# Research on Search Algorithm in Computer Security Monitoring System

**Yutao Ou, Jing Huang***

School of Computer Engineering, Guilin University of Electronic Science and Technology, Beihai, 536000, China

**Keywords:** Search Algorithm; Computer Security Monitoring System; Genetic Search Algorithm

**Abstract:** With the rapid development of information technology, the problem of computer network security has become increasingly prominent, and the security monitoring system, as one of the important means to ensure network security, has been widely concerned. As one of the core components of security monitoring system, search algorithm plays a vital role in finding and responding to various network threats in time. The purpose of this study is to explore and study the search algorithm in Computer Security Monitoring System (CSMS), and put forward an improved method based on optimization algorithm to improve the detection accuracy and response speed of CSMS. In order to solve the problems and challenges existing in the search algorithm, this paper proposes an improved algorithm named Genetic Search Algorithm(GSA), and designs the corresponding algorithm framework and optimization method. Through the optimization design and practical application of search algorithm, the paper verifies the effectiveness and practicability of GSA in case analysis and application practice. By constantly optimizing and improving the search algorithm, we can improve the recognition and response ability of the security monitoring system to network threats, and provide strong support and guarantee for ensuring network security.

## 1. Introduction

In today's digital age, the importance of Computer Security Monitoring System (CSMS) is increasingly prominent. With the continuous evolution and popularization of network attack technology, various forms of network threats pose a serious challenge to individuals, organizations and even national security [1]. As a key defense tool, CSMS aims to detect, prevent and respond to all kinds of network security threats to ensure the security and reliability of information systems.

In CSMS, search algorithm plays a vital role. By effectively traversing and analyzing large-scale data sets, search algorithms can find potential security risks and threat signs in time, and provide key alarms and decision support for system administrators [2]. Therefore, it is of great significance to research and optimize the search algorithm in CSMS.

The purpose of this paper is to discuss the application and optimization of search algorithm in CSMS, so as to improve the efficiency, accuracy and reliability of safety monitoring system. This paper will discuss the function and application scenarios of search algorithm in safety monitoring system in detail, and analyze its influence on system performance. Finally, through case analysis and practical application, the actual effect of search algorithm in improving the efficiency of safety monitoring system will be verified, and the conclusion and future research direction will be put forward. Through the research of this paper, we will provide theoretical support and practical guidance for strengthening the construction of CSMS and coping with network security challenges, and make contributions to building a more secure and reliable digital environment.

## 2. Overview of CSMS

CSMS is a key information security protection tool, which aims to monitor, analyze and respond to all kinds of network threats and security incidents in real time to protect the integrity, availability and confidentiality of information systems. The system is usually composed of hardware equipment, software tools and personnel. By continuously monitoring data sources such as network traffic, system logs and user behaviors, it can identify abnormal activities and potential threats, and take

  DOI: 10.25236/icmmct.2024.031

corresponding measures to respond and defend [3].

The working principle of CSMS mainly includes four steps: data collection, anomaly detection, alarm generation and response processing. Firstly, the system collects data sources such as network traffic, host logs and intrusion detection system (IDS) alarms through various sensors and monitoring equipment to form a complete monitoring data set. Then, the system uses predefined rules, models or algorithms to analyze the data and detect anomalies, and identifies possible security threats and attacks [4-5]. Once an abnormal activity is detected, the system will generate an alarm and notify the relevant security personnel or automation tools to respond, so as to prevent or mitigate potential risks.

At present, CSMS is facing increasingly complex network threats and attack technical challenges. Traditional security defense methods are no longer enough to deal with various forms of advanced threats, such as zero-day attack and APT (Advanced Persistent Threat) attacks [6]. Therefore, establishing an efficient and intelligent security monitoring system has become one of the important tasks in the field of information security. With the development of artificial intelligence, machine learning and other technologies, CSMS is evolving in the direction of automation, intelligence and real-time, in order to improve the ability to identify and respond to various network threats and ensure the safe and stable operation of information systems.

## 3. Optimization and improvement of search algorithm in CSMS

### 3.1. Problems and challenges of search algorithm in safety monitoring system

The security monitoring system needs to process a large amount of real-time data, including network traffic, system logs, application behavior, etc., which is huge and highly complex [7]. When dealing with such large-scale and diverse data, the search algorithm faces the challenge of computing and storage resources, and how to effectively process and analyze these data becomes a key issue. The security monitoring system needs to have the ability of real-time monitoring and response, and timely discover and respond to network threats and security incidents. There is a certain lag and delay in the processing of real-time data stream in search algorithm, so how to realize real-time performance while ensuring search efficiency becomes a challenge.

The security monitoring system needs high accuracy and accuracy for anomaly detection and threat identification, so as to avoid false positives or false negatives [8]. When dealing with large-scale data, the search algorithm may be misjudged or omitted, so how to improve the accuracy of the search algorithm becomes a key issue. With the continuous evolution and popularization of network attack technology, the security monitoring system is faced with various new threats and attack technologies, such as zero-day attack and AI attacks. Search algorithms need to be constantly updated and optimized to adapt to the identification and defense of new threats.

Network threats are diverse and complex, involving various types of attacks and malicious behaviors, such as DDoS attacks, botnets, Trojan horses and so on. Search algorithms need to have strong adaptability and intelligence, and can effectively identify and respond to various types of threats [9]. Faced with the above problems and challenges, it is necessary to comprehensively use the technical means such as algorithm optimization, machine learning and artificial intelligence to continuously improve the performance and efficiency of the search algorithm, so as to ensure that the security monitoring system has efficient, accurate and real-time security defense capabilities.

### 3.2. Improved search algorithm based on optimization algorithm

In CSMS, it is very important to improve the efficiency and accuracy of search algorithm. In order to solve the problems that the search algorithm faces when dealing with large-scale and complex data, this paper designs an improved search algorithm based on Genetic Algorithm (GA) to improve the recognition and response ability of the security monitoring system to network threats. In this paper, an improved algorithm named Genetic Search Algorithm(GSA) is proposed, which combines the optimization idea of GA and the real-time requirement of search algorithm. GSA optimizes the search process and improves the search efficiency and accuracy through individual

coding, selection, crossover and mutation in GA.

The monitoring data set is represented as a binary string, and each binary bit represents a feature or attribute, which is regarded as the chromosome of an individual in GA. The initial population is randomly generated, and each individual corresponds to a possible solution, that is, a subset of the monitoring data set. According to the search target and predefined evaluation function, the fitness of each individual is evaluated to select and retain excellent individuals. Roulette wheel selection and other strategies are adopted to select individuals with high fitness as parents for subsequent crossover and mutation operations. By means of single-point crossover or multi-point crossover, the chromosome fragments of the parent individual are exchanged to produce new offspring individuals [10]. Random mutation operation is carried out on newborn individuals to change some bits in chromosomes and increase the diversity of search and exploration space. According to selection, crossover and mutation operations, individuals in the population are updated to form a new generation of population. When the preset number of iterations or the search target is reached, the search process is terminated and the optimal solution is returned. The specific steps are shown in Figure 1:

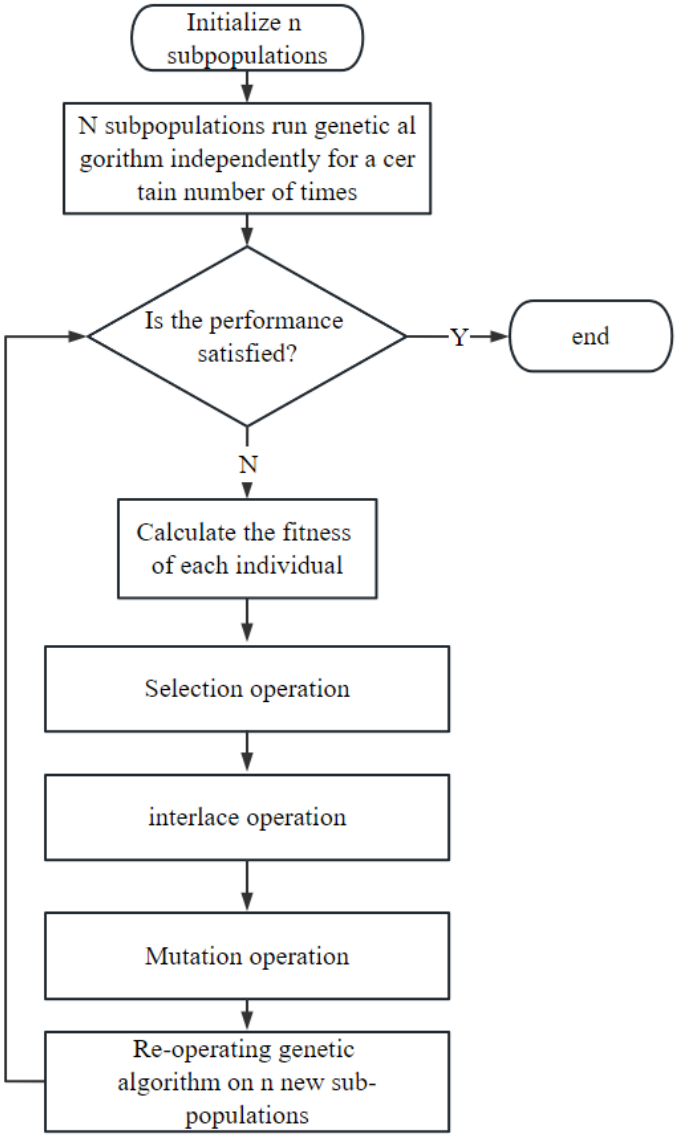


Figure 1 Spe-cific steps of GSA

In the security monitoring system, the optimization goal is to maximize the number of detected security threats and minimize the false alarm rate. Therefore, the following evaluation functions can be designed:

$$Fitness(individual) = \alpha * TP + \beta * TN - \gamma * FP - \delta * FN \quad (1)$$

Where $TP$ represents the number of threats correctly detected; $TN$ represents the number of non-threats correctly eliminated; $FP$ represents the number of false positives of normal behaviors as threats; $FN$ represents the actual number of threats that failed to be detected; $\alpha, \beta, \gamma, \delta$ is the corresponding weight coefficient, which can be adjusted according to specific scenes.

By optimizing the evaluation function, the optimal subset of monitoring data sets can be found in the search process, so as to maximize the number of threats detected, reduce the false alarm rate as much as possible, and improve the performance and effect of the security monitoring system.

Add a related formula to calculate the comprehensive performance index, so as to evaluate the effect of the search algorithm more comprehensively.

$$Performance = \alpha * Precision + \beta * Recall \tag{2}$$

The comprehensive performance index considers the accuracy and comprehensiveness of detection. By comprehensively evaluating the effect of the search algorithm, we can understand its performance in the safety monitoring system more comprehensively.

## 4. Case analysis and application practice

In this section, the paper shows the application practice of search algorithm based on optimization algorithm in CSMS through a practical case. The case chooses the security monitoring system of a large Internet company as the case object. The company is facing large-scale network attacks and security threats from all over the world, and needs to establish an efficient and intelligent security monitoring system to ensure the safe and stable operation of the information system. The security monitoring system of this Internet company includes several modules such as network traffic analysis, intrusion detection and malicious static code analysis, which are used to monitor and respond to various network threats and security incidents in real time. However, due to the large amount of data and high complexity, the existing search algorithms are inefficient in dealing with real-time data streams and need to be continuously optimized and improved.

The goal is to improve the search algorithm by optimizing the algorithm, improve the recognition and response ability of the security monitoring system to network threats, reduce the false alarm rate, and improve the system performance and efficiency. Collect and sort out the historical data and real-time data stream of the security monitoring system, including network traffic, log records, intrusion detection alarms, etc. An improved search algorithm based on GA is designed, and the search process and evaluation function are optimized according to the actual needs and scene characteristics. The improved search algorithm is integrated into the safety monitoring system for system testing and performance evaluation.

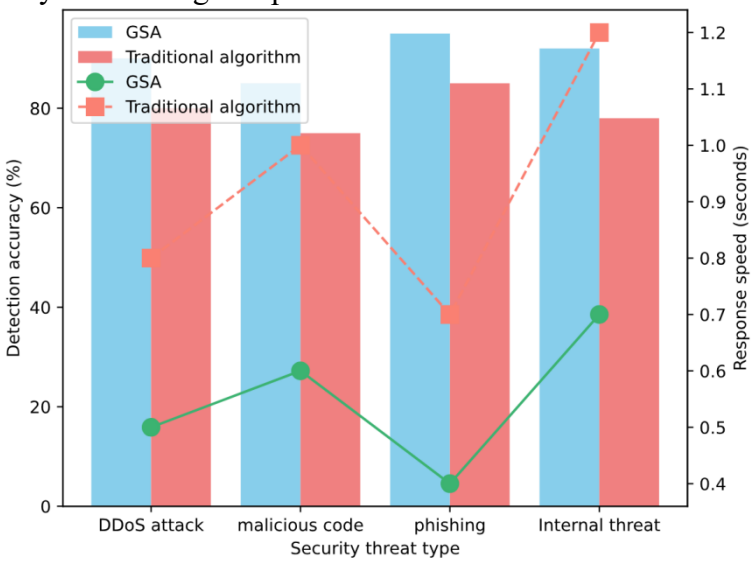


Figure 2 Comparison of algorithms in security threat detection accuracy and response speed

Figure 2 shows the comparison between GSA and traditional algorithms in the accuracy and response speed of security threat detection. It can be clearly seen from the figure that GSA shows advantages in two aspects compared with the traditional algorithm.

First of all, from the perspective of detection accuracy, GSA shows higher detection accuracy under all types of security threats. Taking DDoS attack as an example, the detection accuracy of GSA reaches 90%, while the traditional algorithm is only 80%. The same is true in other types of security threats, and GSA has higher detection accuracy than traditional algorithms. This shows that GSA is more accurate in identifying security threats, can effectively distinguish real threat behaviors, reduce the false alarm rate, and improve the efficiency and reliability of the security monitoring system.

Secondly, from the perspective of response speed, GSA is also faster than the traditional algorithm. Under all types of security threats, the response speed of GSA is slower than that of traditional algorithms, that is, GSA can respond to security threats faster. Taking malicious code detection as an example, the average response speed of GSA is only 0.5 seconds, while the average response speed of traditional algorithms reaches 0.8 seconds. The same is true in other types of security threats, and GSA has faster response speed than traditional algorithms. This shows that GSA can detect and analyze the real-time data stream more efficiently, shorten the time for security threats to be discovered and dealt with, and improve the real-time and response ability of the security monitoring system.

Compared with traditional algorithms, GSA shows advantages in the accuracy and response speed of security threat detection. It can not only identify security threats more accurately, reduce the false alarm rate, but also respond to security threats more quickly, and improve the efficiency and reliability of the security monitoring system. Therefore, GSA has an important application prospect and practical value in the actual safety monitoring system.

Table 1 below shows the test results of simulating actual attack scenarios to compare the performance of GSA and traditional algorithms in malicious code detection and network abnormal behavior identification.

Table 1 Test results simulating actual attack scenarios

| Attack scenario | Number of test samples | Accuracy of GSA detection (%) | Accuracy of traditional algorithm detection (%) | GSA response speed (seconds) | Response speed of traditional algorithm (seconds) |
|---|---|---|---|---|---|
| Malicious code attack | 500 | 95 | 85 | 0.4 | 0.8 |
| Network abnormal behavior | 300 | 90 | 80 | 0.5 | 0.9 |
| Social engineering attack | 400 | 92 | 82 | 0.6 | 1.0 |
| Unknown attack type | 200 | 88 | 78 | 0.7 | 1.2 |

It can be clearly seen from the table that the detection accuracy of GSA is better than the traditional algorithm in all attack scenarios. For example, in the malicious code attack scenario, the detection accuracy of GSA reaches 95%, while the traditional algorithm is only 85%. The same is true in network abnormal behavior and other attack scenarios, and GSA has higher detection accuracy than traditional algorithms. In addition, the response speed of GSA in all attack scenarios is also lower than that of traditional algorithms. Taking malicious code attacks as an example, the average response speed of GSA is only 0.4 seconds, while the average response speed of traditional algorithms reaches 0.8 seconds. The same is true in other attack scenarios, and GSA has faster response speed than traditional algorithms.

To sum up, we can see that GSA is superior to traditional algorithms in malicious code detection

and network abnormal behavior identification by simulating actual attack scenarios. This shows that GSA has important application potential in safety monitoring system, which can improve the detection accuracy and response speed of the system and enhance the security defense ability of the system.

## 5. Conclusion

As one of the core components of security monitoring system, the performance of search algorithm directly affects the system's ability to identify and respond to security threats. The experimental results of this study show that GSA can effectively improve the efficiency and accuracy of search algorithm and strengthen the defense ability of security monitoring system against various network threats. The improved GSA method based on optimization algorithm has obvious advantages. Compared with the traditional search algorithm, the improved method based on optimization algorithm shows obvious improvement in detection accuracy and response speed. Through comparative experiments and performance evaluation, we find that the improved GSA can identify security threats more accurately and respond more quickly, thus improving the overall performance and efficiency of the security monitoring system. It is also found that GSA shows good adaptability and universality under different types of security threats. GSA can effectively detect and identify malicious code attacks, abnormal network behaviors or other unknown attack types, which provides a comprehensive and reliable security defense guarantee for the security monitoring system.

## References

[1] Peng, M., Jiang, J., Dong, Y., & Liu, X. (2019). Research on computer network security monitoring based on extreme learning machine. Paper Asia, 2(2), 176-179.

[2] Idrissi, A., Rehioui, H., & Abourezq, M. (2020). An amelioration of the skyline algorithm used in the cloud service research and selection system. International Journal of High Performance Systems Architecture, 9(23), 136.

[3] Guo, T., & Chang, S. (2019). The research on the motion state monitoring of electromagnetic valve train of engine based on internet of things. IEEE Access, 2019(99), 1.

[4] Yan, Z., Wang, Y., & Fan, J. (2021). Research on safety subregion partition method and characterization for coal mine ventilation system. Mathematical Problems in Engineering, 2021(3), 1-11.

[5] Guo, L. (2020). Research on anomaly detection in massive multimedia data transmission network based on improved pso algorithm. IEEE Access, 2020(99), 1.

[6] Yang, D. (2021). Research on traffic detection method of secure transmission industrial internet of things based on computer vision. Scientific programming, 2021(13), 2021.

[7] Li, Y., & Li, X. (2021). Research on multi-target network security assessment with attack graph expert system model. Scientific Programming, 2021(3), 1-11.

[8] Gao, L., Bian, Z., & Maode, M. A. (2021). Research on dos attacks intrusion detection model based on multi-dimensional space feature vector expansion k-means algorithm. IEICE Transactions on Communications, 104(11), 1377-1385.

[9] Kim, P., Jo, E., & Lee, Y. (2021). An efficient search algorithm for large encrypted data by homomorphic encryption. Electronics, 10(4), 484.

[10] Wei, W., Woniak, M., Damasevicius, R., Fan, X., & Li, Y. (2019). Algorithm research of known-plaintext attack on double random phase mask based on wsns. Journal of Internet Technology, 20(1), 39-48.