase the risk of private information being stolen by other untrusted users or malicious eavesdroppers [11, 12]. Wireless network security has been one of the key concerns in UAV communication in recent years. Although the traditional upper-layer network digital encryption methods are relatively mature, it may not be suitable for UAV communication networks [13, 14]. The security factor of cryptography-based encryption methods is directly proportional to the complexity of the encryption algorithm [15, 16].

With the development of chip computing power, the cracking ability of eavesdroppers is getting stronger and stronger. Ordinary encryption algorithms can easily be brute-force cracked, but complex encryption algorithms will inevitably bring more signaling overhead. When UAVs communicate, their airborne energy is usually limited, and they need to fly to replenishment points regularly for charging [17, 18]. Complex encryption algorithms will increase the energy consumption of UAV, thereby reducing the service time of UAV. Therefore, the physical layer security technology is a suitable security measure for UAV communication. Physical layer security uses the rich physical characteristics of wireless channels to improve communication security. Specifically, power control, beamforming, artificial noise and other technologies are used to enhance the channel gain of the main link and suppress the channel gain of the eavesdropping channel to improve the safe capacity of the system [19, 20]. Compared with the traditional encryption algorithm, it does not need to encrypt the signal at the network layer, and only needs to understand the channel conditions to achieve better security.

Since UAVs are easy to establish line-of-sight links, their channel parameters are easy to obtain, channel parameters for complex environments can also be obtained through reinforcement learning [21].

For UAV secure communication, this paper studies two UAV secure communication scenarios in which UAV acts as a friendly jammer and an air mobile base station. A robust optimization algorithm is designed under the condition that the eavesdropper's position is not completely determined; The trajectory planning of UAV in the presence of NFZs is studied; It is proved that IRS can improve the channel condition of UAV in non-line-of-sight link, and has obvious suppression effect on eavesdropping link and interference link in cognitive wireless network.

The application of UAV as friendly jammer in secure communication is studied in this paper. The communication scenario with multiple security users and multiple eavesdroppers is considered. In order to protect the information transmission between the ground base station and the security user from being eavesdropped by the eavesdropper, UAV is used to send artificial noise to deteriorate channel quality of the eavesdropping link, so as to ensure the security performance of the system. In addition, we also consider the incomplete certainty of the eavesdropper's location and the presence of NFZs in the UAV flight path. Using the idea of robustness to improve the user's security capacity based on the worst case.

2 UAV Communication and Physical Layer Security Optimization

2.1 Construction of Channel Model of UAV

While small-scale fading channel models have been well explained in the existing literature, modeling large-scale fading in air-to-ground communications is often more complex and the resulting three-dimensional space propagation [22]. Based on the current research, the channel models of UAV-to-ground communication can be divided into two types: free space channel and probability-based line-of-sight link channel.

Given the rapid popularity of drones in the civil sector, it is crucial to deepen the discussion of privacy protection strategies. Differential privacy and anonymisation techniques have become the focus of research, with the former guaranteeing that individual information is not accurately identified through data noise injection and the latter processing image and sensor data collected by UAVs to ensure that personally identifiable information is

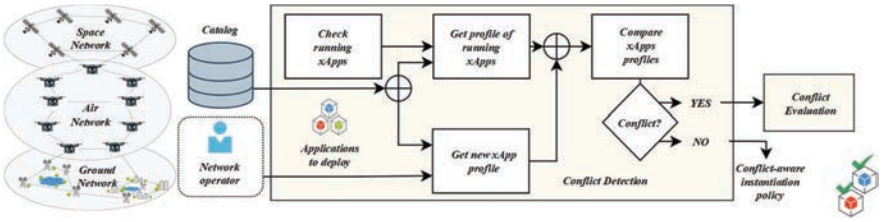

Figure 1 Channel model of UAV.

not leaked, together constructing a privacy protection barrier in civil UAV applications.

Figure 1 is a channel model of an unmanned aerial vehicle, starting first with a wireless channel model for general frequency non-selective baseband communication, wherein channel coefficients between transmitter and receiver can be represented by Equation (1):

$$h = \sqrt{\beta(d)}\tilde{h} \tag{1}$$

Where large-scale signal attenuation $\beta(d)$ is represented, including distance-dependent path loss and shadow fading, where distance d between the transmitter and the receiver is represented. Due to multipath fading, $\tilde{h}$ is usually expected to be 1. Path loss model is Equation (2):

$$PL(dB)[dB] = 10\alpha log_{10}(d) + X_0[dB] + X_\sigma[dB] \tag{2}$$

Among them, α is the path loss index, usually taken between 2 and 6, which X_0 is the path loss per unit distance of 1 meter.

Free-space path loss channel model: In the ideal case of no signal blocking or obstruction reflection, the UAV communication channel is modeled as a free-space loss model, in which the influence of shadow fading and small-scale fading disappears. In this case, if $|\tilde{h}| = 1$, the channel gain can be simplified to the form of Equation (3).

$$\beta(d) = \left(\frac{\lambda}{4\pi d}\right)^2 = \widetilde{\beta}_o d^{-2} \tag{3}$$

Among them, λ is the channel gain when the unit distance of the communication carrier wavelength is 1 meter. In the free space path loss channel model, the channel gain is determined entirely by the transmission and reception distance, and if their positions are known to each other, the channel model is easy to predict. This kind of model generally appears in the

non-city scene, this paper first uses the air-ground channel model. In the free space path loss channel model, the channel gain is determined entirely by the transmission and reception distance, and if their positions are known to each other, the channel model is easy to predict. This kind of model generally appears in the non-city scene, the first work of this paper is to adopt this kind of air-to-ground channel model.

The probability can be given by $P_{NLoS}(\theta) = 1 - P_{LoS}(\theta)$. With increasing elevation, the probability increases, and when it is large enough, this probability tends to 1. Using such a model, the expectation of channel gain can be shown as in Equation (4):

$$\bar{h}(d_{2-D}, H_U) = P_{LoS}(\theta)\beta_0 d^{-\alpha} + (1 - P_{LoS}(\theta))\kappa\beta_0 d^{-\alpha} \tag{4}$$

2.2 Physical Security Layer Optimization

This study aims to promote the interdisciplinary integration of cutting-edge technologies, such as artificial intelligence and blockchain, to enhance the security of drone communication networks. Through this integration, explore the application of smart contracts in the security management of drone clusters and how to use blockchain technology to achieve efficient management of drone network spectrum.

Acknowledging the inherent broadcast nature of wireless channels, UAVs are prone to eavesdropping by malicious entities during communication with ground nodes. While traditional network encryption techniques effectively enhance data transmission security, their reliance on complex critical management systems and the potential for increased eavesdropping capabilities can limit their suitability for UAV communications [23, 24]. We emphasize the complementary role of physical layer security in addressing these limitations. By leveraging the distinctive properties of wireless channels, physical layer security offers an alternative approach that achieves superior security performance, making it a robust addition to traditional encryption algorithms in the UAV communication context.

We propose an innovative solution that addresses the challenges inherent in this dynamic environment. Our strategy begins with secure key generation, utilizing robust algorithms resistant to potential threats. For distribution, we implement a hierarchical scheme that leverages the hierarchical structure of drone clusters, enabling efficient and secure critical dissemination. Updating keys is streamlined through an adaptive mechanism that considers the real-time mobility and network topology changes. Finally, critical destruction is

managed through a secure deletion protocol that ensures no trace of keys remains post-termination.

2.2.1 Safety capacity optimization

Security capacity is an important index to measure system security in the physical layer, which is proposed based on information theory. First, the channel capacity of a white Gaussian noise continuous channel with finite bandwidth and finite average power can be defined as Equation (5):

$$C = B\, log_2 \left(l + \frac{S}{N} \right) \tag{5}$$

Among them, C is the channel capacity, the bandwidth occupied when communicating, and the noise power on the frequency band. Alice generally refers to the information transmitter in secure communication, while Bob and Eve refer to the legitimate receiver and the information eavesdropper respectively. Alice transmits confidential information to Bob through legal links A $\rightarrow$ B, while eavesdropper Eve eavesdrops on the confidential information through eavesdropping links A $\rightarrow$ E. Here, C_b is used to represent the channel capacity of the legal link, and C_e is used to represent the channel capacity of the eavesdropping link. Equations (6) and (7) are available from the previous definition of channel capacity.

$$C_b = log_2 \left(1 + \frac{P_a h_{ab}}{N_b} \right) \tag{6}$$

$$C_e = log_2 \left(1 + \frac{P_a h_{ae}}{N_e} \right) \tag{7}$$

2.2.2 Security capacity enhancement

When designing a communication system based on security, it is necessary to make the channel capacity of the legal link larger than that of the eavesdropping link as much as possible. Table 1 shows the application of encryption technology in UAV communication [25]. The commonly used technical means are as follows. (1) Artificial noise jamming technology, through introducing a jammer, sending designed artificial noise, reducing the signal-to-noise ratio of Eve to achieve the purpose of weakening the eavesdropping link. It should be noted that artificial noise can also affect Bob noise, and the interference strategy needs to be designed. (2) Beamforming technology, by controlling the propagation direction of the communication

Table 1 Application of encryption technology in UAV communication

Encryption Technology	Types of Drones	Application Scenario	Proportion of Deployment (%)
AES-256	Military reconnaissance drone	Secure data transmission	95
RSA-4096	Civil logistics drone	Key exchange	70
ECC (P-256)	Commercial aerial UAV	Authentication and Encryption	85
Blowfish	Research test UAV	Temporary encrypted communication	50
Custom Encryption	Industry-specific drones	Customized security requirements	30

carrier, it can be transmitted to the legitimate user as much as possible, and then achieve the purpose of increasing the channel quality of the legitimate link. (3) Resource allocation technology, which reasonably allocates resources such as information transmission power, communication time, and trajectory in UAV communication, so as to maximize the security capacity.

3 Optimization Framework of UAV Communication Network Security Protection Based on Advanced Encryption Technology

3.1 Encryption Technology Design

Encryption specifically refers to changing the original data information with a certain algorithm [26]. Encryption is to convert the representational form of data information from plaintext visible to ciphertext visible to the specified person. The sender of the information encrypts the data through encryption technology and sends it to the receiver. When the receiver receives the data, it needs to decrypt the data to make it readable. If the data is intercepted by network hackers during this process, because the hackers do not know the decryption method, they cannot obtain the content in it, and the security of the data is guaranteed. Table 2 shows encryption technology and its security performance. In data encryption technology, there are two very critical elements. One is the key, which can be understood as a parameter and is a tool for converting plaintext and ciphertext; The other is the algorithm, different encryption methods, the algorithm is different.

In order to enhance the security of drone communication networks, an adaptive encryption strategy is proposed, which will enable drones to

Table 2 Encryption technology and its security performance

Encryption Technology	Key Length (Bits)	Crack Time (Years)	Safety Rating (1–10)
AES-256	256	Non-calculable	10
DES	56	A few days	3
RSA-4096	4096	Non-calculable	9
ECC (P-256)	256	Non-calculable	10
Blowfish	448	Non-calculable	8

automatically adjust their encryption strength according to real-time environmental changes, effectively responding to unexpected security threats. Through this dynamic adjustment, the drone network will be able to ensure the security and integrity of data transmission while maintaining communication efficiency. Our research will consider the latest technological advancements, such as commercial cryptography, trusted computing, privacy computing, etc., to ensure that the encryption scheme for drone data throughout its entire lifecycle can resist various network attacks.

3.2 UAV Network Security Protection Model Construction

The ground base station communicates confidentially with a secure user, but there are also passive eavesdroppers in this scenario, which try to intercept the confidential information between the ground base station and the secure user. In order to protect the information between the user and the security user from being eavesdropped by the eavesdropper, we introduce a UAV as a jammer, which strategically generates artificial noise to interfere with the eavesdropper [27]. Figure 2 shows the establishment of a system model based on encryption technology. By conducting a more in-depth analysis of secure users and potential eavesdroppers in communication networks, probability and statistical methods are used to quantify the likelihood of different threats occurring and their potential impact on communication security. Assign a quantified risk value to each threat to determine its priority more accurately. To guide the development of security policies, which threats need to be mitigated first will be determined based on the risk value of the threats and the specific environment of the network (such as the dynamic characteristics of drone swarms). A comprehensive risk assessment of communication channel security, including but not limited to threats such as eavesdropping, interference, and signal tampering.

In order to describe the spatial position of the system nodes, a three-dimensional Cartesian coordinate system is established. Under normal

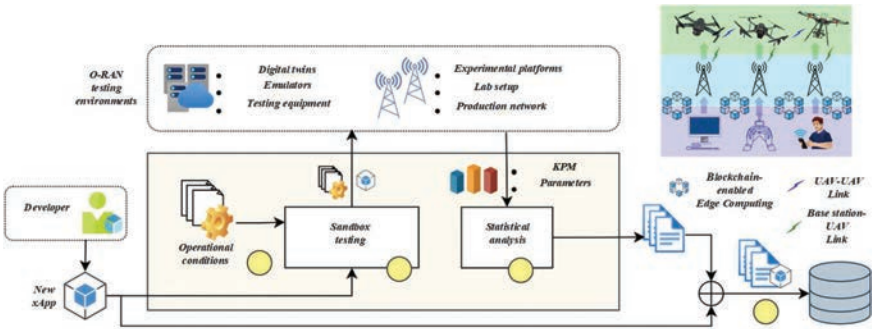

Figure 2 Establishment of system model based on encryption technology.

circumstances, only the estimated value of the eavesdropper's position can be obtained, but the estimation error is usually bounded. The mathematical relationship between the possible actual position of the eavesdropper and the estimated position is shown in Equations (8) and (9).

$$q_k = q_{ak} + \Delta_k, \forall k \in \mathcal{K} \tag{8}$$

$$x_k = x_{ak} + \Delta x_k, y_k = y_{ak} + \Delta y_k \tag{9}$$

Assuming that the flight altitude of the UAV is fixed, it satisfies the minimum altitude of the UAV to avoid collision with objects and maintain the line-of-sight link. Because the airborne energy on the UAV is limited, its flight time is also fixed. Generally, it takes off from one location and flies to another location for charging and maintenance after completing the flight mission. The flight constraint of UAV can be expressed by Equations (10) and (11).

$$p(n+l) - p(n)^2 \leq (L_{max})^2 \tag{10}$$

$$q_i^2 \leq (L_{max})^2 \tag{11}$$

Due to the presence of NFZs, the flight of the UAV must take into account the constraints of NFZs, as shown in Equation (12):

$$L_{NFZ}^z{}^2 \leq q[n] - q_{NFZ}^z{}^2, \forall n \in \mathcal{N} \tag{12}$$

To describe the basic characteristics of the communication link, we adopt a free-space path loss model. The channel gains of the UAV with the first secure user and with the first eavesdropper in the first slot are shown in

Equations (13) and (14), respectively.

$$h_{jm}[n] = \rho_o d_{jm}[n]^{-2}, \ \forall\, n \in \mathcal{N} \tag{13}$$

$$h_{jm}[n] = \rho_o d_{jm}[n]^{-2}, \ \forall\, n \in \mathcal{N} \tag{14}$$

Unlike the air-to-ground line-of-sight link from a UAV to a ground node, the channel between a ground base station and a ground node. The channel gain for the k-th eavesdropper is shown in Equations (15) and (16):

$$g_{gm} = \rho_0 d_{gm}^{-\varphi} \zeta_m \tag{15}$$

$$g_{gk} = \rho_0 d_{gk}^{-\varphi} \zeta_k \tag{16}$$

3.3 IRS Optimization Construction

As a mobile base station in the air, UAV multiplexes the communication band of a primary user and communicates securely with a secondary user on the ground. There is also an eavesdropper in the scene [28]. The eavesdropper is an ordinary authorized user in the cognitive network, but it is an untrusted user for the UAV. Simply put, the UAV does not want confidential communications with secondary users to be received by it. Therefore, the eavesdropper's location information is fully known, because the UAV can obtain its location information by querying its network access information. In particular, due to the complex urban environment, the direct link between secondary users and UAVs is completely blocked by buildings. In order to improve the channel quality of air-to-ground communication, reduce the receiving rate of secret information by stealers and the interference caused by secure communication to the main user, a planar IRS is installed on the surface of the building, and the channel environment is re-controlled by IRS to achieve the purpose [29, 30]. The optimization variables are constrained by UAV flight constraints, NFZs constraints, interference, peak and average of transmission power constraints, and the mathematics of the optimization problem is shown in Equation (17).

$$f(x) = \sum_{i=1}^{N} R_{sec}^{m}[i] \tag{17}$$

The interference power and transmission power are optimized under given UAV trajectory variables, and the mathematical description is shown

in Equation (18).

$$\frac{l}{N}\sum_{n=l}^{N}\left[log_2\left(1+\frac{D_m p_{gm}/[n]}{l+p_j\hat{h}_{jm}[n]}-c_m[n]\right)\right]\geq\eta,\forall m \tag{18}$$

The transmission power is optimized as shown in Equation (19). The optimization problem is shown in Equations (20) and (21).

$$max\frac{1}{N}\sum_{n=1}^{N}\left(log_2(1+a[n]p[n])-log_2(1+b[n]p[n])\right) \tag{19}$$

$$f(x)=max\frac{1}{N}\sum_{n=1}^{N}R_s[n]-R_e[n] \tag{20}$$

$$R_s[i]=log_2\left(l+\frac{p[i]\beta_0}{\sigma_s^2}S[i]\right) \tag{21}$$

Our ongoing research is dedicated to enhancing the cost-benefit analysis at the strategy implementation phase for UAV systems. Our focus is optimizing operations to reduce energy consumption and minimize the strain on computing resources while maintaining stringent safety standards. By scrutinizing the cost-effectiveness of each operational component, we aim to devise strategies that ensure sustainable and efficient UAV performance, aligning with our commitment to innovation and fiscal responsibility. This approach will contribute significantly to the broader adoption and operational effectiveness of UAV technologies in various sectors.

Legal compliance is paramount in the realm of UAVs, especially when navigating the complexities of cross-border flights and data transmission. To ensure operational legitimacy, it is essential to meticulously adhere to the diverse legal frameworks of different countries and regions. This includes understanding and complying with airspace usage regulations, privacy protections, and data privacy laws. By doing so, UAV operators can mitigate legal risks, foster international cooperation, and maintain the integrity of their operations' integrity globally.

4 Experimental Results and Analysis

In order to improve spectral efficiency, UAV multiplexes the spectrum resources of the primary user to communicate with a secondary security user

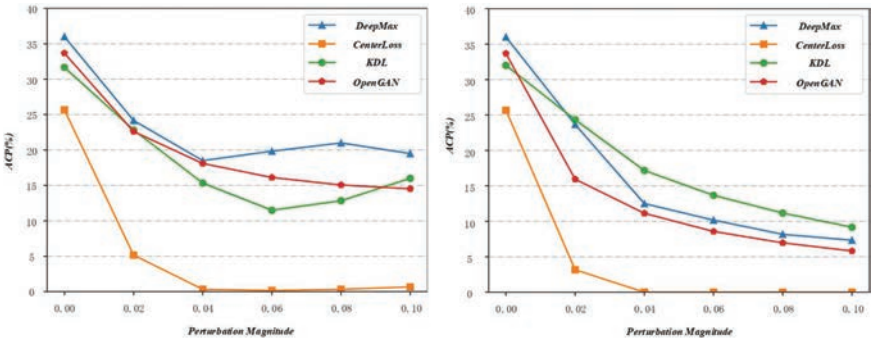

Figure 3 Convergence of maximum-minimum average security capacity of secure users in different benchmark schemes.

on the ground. At the same time, there is an eavesdropper on the ground to eavesdrop on the transmitted confidential information. In order to improve the channel quality of UAV, suppress the eavesdropping effect of eavesdroppers, and reduce the interference caused by primary users, IRS is introduced into this scene, and the transmission signal of UAV is aimed at secondary security users as much as possible by using the characteristics of intelligent reflector that can control the propagation path of wireless signals.

Through simulation experiments, it is possible to accurately evaluate the specific impact of different encryption strategies on latency and throughput in a controlled variable environment. These experimental data will provide an empirical basis for optimizing encryption strategies to ensure maximum communication efficiency without sacrificing security. Introducing real-world test data will further enhance the practicality and reliability of the research, making our recommendations closer to the actual operating environment of drone communication networks.

Figure 3 shows the convergence of the maximum-minimum average security capacity of secure users in relation to the number of iterations in different benchmark schemes. The convergence result of the security capacity of the proposed optimization scheme is better than that of other contrasting schemes.

Figure 4 shows the flight trajectory design of the UAV under different schemes. As the UAV approaches the optimal jamming point, it slows down its flight speed and hovers as much as possible. In non-robust scheme, the UAV chooses to hover between the two eavesdroppers in order to have a better jamming effect on the two eavesdroppers at the same time. Compared with the "non-robust" scheme, flight trajectory with the robust design scheme is

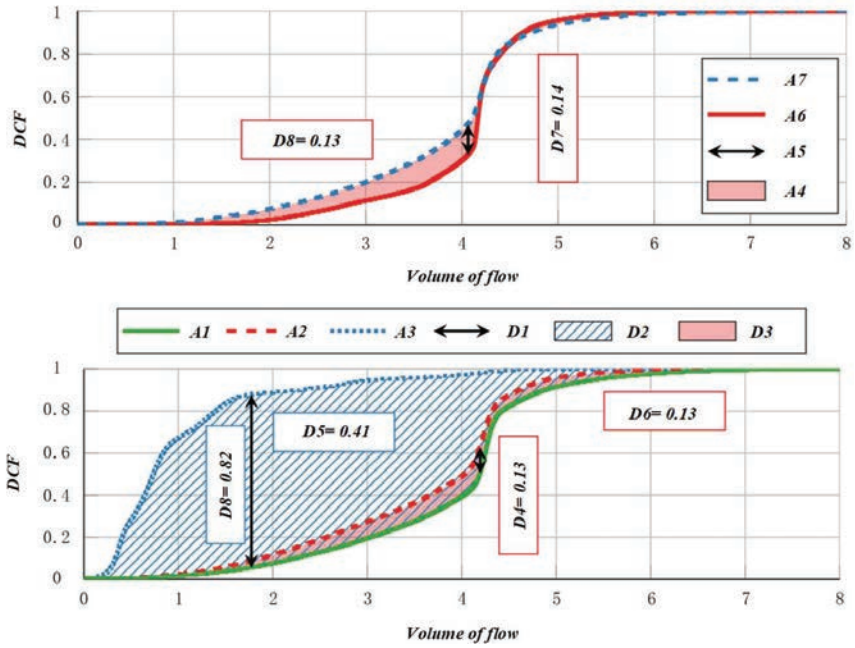

Figure 4 The relationship between the maximum-minimum average safe capacity of the UAV and the total flight time.

closer to eavesdropper 1, because the position estimation error of eavesdropper 1 is smaller than that of eavesdropper 2. Therefore, the robust design of the system can guarantee a higher safe capacity in the worst case.

Figure 5 shows the relationship between the maximum-minimum average safety capacity of the UAV and the total flight time under different schemes. As for the fixed trajectory scheme, since UAV flies at a uniform speed and the flight time of each segment in the flight trajectory is the same, the average safe capacity does not change. In the "non-robust" scheme, UAV hovers over a non-ideal jamming position; In the fixed interference power, the interference power at the ideal position is the same as that at other positions. Therefore, with the increase of the total flight time, the performance gap with the proposed scheme will also increase.

Figure 6 shows the safety capacity of two safety users in each flight slot in our proposed scheme. Figures 7 and 8 show the optimization results of transmission power and interference power in each time slot of this scheme. All three of them increase rapidly with the increase of time slot, then rise slowly, and finally tend to be stable. Combined with the trajectory analysis of

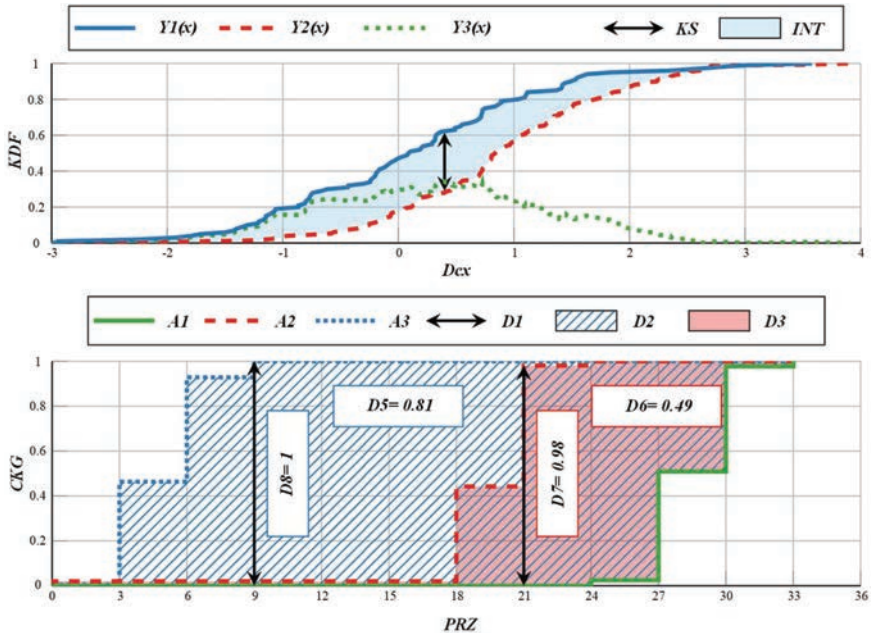

Figure 5 The relationship between the maximum-minimum average safe capacity of UAV and the total flight time.

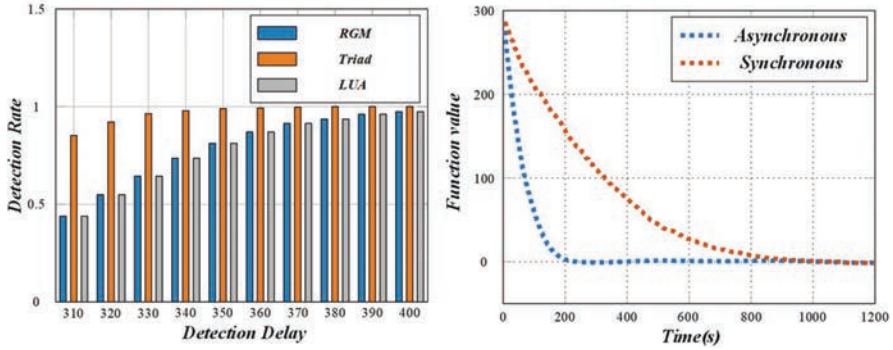

Figure 6 Safe capacity of a safe user in each flight slot.

UAV, it shows that the jamming effect of UAV near the eavesdropper will be better.

In Figure 8, the interference power is 0 in the start-end slot. This is because the UAV is far away from the eavesdropper, and even if a high

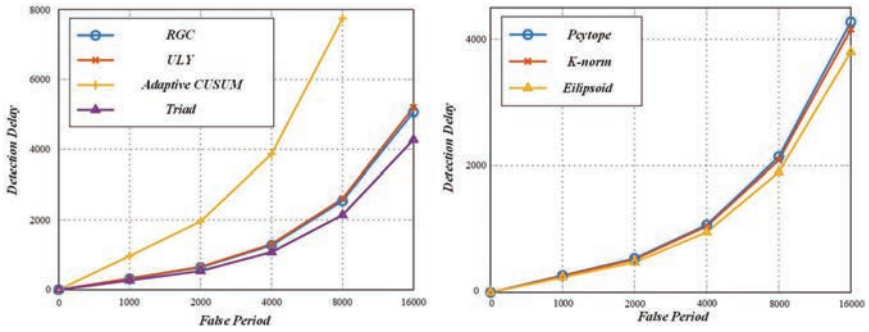

Figure 7 Optimization curves of transmission power and interference power.

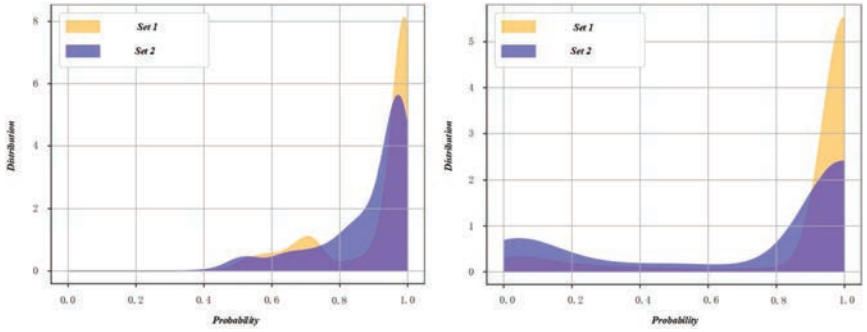

Figure 8 Comparison of transmission power and interference power effects of different schemes.

interference power is used, the safety rate of the safe user will be particularly low. Therefore, in order to ensure the efficiency of interference, no interference is carried out in these time slots. When the UAV flies close to the eavesdropper, it will be more efficient to jam with a larger jamming power. In addition, since the system contains multiple security users, in order to ensure the security of each security user, the ground base station allocates more transmission power to the security user 2. Because secure user 2 is farther away from the ground base station than secure user 1, its channel conditions will be worse, which also reflects the effectiveness of the maximum-minimum optimization method proposed in this paper.

Figure 9 shows the relationship between the maximum-minimum average safe capacity and average interference powers, where flight time of UAV is 70 s and average transmission power is 1.5 w. As interference power

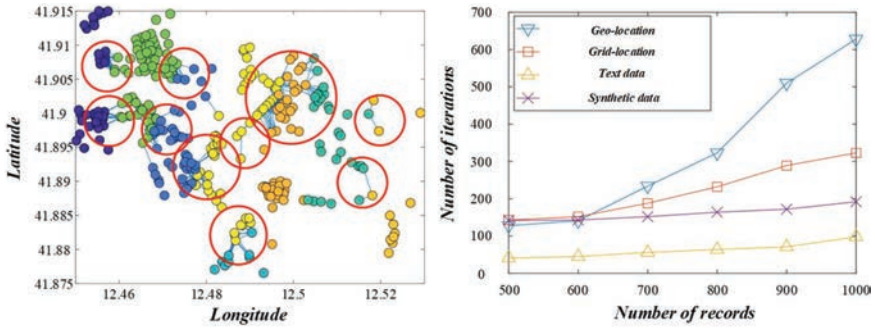

Figure 9 Relationship to average interference power under different schemes.

continues to increase, security capacity tends to be constant. In particular, under the scheme of fixed interference power, the security capacity gradually decreases when the average interference power is greater than 0.0012 W. Too high interference power not only affects the eavesdropping rate of the eavesdropper, but also has a significant impact on the information receiving rate of the secure user. Therefore, a scheme with interference power control selects an appropriate interference power to suppress the eavesdropper, rather than rashly increasing the interference power as in a fixed interference power scheme. Therefore, it is very important to distribute the interference power reasonably when designing the optimization scheme.

In order to investigate the influence of different average transmission power on the security capacity and the relationship between average transmission power and average interference power, the relationship between the maximum-minimum average security capacity and the average transmission power of the ground base station under different average interference power is studied. The results under different schemes are shown in Figure 10, where the total flight time of the UAV is 70 s. It can be clearly seen from Figure 10 that the average security capacity of the four schemes increases rapidly with the increase of the average transmission power at different average interference power. Because the ground base station increases the transmission power at the same time, the eavesdropping effect of the eavesdropper will also increase accordingly. Simply increasing the transmission power will make the safety capacity gradually saturated. When the interference power of UAV is increased from 0.0007 W to 0.0012 W, the value and growth rate of the safe user capacity are improved to varying degrees, which also proves this point of view.

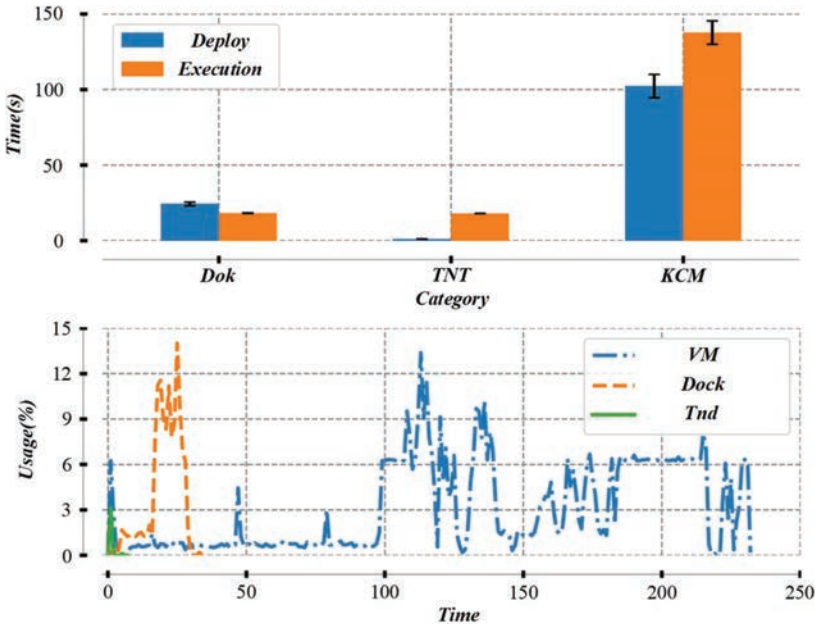

Figure 10 Maximum-minimum average safe capacity under different average interference power.

5 Conclusion

Our study addresses the critical issue of identity security threats in ad-hoc networks, mainly due to the flexible structure and absence of infrastructure support. The conventional schemes are marred by low performance and inadequate security, making them unsuitable for UAV ad-hoc networks. To tackle these challenges, we devised an authentication scheme based on Identity-Based Encryption, which leverages entity identity information as the public key, eliminating the need for additional public key storage and reducing overhead. This scheme supports batch authentication, significantly enhancing efficiency. By incorporating hash chain technology, we have effectively retained and reused UAV status information post-initial certification, reducing subsequent authentication costs. Integrating UAV communication, physical layer security theory, cognitive radio, and IRS technology has enabled us to construct a robust network system that ensures user security capacity. Our joint optimization algorithm, designed for wireless secure communication networks, optimizes UAV trajectory, jamming power, and base station transmission power based on S-process and convex optimization

theory, maintaining high-security capacity under eavesdropping conditions. We have also modelled UAV flight energy, considering energy efficiency in optimizing security capacity and enabling longer UAV service times through energy communication with stable energy nodes like ground base stations. Although our proposed scheme offers notable improvements and innovations, it assumes a certain level of computational resources and infrastructure support that may not be universally available.

Moreover, the performance gains are contingent upon specific conditions and may vary in real-world applications. Future work will focus on enhancing the scheme's adaptability to resource-constrained environments and improving security and efficiency under dynamic network conditions. We aim to explore the integration of additional security mechanisms and optimization algorithms to address emerging threats and network complexities. To provide clear guidance for subsequent research, our findings highlight the effectiveness of using straightforward logic and practical technologies in security solutions for ad-hoc networks. The proposed method reduces computation delay and improves single-point and batch authentication performance compared to existing schemes, offering a promising direction for enhancing security in UAV ad-hoc networks.

References

[1] Emad H. Abualsauod, "A hybrid blockchain method in internet of things for privacy and security in unmanned aerial vehicles network," Computers and Electrical Engineering, vol. 99, pp. 107847, 2022.

[2] Amrin Maria Khan Adawadkar and Nilima Kulkarni, "Cyber-security and reinforcement learning – A brief survey," Engineering Applications of Artificial Intelligence, vol. 114, pp. 105116, 2022.

[3] Wasyihun Sema Admass, Yirga Yayeh Munaye, and Abebe Abeshu Diro, "Cyber security: State of the art, challenges and future directions," Cyber Security and Applications, vol. 2, pp. 100031, 2024.

[4] Aamina Akbar, Sobia Jangsher, and Farrukh A. Bhatti, "NOMA and 5G emerging technologies: A survey on issues and solution techniques," Computer Networks, vol. 190, pp. 107950, 2021.

[5] Ghada Alsuhli, Ahmed Fahim, and Yasser Gadallah, "A survey on the role of UAVs in the communication process: A technological perspective," Computer Communications, vol. 194, pp. 86–123, 2022.

[6] Sakshi Anand and Avinash Sharma, "Comprehensive analysis of services towards enhancing security in IoT-based agriculture," Measurement: Sensors, vol. 24, pp. 100599, 2022.
[7] Afia Anjum, Paul Agbaje, Arkajyoti Mitra, Emmanuel Oseghale, Ebelechukwu Nwafor, and Habeeb Olufowobi, "Towards named data networking technology: Emerging applications, use cases, and challenges for secure data communication," Future Generation Computer Systems, vol. 151, pp. 12–31, 2024.
[8] R. M. Bhavadharini and B. Surendiran, "Secured osprey-based energy efficient routing and congestion control in WSN," Sustainable Computing: Informatics and Systems, vol. 44, pp. 101026, 2024.
[9] Khan Maaz Bin Hasan, Mohammad Sajid, Maria A. Lapina, Mohammad Shahid, and Ketan Kotecha, "Blockchain technology meets 6 G wireless networks: A systematic survey," Alexandria Engineering Journal, vol. 92, pp. 199–220, 2024.
[10] Alessio Botta, Sayna Rotbei, Stefania Zinno, and Giorgio Ventre, "Cyber security of robots: A comprehensive survey," Intelligent Systems with Applications, vol. 18, pp. 200237, 2023.
[11] Yue Cao et al., "Towards cyber security for low-carbon transportation: Overview, challenges and future directions," Renewable and Sustainable Energy Reviews, vol. 183, pp. 113401, 2023.
[12] Niccolò Cecchinato, Andrea Toma, Carlo Drioli, Giuseppe Oliva, Gianluigi Sechi, and Gian Luca Foresti, "A Secure Real-time Multimedia Streaming through Robust and Lightweight AES Encryption in UAV Networks for Operational Scenarios in Military Domain," Procedia Computer Science, vol. 205, pp. 50–57, 2022.
[13] Runqi Chai, Yunlong Guo, Zongyu Zuo, Kaiyuan Chen, Hyo-Sang Shin, and Antonios Tsourdos, "Cooperative motion planning and control for aerial-ground autonomous systems: Methods and applications," Progress in Aerospace Sciences, vol. 146, pp. 101005, 2024.
[14] Indu Chandran and Kizheppatt Vipin, "Multi-UAV networks for disaster monitoring: challenges and opportunities from a network perspective," Drone Systems and Applications, vol. 12, pp. 1–28, 2024.
[15] Liquan Chen, Yaqing Zhu, Suhui Liu, Hongtao Yu, and Bing Zhang, "PUF-based dynamic secret-key strategy with hierarchical blockchain for UAV swarm authentication," Computer Communications, vol. 218, pp. 31–43, 2024.
[16] Runfeng Duan, An He, Guangwei Wu, Guangrong Yang, and Jinhuan Zhang, "A trustworthy data collection scheme based on active

spot-checking in UAV-Assisted WSNs," Ad Hoc Networks, vol. 158, pp. 103477, 2024.

[17] Massimo Ficco, Daniele Granata, Francesco Palmieri, and Massimiliano Rak, "A systematic approach for threat and vulnerability analysis of unmanned aerial vehicles," Internet of Things, vol. 26, pp. 101180, 2024.

[18] Chunpeng Ge, Xinshu Ma, and Zhe Liu, "A semi-autonomous distributed blockchain-based framework for UAVs system," Journal of Systems Architecture, vol. 107, pp. 101728, 2020.

[19] Hassan Jalil Hadi, Yue Cao, Sifan Li, Lexi Xu, Yulin Hu, and Mingxin Li, "Real-time fusion multi-tier DNN-based collaborative IDPS with complementary features for secure UAV-enabled 6G networks," Expert Systems with Applications, vol. 252, pp. 124215, 2024.

[20] Khalid Haseeb, Amjad Rehman, Tanzila Saba, Saeed Ali Bahaj, Huihui Wang, and Houbing Song, "Efficient and trusted autonomous vehicle routing protocol for 6G networks with computational intelligence," ISA Transactions, vol. 132, pp. 61–68, 2023.

[21] Diana Hawashin et al., "Blockchain applications in UAV industry: Review, opportunities, and challenges," Journal of Network and Computer Applications, vol. 230, pp. 103932, 2024.

[22] Atefeh Hemmati, Mani Zarei, and Alireza Souri, "UAV-based Internet of Vehicles: A systematic literature review," Intelligent Systems with Applications, vol. 18, pp. 200226, 2023.

[23] Aicha Idriss Hentati and Lamia Chaari Fourati, "Comprehensive survey of UAVs communication networks," Computer Standards & Interfaces, vol. 72, pp. 103451, 2020.

[24] Abeer Iftikhar, Kashif Naseer Qureshi, Muhammad Shiraz, and Saleh Albahli, "Security, trust and privacy risks, responses, and solutions for high-speed smart cities networks: A systematic literature review," Journal of King Saud University – Computer and Information Sciences, vol. 35, no. 9, pp. 101788, 2023.

[25] Fauzia Irram, Mudassar Ali, Muhammad Naeem, and Shahid Mumtaz, "Physical layer security for beyond 5G/6G networks: Emerging technologies and future directions," Journal of Network and Computer Applications, vol. 206, pp. 103431, 2022.

[26] Preksha Jain, Akhil Gupta, and Neeraj Kumar, "A vision towards integrated 6G communication networks: Promising technologies, architecture, and use-cases," Physical Communication, vol. 55, pp. 101917, 2022.

[27] R. Lakshmana Kumar, Quoc-Viet Pham, Firoz Khan, Md Jalil Piran, and Kapal Dev, "Blockchain for securing aerial communications: Potentials, solutions, and research directions," Physical Communication, vol. 47, pp. 101390, 2021.

[28] Asif Ali Laghari, Awais Khan Jumani, Rashid Ali Laghari, Hang Li, Shahid Karim, and Abudllah Ayub Khan, "Unmanned aerial vehicles advances in object detection and communication security review," Cognitive Robotics, vol. 4, pp. 128–141, 2024.

[29] Debashisha Mishra and Enrico Natalizio, "A survey on cellular-connected UAVs: Design challenges, enabling 5G/B5G innovations, and experimental advancements," Computer Networks, vol. 182, pp. 107451, 2020.

[30] Ahmed Burhan Mohammed, Lamia Chaari Fourati, and Ahmed M. Fakhrudeen, "Comprehensive systematic review of intelligent approaches in UAV-based intrusion detection, blockchain, and network security," Computer Networks, vol. 239, pp. 110140, 2024.

Biography

Yue Zhang received his B.S. degree from Information Engineering University, China, in 1998. He is a renowned expert inthe field of network security and internet crime investigation. He, currently affiliated with Henan Police College, is actively exploring innovative approaches to network security and internet crime investigation.