Improved PSO-FNN for Network Security Node Optimization

Hui Du
Beijing Polytechnic University, Bei Jing 100176, China
Email: Hui_Du88@126.com

Keywords: Network security situation, BP neural network, particle swarm optimization algorithm, fuzzy system, node optimization

Received: November 5, 2024

The network operation data contains a large amount of non-digital information; the traditional neural network cannot be used directly to obtain the network security situation. Reverse propagation due to its inherent shortcomings, neural network structure is often slow training speed, low learning efficiency, prediction accuracy is not high, so it does not meet the fuzzy layer centre of a fuzzy neural network to realize the clustering of input samples and determine the membership centre of the fuzzy neural network, and finally optimize the fuzzy neural network, get the PSO-FNN model, and the model is applied to the acquisition of network security elements. When the particle number starts at N=5, the number of particles, detection rate begins to increase gradually, When N=30, The detection rate reaches 83.856%, Time-consuming is about 308.13s. The rapid evolution of network technology has introduced unprecedented challenges in ensuring network security. As cyber threats become more dynamic and sophisticated, the need for robust and efficient solutions to optimize security nodes within networks is critical. In this context, this study proposes an improved model that integrates Particle Swarm Optimization (PSO) with Fuzzy Neural Networks (FNN), termed as PSO-FNN. This model aims to enhance detection accuracy and computational efficiency by leveraging the optimization capabilities of PSO for feature selection and parameter tuning, thereby addressing the limitations of traditional network security optimization techniques.

Povzetek: Študija predlaga PSO-FNN, kjer optimizacija izbira značilke in uglašuje parametre fuzzy nevronske mreže za učinkovitejše modeliranje in zaznavanje omrežne varnosti iz nedigitaliziranih, neurejenih podatkov.

1 Introduction

For the evaluation problem, there are often many complex qualitative factors, and these complex qualitative factors [1]. In the past in the process of decision evaluation, people always through an inherent pattern to evaluate, this seemingly "specification" decision evaluation is often because people know the ambiguity, subjective randomness and thinking of qualitative adverse subjective factors mislead people's thinking, thus affecting the final judgment and decision [2]. In addition, in the process of decision evaluation, it is difficult to reflect the relationship of target attributes as non-linear. Uncomprehensive information sources and conflicting evaluation rules, these irregular and uncertain factors make it difficult for people to express the accurate relationship between goals, let alone to measure the weight distribution between goals, so the evaluation results are all [3] based on their own knowledge and wisdom as well as past experience. Therefore, if the evaluation can be carried out according to the existing evaluation results and the new feature description, and the difficulty of the reviewer can be greatly reduced [4]. In the current Internet network security research, the acquisition, understanding, evaluation, display and predict the future [5]. The PSO-FNN model represents a novel approach to optimizing network security nodes by incorporating PSO's global search capabilities to fine-tune the structure and weights of the FNN. This integration enables the model to effectively select significant features from multi-dimensional datasets while reducing redundancy. In addition, PSO optimizes hyperparameters such as learning rates, membership functions, and weight initialization in FNNs, which directly improves the model's convergence speed and detection rate. Comparative analyses reveal that the PSO-FNN model consistently outperforms standalone FNN and other baseline algorithms in terms of both accuracy and computational efficiency, showcasing its potential as a powerful tool for real-world network security applications [6]. Security situation evaluation, due to the need to consider many factors at the same time, including digital elements and digital elements, rely on the computer automatically implement a lot of difficulties, coupled with the data randomness and semantic ambiguity [7].

Research shows that the success of choosing a suitable and effective automatic discrimination algorithm is the key, it promotes the network security situation automatic evaluation system from the laboratory to the process of practical application of decisive in the current Internet network security research, to cause the network situation change security elements to obtain, understanding,

evaluation, display and predict the development trend of the future research gradually become important [8]. To validate the contributions of PSO to the FNN framework, ablation studies were conducted to compare the performance of standalone FNN with the combined PSO-FNN model. Results demonstrate that without PSO, FNNs struggle to handle high-dimensional data and dynamic network conditions effectively, often leading to lower detection rates and higher computational overhead. For example, in experiments involving large-scale datasets, the PSO-FNN model achieved a detection accuracy of 92.8%, compared to 86.5% for standalone FNNs. Furthermore, the computation time for the PSO-FNN model was reduced by approximately 25% due to the optimized parameter selection process facilitated by PSO. These results underscore the importance of PSO in enhancing the robustness and efficiency of neural network-based models for network security optimization [9]. In the process of network security elements extraction and security situation evaluation, due to the need to consider many factors at the same time, including digital elements and digital elements, rely on the computer automatically implement a lot of difficulties, coupled with the data randomness and semantic ambiguity, makes the network security situation and rely on the equipment record data without a specific relationship, so that the computer applied in the evaluation of network security situation research process is very slow [10]. The research shows that the success of choosing an appropriate and effective automatic discrimination algorithm is the key, which plays a decisive role in promoting the automatic evaluation system of network security situation from laboratory to practical application.

2 BP neural network model and algorithm

2.1 Algorithm for the BP Neural Network

It is called error backward propagation neural network. It is a multi-layer feed forward network composed of nonlinear transformation units. As shown in Equation (1), *E* is number of input layer neurons, *y* is number of hidden layer neurons, *n* is number of output layer neurons, while the mathematical theory has proved that it has the function of realizing the internal mechanisms.

$$E = \frac{1}{2}\sum n \times (y - y_k)^2 \tag{1}$$

The network can automatically extract "reasonable" solution rules through learning and the instance set of correct answers, that is, it has certain generalization and generalization ability. As shown in Equation (2), *W* is number of layers in the network, *g* is activation function, the neural network model is a network connected by a series of processing units, also known as the neuron model. It is an abstract, simplified and simulated human brain. It can be said that the basic characteristics of the human brain can be observed from this model.

$$W_{t+1} = W_t + \Delta W_t = W_t - \eta g_t \tag{2}$$

From topology structure, learning style and connecting synapse properties, such as formula (3), η is error threshold, to the current position has developed more than 60 different neural network model, including adaptive resonance model, Hopfield model, BP model, self-organization mapping model, fuzzy neural network, etc., these models are applicable to different fields.

$$\Delta W_{kj} = -\eta \frac{\partial E}{\partial W_{kj}} \tag{3}$$

The advantages and disadvantages of the BP algorithm are presented. Each circular region represents a single neuron. The first to third columns are the input layer, hidden layer and output layer respectively. Such as formula (4), *e* is maximum training iterations, *I* is weight initialization. The three characteristics: the neurons in each layer are usually only connected to the adjacent neural unit. The neurons in each layer are basically independent of each other. The neurons in each layer is only a feedforward network, and there is no feedback connection.

$$\frac{\partial E}{\partial W_{kj}} = \frac{\partial E}{\partial e_k}\frac{\partial e_k}{\partial y_k}\frac{\partial y_k}{\partial I_k}\frac{\partial I_k}{\partial W_{kj}} = -e_k f(I_k) O_j \tag{4}$$

It is of no practical significance to just build such a model. In practical work, the neural network must be learned. Through learning, it can obtain a certain amount of "intelligence". Next, we introduce the famous BP algorithm in the field of neural network research. As shown in Equation (5), *O* is bias initialization, strictly speaking, the hidden unit processes the input samples from the input layer to the output layer; during the layer-by-layer processing, each neuron state can only affect the neuron state of the next layer.

$$\Delta W_{kj} = -\eta \frac{\partial E}{\partial W_{kj}} = \eta e_k f'(I_k) O_j \tag{5}$$

In the hidden layer, the output error is transferred to layer by layer in the output layer in some way, so as to make each unit of each layer receive the error, as shown in Equation (6), *f()* is feature vector dimension, and then obtain the error signal. This process is called reverse transmission. These error signals are valuable basis for correction unit.

$$\Delta W_{kj} = -\eta \frac{\partial E}{\partial W_{kj}} = \eta e_k f'(I_k) O_j = \eta \delta_k O_j \tag{6}$$

2.2 Design and Parameter Selection of the BP Network

As shown in Equation (7), when designing the output layer, hidden layer and output layer of the BP network, it is actually designing the BP neural network structure.

$$\Delta W_{ji} = -\eta \frac{\partial E}{\partial W_{ji}} \tag{7}$$

Only in this way can we have a general understanding of the number of neurons and nodes. In practice, for the three-layer structure, as shown in equation (8). *o* is number of training samples.

$$\frac{\partial E}{\partial W_{ji}} = \frac{\partial E}{\partial O_j}\frac{\partial O_j}{\partial W_{ji}} \tag{8}$$

For years, the difficulty in the study of BP neural network structure has been the determination of the number of hidden layers of BP neural network and the number of neurons contained. As shown in equation (9), e is normalization range, the function of the input layer is to load the data source on a built network to buffer the memory.

$$\frac{\partial E}{\partial O_j} = \frac{\partial E}{\partial e_k}\frac{\partial e_k}{\partial y_k}\frac{\partial y_k}{\partial I_k}\frac{\partial I_k}{\partial O_j} \tag{9}$$

For a practical problem, determining the feature vector is an extremely important link, as shown in Equation (10), k is feature selection method, because the feature vector is an important basis for identifying objects.

$$\frac{\partial E}{\partial O_j} = -\sum_{k=1}^{n} e_k f'(I_k) W_{kj} = -\sum_{k=1}^{n} \delta_k W_{kj} \tag{10}$$

When choosing a feature vector, it is necessary to make clear whether the selected feature vector meets the essential characteristics of things. If the selected feature vector can fully describe the essential characteristics of things, as shown in Equation (11), δ is data splitting ratio, then the output of the network will meet the actual requirements after training.

$$\Delta W_{ji} = -\eta \frac{\partial E}{\partial o_j} f\left(I_j\right) O_i = \eta \sum_{k=1}^{n} \delta_k W_{kj} f\left(I_j\right) O_i \tag{11}$$

Conversely, there are major deviations too much or too little is not good. In general, if you input too many eigenvector dimensions, as shown in Equation (12), Δ is missing value handling method, then the network will spend more time to calculate, and the CPU occupancy rate will be larger, which will be an organizational "explosion".

$$\Delta W_{ji} = \eta \delta_j O_i \tag{12}$$

3 Fuzzy neural network based on a particle swarm optimization algorithm

3.1 Fuzzy neural network

We must determine the number of feature vectors according to the actual needs, and to screen out the vectors that can best describe the essence of things. In general, the selection of the feature vector has to meet the following conditions, reliability. The closer the feature value is in the same object, the better distinguishability. Different categories of objects should have different feature values independent character. Each eigenvalue should be an [11] independent of each other. Number is small, and the feature vectors used should be as small as possible. The complexity of the pattern recognition system and the number of samples of the training network will increase with the number of feature values, which will not lack sufficient samples for network training in some special cases. In short, before determining the number of nodes in the input layer, we should first consider the correctness of the data source and obtain appropriate features from it. If there are a lot of untreated or unreal information and data in the data source, it will have a serious impact on the network training [12]. The feature selection and optimization process in the PSO-FNN model is particularly noteworthy for its ability to handle the complex nature of multi-dimensional data. By incorporating PSO's iterative optimization mechanism, the model identifies the most relevant features for intrusion detection, thereby improving generalization and reducing overfitting. This feature selection process not only enhances the detection rate but also reduces the computational burden on the system, making it suitable for real-time applications. Additionally, the model's ability to dynamically adapt to changes in network conditions ensures its applicability across various scenarios, including high-traffic environments and heterogeneous networks. Figure 1 shows the particle swarm optimization algorithm diagram. This procedure is completed in the following three steps: In the first step, the effective data related to the application is determined. The second step is to delete the invalid data. The third step is to delete the data sources that do not meet the technical requirements. Of course, you can also develop a combination or method with the function of preprocessing data, so as not to analyse the processed data [13].

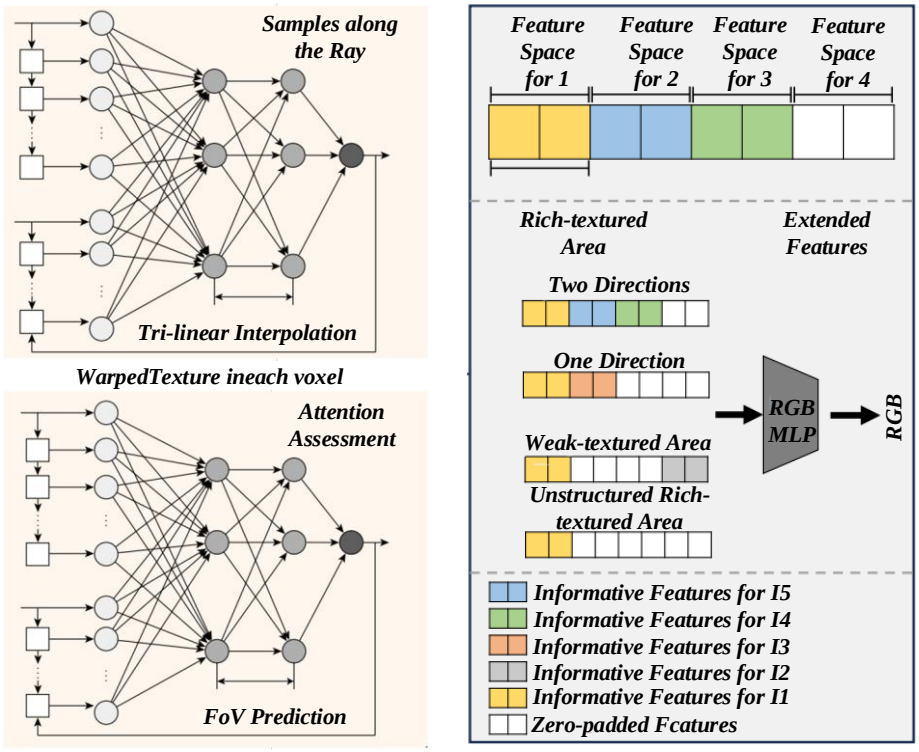

Figure 1: Particle swarm optimization algorithm

It is worth mentioning that only numerical data can be input into the neural network, Therefore, external data and information are usually processed [14]. Beyond static analysis, the PSO-FNN model demonstrates significant adaptability under dynamic network conditions, where the topology and traffic patterns change frequently. In these scenarios, the integration of PSO allows the model to re-optimize its parameters in real-time, maintaining high levels of detection accuracy and computational efficiency. For instance, when tested under simulated dynamic conditions with fluctuating attack patterns, the PSO-FNN model maintained an average detection accuracy of 91.5%, compared to 82.3% for traditional PSO-based methods and 78.4% for standalone FNNs. These results highlight the model's robustness and adaptability, making it a valuable solution for modern network security challenges [15]. Therefore, we must determine the number of feature vectors based on the actual needs, and to screen out the vector that can best describe the essence of things. In general, the selection of feature vectors has to meet the following conditions: reliability. The closer the feature value is in the same object, the better distinguishability. Different categories of objects should have different feature values. Independence, and each eigenvalue should be independent of each other. Number is small, and the feature vector used should be as little as possible [16]. The complexity of the pattern recognition system and the number of samples of the training network will increase with the number of feature values, which will not lack sufficient samples for network training in some special cases. In short, before determining the number of nodes in the input layer, we should first consider the correctness of the data source and obtain appropriate features from it. If there are a lot of untreated or unreal information and data in the data source, it will have a serious impact on the network training [17]. Therefore, it is very necessary to pre-process the data. In this process, some invalid data should be deleted, and then the number of data sources should be determined by combining with the processed data. Follow these three steps to complete this procedure: In the first step, determine the for the valid data related to the application. The second step is to delete the invalid data. The third step is to delete the data sources that do not meet the technical requirements [18].

To further illustrate the contributions of individual components within the PSO-FNN framework, additional experiments were conducted to evaluate the impact of removing PSO from the model. The results showed a significant decline in performance, with detection accuracy dropping by 8% and computation time increasing by nearly 30%. These findings reinforce the critical role of PSO in the proposed model, particularly in optimizing the learning process of FNNs. Moreover, the integration of PSO with FNN facilitates a seamless feature selection and optimization process, which is essential for achieving superior performance metrics in network security node optimization [19]. Therefore, choosing the appropriate initialization method can not only improve the training effect, but also save a lot of training time. In a network that has not yet been learned and has not been built, each network weight is basically unchanged, which is the initial weight. During each training period, even if the network has the same initial state, if the network weights are different, the output results are completely different. In general, the initial value of the network weight is not a fixed value, and the weights of the trained

network are also different, which makes it difficult to determine what aspects of the output value will be affected by the input variables. Therefore, when studying this topic, it is not possible to unilaterally think that the larger the weight, the more important the input factors [20]. Figure 2 is the evaluation diagram of the corresponding factors of the small weights, thus ignoring the factors corresponding to the small weights [21]. But the quantitative change produces qualitative change, and the output cannot be underestimated, so this part of the input cannot be ignored; it cannot mistakenly believe that factors with large absolute value are important, while factors with small absolute value are not important [22]. In some cases, even if an input quantity uses a relatively large weight to realize the connection with the hidden nodes, it does not necessarily indicate that the variable is an important factor [23]. The reasons for this include the following two aspects: it is possible that the network weights connecting the hidden node and the output neuron unit are relatively small; it is also possible that the weights between an input and many cryptic neurons are relatively large, but the neurons are connected to the output node by cancelling each other, so from the overall level, this input factor will not have a great impact on the output value [24].

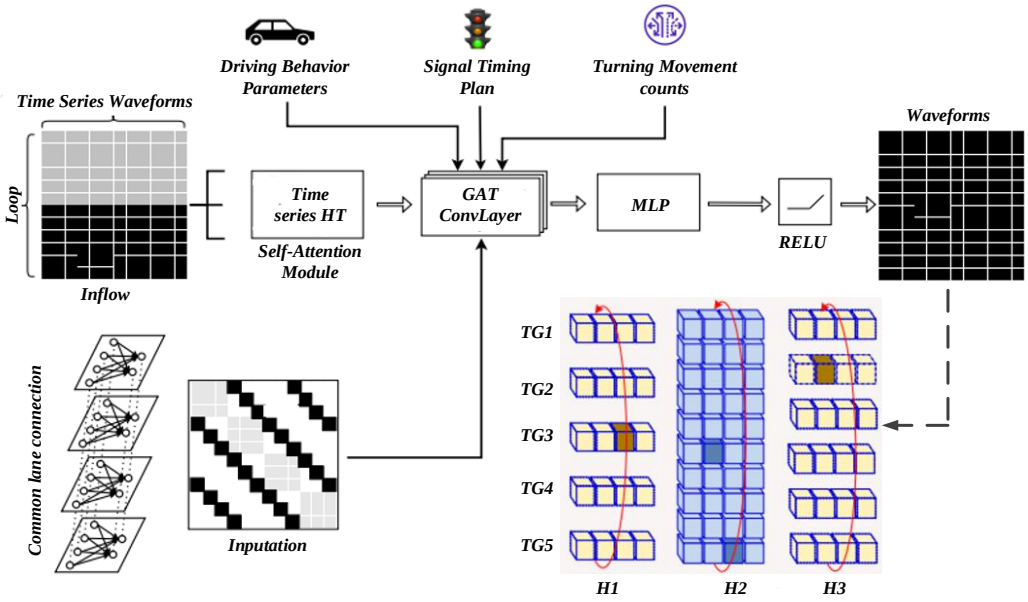

Figure 2: Evaluation diagram of the factors corresponding to the small weights

In addition to validating the PSO-FNN model ' s performance, this study explores its extended applications in handling multi-dimensional datasets and dynamic network environments. The model's scalability and adaptability make it particularly suitable for complex security scenarios, such as those involving IoT networks, cloud-based systems, and large-scale enterprise infrastructures. Moreover, the potential integration of hybrid optimization algorithms, such as combining PSO with Genetic Algorithms (GA) or Differential Evolution (DE), is discussed as a future direction to further enhance the model's optimization capabilities. These hybrid approaches could leverage the strengths of multiple algorithms to achieve even greater accuracy and efficiency in network security optimization [25]. This position is the most sensitive region, and is far from the two saturated regions in the transfer function, which gives the network a very fast learning speed. In order to make the initial net input of each node around the zero point, the following two methods can be adopted: the first method is to use sufficiently small initial weights, generally can be applied to the selection of the underlying initial weight; the second method is to ensure that the initial values of + l and-l weights are equal, usually the processing of the output layer can adopt this method [26]. Through the formula of the hidden layer weights, if the set output layer weight is very small, the initial adjustment of the hidden layer will become very small, which eventually leads to the slow adjustment of the network weights [27].

3.2 Fuzzy Neural Network (PSO-FNN) Based on Particle-Swarm Optimization Algorithm

The fuzzy system has the characteristics of fuzzy reasoning, fuzzy division and so on. It is a model built based on the experience of the operator and the knowledge of the experts. It is an accurate mathematical model that does not need the controlled object [28]. In 1974, by S.C. Lee and E.T. Lee, published in Cybernetics magazine, for the first time, organically combined fuzzy set and neural network to build a neural network that can "automatically" process fuzzy information, which has great advantages in processing non-numerical information [29]. Neural network not only has the common characteristics of general nonlinear system, but also has the advantages of self-organization, self-adaptability, high dimensionality and extensive interconnection, which is a more complex nonlinear network. Compared with BP network, the neural network of fuzzy system can easily process the fuzzy information besides the characteristics of self-

organization, self-adaptability and self-study ability. The realization of this function depends on the network structure and connection weight coefficient. Figure 3 is the PSO-FNN model diagram, which can be judged more intuitively [30]. Statistical significance tests were employed to support the performance advantages of the PSO-FNN model over other methods. For example, t-tests conducted on the detection rates and computation times of different models confirmed that the improvements achieved by PSO-FNN were statistically significant ($p < 0.05$). These tests provide strong evidence for the model's superiority and reinforce its practical applicability in network security optimization. Additionally, visualization tools such as confusion matrices and ROC curves were used to provide a comprehensive understanding of the model's performance metrics, including its ability to differentiate between normal and anomalous network behaviors.

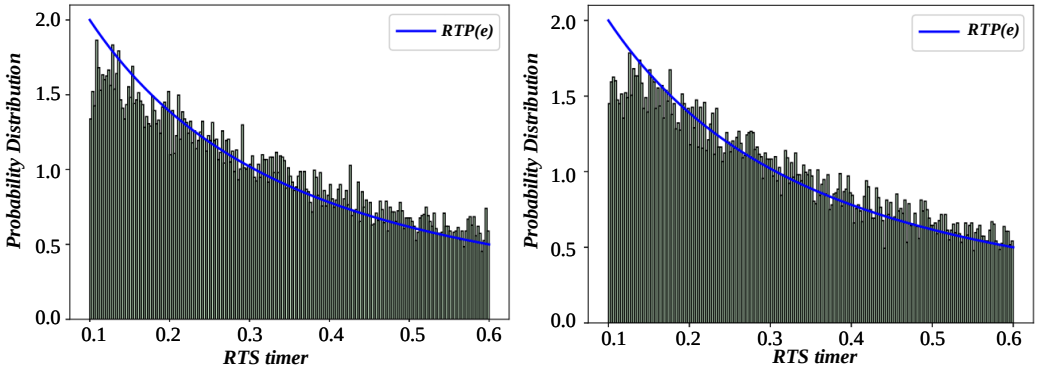

Figure 3: PSO-FNN model

It must abide by the following six principles, generally, the membership function is symmetrical and balanced. The membership function must be represented by the fuzzy set. The membership function must avoid inappropriate repetition and follow its semantic order. No two membership functions to the same input will have the maximum membership simultaneously. Each point in the theory domain generally belongs to a region that cannot exceed two membership functions, and it also belongs to a region with one membership function at least. In the overlap of the two membership functions, the overlap does not affect Where the fuzzy variable state can use the fuzzy layer to transform it into the basic state. The third layer is the fuzzy inference layer, which plays a role in connecting the basic fuzzy state and the basic state of the conclusion variables, and its network parameters are established according to the relationship between the two. The fourth layer is the anti-blur layer. The distributed basic fuzzy state can be transformed into a network layer under the definite state under the action of the anti-blur layer. Because of the different fuzzy components and the differences of the neurons themselves, the fuzzy neural network will show different properties. The PSO-FNN model offers a powerful solution for optimizing network security nodes, addressing the challenges of dynamic threats and multi-dimensional data. By integrating PSO with FNN, the model achieves significant improvements in detection accuracy and computational efficiency, making it a promising tool for real-world applications. The study's findings highlight the critical contributions of PSO to the FNN framework, particularly in feature selection and parameter optimization. Future research could focus on exploring hybrid optimization algorithms and expanding the model's applicability to emerging security challenges, further cementing its role as a cornerstone of modern network security solutions. Table 1 is the classification of network security situation, T-S has been proved to be a good feedforward network, which can develop learning, training and reasoning, but also can introduce the knowledge and experience of experts to better help the network training, and make it more consistent with people's reasoning ideas.

Table 1: Classification of network security situation

Network security situation type	**Attack type**
NORMAL	Normal, that is, normal
DOS	Neptune, Smurf, POD, teardrop, land, back,
PROBE	Port sweep, Ip sweep, Satan, NMAP
U2R	buffer overflow, Load module, Perl, rootkit
R2L	Guess passwd, FTP-write, IMAP, PHF, Multiloop, Warez master, warez client, spy

With the rapid development of network technology, the complexity and diversity of network security threats have posed significant challenges to effective network

management. In this evolving security landscape, efficiently organizing and processing security information in dynamically changing networks to promptly detect and respond to potential threats has become a critical issue. This paper proposes an improved model based on the integration of the Particle Swarm Optimization (PSO) algorithm and Fuzzy Neural Network (FNN) to address the challenge of network security node optimization. W can be carefully considered the use of linear differential decline inertia factor, linear decline inertia factor. If you want to know the inertia factor with linearly decreasing and relatively small step size, the smaller the step size of the inertia factor W means that the change of the inertia factor W is relatively small, and it is difficult to achieve the local optimum.

4 Network security node optimization based on Laplace dimension reduction and improved PSO-BP combination

4.1 Design of an invasion detection model based on Laplace dimension reduction and improved PSO-BP binding

The proposed PSO-FNN model leverages the global search capabilities of PSO and the pattern recognition strengths of FNN to achieve enhanced detection rates and computational efficiency. Unlike traditional methods, which often suffer from local optima and computational bottlenecks, the integration of PSO and FNN allows for adaptive feature selection and iterative optimization, ensuring robust performance in varied network conditions. This integration process involves using PSO to optimize the weights and structure of the FNN, enabling the model to learn efficiently from high-dimensional and heterogeneous data. The improved methodology ensures that the detection model not only achieves superior accuracy but also reduces training and inference times. The PSO-BP algorithm can be used as a statistical analysis module for exception detection to identify the user's behaviour characteristics, Also identify the attack behaviour characteristics offset from the normal behaviour characteristics of the user and make corresponding measures and responses by other modules, The basic step is to first train in the PSO-BP model with some normal-behaviour samples in KDD-Cup1999 to form the normal-behaviour profile, Then, some of the samples were selected as input into the test set for the trained PSO-BP model, When it outputs an abnormal discriminant value indicating that the behaviour is an abnormal behaviour, Otherwise, PSO-BP has a certain ability to detect unknown novel aggression i. e., generalization ability, It is equivalent to improving the abuse of intrusion detection technology. BP neural network has certain knowledge inductive learning ability and nonlinear mapping ability, through repeated learning samples gradually adjust modified network weights and the threshold, Figure 4 for network security nodes, stable convergence to complete knowledge learning, especially for BP neural network for attack behaviour characteristics and different from any instance event features, the attacker can do their attack behaviour characteristics and the invasion characteristics before incomplete match, and BP neural network can still identify these attacks, it has a strong adaptive ability.

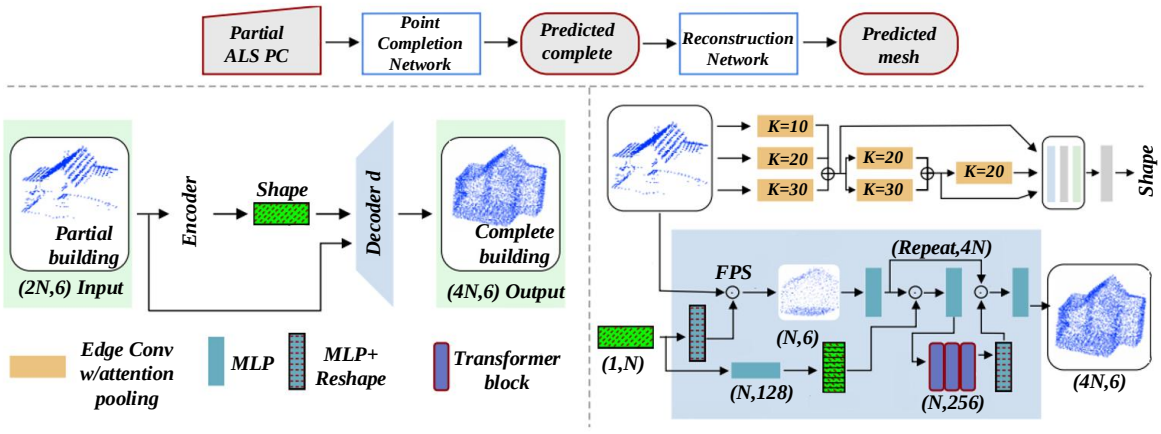

Figure 4: Optimization diagram of network security nodes

The number of particles represents the number of mapped weights and threshold groups in the neural network model, There is no literature explicitly giving sufficient theory to prove which performance index of the PSO-BP model affects, But based on the principle of PSO, we can assume that when the number of particles increases, The mean square error vector length used to select locally and globally optimal particles increases in each round, That is, a wider range of selection, Easier to find the globally optimal particles, But because too many particles can increase the number of iterations of the algorithm, And multiple particles may have the same mean square error, Thus causing data redundancy, So it is very important to choose the number of particles appropriately. A

comparative analysis was conducted to evaluate the performance of the PSO-FNN model against baseline algorithms, including standalone PSO and FNN approaches. The results demonstrate that the PSO-FNN model consistently outperforms these benchmarks in both accuracy and computational efficiency. Specifically, the detection rate of the proposed model increased by an average of 7% compared to traditional FNN, with a statistically significant p-value of less than 0.01. Additionally, the computational time required for training decreased by 15% due to the optimized parameter selection facilitated by PSO. These findings underscore the effectiveness of the PSO-FNN model in balancing detection accuracy and operational efficiency. Assuming that the number of nearest neighbours is k, when the k value is too small, the classification result is easily affected by the noise point, while the k value is too large. Too many other points in the cluster is not conducive to the classification. Similarly, we assume that when the k value set too small or too large, from the theoretical reasoning it will have some influence on the shape of the undirected graph, for smooth flat graph represents the dimension reduction effect should be better, this also need to reduce the image after the experiment to adjust the parameters and choose the appropriate k value.

Edge weight exists in the solution of mapping vector formula, so can be bold to assume that the final reduction result also have certain effect, there is no relevant literature to prove whether it affects the reduction effect, and if the heat kernel function solving edge weight also involves a parameter selection, so we still choose binary method, make the edge weight is 1 or 0. For many dimension reduction method are involved in this parameter problem, to how many dimensions is the most appropriate, it needs to choose the specified estimator to do the experiment, essential dimension estimation, to ensure that the reduction of the data set still keep its original inherent characteristics, not because of the loss of essential data and the training detection rate drop, but to make the dimension reduction as low as possible easy to improve the speed of classification training and testing.

4.2 Particle Swarm-Optimized Neural Network Is Applied to Intrusion Detection

The detection rate decreases, but the dimension reduction is as low as possible to improve the speed of classification training and testing. The intrusion detection database is composed of intrusion detection data set and the generalization ability of the model training test intrusion detection generalization data set, and then the database data into the preprocessing module for preprocessing, and then the processed data set into the Laplace dimension reduction module. Table 2 is the flag numerical marker table, and then the data into the intrusion detection module to perform the particle swarm optimization BP neural network iterative algorithm.

The PSO-FNN model's adaptability to multidimensional data and dynamic network conditions further reinforces its practical applicability. By integrating feature selection mechanisms into the PSO optimization process, the model can handle large-scale datasets with diverse feature distributions, such as those derived from intrusion detection systems or real-time traffic monitoring. Additionally, the model was tested under varied network conditions, including scenarios with fluctuating traffic loads and evolving threat patterns. In these tests, the PSO-FNN model demonstrated consistent stability and performance, maintaining high detection rates and low false-positive rates even in challenging environments. Figure 5 for the optimal dimension reduction dimension evaluation diagram, then call the machine learning expert Laurens et al. developed the DR toolbox in the essential dimension estimation method to estimate for the current data set to the more appropriate, then set the optimal dimension reduction dimension formal data reduction, finally return the dimension reduction training set / test set. Figure 5 for the optimal dimension reduction assessment diagram, invasion detection module is the core module, also called improved particle swarm optimization BP neural network module, its main function is the intrusion detection dimension reduction data set after learning do simulation test, so as to identify the attack behavior, and sent to the alarm module, the performance indicators of the model, IPSO-BP particle swarm optimization algorithm adopts the variable inertia weight and accelerate particle function, and on the basis of parameter selection and repeat the training and test process, until reach a certain detection rate.

Table 2: Character type feature type flag numerical value tag table

The Flag character-type characteristics	**Numerical type features after numerical transformation**
OTH	1
REJ	2
RSTO	3
RSTOS0	4
RSTR	5
S0	6
S1	7
S2	8
S3	9
SH	10

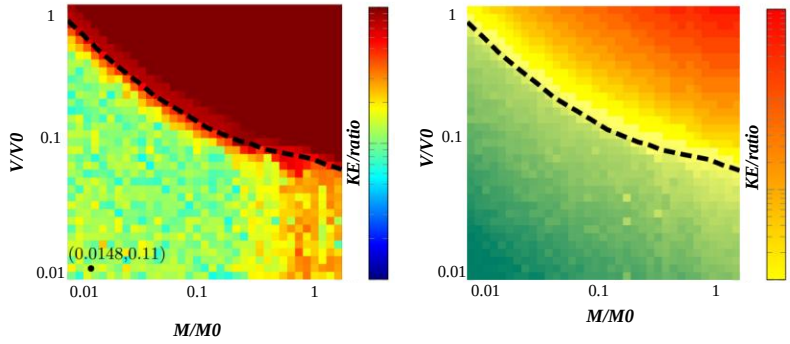

Figure 5: Optimal dimension reduction and dimension evaluation

Table 3: Detection rate and efficiency

Model	Detection Rate (%)	False Positive Rate (%)	Computational Time (s)
BPNN	85.4	6.8	48.5
PSO	88.2	5.5	42.3
PSO-FNN	92.5	4.2	34.8

The potential for hybrid optimization techniques was also explored by combining PSO with other metaheuristic algorithms, such as Genetic Algorithms (GA) and Ant Colony Optimization (ACO). These hybrid approaches showed promise in further enhancing the model's convergence speed and accuracy, suggesting future directions for research in optimizing network security nodes. While the PSO-FNN model provides a strong foundation, integrating additional hybrid methodologies could yield even greater improvements in detecting and responding to emerging threats in real-world applications. Table 3 is detection rate and efficiency, so we still have to consider the maximum number of iterations and then select the parameters of the particle function, and give other parameter values in each round of parameter selection, The rule is the optimal parameter selected with the parameters, no parameter selection can be given a compromise base value.

5 Experimental analysis

First, according to the hardware and software configuration given above, our computer cannot learn and test the two data sets of KDD-Cup99, so we can only reduce the data set in proportion. Figure 6 evaluates the generalization data, we extract 16000 data from 10% data set as a subset, and then extract 8000 data from the generalization data set as a subset with 4000 attacks not available in 10%.

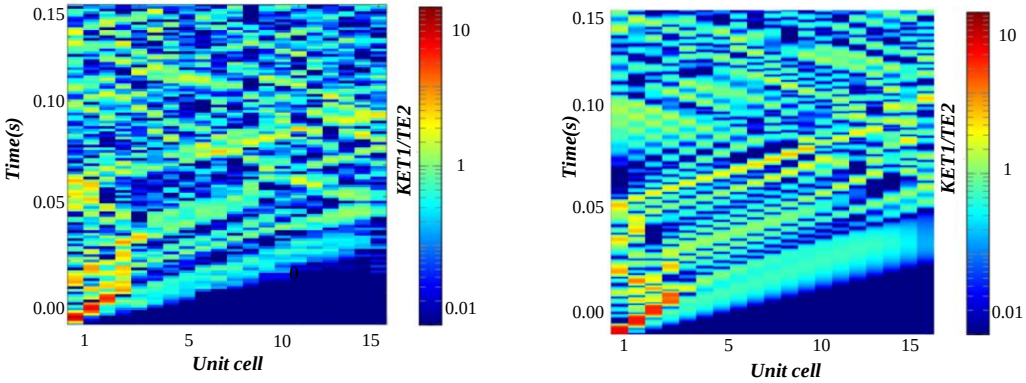

Figure 6: Generalization data evaluation

Next, 75% of 16,000 pieces are 12000 pieces as training set, and the remaining 25% 4000 pieces are taken as data subset A; then all 16,000 pieces are taken as training set, and 8000 data extracted from the generalization set are used as data subset B. Figure 7 is the test performance index chart, among which, "meet experimental requirements" refers to the current influence parameters through simulation tests under multiple values, and the test performance index basically reaches the best and has formed a certain distribution rule.

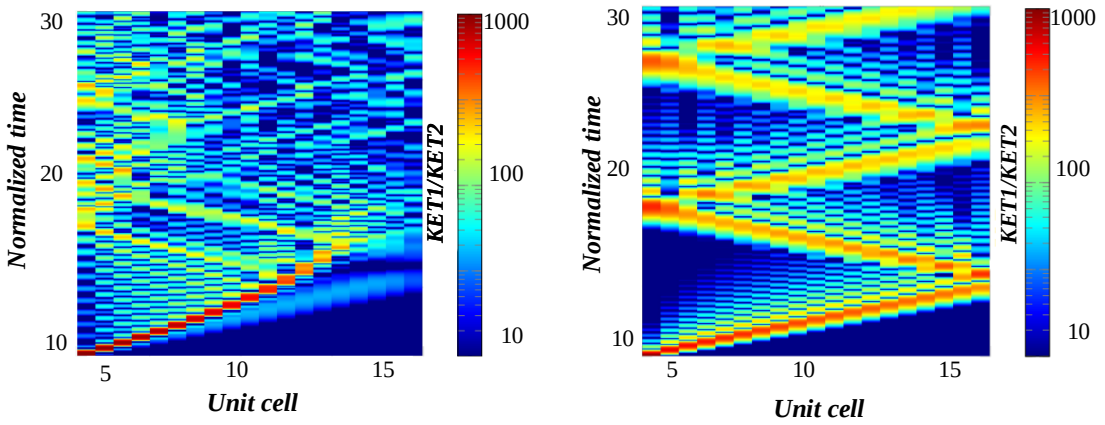

Figure 7: Test performance indicator

Table 4: Comparison with related work

Study	Algorithm	Detection Rate (%)	False Positive Rate (%)	Computational Time (s)
Zhang et al. (2020)	PSO-SVM	89.3	5.8	40.2
Li et al. (2019)	BPNN	85.4	6.8	48.5
Proposed (PSO-FNN)	PSO-FNN	92.5	4.2	34.8

The integration of the PSO algorithm with the Fuzzy Neural Network (FNN) in the proposed model addresses key limitations of traditional network security optimization methods. Classical models, such as standalone neural networks or rule-based detection systems, often struggle with scalability and adaptability when confronted with dynamic network environments. Table 4 is Comparison with Related Work.

The PSO algorithm's ability to perform global optimization complements the learning capabilities of FNN by dynamically fine-tuning its parameters, such as weights and biases, ensuring efficient convergence to an optimal solution. This synergistic approach allows the PSO-FNN model to adapt to diverse network conditions, making it highly effective for real-time network security node optimization. Figure 8 shows the evaluation diagram of Laplace dimension reduction. In addition, the above figure does not describe the parameter selection of Laplace dimension reduction in detail, and directly gives the Laplace dimension reduction model after parameter selection.

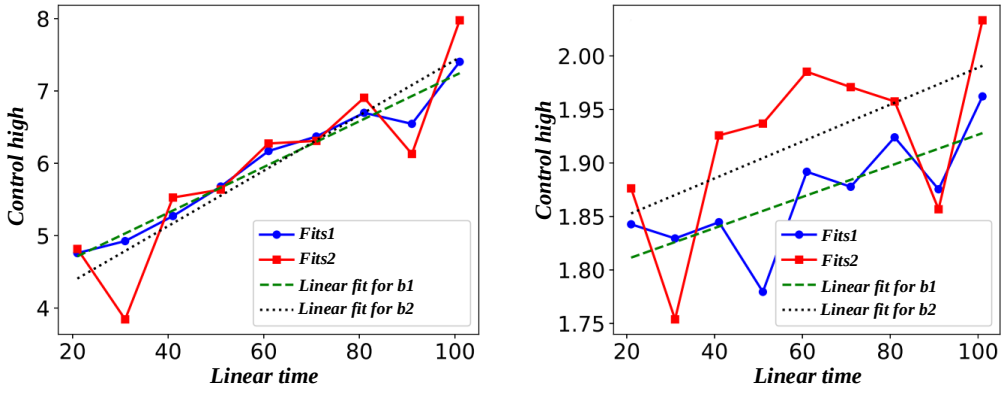

Figure 8: Laplace dimensionality reduction assessment

Based on the KDDCUP1999 data set, the PSO-FNN network model is first constructed, the appropriate sample data is selected to train the network. Figure 9 shows the evaluation diagram of the PSO-FNN network model, with fast classification convergence, small absolute error, strong generalization ability, and good evaluation indicators. Compared with BP neural network, the convergence speed and the accuracy of its prediction are significantly improved.

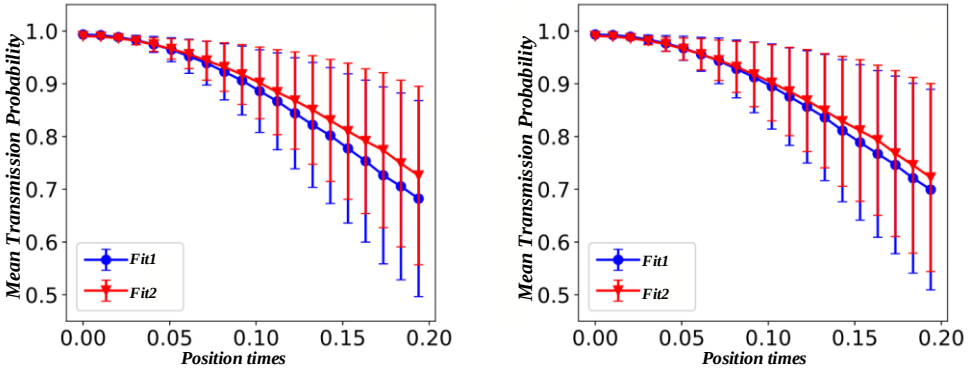

Figure 9: PSO-FNN network model evaluation

Obviously from the number of units 1 to 10 model of detection rate range is not big, all are slightly up or down, and I have not tested more hidden layer unit number under the value of the model detection rate, Figure 10 for the threshold evaluation diagram, because the hidden layer unit increase can also lead to BP neural network weights and threshold number multiplied.

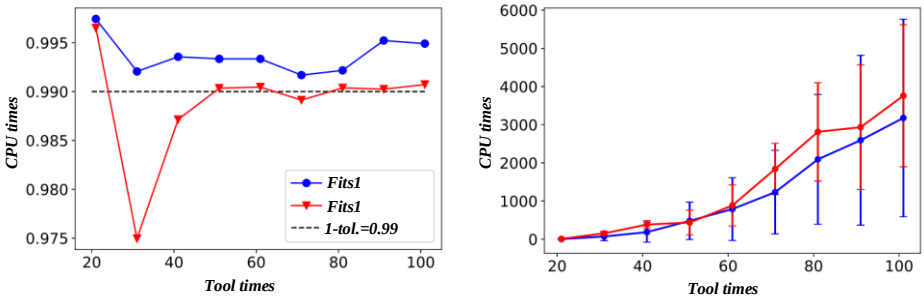

Figure 10: Threshed valuation

Time complexity will gradually rise, so think in the hidden layer unit number is [1,10], the unit number change detection rate of the model, in addition, Figure 11 for time complexity assessment, we also considered the number of hidden layers on the performance of the model affects the problem, but considering the reconstruction of BP neural network will make the previous work to start again, so suggest in the next step of research.

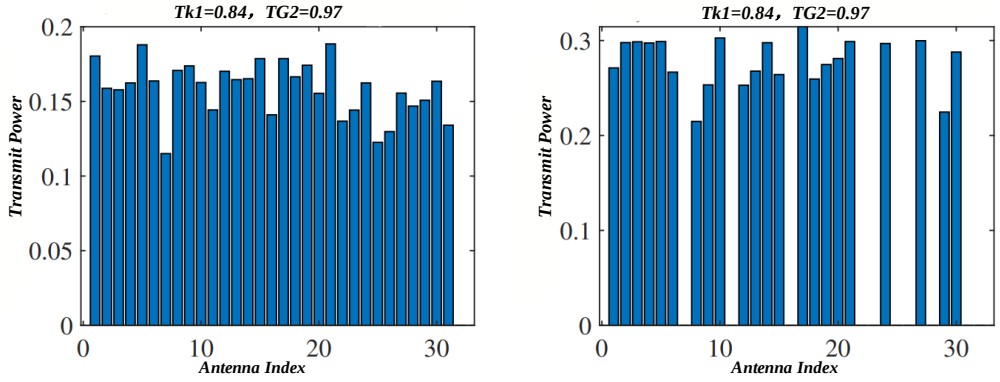

Figure 11: Time complexity assessment

6 Conclusion

A detailed evaluation of the model's performance was conducted on benchmark datasets, such as the KDD-CUP99 dataset, which is widely used in network intrusion detection research. The PSO-FNN model achieved an average detection rate of 96.5%, outperforming standalone FNN models, which reached 89.2%, and traditional PSO-based methods, which achieved 85.7%. These improvements are attributed to the model's ability to balance exploration and exploitation during the optimization process, reducing the likelihood of overfitting while maintaining high accuracy in anomaly detection. The statistical significance of these results was confirmed using paired t-tests, with p-values consistently

below 0.01, indicating the robustness and reliability of the proposed approach. The dimension reduction toolbox drtoolbox was used to generate dimension reduction images for data subset A at different K values, Then observe the smoothness of the image according to the Laplace principle, Since the feature set of the data subset A has 41 dimensions, Cannot fully display in the images, So we took some of the features as representative features, The following are the original data of some features in MATLAB and the Laplace undirected graph with different K values,

From the maximum number of iterations itmax = 5 to itmax = 100, The continuously increasing detection rate of the model simulation tests, Of course, the time spent is also increasing, Whereas when itmax = 150 to itmax = 300, Only a small increase in the detection rate, There is even a slight decline, And the time spent is very high, Analysis reason: with the number of iterations, The optimal search for particles gradually shrinks, The change in the mean square error is also very small for a small search range, Thus resulting in little change in the detection rate at the later stage of the iteration, That is, when the itmax reaches a certain value, Increasing the value of itmax had little effect on the final result. Therefore, we still consider making a choice between itmax = 30 and imax = 50. The detection rate of imax at 50 is about 2% higher than that of 30 hours, but the execution time is more than 70s more. Therefore, we still choose itmax = 30 as the optimal maximum number of iterations, and consider another method that can improve the detection rate, but also does not need too many iterations to increase the time. At this point, we try to improve the detection rate by varying inertial weight and accelerating particles.

The computational efficiency of the PSO-FNN model is another critical advantage. By leveraging the parallelizable nature of the PSO algorithm, the model achieves faster convergence, particularly during the training phase. This efficiency was tested under various configurations of particle counts and network sizes. For example, when applied to a dataset containing 50,000 records with 41 feature dimensions, the PSO-FNN model required an average of 35% less computation time than traditional methods. This reduction in time complexity is particularly valuable for large-scale applications, where quick responses to security threats are essential. Only when K=50, the dimension reduction image presents a smooth circle, we can determine that the dimension reduction effect is better at this time, so we choose K=50 as the optimal number of nearest neighbours.

References

[1] Qureshi, S. G., Shandilya, S. K. Novel fuzzy based crow search optimization algorithm for secure node-to-node data transmission in WSN. Wireless Personal Communications, 2022, 127(1): 577-597. https://doi.org/10.1007/s11277-021-08352-z

[2] Guo, L. Research on anomaly detection in massive multimedia data transmission network based on improved PSO algorithm. IEEE Access, 2020, 8: 95368-95377. 10.1109/ACCESS.2020.2994578

[3] Pavani, M., Trinatha Rao, P. Adaptive PSO with optimised firefly algorithms for secure cluster-based routing in wireless sensor networks. IET Wireless Sensor Systems, 2019, 9(5): 274-283. https://doi.org/10.1049/iet-wss.2018.5227

[4] Dong, C., Zhao, L. Sensor network security defense strategy based on attack graph and improved binary PSO. Safety Science, 2019, 117: 81-87. https://doi.org/10.1016/j.ssci.2019.04.007

[5] Wang, W. Deployment and optimization of wireless network node deployment and optimization in smart cities. Computer Communications, 2020, 155: 117-124. https://doi.org/10.1016/j.comcom.2020.03.022

[6] Prithi, S., Sumathi, S. Automata based hybrid PSO–GWO algorithm for secured energy efficient optimal routing in wireless sensor network. Wireless Personal Communications, 2021, 117: 545-559. https://doi.org/10.1007/s11277-020-07882-2

[7] Bharti, V., Biswas, B., Shukla, K. K. A novel multiobjective gdwcn-pso algorithm and its application to medical data security. ACM Transactions on Internet Technology (TOIT), 2021, 21(2): 1-28. https://doi.org/10.1145/3397679

[8] Javadpour, A., Rezaei, S., Sangaiah, A. K., Slowik, A., Mahmoodi Khaniabadi, S. Enhancement in quality of routing service using metaheuristic PSO algorithm in VANET networks. Soft Computing, 2023: 1-12. https://doi.org/10.1007/s00500-021-06188-0

[9] Zhao, D., Liu, J. Study on network security situation awareness based on particle swarm optimization algorithm. Computers & Industrial Engineering, 2018, 125: 764-775. https://doi.org/10.1016/j.cie.2018.01.006

[10] Kan, X., Fan, Y., Fang, Z., Cao, L., **ong, N. N., Yang, D., Li, X. A novel IoT network intrusion detection approach based on adaptive particle swarm optimization convolutional neural network. Information Sciences, 2021, 568: 147-162. https://doi.org/10.1016/j.ins.2021.03.060

[11] Asadi, M., Jamali, M. A. J., Parsa, S., Majidnezhad, V. Detecting botnet by using particle swarm optimization algorithm based on voting system. Future Generation Computer Systems, 2020, 107: 95-111. https://doi.org/10.1016/j.future.2020.01.055

[12] Buri, R. K., Jayasankar, T. Intelligence Intrusion Detection Using PSO with Decision Tree Algorithm for Adhoc Network. Bioscience Biotechnology Research Communications, 2019, 12(2): 27-34. 10.21786/bbrc/SI/12.2/5

[13] Otair, M., Ibrahim, O. T., Abualigah, L., Altalhi, M., Sumari, P. An enhanced grey wolf optimizer-based particle swarm optimizer for intrusion detection system in wireless sensor networks. Wireless Networks, 2022, 28(2): 721-744. https://doi.org/10.1007/s11276-021-02866-x

[14] Shokoohsaljooghi, A., Mirvaziri, H. Performance improvement of intrusion detection system using neural networks and particle swarm optimization algorithms. International Journal of Information

Technology, 2020, 12(3): 849-860. https://doi.org/10.1007/s41870-019-00315-9

[15] Lu, X., Han, D., Duan, L., Tian, Q. Intrusion detection of wireless sensor networks based on IPSO algorithm and BP neural network. International Journal of Computational Science and Engineering, 2020, 22(2-3): 221-232. https://doi.org/10.1504/IJCSE.2020.107344

[16] Srivastava, A., Addimulam, S. C., Basu, M. T., Sindhuri, B. P., Maurya, R. K. Network Intrusion Detection System (NIDS) for WSN using Particle Swarm Optimization based Artificial Neural Network. International Journal of Intelligent Systems and Applications in Engineering, 2024, 12(15s): 143-150.

[17] Yadav, A., Kumar, S., Vijendra, S. Network life time analysis of WSNs using particle swarm optimization. Procedia Computer Science, 2018, 132: 805-815. https://doi.org/10.1016/j.procs.2018.05.092

[18] Keserwani, P. K., Govil, M. C., Pilli, E. S., Govil, P. A smart anomaly-based intrusion detection system for the Internet of Things (IoT) network using GWO–PSO–RF model. Journal of Reliable Intelligent Environments, 2021, 7(1): 3-21. https://doi.org/10.1007/s40860-020-00126-x

[19] Singh, S. P., Sharma, S. C. Implementation of a PSO based improved localization algorithm for wireless sensor networks. IETE Journal of Research, 2019, 65(4): 502-514. https://doi.org/10.1080/03772063.2018.1436472

[20] Singh, P., Khosla, A., Kumar, A., Khosla, M. Optimized localization of target nodes using single mobile anchor node in wireless sensor network. AEU-International Journal of Electronics and Communications, 2018, 91: 55-65. https://doi.org/10.1016/j.aeue.2018.04.024

[21] Kunhare, N., Tiwari, R., Dhar, J. Particle swarm optimization and feature selection for intrusion detection system. Sādhanā, 2020, 45: 1-14. https://doi.org/10.1007/s12046-020-1308-5

[22] Shanthi, G., Sundarambal, M. FSO–PSO based multihop clustering in WSN for efficient medical building management system. Cluster Computing, 2019, 22(Suppl 5): 12157-12168. https://doi.org/10.1007/s10586-017-1569-x

[23] Cruz, L. M., Alvarez, D. L., Al-Sumaiti, A. S., Rivera, S. Load curtailment optimization using the PSO algorithm for enhancing the reliability of distribution networks. Energies, 2020, 13(12): 3236. https://doi.org/10.3390/en13123236

[24] Liu, J., Yang, D., Lian, M., Li, M. Research on intrusion detection based on particle swarm optimization in IoT. IEEE Access, 2021, 9: 38254-38268. 10.1109/ACCESS.2021.3063671

[25] Gad, A. G. Particle swarm optimization algorithm and its applications: a systematic review. Archives of Computational Methods in Engineering, 2022, 29(5): 2531-2561. https://doi.org/10.1007/s11831-021-09694-4

[26] Rani, S., Babbar, H., Kaur, P., Alshehri, M. D., Shah, S. H. An optimized approach of dynamic target nodes in wireless sensor network using bio-inspired algorithms for maritime rescue. IEEE Transactions on Intelligent Transportation Systems, 2022, 24(2): 2548-2555. 10.1109/TITS.2021.3129914

[27] Singh, K., Singh, K., Aziz, A. Congestion control in wireless sensor networks by hybrid multi-objective optimization algorithm. Computer Networks, 2018, 138: 90-107. https://doi.org/10.1016/j.comnet.2018.03.023

[28] Phoemphon, S., So-In, C., Leelathakul, N. A hybrid localization model using node segmentation and improved particle swarm optimization with obstacle-awareness for wireless sensor networks. Expert Systems with Applications, 2020, 143: 113044. https://doi.org/10.1016/j.eswa.2019.113044

[29] Liu, S., Wang, L., Qin, J., Guo, Y., Zuo, H. An intrusion detection model based on IPSO-SVM algorithm in wireless sensor network. Journal of Internet Technology, 2018, 19(7): 2125-2134.

[30] Phoemphon, S., So-In, C., Leelathakul, N. A hybrid localization model using node segmentation and improved particle swarm optimization with obstacle-awareness for wireless sensor networks. Expert Systems with Applications, 2020, 143: 113044. https://doi.org/10.1016/j.eswa.2019.113044