An Intrusion Detection Model Based on IPSO-SVM Algorithm in Wireless Sensor Network

Shuang Liu[1], Liejun Wang[2], Jiwei Qin[3], Yan Guo[1], Hang Zuo[1]

[1] School of Information Science and Engineering, Xinjiang University, China
[2] School of Software, Xinjiang University, China
[3] Network and Information Technology Center, Xinjiang University, China
iejunaang@sina.com, wljxju@xju.edu.cn, 411975748@qq.com, uesongan@sina.com, 714688382@qq.com

Abstract

Aiming at the energy constrained of wireless sensor network (WSN) and the low detection accuracy of intrusion detection mechanisms in WSN, an intrusion detection model based on improved Particle Swarm Optimization (IPSO) and Support Vector Machine (SVM) is proposed in this paper. Firstly, the improved LEACH algorithm is applied to our intrusion detection model to cluster the nodes to reduce energy consumption. Nextly, Anomaly detection based on SVM algorithm is used in this model to ensure that detector has a high detection accuracy. Finally, the SVM algorithm is optimized by using the IPSO algorithm to obtain the optimal SVM parameters, so as to improve the detection precision and convergence speed of the model. The experimental results show that the intrusion detection model mentioned in this paper has higher detection precision, faster convergence speed and more balanced use of node energy compared with other detection models.

Key words: Wireless sensor network, intrusion detection, Particle swarm optimization, Support vector machine, LEACH algorithm, Anomaly detection

1 Introduction

Wireless sensor network (WSN) because of its sensor node has the advantages of small volume, easy deployment and low cost, which has been widely used in many fields, such as urban management, industrial and agricultural production, military, environmental monitoring, biology medicine, remote control of danger areas, emergency rescue and so on [1]; Simultaneously, wireless sensor networks are often placed in unmanned areas or hostile environments, and sensor nodes in wireless sensor networks are devices with limited capacity and limited processing capacity, which makes the network vulnerable to various attacks [2]; therefore, There is a need of proper security mechanisms for protecting sensor networks against potential security threats and attacks [3].

At present, there are two kinds of defense measures against attacks: passive defense and active defense. passive defense, such as encryption, security protocol, identity authentication, security routing. active defense, including intrusion detection [4]. Intrusion has more responsiveness and adaptability, and consequently, can be applied as the supplement and a second line of defense for passive prevention security systems [5]. Due to the limitation of wireless sensor network communication bandwidth, packet delay, and node energy and so on, the intrusion detection technology for traditional limited network and ad hoc network can not be applied to wireless sensor networks [6]. Therefore, it is necessary to design an intrusion detection system which conforms to the characteristics of wireless sensor network.

2 Relate Work

The security mechanism of wireless sensor network is divided into low-level defense mechanism and high-level defense mechanism. Intrusion detection in high level is called second defense mechanism. As the second defense mechanism, intrusion detection can not only detect external attacks, but also detect internal attacks. It plays a vital role in the security of wireless sensor networks. At present, there are many methods about intrusion detection which are used in Wireless Sensor Network. For example, In [7], A detection mechanism based on artificial immune algorithm is proposed, the negative selection and dynamic selection algorithm are adopted to detect attackers, to a great extent, this scheme ensures the security of data in the network, but it needs to be improved and optimized. In [8], an intrusion detection mechanism based on machine learning is proposed, Intrusion detection is realized by feedforward neural network, and the final intrusion classification is done by self-organizing mapping. Although this scheme has a high detection rate for known attacks, the detection of unknown

*Corresponding Author: Liejun Wang; E-mail: wljxju@xju.edu.cn
DOI: 10.3966/160792642018121907015

attacks is still uncertain. In [9], A hierarchical security mechanism for complex attacks in wireless sensor networks is proposed, usage control is employed to defend against ongoing threats, dynamic adaptive chance discovery mechanism is uesd to detect unknown attacks, the mechanism can not only detect attacks, but perform attack mitigation, however, it is too complex. In [10], the intrusion detection system in the network is put into a reasonable place to resist attack, This scheme is valid and available, but further research is needed to find the optimal location. In [11], an adaptive early node compromise detection scheme based on cluster is proposed, In this scheme, the network is clustered according to a certain proportion, and then the number of heartbeat rounds under certain conditions is obtained according to the known conditions, Finally, the data monitored from the member nodes is carried out bitwise or operations by the management nodes of each cluster. Although this program has low false alarm rate, its computational complexity is too high. In [12], one-class support vector machine based on local density degree is used for the anomaly detection. The relaxation variable of the support vector machine is expressed by the density of the data set. Although this method is better than the performance of the other one-class learning model, the penalty factor has a great influence on the performance of the support vector machine, so the choice of the penalty factor needs to be considered. In [13], an adaptive support vector machine is proposed for intrusion detection, the relationship between the precision of the classifier training and the feature weight is found by the feature reduction algorithm in this paper, then, this relation expression is used to replace the original weight update formula in support vector machine, the new SVM is likely to get good results, but the SVM parameter setting is difficult to grasp, parameter Settings has a great influence on test results, and anomaly detection model should be as much as possible to avoid artificially adjusted the parameters. In [14], A PCA-based method is used for anomaly detection. The sample is tested based on mean dissimilarity between the sample to be detected

and other samples and the degree to which the projection of the sample to the first principal axis deviates from the mean state. This method has a high detection accuracy and low error However, with the increase in the number of nodes, the parameters of the algorithm should be adjusted as well. In [15], A cooperative model detection mechanism is used for anomaly detection of wireless sensor networks. Firstly, the multivariate Gaussian model is used to detect the abnormal changes of the sensor data. Then, the sensor is detected by the PCA-based detection model. The scheme has good detection rates with limited false alarms, but the performance of the algorithm has yet to be improved. In [16], A Bayesian algorithm based on probabilistic prediction is used to perform ARP attack detection. It is determined whether the node is attacked based on the relationship between the predicted probability value and the set probability value. This scheme effectively reduces the probability of miscarriage of justice, but when the attack frequency is low and attack characteristics are included in the conventional characteristics, this program can not identify the attacker. In [17], a intrusion detection system based on flexible manet prevention algorithm is used to prevent and detect DDOS attacks, an attack profile database is used to track the malicious state of each node in this paper, when number of times of a node tracked by A is more than the defense threshold. it is considered that the node is a malicious node and added to the blacklist, this algorithm can guarantee that the network is still running under attack, but the algorithm was verified only for a single attack. In [18], an approach was presented, which was based on immune algorithm (IA) and support vector machine (SVM). immune algorithm is used to preprocess the network data ， SVM is adopted to classify the optimization data, and recognize intruders. The data are preprocessed and then classified, which reduces computational complexity and achieves higher detection accuracy. However, the parameter setting of SVM algorithm is still a problem. In [15], an algorithm based on SOA-SVM was applied to intrusion detection in WSN, although avoids artificially adjusted of the SVM parameters, but the training time is longer. In [19], a intrusion detection model based on GA-SVM for wireless sensor networks was proposed. Genetic algorithm is applied to optimize SVM parameter, although the detection results are good, genetic algorithm needs to go through the process of selection, crossover and mutation, the algorithm process is complex and the convergence speed of SVM parameter optimization is slow. In [20-21], proposed an intrusion detection model based on PSO-SVM, using PSO can avoid the problem that the extremum of the optimization object falls into the local optimal value. Although the detection model can meet certain requirements, the optimization time and the global search precision can be improved. In [17], firstly, according to the position of WSN, the improved K-means algorithm is used to cluster the nodes of WSN, and SVM algorithm is applied to different clusters to detect anomaly. The K-means algorithm is used to classify the clusters without taking into account the energy utilization of the sensor nodes, leading to the early death of some nodes and other nodes with higher residual energy, thus shortening the life cycle of the whole network.

To sum up, our contribution in this paper is to propose an IPSO-SVM intrusion detection model based on clustering. Firstly, the model classifies the clusters using the improved LEACH algorithm, taking the differences in initial energy and residual energy of the nodes and the different network structures into

account, so that the energy usage of the network nodes is homogenized. Secondly, SVM parameters are optimized by using IPSO, which not only avoids the artificial adjustment of SVM parameters and the local optimal value, but also improves the global search efficiency and local search precision. Experimental results show that the proposed method not only can improve the detection accuracy and speed up the convergence rate, but also extend the life of the whole network.

3 The Principle of SVM

SVM is a machine learning method based on statistical learning theory，due originally to Vapnik. Its basic idea is that for a given small training sample, in order to obtain the best generalization performance, how to achieve a tradeoff between the accuracy of the given training set and the learning ability of test set [22]. SVM can solve the problems of small sample, nonlinear, high dimension and the classification of local minimum points. Therefore, the SVM method is suited to classify the high-dimension data in IDS [23]. When SVM is used in intrusion detection system, classification hyperplane of training data which may be divided by linear classification plane or not via mapping the training data to higher dimensional space with nonlinear function and Transferring into linear separable patterns in the sample feature space. After the mapping procedure, SVM finds out a linear separating hyperplane with the maximum margin in the space.

Suppose the linearly separability sample set $(x_i, d_i)_{i=1}^{M}$, $x \in R^d$, $d \in \{+1, -1\}$ is the corresponding target output. For linear separable modes, the classify hyperplane equation is:

$$\omega^T x + b = 0 \tag{1}$$

Where, ω is adjustable weight vector and the parameter b is offset. In order to the hyperplane can classes all samples correctly, it needs to be satisfied:

$$d_i\left(\omega^T x_i + b\right) \geq +1,\ i = 1, 2, \cdots, M \tag{2}$$

Therefore, the hyperplane that satisfies formula (2) and minimizes the $\|w\|^2$ is the optimal hyperplane. If training sample (x_i, d_i) which satisfies the equal sign of the formula (2) are called Support Vectors, because they support the optimal classify hyperplane. So our problem can be formulated as follow:

$$\min \varphi(\omega) = \min \frac{1}{2}\|\omega\|^2 = \min(\frac{1}{2}\omega^T \omega) \tag{3}$$

$$subject\ to\ d_i\left(\omega^T x_i + b\right) \geq 1,\ i = 1, 2, \cdots, M$$

Slack variable $\{\varepsilon_i\}_{i=1}^{M}$ are introduced to process inseparable data points and data noise, then the formula (2) can be described as follow:

$$d_i\left(\omega^T x_i + b\right) \geq 1 - \varepsilon_i,\ i = 1, 2, \cdots, M \tag{4}$$

In order to improve the generalization ability and to minimize the structural risk, Equation (5) is obtained:

$$\varphi(\omega, \varepsilon) = \frac{1}{2}\omega^T \omega + C\sum_{i=1}^{M} \varepsilon_i \tag{5}$$

Where C is penalty factor, and the objective is to minimize the structural risk of constructing the optimal classification hyperplane by optimization. At this point, our optimization problem can be expressed as follow:

$$\min[\phi(\omega, \varepsilon)] = \min(\frac{1}{2}\omega^T \omega + C\sum_{i=1}^{M} \varepsilon_i) \tag{6}$$

$$subject\ \ to\ \begin{cases} d_i(\omega T x_i + b) \geq 1 - \varepsilon_i, i = 1, 2, \cdots, M \\ \varepsilon_i \geq 0, i \in R^d \end{cases}$$

For the curse of dimensionality and dual problem in inseparable model, Lagrange multiplier α_i and kernel function are introduced. Then, the optimization problem of formula (6) can be expressed by the following formula:

$$\max\left[Q(\alpha)\right] = \max[\sum_{i=1}^{M} \alpha_i - \frac{1}{2}\sum_{i=1}^{M}\sum_{j=1}^{M} \alpha_i \alpha_j d_i d_j k(x_i, x_j)] \tag{7}$$

$$subject\ \ to\ \begin{cases} \sum_{i=1}^{M} \alpha_i d_i = 0 \\ 0 \leq \alpha_i \leq C, i = 1, 2, \cdots, M \end{cases}$$

Where, $k(x_i, x_j)$ is kernel function. The kernel function has many kinds, such as radial basis kernel function, Gauss kernel function, polynomial kernel function. This paper chooses the RBF kernel function, and it can be described as below:

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

Finally, the optimal classify function as follow:

$$f(x) = \operatorname{sgn}\left\{(\omega \cdot x) + b\right\} = \operatorname{sgn}\left\{\sum_{i=1}^{M} \alpha_i d_i k(x_i \cdot x_j) + b\right\} \tag{8}$$

Parameter setting in SVM influences the performance of algorithm greatly, Especially the penalty factor C and the width σ^2 of the kernel function, these two parameters have a great influence on the generalization ability and classification accuracy of SVM. So it is important to find the appropriate values of C and σ^2. The improved particle swarm

optimization algorithm (IPSO) is used to optimize SVM parameters to find the appropriate values of C and σ^2 in this paper.

4 Improved Particle Swarm Optimization Algorithm (IPSO)

Particle swarm optimization [24] is a inspiration algorithm proposed by Kennedy and Eberhart for the process of foraging birds, which is mainly used to solve fast convergence and optimization problems. Particle Swarm Optimization is suitable for SVM parameters optimization for the following reasons:easy to code, global search sensitive, reasonable calculation, less parameters, easier to implement. The PSO algorithm is described as follows:

PSO is initialized to a group of random particles (random solutions), and then find the optimal solution through iteration. At each iteration, the particle is updated by tracking individual extremum p_{id} and global extremum p_{gd}.

Next, we search for a group with u particles in the d-dimensional space, where d is the dimensionality of the search space. Thus, in a physical d-dimensional search space, the position and velocity of each particle i are represented as the vectors $Z_i = (z_{i1}, z_{i2}, \cdots, z_{id})$ and $V_i = (v_{i1}, v_{i2}, \cdots, v_{id})$, respectively. In course of movement in the search space looking for the optimum solution of the problem being optimized, the particle's velocity and position are updated as follows:

$$\begin{aligned} v_i(t+1) = {} & w v_i(t) + \eta_1 rand_1(p_{id}(t) - z_i(t)) \\ & + \eta_2 rand_2(p_{gd}(t) - z_i(t)) \end{aligned} \tag{9}$$

$$z_i(t+1) = z_i(t) + v_i(t+1) \tag{10}$$

Where, t is number of iteration; η_1 and η_2 are acceleration (weighting) factors; $rand_1$ and $rand_2$ random numbers between 0 and 1; w is the inertia weight which is used to balance the global search and local search, the traditional w update formula is expressed as follows:

$$w = w_{\max} - t \times \frac{w_{\max} - w_{\min}}{iter\max} \tag{11}$$

Where $w_{\max}$ and $w_{\min}$ are maximum weight and the minimum weight, respectively; $iter\max$ is the maximum iteration number; t is the current iteration number. Since the traditional method of linear reduction w is not strong enough to search for a solution, it is likely to miss the optimal solution. In this paper, a method of nonlinear decreasing weight w is used in place of the traditional method, as shown in equation (12):

$$w = w_{\max} - (w_{\max} - w_{\min}) \times \exp(-50 \times (\frac{(iter\max - t)}{iter\max})^n) \tag{12}$$

The nonlinear decreasing wight method is used, which not only can improve the efficiency of global search, but also can improve the precision of local search [25].

5 Implementation of Intrusion Detection System Based on IPSO-SVM in WSN

The network topology of wireless sensor networks can be divided into: planar structure, cluster structure and hierarchical [26]. In this paper, a clustering-based wireless sensor network [27] is adopted., which can control the communication of most nodes within the cluster, and more importantly, reduce the communication between common node and sink node. This greatly reduces the communication overhead of the network and prolongs the network life cycle [28]. Cluster-based network structure is mainly composed of three parts: common node (CN), cluster head node (CH), Sink node (SN). Cluster-based network structure is shown in Figure 1.

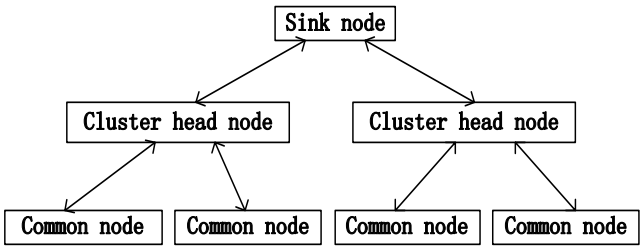


Figure 1. Cluster-based network structure

Before the network intrusion detection, IPSO-SVM algorithm should be applied to a large number of experimental data for offline learning. In this way, we can get the IPSO-SVM detection mechanism. Then the IPSO-SVM detection mechanism is loaded on all nodes in the wireless sensor network.

Intrusion detection stage, the multi-layer co-detection mechanism is adopted in this paper. In the first layer, the Sink node perceived itself threatened, Sink node will send a broadcast to the cluster head node to activate the IPSO-SVM detection mechanism of cluster head node. In the second layer, the cluster head node began to detect, if an anomaly is detected, the cluster head node sends the abnormal node data to the Sink node. If an anomaly can not be determined, the cluster head node sends a broadcast to the common node within the cluster to deactivate the IPSO-SVM detection mechanism of the common node. In the third layer, the data is detected by the common node, if the anomaly is detected, the abnormal data is reported to the Sink node by the common node. Finally, Sink node according to their own possession of the detailed data, to make the final decision.

5.1 Cluster Election

CH is elected dynamically according to his energy. The most common clustering method is the LEACH (Low Energy Adaptive Clustering Hierarchy) algorithm, the LEACH algorithm randomly chooses the cluster head nodes in a round way, and distributes the energy load of the whole network to each sensor node in an average way, thus reducing the network energy consumption and improving the overall network lifetime. The LEACH algorithm selects the cluster head with the idea that each sensor node randomly generates a random number between 0 and 1, if the random number is selected to be less than a certain threshold, then the node is elected as the cluster head node. The representation of the threshold is given by the formula (13):

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

Where p is the probability that the node is selected as the cluster head node, r is the current round number,, and G is the set of nodes that have not been elected as cluster heads in the last round of $\frac{1}{p}$.

In this paper, the method of literature [29] is adopted, on the basis of the LEACH algorithm, the initial energy and the residual energy of the node and the different network structure are considered. Thus, the life cycle of the network is increased and the probability that each node is elected as the cluster head is no longer the same. The formula for the probability of a node being selected as the cluster head node is as follows:

$$p_i=\frac{P*n*S_i.E*E_i}{E_i*E_i*\left(1-r/r_{\max}\right)/n} \tag{14}$$

Where, P is the initial cluster head election probability, $S_i.E$ is the current energy of the node, E_i is the initial energy of the node, r is the current round, and $r_{\max}$ is the maximum number of rounds.

The relationship between the probability p_i of the *ith* node s_i being elected as a cluster head and the improved threshold T_n is expressed as follows:

$$T(s_i)=\begin{cases}\dfrac{p_i}{1-p_i(r \bmod \frac{1}{p_i})}, & if(s_i\in G)\\ 0, & otherwise\end{cases} \tag{15}$$

The pseudo code for cluster-head election is described as follows:

……

$E_a=E_i*\left(1-r/r_{\max}\right)/n$

For $i=1:1:n$

if $(E_a>0)$

$p_i=P*n*s_i.E*E_i/\left(E_i*E_a\right)$

if $(s_i.E>0)$

if $(s_i.G\le 0)$

……

The cluster head stores var*ious* inf*ormation*

……

Calculate the energy consumed by the cluster head to send data packets to the base station

… …

End

End

End

5.2 IPSO-SVM Intrusion Detection Engine

The parameters of SVM have important influence for the classification capability, if the parameters do not enactment appropriate, we can't get the good classification result. The IPSO algorithm is used to optimize SVM parameters in this paper, For the optimization of the penalty parameter C and the width σ^2 of the kernel function, each particle is set as (c_i,σ_i), SVM detection accuracy is used to express the fitness value $fitness(i)$. The steps of optimize the parameters as follow (Figure 2):

(1) Initialization the IPSO algorithm parameters, given the maximum number of iterations of *iter* max, the acceleration factors η_1,η_2, the maximum weight $w_{\max}$ and the minimum weight $w_{\min}$.

(2) The particle position is initialized according to the penalty parameter and the width of the kernel function, that is, the particle position is expressed as: $z_i=[c_i,\sigma_i]$.

(3) Initialize the velocity v_i of the particle.

(4) Calculate the initial fitness value of the particle.

(5) Find the global extreme value p_{gd} and the global

extreme point p_{gd}_x of the particle according to the fitness value, and initialize the extremum p_{id} of the individual and the extreme point p_{id}_x of the individual.

(6) The particle velocity, particle position, and weight are updated according to equations (9), (10), and (12).

(7) Calculate the particle fitness value $fitness(i)$.

(8) Update the individual extremum p_{id} and the global extremum p_{gd}.

(9) To determine whether to achieve the maximum number of iterations, if the maximum number of iterations to reach the end of the process. Otherwise go to Step6, continue to carry out.

(10) Output the parameter sets which are optimized.

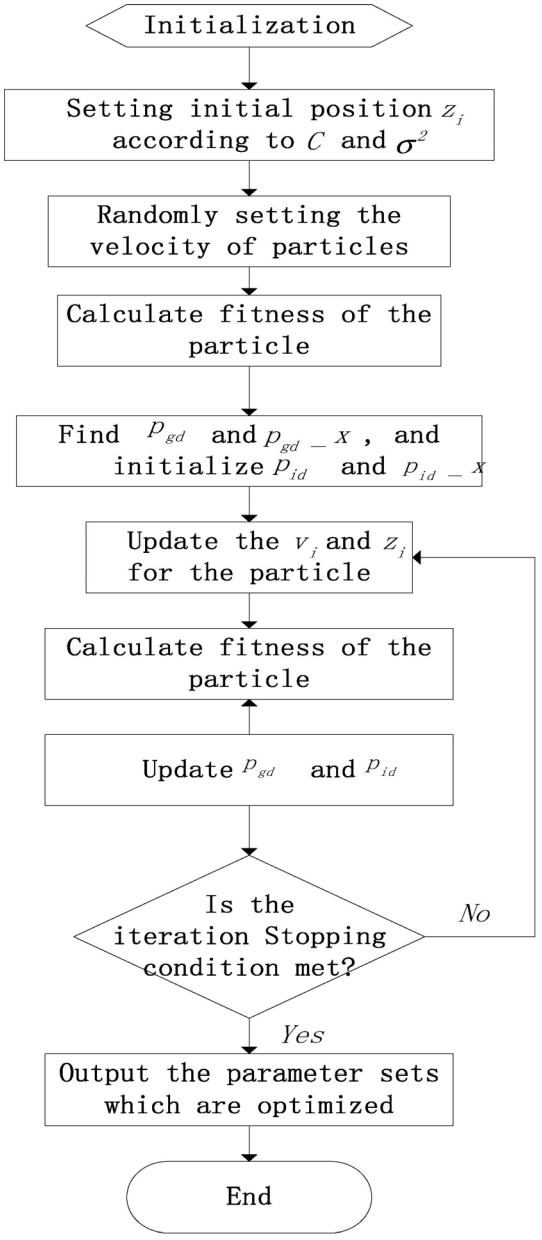


Figure 2. The implementation process of IPSO-SVM algorithm

6 Experimental Simulation and Results

The performance of the detection model is analyzed from the aspects of detection rate, false detection rate and energy consumption by using the simulation experiment to verify the advantage of IPSO-SVM detection model based on clustering to wireless sensor network. In this paper, MATLAB2015a is used as the experimental platform, and 100 nodes are evenly distributed to 100 × 100m, the location of the sink node is (50,50). After cluster head election probability p = 0.1 forming cluster, the cluster member node communication radius is 50m; the communication area of the cluster head node can cover the whole deployment area; the communication distance of the sink node covers the whole area, and its processing capacity is strong and storage space is large.

The network training and test data were generated using the KDDcup`99 dataset [23, 28], which contained the normal data set and the attack data set. Among them, the attack data set simulation to achieve DOS, Probe, R2l, U2l four kinds of attack scenarios, which also includes a large number of normal data information. As U2l's data set is too small, this article only selected DOS, Probe and R2l attack data to experiment, which randomly selected training set and test set in a ratio of 3:1. In this paper, the parameters of IPSO algorithm are selected according to several experiments. The parameters of IPSO algorithm are shown in the Table 1.

Table 1. Parameter setting of IPSO algorithm

Parameters	Value
Population number	30
Acceleration factor η1	1.5
Acceleration factor η2	1.6
itermax	50
w_{max}	1.2
w_{min}	0.8

6.1 Feature Selection and Preprocessing of Data

Because the data collected is multi-dimensional, the ReliefF algorithm is used to select some features with higher trust value in this paper, so as to reduce dimension and remove noise. The specific steps of ReliefF algorithm are described as follows [24].

Suppose that the data set is D, m is the sampling number of samples, the threshold of feature weight is δ, k denotes the number of nearest neighbor samples, and the output weight of each attribute is T. The pseudo code is represented as follows:

Set all feature weights *to* 0 *and T to empty sets.*

For $i = 1$ *to* m *do*

Randomly select a sample R from D

Find the k nearest neighbors $\mathrm{H_j(j=1,2,\cdots,k)}$ *of R from the same sample set of R,*

and find k nearest neighbors $\mathrm{M_j(C)}$ *from each different kind of sample set;*

For $A = 1$ *to N all feature do*

W(A)

End

End

For $A = 1$ *to N do*

if $W(\mathrm{A}) > \delta$

Add the Ath *feature to T*

End

Where $W(A)$ is the weight of feature A, the expression for $W(A)$ is as follows:

$$w(A) = w(A) - \sum_{j=1}^{k} diff(A, R_i, H_j)/(mk) + \sum_{C \neq class(R_i)} \left[\frac{p(C)}{1 - p(class(R_i))} \sum_{j=1}^{k} diff(A, R_i, M_j(C))/(mk) \right] \quad \textbf{(16)}$$

Here, R is the extracted sample, H is the immediate sample of R, $p(C)$ is the ratio of class C samples on the total samples, $diff(A,R,H)$ is the distance between the sample R and the sample H with respect to the feature A, $M_j(C)$ is the jth nearest neighbor sample of the different class C.

The results of feature extraction by ReliefF algorithm are shown in Table 2.

Table 2. Select the attributes by the feature selection

Attribute	6	12	23	24	29	32	33	34

Since the raw data after feature selection can not be directly applied to the detection model, the data need to be preprocessed into IPSO-SVM detection mechanism to identify data. In this paper, **Min-Max** is used to preprocess the data, as shown in equation (17):

$$x = \frac{x - \min(x)}{\max(x) - \min(x)} \quad \textbf{(17)}$$

6.2 Detection Performance Analysis

To evaluate the effectiveness of the proposed model, the most efficient intrusion detection model is determined by two metrics:detection rate and false alarm rate [22-23].

Detection Rate, called DR, is defined as: $DR = \frac{m}{M}$, m indicates the number of sample that correctly detects the attack, M represents the total number of attacks.

False positive rate, called FPR, is defined as: $FPR = \frac{n}{N}$, n indicates the number of sample that wrongly detects the attack, N represents the total number of normal samples.

In order to find the best SVM parameters, we use the improved PSO (IPSO) algorithm to optimize the SVM parameters. Population size in the IPSO algorithm is 30, the acceleration constants η_1 and η_2 are 1.5 and 1.6 respectively, evolutionary times take 50 times, the number of cross validation is v = 4, and the penalty factor and the kernel function width are between [2^-5, 2^5]. In order to get the best parameters of the SVM, we first need to determine the value n of the weight update in the IPSO algorithm. After several experiments, we get n = 3, the optimal curve shown in Figure 3.

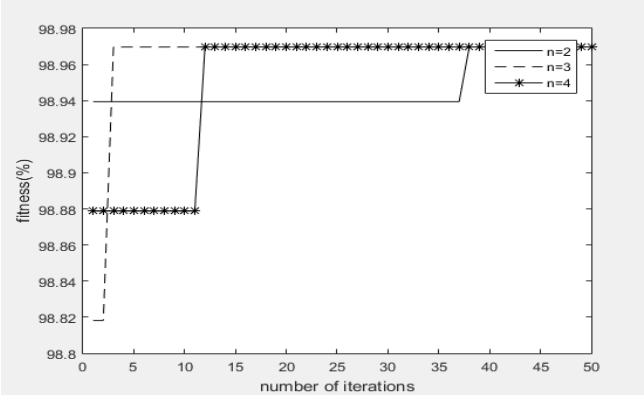


Figure 3. Different optimization curves of different n values

In terms of algorithm performance improvement, the

IPSO-SVM model is compared with the standard PSO-SVM model [13] and the GA-SVM model [7], and the optimal curve and the best penalty factors and kernel widths are shown in Figure 4 and Table 3, respectively.

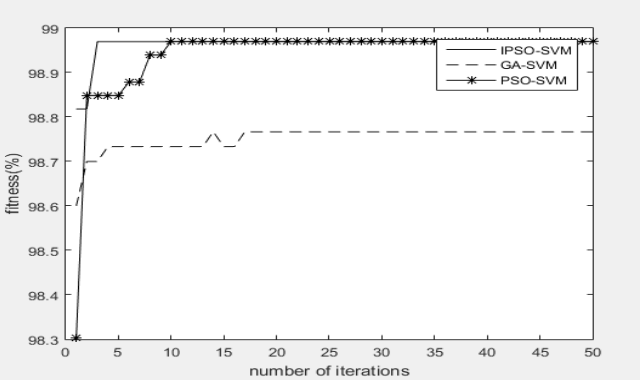


Figure 4. IPSO, PSO and GA on the SVM parameters of the optimized curve

Table 3. Best c and best σ are obtained by different optimization algorithms

category	*bestc*	*best*σ
GA-SVM	8.1165	29.4262
PSO-SVM	21.9228	29.3232
IPSO-SVM	8.0493	27.5853

It can be seen from Figure 2 that the IPSO for SVM parameters optimization step of convergence is 5, the PSO and GA for SVM parameters optimization step of convergence are 10 and 18 respectively. IPSO and PSO algorithm to optimize the SVM for fitness values are reached 98.9697, the fitness value of SVM optimized by GA algorithm is 98.76。It can be seen that the IPSO-SVM model is superior to the PSO-SVM and GA-SVM in terms of convergence speed and detection accuracy.

In order to verify the effectiveness of the proposed IPSO-SVM algorithm, the test samples are tested and compared with PSO-SVM algorithm and GA-SVM algorithm. The test results are shown in Table 4.

Table 4. test results of the three algorithms on the test sample

category	Detection rate			False positive rate		
	Dos	Probe	R2l	Dos	Probe	R2l
PSO-SVM	98.40%	95.20%	93%	1.76%	2.35%	5.65%
GA-SVM	98.40%	95.40%	92.5%	2.30%	3.94%	5.23%
IPSO-SVM	98.40%	96.20%	95.5%	1.54%	2.36%	4.50%

As shown in Table 3, the IPSO-SVM detection model is superior to the GA-SVM model and the PSO-SVM model in detection rate and false positive rate. In terms of detection rate, the detection rate of the three detection algorithms for Dos attack is the same. For the Probe attacks and R2l attacks, the detection rate of IPSO-SVM was 0.8% and 3% higher than that of GA-SVM, respectively; And the detection rate of IPSO-SVM was 1.0% and 1.5% higher than that of PSO-SVM, respectively. This model is better than the other two models in terms of detection rate, because this article with the improved PSO algorithm and SVM algorithm fusion, combines the local search ability of IPSO algorithm and global search ability and ability of detecting the SVM, that allows the model to quickly found invasion and improves the detection rate. In terms of the false positive rate, the FPR of IPSO-SVM was 0.76%, 1.58% and 0.73% lower than that of GA-SVM for three attacks, respectively; the FPR of IPSO-SVM was 0.22%, 0.01% and 1.15% lower than that of PSO-SVM for three attacks, respectively. Because multi-layer co-detection mechanism is adopted in this paper, which reduces the possibility that there are other models where the anomaly is mistaken for an intrusion, thereby reducing the False positive rate.

In order to evaluate the time of calculation of the algorithm proposed in this paper, in the case of the same training samples and the same number of iterations, the computational complexity of the new algorithm is evaluated by comparing with the training times of the PSO-SVM and GA-SVM algorithms, the training time of the three algorithms obtained from the experiment is shown in the Table 5.

Table 5. Training time for three different algorithms

Algorithm	Training time(s)
GA-SVM	360.63
PSO-SVM	330.32
IPSO-SVM	323.86

6.3 Analysis of Energy Equilibrium

In order to verify the effectiveness of the improved LEACH algorithm, the algorithm proposed in this paper is compared with the LEACH algorithm. After the experiment, we get the number of dead nodes and the residual energy of the nodes in each cycle as shown in Figure 5 and Figure 6.

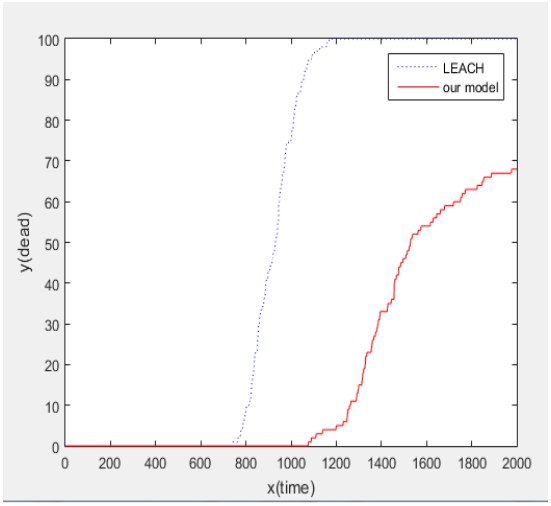


Figure 5. The change of death node with time

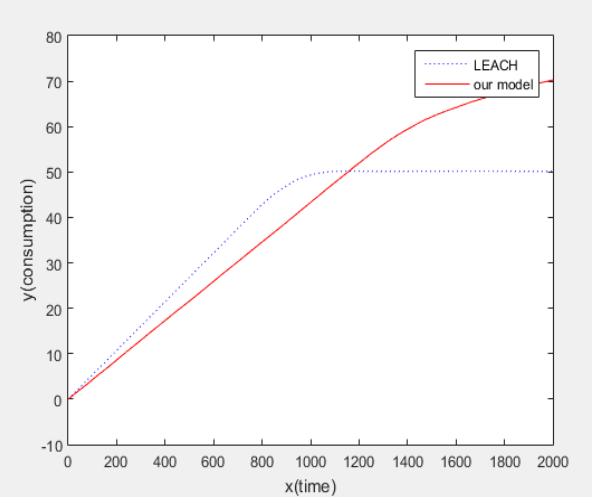


Figure 6. the variation of residual energy with time

It can be seen from Figure 5 and Figure 6 that the two algorithms have no node death in the first 700 cycles. Since cluster nodes selected based on cluster distribution are nodes with more residual energy, the energy consumption is homogenized, thus increasing the life cycle of the entire network. In the 1000th cycle, LEACH algorithm nodes have all died, so the energy consumption does not change, while our model, there are 40 surviving nodes, energy consumption is half of the total energy. Therefore, our model has advantages over the LEACH algorithm, both in terms of dead nodes and energy consumption.

7 Conclusion

In this article, IPSO algorithm and SVM algorithm are combined as the detection mechanism of wireless sensor networks. The detection mechanism has a strong global search capability and classification ability, which not only improves the detection accuracy of known attacks, but also improve the detection rate of unknown attacks. In addition, our intrusion detection model takes advantage of cluster-based architecture, which uses the improved LEACH algorithm to cluster the wireless sensor networks, so that the energy of the sensor nodes is balanced. compared with the GA-SVM and PSO-SVM detection mechanisms, the experimental results show that the model proposed in this paper, both the detection rate and the false alarm rate are better than the GA-SVM and PSO-SVM detection mechanisms; At the same time, The convergence rate of the IPSO-SVM is faster than that of GA-SVM and PSO-SVM. In addition, In addition, compared with the LEACH stratification algorithm, the algorithm used in this paper makes the energy of the node more balanced, effectively reducing the energy consumption of the network, greatly prolonging the whole network life cycle.

Acknowledgments

This work was supported by National Natural Science Foundation of China (Under grant No. 61471311) and National Natural Science Foundation of China (Under grant No. 61402392), and the work also provided by Graduate Student Research Innovation Foundation of Xinjiang Uygur Autonomous Region (Under grant No. XJGRI2015030). The authors would like to thank the anonymous reviewers for their constructive comments that helped to improve the quality of this paper.

References

[1] Y. Sun, Y. Zhang, New Developments of Characteristic Analysis in Wireless Sensor Networks, *IETE Journal of Research*, Vol. 62, No. 2, pp. 1-7, September, 2015.

[2] S. Shamshirband, N. B. Anuar, M. L. M. Kiah, V. A. Rohani, D. Petkovic, S. Misra, A. N. Khan, Co-FAIS: Cooperative Fuzzy Artificial Immune System for Detecting Intrusion in Wireless Sensor Networks, *Journal of Network & Computer Applications*, Vol. 42, No. 3, pp. 102-117, June, 2014.

[3] A. H. Farooqi, F. A. Khan, A Survey of Intrusion Detection Systems for Wireless Sensor Networks. *International Journal of Ad Hoc and Ubiquitous Computing*, Vol. 9, No. 2, pp. 69-83, February, 2012.

[4] X. Sun, B. Yan, X. Zhang, C. Rong, *An Integrated Intrusion Detection Model of Cluster-Based Wireless Sensor Network, Plos One*, Vol. 10, No. 10, pp. 1-16, October, 2015.

[5] S. Rajasegarar, A. Gluhak, M. A. Imran, M. Nati, M. Moshtaghi, C. Leckie, M. Palaniswami, Ellipsoidal Neighbourhood Outlier Factor for Distributed Anomaly Detection in Resource Constrained Networks, *Pattern Recognition*, Vol. 47, No. 9, pp. 2867-2879, September, 2014.

[6] S. L. Wang, Intrusion Detection System for Wireless Sensor Networks Based on Support Vector Machines, *Sensors and Micro Systems*, Vol. 31, No. 7, pp. 73-76, July, 2012.

[7] C. Jinyin, Y. Dongyong, Data Security Strategy Based on Artificial Immune Algorithm for Cloud Computing, *Applied Mathematics & Information Sciences*, Vol. 7, No. 1, pp. 149-153, December, 2013.

[8] G. Bujas, M. Vukovic, V. Vasić, M. Mikuc, Smart Detection and Classification of Application - Layer Intrusions in Web Directories, *Smart Computing Review*, Vol. 5, No. 6, pp. 510-519, December, 2015.

[9] J. Wu, K. Ota, M. Dong, C. Li, A Hierarchical Security Framework for Defending Against Sophisticated Attacks on Wireless Sensor Networks in Smart Cities, *IEEE Access*, No. 4, pp. 416-424, March, 2016.

[10] S. K. Majhi, S. K. Dhal, Smart Placement of Security Devices in Cloud Data Center Network, *Smart Computing Review*, No. 5, pp. 408-416, October, 2015.

[11] A. Al-Riyami, N. Zhang, J. Keane. An Adaptive Early Node Compromise Detection Scheme for Hierarchical WSNs, *IEEE Access*, Vol. 4, pp. 4183-4206, December, 2016.

[12] J. Tian, H. Gu, C. Gao, J. Lian, Local Density One-class Support Vector Machines for Anomaly Detection, *Nonlinear Dynamics*, Vol. 64, No. 2, pp. 127-130, April, 2011.

[13] N. Macek, B. Dordevic, V. Timcenko, M. Bojovic, M. Milosavljević, Improving Intrusion Detection with Adaptive Support Vector Machines. *Elektronika Ir Elektrotechnika*, Vol. 20, No. 7, pp. 57-60, September, 2014.

[14] M. Ding, H. Tian, PCA-based Network Traffic Anomaly Detection, *Tsinghua Science and Technology*, Vol. 21, No. 5, pp. 500-509, October, 2016.

[15] R. Zhang, P. Ji, D. Mylaraswamy, M. Srivastava, S. Zahedi, Cooperative Sensor Anomaly Detection Using Global Information, *Tsinghua Science and Technology*, Vol. 18, No. 3, pp. 209-219, June, 2013.

[16] H. Ma, H. Ding, Y. Yang, Z. Mi, J. Y. Yang, Z. Xiong, Bayes-based ARP Attack Detection Algorithm for Cloud centers, *Tsinghua Science and Technology*, Vol. 21, No. 1, pp. 17-28, February, 2016.

[17] V. V. Timcenko, An Approach for DDoS Attack Prevention in Mobile Ad Hoc Networks, *Elektronika Ir Elektrotechnika*, Vol. 20, No. 6, pp. 150-153, March, 2014.

[18] Y. S. Chen, Y. S. Qin, Y. G. Xiang, J. X. Zhong, X. L. Jiao, Intrusion Detection System Based on Immune Algorithm and Support Vector Machine in Wireless Sensor Network, in: L. Qi (Ed.), *Information and Automation*, Springer Berlin Heidelberg, 2011, pp. 372-376.

[19] J. Tian, M. Gao, S. Zhou, Wireless Sensor Network for Community Intrusion Detection System Based on Classify Support Vector Machine, *International Conference on Information and Automation*, Zhuhai, China, pp. 1217-1221, 2009.

[20] Z. W. Sun, G. W. Liang, Y. Bai, et al. A Hierarchical Intrusion Detection Model for Wireless Sensor Networks, *Information and Control*, Vol. 42, No. 6, pp. 670-676, June, 2013.

[21] J. Tian, H. Gu, Anomaly Detection Combining One-class SVMs and Particle Swarm Optimization Algorithms, *Nonlinear Dynamics*, Vol. 61, No. 1, pp. 303-310, July, 2010.

[22] Z. H. Xiao, Z. G. Chen, X. H. Deng, A Novel Method Based on Clustering Algorithm and SVM for Anomaly Intrusion Detection of Wireless Sensor Networks, *Applied Mechanics & Materials*, Vol. 121-126, pp. 3745-3749, October, 2011.

[23] Y. Maleh, A. Ezzati, Y. Qasmaoui, M. Mobida, A Global Hybrid Intrusion Detection System for Wireless Sensor Networks. *Procedia Computer Science*, Vol. 52, No. 1, pp. 1047-1052, July, 2015.

[24] R. Eberhart, J. Kennedy, A New Optimizer Using Particle Swarm Theory, *Proc of the Sixth International Symposium on Micro Machine and Human Science*, Nagoya, Japan, pp. 39-43, 1995.

[25] T. Li, J. Li, Study on SOM Network Traffic Classification Based on PSO-mixture Kernel Function, *Computer Application and Software*, Vol. 32, No. 11, pp. 117-120, November, 2015.

[26] Z. H. Xiao, *Research on Anomaly Intrusion Detection in Wireless Sensor Networks*, Central South University, 2012.

[27] Z. Bankovic, J. M. Moya, A. Araujo, D. Fraga, J. C. Vallejo, J.-M. de Goyeneche, Distributed Intrusion Detection System for Wireless Sensor Networks Based on a Reputation System Coupled with Kernel Self-organizing Maps, *Integrated Computer Aided Engineering*, Vol. 17, No. 2, pp. 87-102, April, 2010.

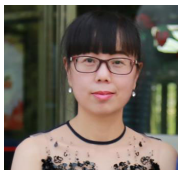
[28] F. Lu, L. J. Wang, Research of Intrusion Detection Based on GA-LMBP Algorithm for Wireless Sensor Network, *Laser Journal*, No. 8, pp. 36-40, August, 2014.

[29] X. F. Huang, G. Z. Liu. The improvement of DEEC Protocol in Wireless Network, *Microcomputer and Application*, Vol. 32, No. 10, pp. 51-53, October, 2013.

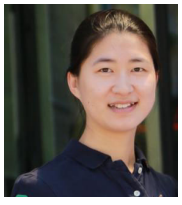
Biographies

Shuang Liu (1988-) received his Master's degree in information and communication engineering from Xinjiang University in 2017. His research interests include intrusion detection of Wireless Senor Network.

Liejun Wang (1975-) received his PhD degree in information and communication engineering from Xi'an Jiaotong University in 2012. He is currently a professor in the college of software of Xinjiang University.His research interests include wireless sensor network and image processing.



Jiwei Qin (1978-) received her PhD degree in computer architecture from Xi'an Jiaotong University in 2013. She is currently a engineer in the Network and Information Technology Center of Xinjiang University. Her research interests include network and information technology.



Yan Guo (1992-) received her MSc degree in science and technology of instrument from Xinjiang University in 2017. Her research interests include encryption certification of Wireless Senor Network.

Hang Zuo (1990-) received his Master's degree in information and communication engineering from Xinjiang University in 2017. His research interests include digital signal processing.