Spatial Optimization Information Security Algorithm for UAV Cluster Oriented to RSA

Guilan Luo¹, Yuanbo Zhu¹*, Shuailin Wang¹, Zhongmu Li², Mei Zhang¹ and Xi Wang¹

¹School of Mathematics and Computer Science, Dali University, Dali 671003, China
²Institute for Astronomy and History of Science and Technology, Dali University, Dali 671003, China

*Corresponding author email: zyb@stu.dali.edu.cn

Abstract. In the face of the limited communication and computing capacity of UAV network in complex environment, in order to improve the operating efficiency of UAV cluster information security algorithm, this paper proposes a spatial optimization information security algorithm for Public Key Cryptography (RSA). Firstly, the UAV location and cluster space optimization algorithm (CA-PSO) is used to obtain the UAV location. Secondly, the optimal particle of UAV swarm is found through spatial optimization. Then the optimal particle is loaded with the UAV Cluster Information Security Optimization Algorithm (RSA-UAV). Finally, the UAV network simulation process is given. Through algorithm simulation and performance analysis, it is found that the positioning accuracy and convergence of the loaded information security algorithm are better after the improved algorithm space optimization.

1. Introduction

With the development of science and technology, Unmanned Aerial Vehicle (UAV) scheduling, as a high-profile emerging technology, has begun to show up in all walks of life, such as natural disaster monitoring, real-time target tracking and smart city. With the proposal of the national strategy "Made in China 2025 Plan" and the steady advancement of the civil-military integration strategy, China's civil UAV industry has developed rapidly and started to change from quantity to quality.

UAV industry brings more convenience to people's life, and its safety problems are gradually exposed. As a kind of intelligent equipment, the network security problem of UAV needs to be solved urgently. Many scholars have carried out research. A. Jangra proposed E-ARAN in 2012 to detect and deal with malicious nodes in the network [1]. In 2017, Sameh A proposed that Reequal - Aran introduces the concept of reputation [2] on the basis of Aran, which enables the protocol to realize detection and resistance to malicious nodes. Although ARAN has the best security, its reliable security is at the cost of high delay of some nodes, which does not meet the real-time characteristics of UAV network requirements.

At present, the UAV network is dominated by line-of sight circuit, and the communication between UAV clusters and bases and UAVs has the nature of broadcasting, which is vulnerable to attack [3]. And the UAV network has the characteristics of rapid changes in topology and needs to broadcast information transmission, so it is imperative to seek an efficient UAV cluster information security algorithm.

At present, the best public key cryptography algorithm (Rivest-Shamir-Adleman (RSA)) cannot be applied directly because it does not meet the real-time and energy saving requirements of UAV
network\(^4\). For the optimization of information security of UAV cluster, it is necessary to firstly locate UAV cluster and optimize its spatial information, and then load the information security algorithm to reduce the time consumption and energy consumption of the algorithm in the whole process of encryption and decryption of the cluster. Therefore, this paper comprehensively considers the unique application characteristics of UAV network. An improved RSA algorithm based on spatial optimization of UAV swarm is proposed.

2. Principle of UAV Positioning and Swarm Space Optimization Algorithm (CA-PSO)

Cultural Algorithm (CA)\(^5\) and Particle Swarm Optimization (PSO)\(^6\) are two different Swarm intelligence Optimization algorithms. In this paper, an improved algorithm, CA-PSO, is proposed by combining the advantages of the two algorithms. Guided by cultural algorithm and combined with the optimization ability of PSO algorithm, this algorithm is used to solve the problem of traditional PSO particles' early convergence and prematurity\(^7\). On the basis of the traditional PSO algorithm, the belief space is introduced, the experience is used as a reference to guide, and the knowledge is updated by its own update operation, so as to enhance the superiority of the population evolution. Through tracking elite individuals and using excellent information to guide inferior individuals, the search effect of the whole population is eventually improved. First, each drone in the cluster is given a certain speed and direction in the form of particles. At the end of the algorithm, according to the convergence position of particles, the region with the most particle aggregation points is judged as the optimal position, and the final coordinates of positioning are output finally. The CA-PSO algorithm flow is shown in Figure 1.

![CA-PSO algorithm flow chart](image1)

3. Principle of UAV Cluster Information Security Optimization Algorithm (RSA-UAV)

To solve primes generated large RSA algorithm efficiency low power operation and mould large amount of calculation, data storage capacity and the problem of low code execution at the same time considering the unmanned aerial vehicle (uav) equipment encryption requirements of real-time and energy saving, this paper adopts the literature\(^2\) put forward suitable for hardware structure of the RSA algorithm, the improved algorithm optimization, to require the security of the unmanned aerial vehicle (uav) clusters. Firstly, a large probability 2K large prime selection model is used in the process of generating large primes P and Q. Secondly, the linear private key calculation model is used to calculate the private key D. Then, in the process of encryption and decryption, FIPS-2^k modular power operation model is adopted. Finally, the algorithm is loaded onto the UAV. The principle flow of the information security algorithm (RSA-UAV for short) is shown in Figure 2.
4. Simulation Process of UAV Network Optimization
The simulation process of UAV network optimization is divided into three steps. In the first step, the PSO algorithm is implemented. In the main population space (UAV cluster), the space is set through three initialization processes. The second step is to introduce the knowledge space. The knowledge space is designed with five kinds of knowledge. Different kinds of knowledge have different effects in different evolutionary periods, and then it evolves itself according to the existing and existing experience. The third step is to load RSA-UAV, which is mainly to load RSA-UAV on elite individuals to achieve security and confidentiality, and analyze the convergence of its information to test the performance of the algorithm. The detailed optimization simulation process is as follows.

(1) UAV cluster space initialization: First, the size of a given population (UAV cluster) is 1000 particles, and Sizepop =1000; The position of the particle in the population space is represented by two-dimensional coordinates, dimension \( \text{dim}=2 \); Termination condition \( \text{ger}=50 \); Initial value of inertia weight \( c_1 =0.8 \); The initial value of individual learning factor is \( c_2 =0.5 \); The initial value of group learning factor was \( c_3 =0.01 \). Secondly, the flight area and flight speed of particles are constrained to prevent the impact of inertia weight, expand the search range and make the particles far away from the target position.

(2) According to CA-PSO principle, basic simulated data were defined, fitness function was designed, fitness value was compared and iterative optimization was performed. Gbest (individual extremum) and Zbest (population extremum) were found by comparing the fitness values of 1000 particles in the population space. Other inferior individuals update themselves according to the law, but the updated position and speed should not exceed the threshold. The updating method of particles is shown in Equations (1) and (2).

\[
V_{k+1} = wV_k + r_1c_2(gbest_k - x_k) + r_2c_3(zbest_k - V_k) \\
V_{k+1} = x_k + V_{k+1}
\]

Gbest represents individual extremum and Zbest represents group extremum. \( V_{k+1} \) represents the updated velocity of the particle, and \( x_{k+1} \) represents the updated position of the particle. \( K \) represents the number of current iterations, and \( K + l \) represents the number of next iterations. After many tests, the optimal learning factors \( c_1 \) and \( c_2 \) were determined. By comparing the adaptive value after each iteration, it is updated and gradually approaches the extreme value.

(3) the introduction of knowledge space. On the one hand, the knowledge space is self-renewing and evolving; On the other hand, knowledge space acquires elite individuals in population space each time to guide the evolution of other individuals.
(4) Loading and performance analysis of RSA-UAV. The RSA-UAV algorithm is loaded onto the optimal particle, and the optimal particle broadcasts the information to ensure the network security. Performance analysis is based on fitness, number of elite transfers and number of iterations.

5. Algorithm Simulation and Performance Analysis

Matlab was used for simulation, in which PSO was used to simulate the basic optimization loading information security algorithm of UAV cluster, and CA-PSO was used to simulate the spatial optimization loading information security algorithm of UAV cluster. The initial state of space particles in the UAV cluster is shown in Figure 3. It is assumed that all particles (simulated UAV) are randomly distributed in the whole space in a two-dimensional state, and the position and flight speed of each particle in the initial state are random. Then the convergence process of PSO and CA-PSO is shown in Figure 4 and Figure 5.

As can be seen from Fig. 4 and Fig. 5, under the optimization of the two algorithms, most particles gradually approach to the optimal individual, but the optimization effect of CA-PSO is better. During the whole search process, in the early stage of convergence, the global search ability of the two algorithms is not very different. In the middle search period, PSO convergence gradually falls into the local area and the convergence speed is fast. However, in the late search period, PSO's local search ability is worse than CA-PSO's. Therefore, from the whole search process, it can be seen that CA-PSO has better optimization ability.

Figure 6 is an iterative diagram of the two algorithms. Through continuous testing, it is found that when the population size is relatively small, there is little difference in the optimization ability of the two algorithms. However, with the increase of the population size, the optimal adaptive value and iteration times of CA-PSO algorithm are better than that of PSO algorithm.
Figure 6. PSO and CA-PSO iteration diagrams
Fig. 7 shows the elite individuals acquired after the knowledge space optimization, and Fig. 8 shows the number of iterations required by the elite individuals in the transmission process.

Figure 7. The relation graph of the adaptive value of elite number

Figure 8. Graph of number of elites versus number of iterations
As can be seen from Fig. 8, although the number of elite transfers is constantly increasing, the number of iterations required does not change much and almost approaches a stable state. And the number of iterations required is very small. It can be seen that even if the number of the population is increasing and the search area is relatively large, the optimization effect of CA-PSO algorithm still remains stable, and the optimization efficiency will not be reduced.

In conclusion, CA-PSO algorithm has better optimization effect than PSO algorithm in terms of the convergence process, the optimal fitness value or the number of iterations required. Therefore, compared with the optimization ability of PSO algorithm, CA-PSO algorithm has stronger optimization effect, better search ability and more accurate positioning under the guidance of knowledge and experience.

6. Conclusion
Unmanned aerial vehicle network security technology is the unmanned aerial vehicle to the sustainable development of one of the core technology, this paper combines the uav real-time characteristics and energy saving, choose the unmanned aerial vehicle cluster space optimization information security algorithm based on RSA, through the simulation and performance analysis, the results show that the algorithm in solving the problem of unmanned aerial vehicle (uav) web application security at the same time, It also reduces network overhead. But RSA - UAV algorithm to produce key is trivial, is limited by prime produce technology, so the security issue is still depend on
the factorization of large numbers. With the development of the decomposition technique of large number, future applications need to increase to more than 2048-bit key length.

Acknowledgments
Thanks National Natural Science Foundation of China (No.61661001, No.11863002), Project of Basic Applied Research Program in Yunnan Province (No.C0120180115), Scientific Research Fund Project of Yunnan Education Department(2021Y396), and Yunnan Academician Workstation of Wang Jingxiu (No. 202005AF150025), for their support.

References
[1] Jangra, Shalini and N. Goel. E-ARAN: enhanced authenticated routing for ad hoc networks to handle selfish nodes[C]. IEEE-International Conference On Advances In
[2] A. Sameh, A. Mahmoud, S. El-Kassas. RARAN: Authenticated Routing for Ad Hoc Networks Protocol with Reputation[J]. International Journal on Computer and Communications Networks, Computational Intelligence and Data Analytics, 2017, 1(1).
[3] Liu Pengpeng. Research on Key Technology of High Security Transmission of UAV Communication Network [D]. Nanchang University, 2020.
[4] Yang Geng, Xu Jian, Chen Wei, Qi Zhenghua, Wang Haiyong. Security Characteristics and Key Technologies of Internet of Things [J]. Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition), 2010, 30(04):20-29.
[5] Reynolds Robert G.. Cultural Algorithms: Tools to Model Complex Dynamic Social Systems [M]. John Wiley & Sons, Inc.: 2020-10-15.
[6] Sarbazi Azad Saeed, Abadeh Mohammad Saniee, Mowlaei Mohammad Erfan. Using Data Complexity Measures and an Evolutionary Cultural Algorithm for Gene Selection in Microarray Data [J]. Soft Computing Letters, 2020 (prepublish).
[7] Guo Yinan, Chen Meirong, Wang Chun, Liu Haiyuan. Convergence analysis of cultural algorithms [J]. Control and Decision, 2013, 28(09):1361-1364+1371.