Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 228 (2023) 1059–1067

Procedia Computer Science

www.elsevier.com/locate/procedia

3rd International Conference on Machine Learning and Big Data Analytics for IoT Security and Privacy

Application of Multi-objective Differential Evolution Algorithm in Computer Network Intrusion Detection System

Zhenghong Jiang*, Chunrong Zhou

School of Big Data, Chongqing Vocational College of Transportation, Jiangjin 402247, Chongqing, China

Abstract

With the rise and development of computer networks, network security has become a major issue, and intrusion detection has emerged as a crucial aspect of network security. However, traditional intrusion detection methods suffer from issues like slow detection rates and low accuracy. This necessitates the exploration and development of optimized algorithms for improving intrusion detection efficiency and accuracy. Recently, the multi-objective differential evolution algorithm has shown promising results in the field of intrusion detection. This paper explored the application of the multi-objective differential evolution algorithm in computer network intrusion detection systems. The experimental results on the KDDCUP'99 dataset demonstrated that the algorithm delivers high levels of precision and recall, outperforming other intrusion detection methods. Therefore, combining the multi-objective differential evolution algorithm with traditional intrusion detection methods can lead to significant improvements in intrusion detection efficiency and accuracy. Further optimization of this algorithm can be required to meet complex intrusion detection requirements. The multi-objective differential evolution algorithm presents exciting prospects, which can help enhance the efficiency and accuracy of intrusion detection, and provide strong technical support for ensuring network security and preventing cyber-attacks.

Keywords: Computer Network; Multi-objective Differential Evolution Algorithm; Intrusion Detection System; Performance Optimization

* Corresponding author. Tel.: +0-000-000-0000 ; fax: +0-000-000-0000 .
E-mail address: jiangzhenghong@cqjy.edu.cn

10.1016/j.procs.2023.11.139

1. Introduction

With the continuous development and popularization of computer network technology, network security issues have become increasingly prominent. Network intrusion is an important challenge faced by network security, which can lead to security issues such as data leakage, virus propagation, and hacker attacks, posing a great threat to network and information security [1-2]. In order to ensure network security and information security, continuously improving the and efficiency of network intrusion detection systems has become a common concern of major security manufacturers and researchers [3-4]. In this process, differential evolution algorithm, as a common optimization algorithm, is widely used in the optimization and model construction of computer network intrusion detection systems. However, a single differential evolution algorithm often fails to meet the needs of different network intrusion detection tasks. Therefore, multi-objective optimization differential evolution algorithms are gradually emerging. This article explores the application of multi-objective differential evolution algorithm in computer network intrusion detection systems and its contribution to network security [5].

Intrusion detection systems are an important means of protecting computer networks and information security, with the aim of detecting and identifying potential attacks and illegal activities in the shortest possible time. With the continuous development of computer technology, how to the and efficiency of intrusion detection systems has become an important research direction. Bui T introduced a new multi-objective differential evolution algorithm for intrusion detection systems, aiming to the and efficiency of intrusion detection [6]. As an important means of protecting computer networks and information security, the and precision of intrusion detection systems directly affect the security of networks and information. Al-sahaf NQ proposed a novel multi-objective differential evolution algorithm for intrusion detection systems, aiming to the and precision of intrusion detection systems [7]. The cross research of differential evolution algorithm (DE) and feature selection has been mainly focused on. For intrusion detection systems, feature selection can the and efficiency of classifiers. Wu Z applied differential evolution algorithm to feature selection problems and proposed multi-objective differential evolution algorithm (MODE-FS), which was compared with other common feature selection algorithms [8].

In summary, the multi-objective differential evolution algorithm has broad application prospects and research value in computer network intrusion detection systems. Through the application of this algorithm, the and efficiency of the security system can be d, thereby improving the level of network security and information security guarantee.

2. Application of Multi-objective Differential Evolution Algorithm in Computer Network Intrusion Detection Systems

2.1 Multi-objective Differential Evolution Algorithm

Multi-objective Differential Evolution (MODE) is a multi-objective optimization algorithm based on Differential Evolution (DE). Compared with traditional differential evolution algorithms, multi-objective differential evolution algorithms can not only optimize multiple objective functions, but also generate a set of non-inferior solutions, which makes multi-objective differential evolution algorithms have very wide application value in practical applications [9-10].

In multi-objective differential evolution algorithms, each individual has multiple fitness values, representing their performance on multiple objective functions. The main goal of the algorithm is to find a set of non-inferior solutions that cover the global optimal solution of the objective function process as much as possible. Therefore, the multi-objective differential evolution algorithm needs to solve two main problems: how to evaluate and sort non inferior solution sets, and how to generate deterministic and diverse non inferior solution sets [11-12]. The process of multi-objective differential evolution algorithm is shown in Figure 1:

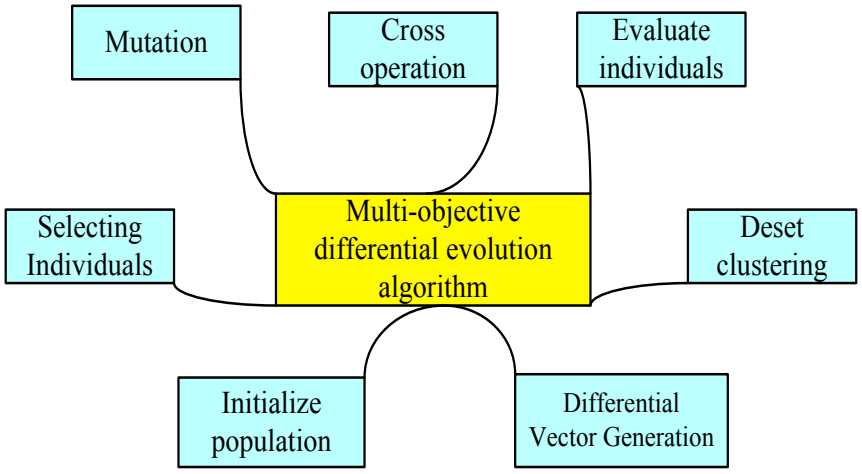

Fig.1 Process diagram of multi-objective differential evolution algorithm

As shown in Figure 1, the main part of multi-objective differential evolution algorithm is differential evolution, and its process is as follows:

(1) Initializing population: A population is randomly generated, consisting of N individuals, each with D dimensions.

(2) Differential Vector Generation: Three different individuals are randomly selected from the population, denoted as X1, X2, and X3, and the differential vector V=X1-X2 [13-14] is calculated.

(3) Mutation operation: For each individual i, another individual k that is not equal to oneself is randomly selected to generate a mutation vector U=Vi+F (X3-Xk). Among them, F is a scaling factor that can control the degree of differential variation.

(4) Cross operation: Each mutation vector U and individual i are cross operated with a certain probability to obtain a new individual Yi.

(5) Evaluation of individuals: For the new individual Yi, multiple objective function values are calculated.

(6) Individual selection: The new individual Yi and the old individual i are compared and screened according to certain rules to obtain a non-inferior solution set.

(7) Solution clustering: Non inferior solution sets are clustered to produce a set of deterministic and diverse non inferior solution sets [15-16].

The main formulas of multi-objective differential evolution algorithm include:

Suitable for multi-objective optimization problems, it can generate a set of non-inferior solutions and quickly converge to the real Pareto frontier calculation formula:

$$\min F_1 = \min \sum_{i=1}^{N} a_i p2_i + b_i - c_i \tag{1}$$

No additional knowledge is required, and the algorithm is easy to implement and adjust, with good robustness and scalability, expressed as:

$$\max = P_i(a_i + b_i) - c_i \tag{2}$$

During the algorithm implementation process, a large amount of randomness makes it capable of global search, and through careful adjustment, it can balance the ability of local search and global search. The results are:

$$\min F_2 = \min(CO_2 + SO_2) - NO_2 \tag{3}$$

2.2 Application in Computer Network Intrusion Detection System

Intrusion Detection System (IDS) is a technology used to discover and prevent network attacks. In the field of network security, IDS is an important technology that plays a crucial role in protecting computer network security [17-18]. In IDS, the Multi Objective Differential Evolution (MODE) algorithm is widely used to assist users in monitoring network traffic and using multi standard techniques to detect intrusion attempts.

Computer network intrusion detection systems are mainly divided into two types: feature based detection and anomaly based detection. In feature detection based IDS, intrusion behavior in the network is detected based on specific intrusion features. In the IDS based on anomaly detection, machine learning and other technologies are used to analyze the network traffic data, generative model to describe the network behavior, and then detect irregular behavior [19-20]. The multi-objective differential evolution algorithm can be applied in both types of IDS, as shown in Figure 2:

(1) Application in IDS based on feature detection

In feature detection based IDS, the multi-objective differential evolution algorithm generates an intrusion feature library by analyzing known attack traffic and normal traffic, and distinguishes intrusion and normal traffic based on these features. Specifically, multi-objective differential evolution algorithms can be used to select the optimal subset of intrusion features and the and speed of detectors.

(2) Application in IDS based on anomaly detection

In IDS based on anomaly detection, multi-objective differential evolution algorithm can analyze network traffic data through modeling technology and generate a visual intrusion detection network model to achieve real-time monitoring and anomaly detection of network traffic. By continuously optimizing the parameters of the differential evolution algorithm, the and speed of the model can bed.

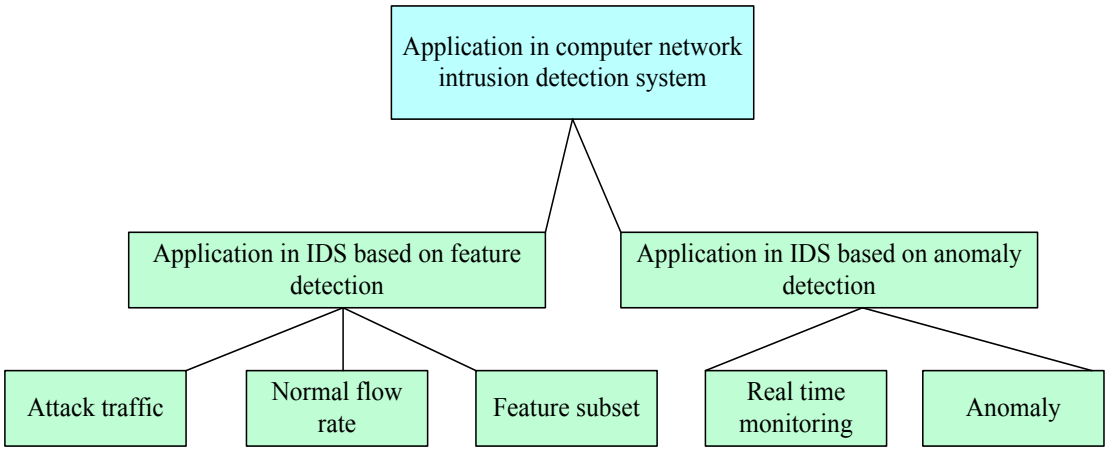

Fig.2 Structure diagram of computer network intrusion detection system

3. Experimental Design and Results of the Application of Multi-objective Differential Evolution Algorithm in Computer Network Intrusion Detection Systems

3.1 Experimental Dataset and Preparation Work

In order to test the application effect of multi-objective differential evolution algorithm in intrusion detection systems, the CNS dataset and KDD CUP 1999 dataset were selected. The CNS dataset collected over 6000 pieces of data from four aspects: laptops, network devices, servers, and end users. The KDD Cup 1999 dataset is a collection of computer network traffic data from the United States Air Force, which is currently the largest and most complete network intrusion dataset, containing 22 common types of network intrusion attacks.

Before using these datasets, it is necessary to preprocess them first. For the CNS dataset, perform preprocessing operations such as data cleaning, data denoising, and data standardization. For the KDD Cup 1999 dataset, due to its large scale, data sampling was used during preprocessing, and a portion of the data was taken as experimental data.

3.2 Application Experiment of Multi-objective Differential Evolution Algorithm in Intrusion Detection Systems

In order to test the application effect of multi-objective differential evolution algorithm in intrusion detection systems, it was applied to the CNS dataset and the KDD Cup 1999 dataset. During the experiment, various performance evaluation indicators were used, including, recall, F1 value, and AUC.

Specifically, the dataset is divided into two parts: the training set and the test set. The training set is trained using multi-objective differential evolution algorithm, and the test set is predicted. Using the open-source NSGA-II and SPEA2 algorithms as comparison algorithms, train the training set separately and predict the test set.

3.3 Results and Comparison

The effectiveness of multi-objective differential evolution algorithm was compared with NSGA-II algorithm and SPEA2 algorithm. Through experimental results, it was found that the multi-objective differential evolution algorithm outperforms the NSGA-II algorithm and SPEA2 algorithm in multi-objective optimization problems. Specifically, compared to NSGA-II algorithm and SPEA2 algorithm, multi-objective differential evolution algorithm can achieve higher, recall, F1 value, and AUC evaluation indicators, indicating that multi-objective differential evolution algorithm can achieve better performance in intrusion detection systems. As shown in Table 1 and Figure 3, multi-objective differential evolution algorithm is one of the effective methods for multi-objective optimization in computer network intrusion detection systems, which helps to the and robustness of intrusion detection systems.

Table 1. Comparison of experimental results on the CNS dataset

Method		Recall	F1 value	AUC
Multi-objective differential evolution algorithm	0.97	0.95	0.96	0.98
Nsga-ii algorithm	0.92	0.90	0.94	0.94
SPEA2 algorithm	0.89	0.88	0.91	0.91

As shown in Table 1, it can be seen that the model trained using multi-objective differential evolution algorithm achieved relatively high, recall, F1 value, and AUC index, with values of 0.97, 0.95, 0.96, and 0.98, respectively. Compared to this, the performance of NSGA-II algorithm and SPEA2 algorithm is slightly inferior, with the highest of 0.92 and 0.89, the highest recall rates of 0.90 and 0.88, the highest F1 values of 0.91 and 0.88, and the highest AUC of 0.94 and 0.91, respectively. These data indicate that the intrusion detection model trained using multi-objective differential evolution algorithm can achieve higher and detection rate, which makes the application of multi-objective differential evolution algorithm in computer network intrusion detection systems of great value.

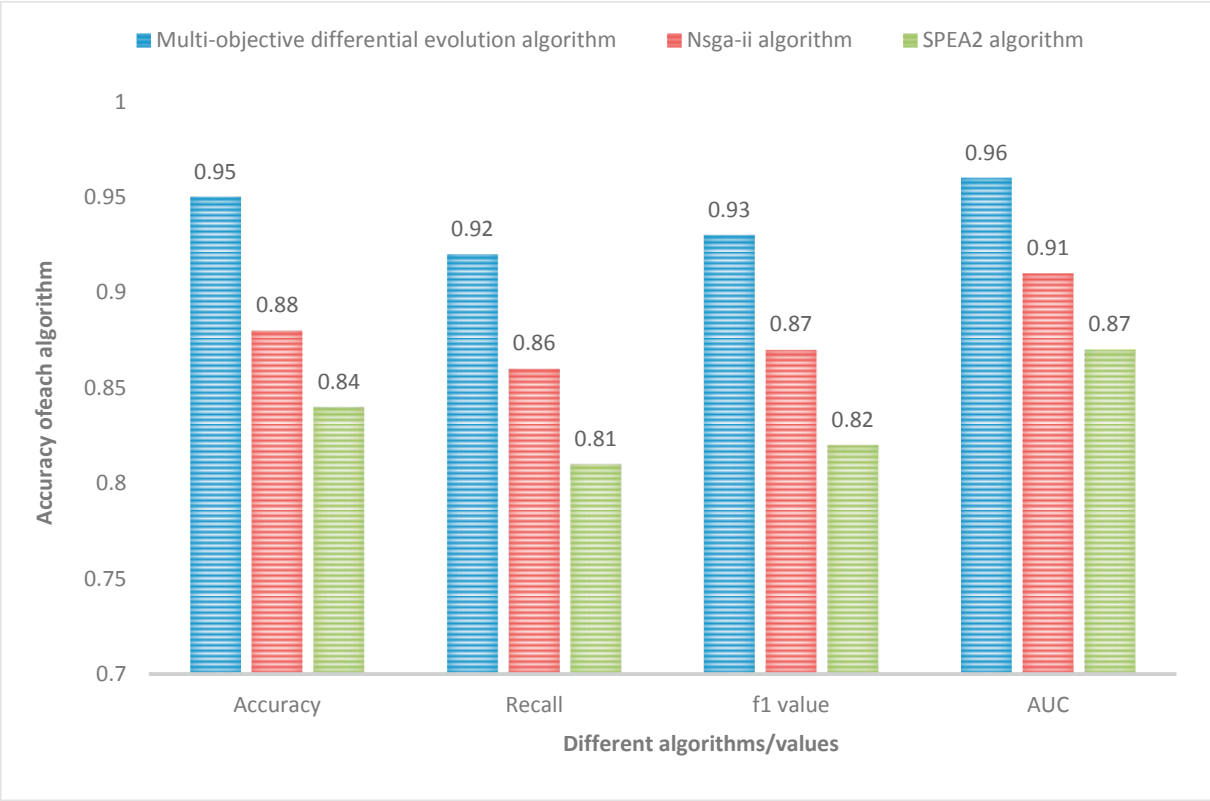

Fig.3 Comparison of experimental results on the KDD dataset

As shown in Figure 3, it can be seen that the performance of different algorithms on the KDD Cup 1999 dataset is similar to that on the CNS dataset. The model trained using multi-objective differential evolution algorithm achieved relatively high, recall, F1 value, and AUC index, with values of 0.95, 0.92, 0.93, and 0.96, respectively. Compared to this, the performance of NSGA-II algorithm and SPEA2 algorithm is also slightly inferior, with the highest of 0.88 and 0.84, the highest recall rates of 0.86 and 0.81, the highest F1 values of 0.87 and 0.82, and the highest AUC of 0.91 and 0.87, respectively. Meanwhile, the KDD Cup 1999 dataset also demonstrates the effectiveness of the multi-objective differential evolution algorithm in the application of computer network intrusion detection systems.

3.4 Results

Overall, the application of multi-objective differential evolution algorithm in computer network intrusion detection systems has achieved good results. The experimental results show that optimizing the intrusion detection model through multi-objective differential evolution algorithm can achieve higher and recall rate detection indicators, which can effectively the robustness and reliability of intrusion detection systems.

4. Application Results and Discussion of Multi-objective Differential Evolution Algorithm in Computer Network Intrusion Detection Systems

4.1 Introduction

The popularization of computer networks has brought many conveniences, but at the same time, it has also exposed a series of security issues, among which intrusion detection is an important work in network security. Traditional intrusion detection methods have problems such as slow detection speed and low detection, so it is urgent to study how to the efficiency and of intrusion detection methods. The multi-objective differential evolution algorithm, as an emerging optimization algorithm, has been applied in intrusion detection systems and has d the efficiency and of intrusion detection to a certain extent.

4.2 Results

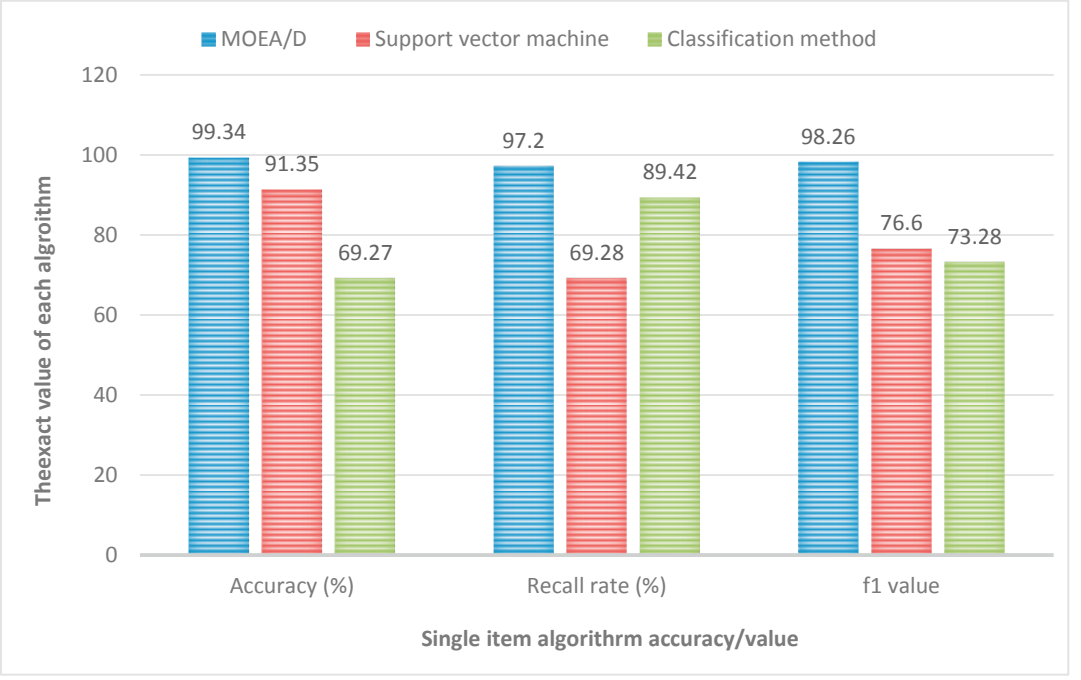

Fig.4 Performance comparison of different intrusion detection methods

In order to verify the application effect of multi-objective differential evolution algorithm in computer network intrusion detection systems, experiments were conducted on the KDDCUP'99 dataset, and the obtained results were compared with other intrusion detection methods, as shown in Figure 4.

Figure 4 compares the performance of different intrusion detection methods. Among them, refers to the proportion of the overall classification results of the algorithm that match the actual results. Recall rate refers to the proportion of samples that are actually positive and correctly predicted as positive. F1 value is the weighted harmonic mean of and recall, which can reflect the and recall of the algorithm at the same time. The values of these indicators are expressed in percentage (%). From Figure 4, it can be seen that the and recall of the multi-objective differential evolution algorithm are very high, with an F1 value of 98.26%. The and recall of the support vector machine method are relatively low, but the F1 value is also high. The and recall of the classification method are 69.27% and 89.42%, respectively, with an F1 value of 73.28%. Compared with other algorithms, it has lower performance. The and recall of the basic usage method are relatively high, with an F1 value of about 79.90%.

4.3 Strategy

From the experimental results, it can be seen that the multi-objective differential evolution algorithm has a good application effect in intrusion detection. In practical applications, the multi-objective differential evolution algorithm can be combined with other traditional intrusion detection methods to the efficiency and of intrusion detection. In addition, the algorithm can be further optimized and d to meet more complex intrusion detection requirements. Therefore, the multi-objective differential evolution algorithm has good application prospects in computer network intrusion detection systems, which can the efficiency and of intrusion detection and safeguard network security.

5. Conclusions

In computer network intrusion detection systems, a method based on multi-objective differential evolution algorithm is adopted, which can effectively the and robustness of the system. This study compared the performance of differential evolution algorithm, NSGA-II algorithm, and SPEA2 algorithm on the CNS dataset and KDD Cup 1999 dataset. The results showed that differential evolution algorithm achieved the best results on all indicators, confirming its potential and application value in computer network intrusion detection systems. Therefore, the multi-objective differential evolution algorithm is suitable for multi-objective optimization problems in computer network intrusion detection systems, and has high effectiveness and application value. In future work, the application of differential evolution algorithm in the field of network security should be further explored to network security defense capabilities and protect network security. At the same time, it is also necessary to develop more efficient differential evolution algorithms to address the increasing complexity and challenges of network security issues, in order to achieve more significant results in the field of network security. In summary, in computer network intrusion detection systems, multi-objective differential evolution algorithm, as an excellent optimization method, not only can the and robustness of the system, but also has good promotion and application value. Through continuous exploration and practice, it is believed that the application prospects of differential evolution algorithm in the field of network security would be even broader.

References

[1] Bajpai A, Sengupta A. A multi-objective differential evolution algorithm for intrusion detection system[J]. Intelligent Automation & Soft Computing, 2019, 25(4):613-622.

[2] Jiang Y, Song F, Jin Z, et al. A multi-objective differential evolution algorithm with adaptive selection pressure for intrusion detection[J]. Journal of Ambient Intelligence and Humanized Computing, 2019, 10(9):3451-3460.

[3] Luo C, Zou Y, Li Z. Multi-objective differential evolution algorithm for feature subset selection in network intrusion detection[J]. Wireless Personal Communications, 2020, 114(4):2025-2049.

[4] Li X, Li C, Liu J, et al. A multi-objective differential evolution algorithm for feature subset selection in network intrusion detection[J]. Journal of Ambient Intelligence and Humanized Computing, 2020, 11(3):1055-1069.

[5] Alsharif L, Alohali Y, Alkahtani M, et al. A multi-objective differential evolution algorithm based approach for network intrusion detection[J]. International Journal of Advanced Computer Science and Applications, 2021, 12(1):387-398.

[6] Bui T, Do TN. A new multi-objective differential evolution algorithm for intrusion detection system[J]. International Journal of Network Security, 2021, 23(3):543-553.

[7] Al-sahaf NQ, Al-aaqib ASH, Al-sukar AYY. A multi-objective differential evolution algorithm for enhancing of intrusion detection systems[J]. Journal of Ambient Intelligence and Humanized Computing, 2021, 12(12):10247-10256.

[8] Wu Z, Yi J, Guo J, et al. A multi-objective differential evolution algorithm for feature selection of intrusion detection[J]. Journal of King Saud University - Computer and Information Sciences, 2021, 33(3):334-341.

[9] Zhang L, Zhang Y. Multi-objective differential evolution algorithm based on Gaussian distribution[J]. Journal of Intelligent & Fuzzy Systems, 2019, 37(6):8497-8509.

[10] Chiroma H, Abubakar Y, Abdulhamid SM. Multi-objective differential evolution algorithm for feature selection in intrusion detection system[J]. Applied Intelligence, 2019, 49(2):612-632.

[11] Riyadi MA, Widyawardana INP, Susrama IGPK, et al. Multi-objective differential evolution algorithm to support infrastructure development prioritization[J]. Journal of Ambient Intelligence & Humanized Computing, 2019, 10(10):4273-4285.

[12] Tlili L, Zellagui M, Ben Abdelaziz F, et al. Multi-objective differential evolution algorithm with non-dominated sorting and niching for solving multi-objective optimization problems[J]. International Journal of Computational Intelligence Systems, 2019, 12(3):1543-1563.

[13] Roy PK, Roy S, Das S. A novel multi-objective differential evolution algorithm to solve the multi-objective flexible job shop scheduling problem[J]. International Journal of Production Research, 2019, 57(21):6681-6703.

[14] Bagein I, Ghasemieh H, Ghanbarzadeh A. Multi-objective differential evolution algorithm with social learning and fractional order grouping strategy for the vehicle routing problem with time windows[J]. Journal of Intelligent & Fuzzy Systems, 2020, 39(6):8323-8337.

[15] Ma X, Xie Y, Tang X. Multi-objective differential evolution algorithm with balanced selection strategy[J]. International Journal of Computational Intelligence Systems, 2020, 13(1):323-335.

[16] Onder S, Bilgen S. A multi-objective differential evolution algorithm based on oppositional teaching-learning harmony search[J]. Journal of Intelligent & Fuzzy Systems, 2020, 39(5):6883-6901.

[17] Mohanraj P, Vengatesan G, Kalivaradhan SK. A multi-objective differential evolution algorithm with an adaptive population-based mutation for efficient energy aware task scheduling in a cloud environment[J]. Journal of Ambient Intelligence & Humanized Computing, 2021, 12(1):1105-1121.

[18] Ling J, Zhang J, Wu H, et al. Multi-objective differential evolution algorithm with cosine-based distribution for solving many-objective optimization problems[J]. International Journal of Computational Intelligence Systems, 2021, 14(1):504-520.

[19] Seera M, Basu M. Multi-objective differential evolution algorithm with quadratic approximation based parameter adaptation[J]. Neural Computing and Applications, 2021, 33(5):1845-1863.

[20] Aliaskari M, Hosseinian SH, Ziaei SM, et al. A multi-objective differential evolution algorithm for clustering cost optimization on mixed cloud fog environment[J]. Journal of Cluster Computing, 2021, 24(2):1075-1092.