Intrusion Detection in Wireless Sensor Networks Based on IPSO-SVM Algorithm

Zhimin Lv[1,*] and Jun Wan[2]

[1]*Faculty of Information and Intelligent Manufacturing, Chongqing City Vocational College, Chongqing, 402160, China*
[2]*Iflytek Big Data Faculty, Chongqing City Vocational College, Chongqing, 402160, China*
E-mail: Zhimin_Lv23@outlook.com
[*]*Corresponding Author*

Received 12 October 2023; Accepted 18 January 2024

Abstract

To optimize node energy consumption and improve its security, this paper uses the DEEC algorithm to layer WSN and reduce the probability of channel information collision and uses the weighted probability of cluster head election to optimize node energy expenditure, so that WSN can obtain a longer lifecycle. Improved Particle Swarm Optimization-based Support Vector Machine (IPSO-SVM) algorithm is used for intrusion detection and experimental testing in WSN. The results showed that the IPSO-SVM algorithm exhibited good convergence, with a convergence step size of 5 steps, which converged earlier than the Support Vector Machine Algorithm based on Particle Swarm Optimization (PSO-SVM), which had a convergence step size of 10 steps. The IPSO-SVM algorithm performed best in WSN intrusion detection, with the highest detection rate of 96.20% in Probe attack data detection, which was 0.80% higher than the Support Vector Machine Algorithm based on Genetic Algorithm (GA-SVM). The PSO-SVM algorithm

Journal of Cyber Security and Mobility, Vol. 13_4, 803–822.
doi: 10.13052/jcsm2245-1439.13410

had the lowest detection rate of 95.20%. The IPSO-SVM algorithm had a minimum false positive rate of 1.54% in Dos attack data detection. In terms of average training time, the IPSO-SVM algorithm had a minimum average training time of 323.45 seconds. Compared to the Low Energy Adaptive Clustering Hierarchy (LEACH) algorithm, the Distributed Energy Efficient Clustering (DEEC) algorithm performs better, has less energy consumption, and retains more nodes. The method adopted in this study can make WSN have a longer life cycle and ensure its security.

Keywords: PSO algorithm, SVM algorithm, wireless sensor network, intrusion detection, DEEC algorithm.

1 Introduction

The application range of wireless sensor network (WSN) has been expanding and has been widely used in many fields [1–3]. WSN contains many randomly deployed sensor nodes in a large area. In WSN, the power supply of nodes is limited and irreplaceable. In this network, its life cycle is highly dependent on the life of sensor nodes. Excessive energy loss will easily lead to rapid shortening of the life cycle of WSN, resulting in premature paralysis of the network [4]. In addition, when WSN nodes are in a bad environment, they will face the danger of being destroyed and physically captured and will be vulnerable to attack, which will lead to the disclosure of important information such as network keys and cause large losses. Therefore, it is necessary to design relevant defense strategies to balance the energy expenditures of nodes, improve the security of their information transmission, make WSNs have a longer life cycle, and complete network intrusion detection. In the performance optimization of heterogeneous sensor networks, some scholars combined the Wolf pack algorithm and proposed the relevant clustering routing algorithm. By improving the Distributed Energy-Efficient Clustering (DEEC) algorithm, the path-fixing problem of the algorithm was solved. In relevant experimental tests, the application effect of the improved DEEC algorithm is good, making the network life longer, and the related energy expenditures have the characteristics of equalization [5]. To improve WSN security, reduce time consumption, and extend the life cycle, some scholars have achieved these goals through two-stage classification technology. In this method, adaptive support vector machine (SVM) classification is applied. In the experimental results, the superiority of this method is confirmed [6]. In this regard, the paper applies DEEC algorithm and SVM algorithm to the research of improving WSN security and balancing node energy consumption, to effectively detect network intrusion and make WSN have a longer life cycle.

2 Related Work

The process of WSN application brings great convenience to people's lives and production and promotes the development of related industries. However, there are certain security problems in the process of application development. Because the energy of the WSN sensor node is limited, its processing capacity is also limited, and it is often in unmanned areas and hostile environments, the network is vulnerable to various attacks. Therefore, it is important to extend the service life of WSN and improve network security. To optimize node performance and ensure data transmission security, Alghamdi et al. [7] proposed a data fusion method to detect malicious nodes by both signature sharing and false sharing. The results showed the feasibility of using the method. Behera et al. [8] established a relevant model based on corona nodes to extend the service time of WSN. Through this model, adjustments were made to relevant nodes to reduce energy expenditure. After verification, this method has certain feasibility. Faced with the security and energy consumption optimization issues of WSNs, Banerje et al. [9] used metaheuristic algorithms to improve the relevant paths under the influence of the ant colony algorithm, and improved particle swarm optimization algorithms to increase the coverage area. The effectiveness of these methods was verified in relevant tests. Amarasimha et al. [10] used the SVM algorithm to optimize related transmission data and reduce transmission energy to detect WSN node faults and reduce energy consumption. They also performed correlation detection on end nodes based on the speed at which they sent data. The experiment showed that the algorithm was effective.

Liang J et al. [11] introduced the DEEC algorithm and proposed a corresponding adaptive collaborative routing algorithm to extend the service life of WSNs and make them more stable. From the relevant simulation analysis, the application effect of this method was relatively good. Xu et al. [12] improved the DEEC algorithm for energy balance optimization to better reduce the energy consumption of nodes in WSN lifetime optimization problems and verified the effectiveness of this method in simulation experiments. Wei et al. [13] improved the SVM algorithm through the PSO algorithm to improve the classification performance of imbalanced datasets. After experiments, the classification results were good. Li et al. [14] constructed a relevant quality evaluation model by the SVM algorithm and optimized the parameters of this algorithm by using the PSO algorithm in the environmental study of livable cities. The experimental analysis showed that the model had a fast classification speed and good classification effect.

To sum up, the security and energy expenditures of WSNs are the focus of many scholars' research. In the energy expenditures research, the research on node energy balance is relatively small, scholars are paying more attention to global energy consumption optimization and communication efficiency, which may lead to insufficient research on node energy balance. Once a node runs out of energy, it will lead to a decrease in data transmission capacity or node death and affect the connectivity and coverage of the entire network. Therefore, to ensure the security of WSN, in the research on reducing the energy expenditures of WSN, the paper chooses the DEEC algorithm as one of the research methods from the perspective of node energy balance, considering the advantages of the DEEC algorithm in node energy expenditure processing. Considering the effectiveness of the PSO-SVM algorithm in classification detection, this paper takes this algorithm as a method of WSN intrusion detection. Because the PSO algorithm has a high probability of local extremum, it is improved to obtain an improved particle swarm optimization (IPSO) algorithm, thus obtaining the IPSO-SVM intrusion detection method.

3 WSN Intrusion Detection Based on DEEC Algorithm and IPSO-SVM Algorithm

3.1 Application of DEEC Algorithm in WSN Hierarchical Processing

The progress of wireless communication promotes the continuous development of relevant WSN technology, which connects the physical world with information technology and is used in many fields such as logistics and healthcare. In the process of development, the security issues of this technology gradually emerged. the energy of WSN sensor nodes is limited, their processing capacity is also limited, and because they are often in no-man's land and hostile environment, the network is vulnerable to various attacks. In this regard, security mechanisms are needed to protect them. Traditional security mechanisms do not meet the needs of WSN sensor nodes and design a security mechanism that meets the characteristics of WSNs [15–17]. Before that, its nodes are first adjusted to improve energy utilization. For this, the paper uses the DEEC algorithm, which is one of the distributed

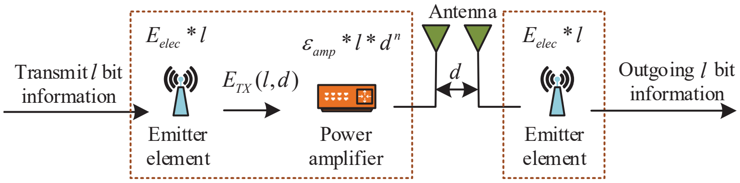


Figure 1 Energy consumption model of radio transceiver.

energy-efficient hierarchical algorithms, to equalize the energy expenditures by making each node become a cluster head in turn. This algorithm divides sensor nodes into different clusters and selects a node with sufficient energy as the cluster head. This can ensure that the distribution of various clusters in the network can be more uniform. This algorithm effectively reduces transmission power consumption and extends the lifespan of the entire network by first aggregating data within each cluster, then transmitting it to the cluster head, and finally to the base station. Before building the hierarchical network model, it is assumed that the number of nodes is N and they are evenly dispersed in the square area of $M * M$, which sends data to the base station from time to time. The base station is far away from the sensing area, and it will receive the data directly from the aggregated cluster heads. Since the network model to be built is two layers, the sensor nodes are also advanced and common. The energy of the latter node is set to E_0 and the energy of the former node is a times that of E_0. The percentage of advanced nodes is m, and the relevant formula is shown in formula (1).

$$E_t = N(1 - m)E_0 + Nm(1 + a)E_0 = N(1 + am)E_0 \tag{1}$$

In formula (1), WSN total energy is set as E_t, and E_t is a multiple of am for the planar network, which means that there are fewer am virtual nodes in the planar network compared to the hierarchical network. In the radio transceiver information energy expenditures model, the correlation is shown in Figure 1.

In Figure 1, the distance between two nodes is set as d, and l-bit message is sent to this node, the expression of energy consumed to send the message is shown in formula (2).

$$E_{TX}(l, d) = \begin{cases} lE_{elec} + l\varepsilon_{fs}d^2, & d < d_0 \\ lE_{elec} + l\varepsilon_{mp}d^4, & d \geq d_0 \end{cases} \tag{2}$$

In formula (2), the energy dissipated by the receiver during l-bit information transmission is E_{elec}, the free space and multipath loss energy are set as

E_{fs} and E_{mp} respectively, and when receiving l-bit information, the energy loss is shown in formula (3).

$$E_{RX}(l) = E_{elec} * l \tag{3}$$

In formula (3), E_{RX} represents the energy consumed to receive the relevant information. In each round, the energy consumed by a normal node to send l-bit information to a cluster head node is shown in formula (4).

$$E_{RX}(l) = E_{elec} * l \tag{4}$$

In formula (4), E_{CN} indicates the energy consumed for sending messages. During this period, each cluster head node also consumes energy, for which the total energy consumed in this round E_r is shown in formula (5).

$$E_r = l(2NE_{elec} + NE_{DA} + k\varepsilon_{mp}d^4_{toBS} + N\varepsilon_{fs}d^2_{toCH}) \tag{5}$$

In formula (5), when fusing data, the cluster head energy expenditure is set as E_{CN}, the number of cluster heads in the current network is k, and the average distances between the cluster head node and base station and other nodes are d_{toBS} and d_{toCH} respectively, which is calculated in formula (6).

$$d_{toBS} = 0.765\frac{M}{2},\ d_{toCH} = \frac{M}{\sqrt{2\pi k}} \tag{6}$$

In the DEEC algorithm, the number of cluster heads and corresponding optimization proportion is selected, and the maximum number of program rotations can be found by formula (1) and formula (5) as shown in formula (7).

$$R = E_t/E_r \tag{7}$$

In formula (7), R represents the maximum number of program turns. The partial derivative of k is calculated in formula (8).

$$k' = \sqrt{\frac{N}{2\pi}}\sqrt{\frac{\varepsilon_{fs}}{\varepsilon_{mp}}}\frac{M}{d^2_{toBS}} \tag{8}$$

In formula (8), for each round of cluster head, the optimal number is set as k', while the cluster head optimization ratio as $P = k'/N$. The cluster head is selected and the remaining energy of node S_i in r rounds is set as $E_i(r)$, and the change in program operation affects the node, some nodes are more likely to become cluster heads, involving the relevant formula shown in formula (9).

$$P_i = P\frac{E_i(r)}{\bar{E}(r)} \tag{9}$$

In formula (9), P_i denotes the probability that S_i is chosen as cluster head, and the average energy of WSN at r rounds of the program is $\bar{E}(r)$, whose related calculation formula is shown in formula (10).

$$\bar{E}(r) = \frac{1}{N}\sum_{i=N}^{N} E_i(r) = \frac{1}{N}E_t\left(1 - \frac{r}{R}\right) \tag{10}$$

If the network nodes have the same energy, then $P_i = P$, if S_i has higher residual energy than other nodes, it has an odds of becoming the cluster head, $P_i > P$. The study uses the weighted probability of cluster head election so that the probability of senior nodes becoming cluster head nodes is greater than that of ordinary nodes and the number of rotations of senior nodes being elected as cluster head nodes is smaller, thus the service life of WSN is longer. Among them, the relevant calculation formula is shown in formula (11).

$$P(S_i) = \frac{PN(1 + a_i)}{N + \sum_{i=1}^{N} a_i} \tag{11}$$

In formula (11), $P(S_i)$ represents the weighted probability of cluster head election. P in formula (9) is replaced with $P(S_i)$, and the odds of node becoming cluster head P_i is shown in formula (12).

$$P_i = \frac{PN(1 + a_i)E_i(r)}{(N + \sum_{i=1}^{N} a_i)\bar{E}(r)} \tag{12}$$

When P_i is calculated, after judging its relationship with the probability threshold, it is then determined whether the node is a cluster head node or not, and the expression of the threshold is shown in formula (13).

$$T(n) = \begin{cases} \dfrac{P_i}{1 - P_i(r \bmod (1/P_i))} & \mathit{if}\ (n \in G) \\ 0 & \mathit{otherwise} \end{cases} \tag{13}$$

In formula (13), $T(n)$ denotes the probability threshold, n denotes the node. In a certain round, the nodes that can be cluster heads are selected

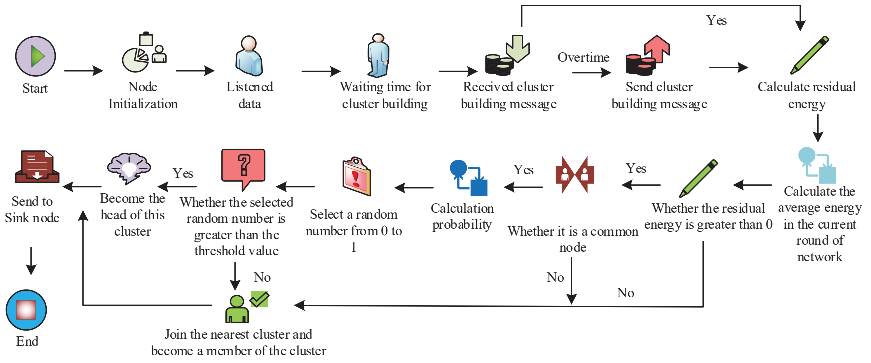

Start
Node Initialization
Listened data
Waiting time for cluster building
Received cluster building message
Overtime
Send cluster building message
Yes
Calculate residual energy
Calculate the average energy in the current round of network
Whether the residual energy is greater than 0
Yes
Whether it is a common node
Yes
Calculation probability
Select a random number from 0 to 1
Whether the selected random number is greater than the threshold value
Yes
Become the head of this cluster
Send to Sink node
End
No
No
No
Join the nearest cluster and become a member of the cluster

Figure 2 DEEC algorithm flow.

and gathered to form a set G. During the period, a random digit is selected, which is within [0, 1]. If the selected digit is less than or equal to the threshold, the node is normal in that round, and vice versa for a cluster head node. Then the information of the cluster head is broadcasted to the whole network, which contains the node's location and identity document (ID). The received signal strength is taken as the standard, the normal node chooses to join the corresponding cluster and sends the join request information to the cluster head node of that cluster, and then they establish communication. In the DEEC algorithm, the overall flow of cluster head number, cluster head optimization ratio selection, cluster head selection, and cluster formation is shown in Figure 2.

3.2 Application of IPSO-SVM Algorithm in WSN Intrusion Detection

To make WSN more secure, the study adds detection mechanisms and analyzes the intrusion detection structure, whose network model is based on a hierarchical network structure, which consists of three main parts: Sink nodes, cluster head nodes, and common nodes. The network structure is shown in Figure 3.

In Figure 3, for cluster head nodes, after collecting node information and fusing and processing that information, the Sink node receives the processed data from this cluster head node. In this way, the transmission of data traffic is reduced, thus reducing the energy expenditures due to data transmission. Facing the WSN intrusion problem, the study selects the SVM algorithm as the detection algorithm, which can handle the classification problem of nonlinear,

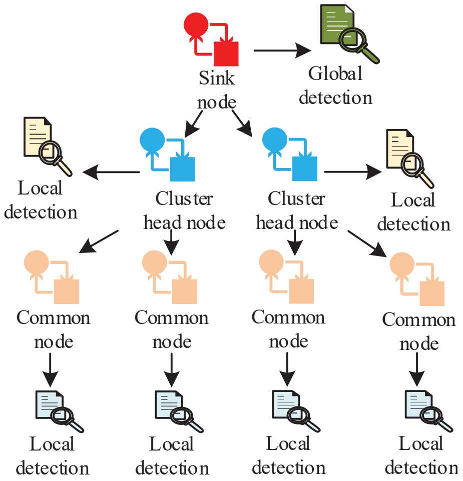


Figure 3 Cluster-based network structure.

high-dimensional minimum points and can classify the high-dimensional data for WSN intrusion detection [18]. Since the parameter settings of this algorithm affect its performance, the study optimizes the SVM algorithm by IPSO algorithm, so that the SVM algorithm can find the appropriate penalty factor C and kernel function width δ^2, and improve the generalization ability and classification accuracy of the algorithm. Among them, in the SVM algorithm, the kernel function used in the study is the radial basis kernel function, and its calculation formula is shown in formula (14).

$$k(x_i, x_j) = \exp\left\{-\frac{|x_i - x_j|^2}{\sigma^2}\right\} \tag{14}$$

In formula (14), $k(x_i, x_j)$ denotes the radial basis kernel function, σ denotes the parameter, x_i denotes the i sample of the input sample, and j denotes the serial number. The classification function is obtained as shown in formula (15).

$$f(x) = \operatorname{sgn}\left\{\sum_{i=1}^{M}\sum_{j=1}^{M} \alpha_i d_i k(x_i, x_j) + b\right\} \tag{15}$$

In formula (15), $f(\bullet)$ denotes the classification function, α_i denotes the Lagrange multiplier, b denotes the bias value, $d_i \in \{+1, -1\}$ is the corresponding target output, $+1$ and -1 denote normal and abnormal respectively, and the number of input samples is set as M. Compared with the PSO algorithm, the IPSO algorithm can avoid the PSO algorithm's tendency to fall into local extrema and improve the ability and accuracy of local search. In the IPSO algorithm, the method of nonlinear reduction of inertia weights w is used to obtain the relevant calculation formula as shown in formula (16).

$$w = w_{\max} - (w_{\max} - w_{\min}) * \exp\left(-50 * \left(\frac{iter_{\max} - iter}{iter_{\max}}\right)^{n}\right) \quad (16)$$

In formula (16), $w_{\max}$ and $w_{\min}$ denote the maximum weight and minimum weight, respectively, and in the number of iterations, its maximum value is $iter_{\max}$. And in the process of IPSO algorithm, the initialization is carried out first, and the maximum velocity interval is set to avoid the situation of exceeding the maximum interval. And the position information is the whole search space, in which the particle velocity and position are randomly initialized and the population size is set. The objective evaluation is performed, which is the calculation of the fitness value, and the relevant operations are performed on the basis of the objective function. Fitness value is a measure of the superiority or inferiority of chromosomes, individuals, or solutions in solving specific problems, commonly used in optimization algorithms such as evolutionary computation. Update the individual extreme value and global optimal value, find the fitness value of the particle's current and optimal position, find the global optimal position fitness value, compare the particle's current fitness value with the latter two fitness values, and if there is better, update its optimal position, update its global optimal position. The particle velocity and position are updated by formula (17).

$$\begin{cases} v_{id}(t+1) = wv_{id}(t) + \eta_1 rand()(p_{id} - z_{id}(t)) \\ \qquad\qquad\qquad + \eta_2 rand()(p_{gd} - z_{id}(t)) \\ z_{id}(t+1) = z_{id}(t) + v_{id}(t+1) \end{cases} \quad (17)$$

In formula (17), $t + 1$ denotes the number of iterations, d denotes the dimension, v denotes the particle velocity, η_1 and η_2 denote the acceleration constants, and z denotes the particle position. In the d dimension, The best position for i is p_{id}, and its global best position is set as p_{gd}. The random number between 0 and 1 is set as $rand()$. The SVM algorithm is optimized in the IPSO algorithm, as shown in Figure 4.

In Figure 4, the PSO algorithm is first initialized, given the values of v_{id}, $iter_{\max}$, $w_{\max}$, and $w_{\min}$. The population is initialized according to C and δ^2 in the SVM algorithm, thus the particle positions z_{id}, $z_{id} = [C_{id}, \sigma_{id}]$.

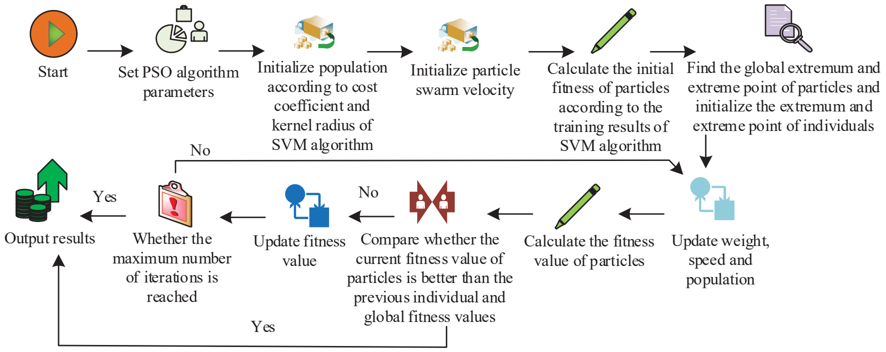
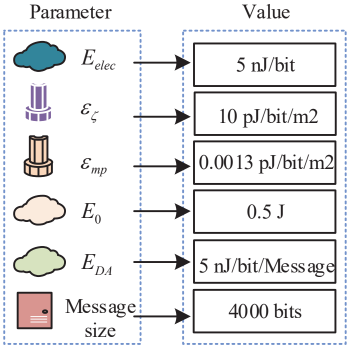

Start
Set PSO algorithm parameters
Initialize population according to cost coefficient and kernel radius of SVM algorithm
Initialize particle swarm velocity
Calculate the initial fitness of particles according to the training results of SVM algorithm
Find the global extremum and extreme point of particles and initialize the extremum and extreme point of individuals
Update weight, speed and population
Calculate the fitness value of particles
Compare whether the current fitness value of particles is better than the previous individual and global fitness values
No
Update fitness value
Whether the maximum number of iterations is reached
No
Yes
Output results
Yes

Figure 4 Related algorithm flow.

Comfortable for v_{id}, the detection accuracy trained in the SVM algorithm is calculated for the particle initial fitness value $fitness(i)$. On this basis, the particle p_{gd} and its corresponding global extremum p_{gd-x} are initialized. v, z, and weight values are updated through formula (16) and formula (17). The fitness values $fitness(i)$ are calculated according to the SVM algorithm. Based on the known current and previous individual and global fitness values of the particle, the immediate fitness value of the particle is compared with the latter two fitness values and the result is output if the previous one is worse. if not, it is updated. If the current number of iterations reaches $iter_{\max}$, the result is output and the operation is terminated. if not, the particle velocity, particle position, and weight are updated again, as well as the calculation of the fitness value $fitness(i)$ is continued until the conditions for the termination of the operation are met. Before the IPSO-SVM algorithm detects network intrusion, it needs to be trained to get the corresponding detection mechanism. Then, it is added to the WSN node for relevant intrusion detection.

In the experimental process, the experimental platform is MATLAB, and 100 nodes are deployed uniformly, its area size is 100 * 100 m, the Sink node location is (50,50), and P_i is 0.1. In the DEEC algorithm simulation, the relevant parameters are set as shown in Figure 5.

The KDDcup'99 dataset is used to select the attack data of DOS, Probe, and R21 for relevant experiments, and the proportion of the training set is 3/4. The collected data are selected by the RelifF algorithm for feature selection, the features with high trust values are selected and normalized, and the obtained data are used as training data as a way to train the IPSO-SVM algorithm. It is evaluated through evaluation indicators. During this period, to get the best parameters of SVM, the IPSO algorithm optimizes it and sets



Parameter	Value
E_{elec}	5 nJ/bit
ε_{ζ}	10 pJ/bit/m2
ε_{mp}	0.0013 pJ/bit/m2
E_0	0.5 J
E_{DA}	5 nJ/bit/Message
Message size	4000 bits

Figure 5 Relevant parameter settings.

the particle population size to 30, $\eta_1 = 1.5$, $\eta_2 = 1.6$, and 50 iterations. The number of cross-validation is 4, and the values of C and δ^2 are taken within $[2^\wedge - 5, 2^\wedge 5]$ to study the adaptation values of the IPSO-SVM method for different n values of weights in IPSO method. In the IPSO-SVM method performance analysis, the SVM method has two optimization methods: the PSO method and genetic algorithm (GA), and these two methods as well as the general SVM method are used as comparison methods of the IPSO method. In MATLAB software, the application effect of the DEEC algorithm is analyzed.

4 Application Analysis of Wireless Sensor Network Intrusion Detection

When optimizing the IPSO method, the n value of the IPSO method weight affected the convergence effect of the method, and the adaptation value of the IPSO-SVM method under different n-values of weights in the IPSO algorithm were studied, and the specific results are shown in Figure 6.

In Figure 6, under different n values, the fitness values of the optimization algorithm are different, and the corresponding convergence steps are different. When n = 2, the improved method starts to converge when the number of iterations is 38. When n = 3, the improved method starts to converge when the number of iterations is 3, 35 less than when n = 2. When n = 4, the improved method starts to converge when the number of iterations is 12. In the optimization fold at n = 2, the corresponding fitness value is 98.94% when the iteration step is 37, which is 0.02% smaller than that of the optimization fold at n = 3 with the same iteration step. When the

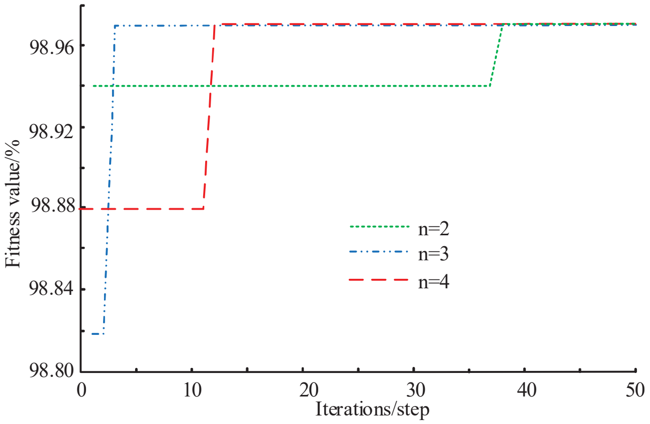


Figure 6 Optimized graphics corresponding to different n values.

iteration step size is 11, the fitness value of the optimization fold at n = 4 is the smallest, and its fitness value is 98.88%, which is 0.09% smaller than that of the optimization fold at n=3 with the same iteration step size. The maximum fitness value of different optimization folds for different values of n is the same, and the fitness value is 98.97%. According to the convergence of different optimization folds, when n = 3, the optimization algorithm folds converge the fastest and best meet the algorithm requirements. That is, the n value of IPSO algorithm weights takes the value of 3. Because when n = 3, the search path of the IPSO algorithm is closer to the local optimal solution, which helps to quickly find the optimal solution. The fitness of the four algorithms was studied under different iteration steps, and the relevant results are shown in Figure 7.

In Figure 7, the fitness values of the four SVM algorithms generally show an increase and then stabilize as the iteration step increases. According to the distribution of the folds of the fitness values of the four SVM algorithms, the fold located at the bottom is the fold where the SVM algorithm is located, while the maximum fitness values of the IPSO-SVM algorithm and PSO-SVM algorithm are the same, both of which are 98.97%, and the fold where the fitness values of these two algorithms are located is above the other two SVM algorithms. The convergence steps of these two algorithms are different, however, the convergence step of the IPSO-SVM algorithm is 5, and when the PSO-SVM algorithm converges, the number of iterations is 10. The SVM algorithm has a convergence step of 25, which corresponds to a fitness value of 98.65%, which is smaller than the other three SVM algorithms.

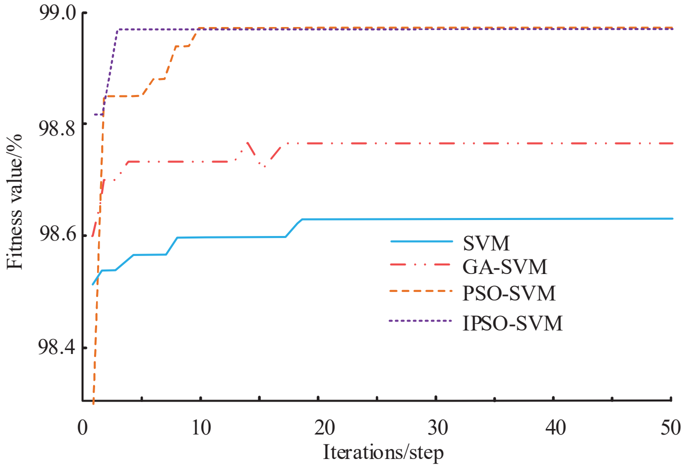
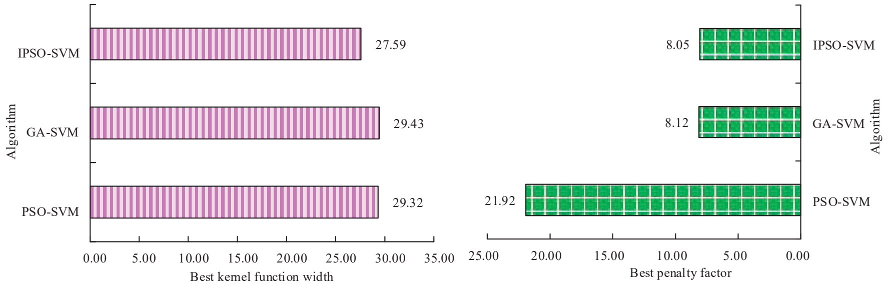


Figure 7 The fitness value of four SVM algorithms.



(a) Best kernel width of different optimization algorithms

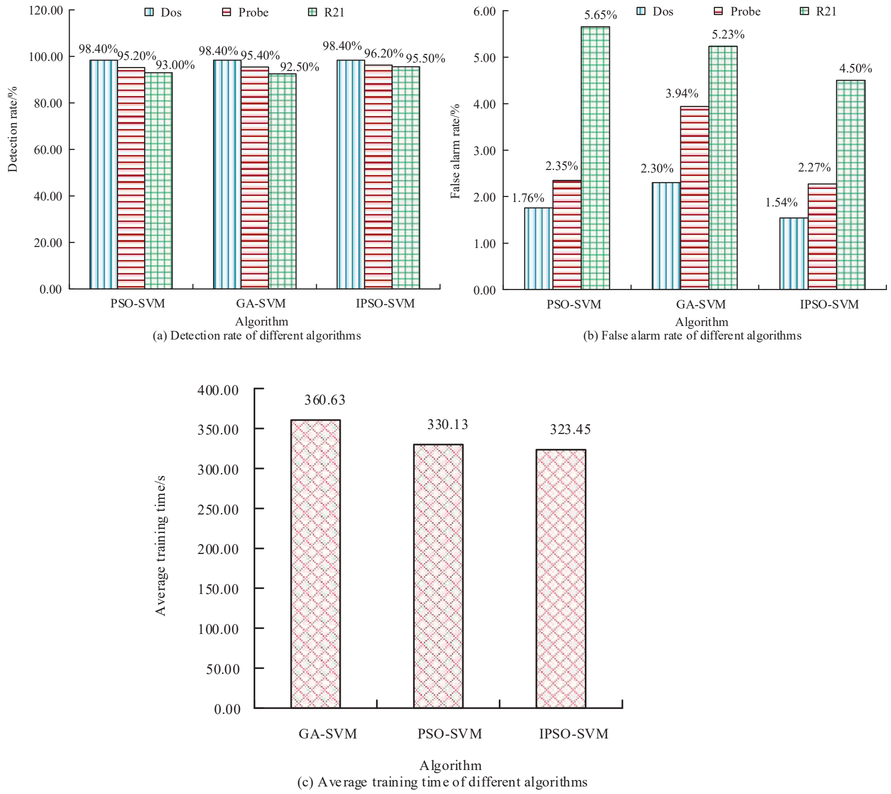
(b) The best penalty factor of different optimization algorithms

Figure 8 Relevant results of three optimization algorithms.

According to the maximum fitness values and the corresponding convergence steps of the four SVM algorithms, the IPSO-SVM method converges faster and has higher detection accuracy than the other three SVM algorithms, i.e., the algorithm outperforms the other three SVM algorithms. The best penalty factor and other related parameters obtained by three optimization methods were studied, as shown in Figure 8.

Figure 8a shows the best kernel function width of the three optimization algorithms, and Figure 8b shows the best penalty factor of the three optimization algorithms. In Figure 8a, the best kernel width of different optimization algorithms is different. Among them, the best kernel width of the GA-SVM algorithm is the largest, and its best kernel width is 29.43, 1.84 larger than the algorithm used in the study, and its best kernel width is 27.59. The best kernel width of the PSO-SVM algorithm is 29.32, which is slightly smaller than that of the GA-SVM algorithm. Compared with the other two optimization algorithms, the best kernel width of the algorithm used in this paper is the smallest. In Figure 8b, the best penalty factor of the algorithm varies according to the algorithm category. Among them, the PSO-SVM algorithm has the largest best penalty factor, its best penalty factor is 21.93, which is 13.88 larger than the algorithm used in the study, and its best penalty factor is 8.05. The best penalty factor of the GA-SVM algorithm is 8.12, which is less different from the best penalty factor of the algorithm used in this paper. Compared with the other two optimization algorithms, the best penalty factor of the algorithm used in this paper is the smallest. Overall, compared to other algorithms, the IPSO-SVM algorithm has a strong global search ability. Under the influence of the IPSO algorithm, this hybrid algorithm can better find the optimal parameters of the SVM algorithm, improving the accuracy and robustness of the intrusion detection system. The IPSO-SVM algorithm has stronger adaptability and can adaptively adjust the particle's motion speed and direction according to the actual situation, to better search for the optimal solution. This adaptability makes the algorithm more suitable for complex intrusion detection problems. The test samples were tested through the three optimization algorithms, and the relevant detection effects of the three algorithms were compared, as shown in Figure 9.

Figure 9a shows the detection rate of the three optimization methods, Figure 9b shows the false alarm rate of the three optimization algorithms, and Figure 9c shows the average training time of the three optimization algorithms. In Figure 9a, the detection rates of three optimization algorithms differ in different types of attack data. In the probe attack data detection, the detection rate of the algorithm used in the study is the highest, 96.20%, 0.80% higher than the GA-SVM method, and the detection rate of the PSO-SVM method is the lowest, 95.20%. In the detection of R21 attack data, the highest detection rate of the method used in the study is 95.50%. In Figure 9b, compared with the two types of attack data, Dos and Probe, the three algorithms have the highest false alarm rate in R21 attack data. Among the false alarm rates of the same type of attack data, the algorithm used in this paper has the lowest false alarm rate, especially in the case of Dos attack data, the false alarm rate of this method is 1.54%. Among the false alarm rates of probe attack data, the false alarm rates of the algorithm used in the study, PSO-SVM method, and GA-SVM method are 2.27%, 2.35%, and 3.94% respectively. The false alarm rate of the IPSO-SVM method is 0.08% lower than that of the PSO-SVM method. In Figure 9c, the average training time of the algorithm



(a) Detection rate of different algorithms

(b) False alarm rate of different algorithms

(c) Average training time of different algorithms

Figure 9 Correlation detection effect of three optimization algorithms.

used in the study, PSO-SVM method, and GA-SVM method is 323.45 s, 330.13 s, and 360.63 s respectively. The IPSO-SVM method has less average training time, 6.68s less than the PSO-SVM algorithm, 37.18 s less than the GA-SVM algorithm, 6.68 s less than the PSO-SVM method, and 37.18s less than the GA-SVM method. The three subgraphs in Figure 9 further prove the advantages of the IPSO-SVM algorithm. The node and energy changes of the DEEC method and low power adaptive clustering hierarchy (LEACH) method were studied at different times, and the results are shown in Figure 10.

In Figure 10a, when the time is less than or equal to 700, the nodes of the DEEC method and LEACH method are alive and not dead. When the time is greater than 700 cycles, under the same cycle, different from the LEACH method, the DEEC method has more nodes alive, and when the time is less than or equal to 1000 cycles, the nodes of the DEEC method are alive and not

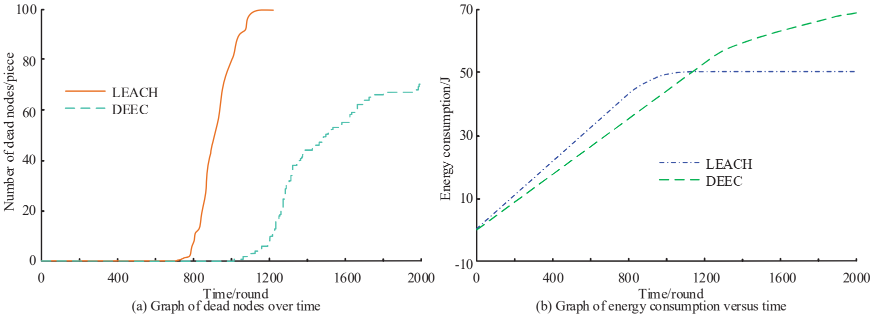


Figure 10 Dead nodes and energy expenditures of the algorithm at different times.

dead. When the time is 1145, all nodes of the LEACH method die, while four nodes of the DEEC method die, which is significantly smaller than the LEACH method. When the time is 2000, 70 nodes of the DEEC method are dead, and the remaining nodes are alive. In Figure 10b, when the time is less than 1145, the DEEC method consumes less energy. Therefore, the DEEC method performs better.

5 Conclusion

To guarantee the security of WSN, this paper uses the IPSO-SVM algorithm to detect WSN intrusion. To prolong the life cycle of the network and reduce the energy expenditures of nodes, the DEEC algorithm is selected to layer the WSN. By selecting the weighted probability of the cluster head, the advanced nodes can become the cluster head more easily, making the network energy load more balanced, and preventing the collision of related information under the hierarchical processing. The IPSO method is used to improve SVM to optimize the detection effect. After relevant tests, it was found that the different n values of the weights in the IPSO method affected the fitness value of the IPSO-SVM method. When n = 3, the convergence step length of the optimization algorithm was 3, which was significantly smaller than that of n = 2 or 4, and when n = 3, the maximum fitness value of the optimization algorithm was 98.97%, so the n value of the weights in IPSO method was 3. Compared with the other three algorithms, the IPSO-SVM method had better performance. Its convergence step was 5, and the iteration number of the PSO-SVM method was 10. Their maximum fitness values were the same, both of which were 98.97%. Among the three optimization algorithms, the IPSO-SVM method performed best. In the probe attack data detection, the IPSO-SVM method had the highest detection rate of 96.20%. The IPSO-SVM method had the lowest average training time, 6.68 s less than the PSO-SVM method. Compared with the LEACH method, the DEEC method had better performance. When the time was 1145, all nodes of the LEACH method died, while four nodes of the DEEC method died. In the first 1145 cycles, the DEEC method consumed less energy. In the future, the study can optimize the process of finding and processing attack nodes, to find attack nodes faster.

Funding

The research is supported by Science and Technology Research Project of Chongqing Education Commission Project: Research on Security Robot based on Multi-Sensor Data Fusion Technology, (No.KJQN202103904); Key Project of Science and Technology Research of Chongqing Education Commission: Research on Cloud Monitoring System for Manhole Cover Safety Applied to Smart City, (No.KJZD-K202203902).

References

[1] DashMeera, PanigrahiTrilochan, SharmaRenu, MM Narayan. Adaptive Parameter Estimation of IIR System-Based WSN Using Multihop Diffusion in International Journal of Cognitive Informatics and Natural Intelligence (IJCINI), 2020,14(4):30–41.

[2] Han Z, Ding H, Yue K, L Bao, Z Yang. New type NP-CSMA of adaptive multi-priority control WSN protocol analysis. International Journal of Reasoning- based Intelligent Systems, 2021, 13(1):24–31.

[3] Jegan J, Sivakumar D, Selvakumar K. Swarm Based Novel Energy Aware Clustering Algorithm for WSN in Realtime Applications. international journal of computational intelligence theory and practice, 2021,16(2):73–89.

[4] Hebal S, Louail L, Harous S. Latency and Energy Optimization Using MAC-Aware Routing for WSNs. International Journal of Business Data Communications and Networking, 2020, 16(1):19–27.

[5] Xiu-Wu Y U, Hao Y U, Liu Y, RR Xiao. a clustering routing algorithm based on wolf pack algorithm for heterogeneous wireless sensor networks. computer Networks, 2019, 167(6):106994.1–106994.10.

[6] Borkar G M, Patil L H, Dalgade D, A Hutke. A novel clustering approach and adaptive SVM classifier for intrusion detection in WSN: A data mining concept. Sustainable Computing, 2019, 23(Sep.):120–135.

[7] Alghamdi W, Rezvani M, Wu H, Kanhere, Salil S. Routing-Aware and Malicious Node Detection in a Concealed Data Aggregation for WSNs. ACM Transactions on Sensor Networks, 2019, 15(2):18.1–18.20.

[8] Behera T M, Mohapatra S K. A novel scheme for mitigation of energy hole problem in wireless sensor network for military application. international Journal of Communication Systems, 2021, 34(11): e4886.1–e4886.10.

[9] Banerjee A, Das V, Biswas A, S Chattopadhyay, U Biswas. Development of Energy Efficient and Optimized Coverage Area Network Configuration to Achieve Reliable WSN Network Using Meta-Heuristic Approaches. international journal of geotechnical earthquake engineering, 2021, 12(3):1–27.

[10] Amarasimha T, Rao V S. Efficient Energy Conservation and Faulty Node Detection on Machine Learning-Based Wireless Sensor Networks. Journal of Grid and High-Performance Computing, 2021, 13(2):1–20.

[11] Liang J, Xu Z, Xu Y, W Zhou, C Li. Adaptive cooperative routing transmission for energy heterogeneous wireless sensor networks. physical Communication, 2021, 49(Dec.):101460.1–101460.10.

[12] Xu Y, Jiao W, Tian M. Energy-Efficient Connected-Coverage Scheme in Wireless Sensor Networks. sensors, 2020, 20(21):1–19.

[13] Wei J, Huang H, Kang P D. PSO-DEC-IFSVM Classification Algorithm for Unbalanced Data. Shu Ju Cai Ji Yu Chu Li/Journal of Data Acquisition and Processing, 2019, 34(4):723–735.

[14] Li Q, Fu Q, Zou Y, Xijun Hu. Evaluation of Livable City Based on GIS and PSO-SVM: A Case Study of Hunan Province. international Journal of Pattern Recognition and Artificial Intelligence, 2021, 35(8):2159030.1–2159030.18.

[15] Varela N, Lezama O, Neira H. Information security in WSN applied to smart metering networks based on cryptographic techniques. journal of Intelligent & Fuzzy Systems: Applications in Engineering and Technology, 2020, 39(6 Pt. 1):8499–8506.

[16] Kala I, Karthik S, Srihari K. Advanced hybrid secure multipath optimized routing in Internet of Things (IoT)-based WSN. International Journal of Communication Systems, 2021, 34(8):e4782.1–e4782.14.

[17] Bayat M, Atashgah M B, Barari M, MR Aref. Cryptanalysis and Improvement of a User Authentication Scheme for Internet of Things Using Elliptic Curve Cryptography. International Journal of Network Security, 2019, 21(6):897–911.

[18] Neethu P S, Suguna R, Rajan P S. Performance evaluation of SVM-based hand gesture detection and recognition system using distance transform on different data sets for autonomous vehicle moving applications. circuit world, 2022, 48(2):204–214.