Intrusion detection algorithm based on OCSVM in industrial control system

Wenli Shang¹, Peng Zeng¹*, Ming Wan¹, Lin Li¹,² and Panfeng An¹,²

¹ Industry Control Network and Systems Laboratory, Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang, China
² Shenyang Ligong University, Shenyang, China

ABSTRACT

In order to detect abnormal communication behaviors efficiently in today’s industrial control system, a new intrusion detection algorithm based on One-Class Support Vector Machine (OCSVM) is proposed in this paper. In this algorithm, a normal communication behavior model is established by using OCSVM, and the Particle Swarm Optimization algorithm is designed to optimize OCSVM model parameters. Furthermore, we adopt the normal Modbus function code sequence to train OCSVM model, and then use this model to detect abnormal Modbus TCP traffic. Our simulation results show that the proposed algorithm not only is efficient and reliable but also meets the real-time requirements of anomaly detection in industrial control system. Copyright © 2015 John Wiley & Sons, Ltd.

KEYWORDS
SVM; intrusion detection; PSO

*Correspondence
P. Zeng, Industry Control Network and System Laboratory, Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang, China.
E-mail: zp@sia.cn

1. INTRODUCTION

With the deep integration of informatization and industrialization, the rapid development of Internet technology causes industrial control system to increasingly use the universal protocols, hardware, and software. Many emerging technologies, including embedded, multi-standard network technology, and wireless technology, expand the development space and bring new development opportunities for the traditional industrial control system. However, it also brings security problems into industrial control system. In particular, advanced persistent threat attacks have become a central issue to ensure the nation’s critical infrastructures’ security.

Intrusion detection is an effective method to identify network attacks, and it can give the alarms and defensive measures before or when suffering a great destruction. Intrusion detection methods can be divided into two categories [1]: misuse detection and anomaly detection. Misuse detection, which is also known as signature-based detection or knowledge-based detection, achieves intrusion detection by matching the known abnormal behaviors. Anomaly detection, which is also known as behavior-based detection, identifies the abnormal behaviors through establishing the normal behavior model. Compared with misuse detection, anomaly detection can detect the intrusion behaviors, which are not known before, and it has a lower false negative, but it has a higher false positive.

Anomaly detection technology in industrial control system can be divided into three categories [2–4]: statistics-based method, knowledge-based method, and machine learning-based method. As one of the machine learning-based methods, support vector machine is a new pattern recognition method based on statistical learning theory. It is of great advantage to solve less sample, nonlinear and high-dimensional pattern recognition problems [5]. The traditional support vector machine algorithm, which uses positive and negative samples to train a classification model, is suitable for solving the multi-classification problems. However, the data characteristics of supervisory control and data acquisition (SCADA), distributed control system (DCS), and other industrial control systems are fewer abnormal samples, high dimensions, and strong correlation [6], most of data in industrial control system belong to the normal communication behaviors, and fault or critical state data are fewer. By using less computational time,
One-Class Support Vector Machine (OCSVM) can train anomaly detection model with only one class of samples. Furthermore, OCSVM can build a more accurate model and has the robustness for noise samples. OCSVM has been proved to be an effective machine learning method for intrusion detection in industrial control system.

This paper firstly introduces the corresponding researches on intrusion detection in industrial control system, and analyzes the features of OCSVM. After that, an improved feature vector extraction and data processing method is proposed for anomaly detection of Modbus/TCP industrial communication protocol, and an OCSVM intrusion detection model is established. Finally, we set up a simulation environment and give the experimental results.

2. RELATED WORK

In recent years, OCSVM has been widely used in various fields. M.H. Nguyen [7] proposed a convex energy-based framework to jointly perform feature selection and support vector machine (SVM) parameter learning for linear and non-linear kernels, this method produced SVM classifiers that used sparse sets of features and support vectors while retaining classification performance. S. Agarwala [8] applied Kernel-based machine learning methods to online learning situations, this method satisfied given space and time constraints, thus making it potentially suitable for such online situations. V. Nguyen [9] extended the model of OCSVM to enable efficiently using the negative data samples and proposed two methods to integrate the semi-supervised learning paradigm to the extended model for novelty detection purpose. Y. Liu [10] proposed the OCSVM parameter optimization by using that PSO algorithm, the algorithm can obtain the higher training efficiency and the less training time compared with the traditional grid search element method. Y.S. Choi [11] proposed the LS one-class SVM by reformulating the hyperplane-based standard one-class SVM, the LS one-class SVM can be reduced to a Kernel ridge regression with a single target value if we set the bias in the hyperplane to a predefined target value as in a regression model. W. Kim [12] presented a filtering method of erroneous GPS data about human mobility, and adapted Radial Basis Function (RBF) as kernel function in OCSVM.

The research of intrusion detection based on one-class SVM for traditional TCP/IP network includes the following: O. Ghorbel [13] investigated a novel online one-class classification method by associating the coherence parameters with a least-squares optimization problem, this method required less computational time by online learning and got a good detection result applying to the wireless sensor network. S. Kaplantzis [14] proposed a centralized intrusion detection scheme based on one-class SVM and sliding window. This system can detect black hole attack and selective forwarding attack with high accuracy without depleting the nodes’ energy. Y.C. Xiao [15] proposed two kinds of methods, DFN and DTL, to select Gauss Kernel function for OCSVM, this method can effectively detect different types of faults and improve the accuracy of detection by training OCSVM model. M. Amer [16] designed two kinds of enhanced OCSVM methods for unsupervised anomaly detection to reduce the influence of outliers on normal data boundary decision. G. Kim [17] proposed a new hybrid intrusion detection method which hierarchically integrates a misuse detection model and an anomaly detection model in a decomposition structure. Multiple one-class SVM models were created for the decomposed subsets and better than the conventional methods combined with an unsupervised learning method. P. Winter [18] designed the intrusion detection system based on inductive learning. This system uses OCSVM to train model and regards the network data based on flow model as data source. The innovation is that this system uses malicious attack data to train OCSVM model, rather than normal data. This model can also be used for a plurality of network attack classification. J. Tian [19] proposed a new local density OCSVM by incorporating distance measurements based on local density degree to reflect the distribution of a given data set; the proposed method can achieve better performance than other one class learning schemes.

Typical research works about intrusion detection based on OCSVM in industrial control system are as follows: L. A. Maglaras [20] presented an intrusion detection model, which can detect malicious network traffic in a supervisory control and data acquisition (SCADA) system. The model was trained by the offline network traces and can accurately distinguish a serious warning from a possible attack, and detect anomalies in real time. J.M. Jiang [21] exploited the concept of OCSVM and adaptively controlled its decision parameter to detect unusual patterns from the inputs. This method provided excellent potential ability for further research and development toward practical tools to protect the SCADA systems. T. Onoda and M. Kiuchi [22] applied OCSVM and SVDD to intrusion detection in an experimental control system network, and compared the differences between the classifications; the experiments clarified that sequence information in control system communication was very important to detect some intrusion attacks. Y.G. Zhang [23] designed a SCADA intrusion detection system based on self-learning semi-supervised OCSVM from the perspective of the process; this system can add typical samples into training set to improve the classification performance and reduced false positive and false negative, but its real-time performance was poor.

In industrial control system, anomaly detection method based on “white-list” can effectively detect the abnormal behavior existing in a single communication protocol, but cannot detect the abnormal behavior existing in multiple communication packets simultaneously. However, anomaly detection method based on the communication patterns can remedy these weaknesses. The difficulty of intrusion detection in industrial control system is to collect abnormal samples, and to build anomaly detection model caused by the imbalance of two classes of samples. By improving OCSVM algorithm, this paper builds the normal communication behavior outline for anomaly detection.
3. optimization parameter selection

Based on the traditional support vector machine, OCSVM is developed to resolve the training classification problem, which only has one type of samples. The basic goal of SVM is to construct a generalized optimal hyper-plane and to make the data points expose on both sides of classification surface, which separates two categories of the training data set. Besides, the classification interval should be as large as possible. Similarly, OCSVM assumes the coordinate origin as abnormal sample, and then tries to use a hyper-plane to separate the data in the feature space from the origin with maximum margin. Currently, there are two kinds of OCSVM [24], namely, the Hyper-Sphere method and the Hyper-Plane method. The Hyper-Sphere method proposed by Tax is designed to find a hyper sphere of minimum volume to cover all the training samples, and the Hyper-Plane method proposed by Bernhard Scholkopf in 1999 is designed to find a hyper plane in the feature space that separates training samples from the origin maximum margin. In fact, when using the Gaussian Kernel function, which is shown in (1), these two methods are the same.

\[ K(x_i, x_j) = \Phi(x_i) \Phi(x_j) = \exp\left(-\beta ||x_i - x_j||^2\right) \] (1)

The basic idea is to map the input space into a high-dimensional space by the Kernel function and try to separate samples from the origin in the high dimensional space. By the training data set, OCSVM makes the decision function \( f(x) \). As shown in Figure 1, the result of \( f(x) \) can explain the classification situation: positive is considered as normal class, otherwise is abnormal class.

To separate the data from the origin, we solve quadratic programming problem as follows [25]:

\[
\begin{align*}
\min_{\omega, \rho, \xi} & \quad \frac{1}{2} ||\omega||^2 + \frac{1}{L} \sum_{i=1}^{L} \xi_i - \rho \\
\text{s.t.} & \quad \Phi(x_i)\omega \geq \rho - \xi_i, \xi_i \geq 0,
\end{align*}
\] (2)

where \( x_i \) the sample form is input space, \( L \) is the number of training samples, and \( \Phi \) is the map from input space to feature space. \( \omega \) and \( \rho \) is normal vector and compensation parameters of hyper-plane in feature space, respectively. The adjustable parameter \( \nu \) is used to control the asymptotic fraction of outliers allowed. As a slack variable, \( \xi_i \) allows that some training samples are misclassified. If \( \omega \) and \( \rho \) is the solution of the previous quadratic programming problem, their decision-making function is shown in (4).

\[ f(x) = \text{sgn}(\Phi(x)\omega - \rho) \] (4)

Here, most of the point values in data sets are positive. At the same time, the value of \( ||\rho||^2 \) should be relatively small. Therefore, the parameters \( \nu \) and \( g \) are the key to solve the problem, and this paper will take \( (g, \nu) \) as parameters to optimize.

4. Feature Extraction and Data Preprocessing

Industrial control network is a complex system, which may vary a variety of different communication protocols. Modbus/TCP protocol is an open-communication protocol of industrial control; it extended by international Modbus organization in 2002 and has been widely used in petroleum, chemical, energy, electric power, and other typical industrial control system and SCADA system. In this paper, the Modbus/TCP is chosen as the detection object, and an intrusion detection model is established by using PSO-OCSVM algorithm, in order to expand the application of the algorithm in the industrial control network communication, it will be applied to Profinet, DeviceNet and other industrial communication protocols in the further research.

In order to make Modbus to be suitable for transmission in the TCP/IP network, Modbus/TCP message format extends some data structure on the basis of the Modbus protocol. As shown in Figure 2, the Modbus/TCP packet format [26] mainly includes three parts: MBAP packet header, Modbus function code, and data.

MBAP is Modbus application protocol packet header, and it is used to identify Modbus application data unit. Modbus function code is used to inform the server to operate the corresponding function. Modbus data are used to store transmission data.

The OCSVM algorithm in this paper is designed to detect potential attacks in multiple Modbus data packets; the function code of Modbus protocol is extracted from the communication data, which represents a communication operation.
command, such as functional code 01 for the read coil, function code 03 for read holding registers, and function code 06 to write a single register. A function code of single packet may indicate a normal communication operation; however, the continuous function code sequence of multiple packets can indicate potential attacks. The function code sequence is used as the input feature data of intrusion detection system to detect the abnormal communication behaviors.

The data processed by OCSVM are required to have the same dimensions. In this paper, different numbers of Modbus function code sequences are converted into the vector with the same length on the basis of our previous research [27].

Firstly, set the length of the short sequence $r$ process Modbus function code samples with a sliding window of the length $r$, remove the repeated sequences, and obtain the short sequence set.

Secondly, for any Modbus function code sequence, construct the OCSVM feature vector according to the frequency of each short sequence pattern.

Finally, normalize the obtained vector. Each element in the vector may not belong to the same magnitude, and there are many differences between the input variables. So we should normalize the input vector matrix before building the model.

5. ONE-CLASS SUPPORT VECTOR MACHINE ALGORITHM FOR INTRUSION DETECTION

As mentioned earlier, OCSVM optimization process is a convex constrained quadratic programming problem, namely, “training” or “learning” problem. Lagrange function is introduced as Formula (5).

$$L_{p} = \frac{1}{2} \| \omega \|^2 + \frac{1}{l} \sum_{i=1}^{l} \xi_i - \rho - \sum_{i=1}^{l} \xi_i \beta_i - \sum_{i=1}^{l} (\Phi(x_i)\omega - \rho + \xi_i) a_i$$

(5)

Similar to the traditional SVM, the input samples are mapped into feature space by Kernel function and Lagrangian optimization method, and then dual problem of the original problem is obtained [28], shown as follows:

$$\min_{a_i} LD = \frac{1}{2} \sum_{i=1}^{l} \sum_{j=1}^{l} a_i a_j K(x_i, x_j)$$

s.t. $0 \leq a_i \leq \frac{1}{l}$

(6)

(7)

Because support vectors are on the hyper-plane, we can get $\rho$ from a certain support vector $x_i$ and the corresponding $a_i$ with Formula (8).

$$\rho = \sum_{i=1}^{l} a_i K(x_i, x_j)$$

(8)

Finally, we get a decision function as follows:

$$f(x) = \text{sgn} \left( \sum_{i=1}^{l} a_i K(x_i, x) - \rho \right)$$

(9)

According to the previous analysis, OCSVM algorithm designed in this paper can be described as follows:

Step 1: Get the data to extract the available Modbus function codes and obtain the training samples and test samples.

Step 2: Data preprocessing. Modbus function sequences should be converted to the short sequences, whose length is $r=3$. Then construct the sample data according to the frequency of short sequences.

Step 3: Data normalization. Each element in the vector may not belong to the same magnitude, and there are many differences between the input variables. It may cause that the training time increases and the model cannot converge. So we should normalize the input vector before building the model.

Step 4: Chose the appropriate Kernel function and the parameter $\nu$, construct and solve the optimization problems (6) (7), get the solution $a_i$, get a positive component $a_i$, and calculate $\rho$.

Step 5: Calculate decision function $f(x)$, and build the OCSVM model [29].

In Step 4, the Kernel function and the parameter $\nu$ are related to the classification accuracy of the OCSVM model and its generalization ability. In this paper, Kernel function usually uses the Gauss Kernel function, and we optimize the parameters $g$ and $\nu$ with the PSO (Particle swarm optimization) algorithm.

Particle swarm algorithm (PSO), which stems from the simulation of birds flock’s foraging, is simple, fast convergence, less adjustable parameters, and can be easily applied to optimize the parameters $g$ and $\nu$ of OCSVM. The grid optimization method is based on the partition of the parameter spaces, the finer partition may obtain a better result, but also increases the training time.

A method of PSO to optimize the OCSVM parameters is proposed in [10], which uses the standard global PSO algorithm to update the particle speed, and uses $K$ to control the update rate, the $K$ value is related to learning factor $c_1$ and $c_2$. In this paper, the standard global PSO algorithm is used to optimize the parameters $g$ and $\nu$ by adjusting inertia weights $\omega$ and improve the detection efficiency of intrusion detection system, a larger inertia weight cannot easily fall into the local optimum, and a smaller inertia weight can increase the convergence speed; the method of dynamic adjustment inertia weight can improve the optimization performance of PSO algorithm.

Firstly, we begin with the initial populations and velocities sampled randomly from the feasible space. $k$ is the number of iteration steps (Here, $k=0$ is the initial state), and $D$ is the dimension of the solution space.
Current fitness of the particle is determined by the position vector of the particle, and current individual optimal value and group optimal value are determined by comparing the fitness of each generation. Speed and position of a particle are updated by the following equations [30]:

\[
V^{k+1} = \omega V^k + c_1 r_1 (P^k - X^k) + c_2 r_2 (G^k - X^k) \quad (10)
\]

\[
X^{k+1} = X^k + V^{k+1}, \quad (11)
\]

The first part of Equation (10) is the current velocity of the particles, which reflects that the next generation speed is influenced by the current speed. The second part reflects the cognitive ability of a single particle, and it is used to control the global search ability of the particles and avoids falling into the local optimum. The third part reflects the social cognitive ability of the whole particle swarm, and it represents information interaction between the particles, and it is beneficial to improve global search ability of the particles, where \( c_1 \) and \( c_2 \) is the learning factor, and \( r_1 \) and \( r_2 \) is the acceleration factor in the range [0-1].

In this paper, by using Modbus function codes, we design an anomaly detection model based on PSO–OCSVM. The algorithm process is shown in Figure 3. PSO algorithm is used to optimize the parameters and structures of OCSVM model, so it increases the accuracy of classification model. The optimization algorithm for the parameter \( \nu \) of OCSVM and \( g \) of kernel function based on PSO is described as follows:

Step 1: Set the maximum number of iterations.
Step 2: Initialization. Randomly generate the particle position and particle velocity in the D dimensional space, where \( N \) is the number of particles. \( X_i = (x_{ig}, x_{iv}) \) denotes the particle \( i \), which is constituted by two components, representing the location of the parameter \( g \) of Kernel function and \( \nu \) of OCSVM, respectively. The limited ranges of two components are \([X_{g \text{min}}, X_{g \text{max}}]\) and \([X_{\nu \text{min}}, X_{\nu \text{max}}]\).
Step 3: Calculate fitness of the particles. The particle fitness value select the component \( x_{ig} \) and \( x_{iv} \) as the parameters, and \( \text{Fit}(x) \) is the classification accuracy under the cross-validation based on the Modbus function code sequence.
Step 4: Update the individual and group’s extreme values according to the fitness. If \( \text{Fit}(X_i^{k+1}) > \text{Fit}(X_i^k) \), then \( p^k = X_i^{k+1} \), otherwise, \( p^k = X_i^k \). If \( \text{Fit}(X_j^{k+1}) > \text{Fit}(X_j^k) \) and \( \text{Fit}(X_j^{k+1}) > \text{Fit}(G^k) \), then \( G_j^{k+1} = X_j^{k+1} \), otherwise, \( G_j^{k+1} = G_j^k \).
Step 5: adjusting inertia weight value \( \omega \). According to the function of different weight values, the weight is adjusted by the method of linear decreasing, which can avoid the local optimum and increase the convergence speed.
Step 6: Stop. If the number of iterations exceeds the maximum number of iterations or the change of fitness is less than 0.01% over 50 times, then stop the iteration.
Step 7: Update according to Formulas (10) and (11). Determine whether the position in the specified range \([X_{g \text{min}}, X_{g \text{max}}]\) and \([X_{\nu \text{min}}, X_{\nu \text{max}}]\). If the position is not in the range, the corresponding component needs to be redefined in the range. For example, if \( x_{ig} < x_{g \text{min}} \), then \( x_{ig} = x_{g \text{min}} \). If \( x_{ig} > x_{g \text{max}} \), then \( x_{ig} = x_{g \text{max}} \).

6. EXPERIMENTAL DATA ANALYSIS

In order to verify the proposed intrusion detection algorithm based on PSO–OCSVM in this paper, we set up the simulation environment in our laboratory, and the topological structure is shown in Figure 4.

The experiment simulates the speed control of the motor generator with PLC. In the control unit layer, we adopt Schneider M340 PLC whose CPU is 2020, and it communicates with the host via Modbus/TCP protocol.
In the data-acquisition layer, monitoring interfaces are developed with King SCADA software. In the engineering station, the PLC programming is configured by UnityPro. We simulate the infected site as the attack source, which sends the malicious packets to the important PLC controller and causes the motor speed change to make the field equipment paralysis.

Modbus standard protocol specifies the data communication format and transmission. But actually the control equipment has its own special protocol, including the data communication format and transmission [31]. As shown in Figure 4, when the system is running, the operator captures the Modbus TCP traffic data packets through the “Wireshark” software and removes the packets without Modbus function code. By this, the operator obtains the traffic between Modbus/TCP client and Modbus/TCP server.

Figure 5 shows one of the captured traffic data packets, the packet size is 66 bytes, including networking protocol data, transmission control protocol data, and application layer Modbus protocol data. The Modbus protocol data are used for intrusion detection; it can be seen from the figure that the function code is 3, which specifies the communication operation, and is also the extracted feature.

About 600 Modbus function code sequences are selected after feature extraction in this paper, and the data are preprocessed by libsvm. Here, 500 samples are the training samples, and 100 samples are the test samples. The training samples include +1 class and the test samples include +1 class and −1 class.

In PSO–OCSVM, we set $c_1 = 1.7$ and $c_2 = 1.5$. The population size is 20, and the evolution algebra is 50. Besides, the classification accuracy of OCSVM is obtained by fivefold cross-validation approach. The simulation results are shown in Figure 6.

Figure 6b shows the test sample results, which contains two types of data, +1 and −1 class, the two classes have 500 test data. The different points of two curves in the figure are the error-detection samples, and moreover, we can see that the detection rate is 98%. The training sample results for PSO–OCSVM algorithm is shown in Figure 6c, because the intrusion detection model is established by using OCSVM, the training sample contains only a class of 500 normal data. According to the diagram, the prediction data have some error training results of the −1 class, and the detection rate is 98.8%. In order to illustrate the advantages of PSO–OCSVM in the speed and generalization ability, this paper also designs OCSVM based on the traditional grid parameter optimization, and the advantages of PSO–OCSVM are obviously by comparing with the simulation results.

As seen from Figure 6d and e, for the traditional grid search method, its training sample accuracy is 98.6%, and its test sample accuracy is 94%. The two methods can obtain different optimal results with different set parameters, as shown in Table I, the $g$ and $v$ parameters value optimized by PSO are 0.01 and 0.0165, the value of grid optimization method are 6.7 and 0.16, while the training time and detection accuracy of PSO algorithm are better than grid optimization method, this can show that the $g$ and $v$ optimization parameters of PSO are better results. However, two optimization results may not be the actual best values; it can be seen from the experimental results that the PSO algorithm is easily applied to optimize the parameters and has better detection performance.
The proposed algorithm in this paper not only is compared with the traditional grid optimization method but also is compared with the RBF neural network and BP neural network. The classification experiment of each model is performed 50 times in order to reflect the performance of each model objectively. The statistical data of the key indicators are shown in Table I.

Statistical data on the key indicators are listed in the Table I later: $v_{best}$ is the optimal value of the parameter $v$, $g_{best}$ is the optimal value of the parameter $g$, $Acc_{test}$ is the test set accuracy, $Acc_{train}$ is the training set accuracy, $T_{train}$ is the time that the training set builds a model, whose unit is second, $T_{test}$ is the response time that model predictions of training set, and FP is the false positive rate.
From Table I, the classification ability of PSO–OCSVM model is superior to the traditional grid searching, and the training time is less than the traditional grid searching. The prediction time of PSO–OCSVM algorithm is 0.04125 s, and the modeling time is 25.9363 s. In fact, the number of the grid algorithm called OCSVM is 100*100 = 10 000 times, but the time called PSO–OCSVM is only 20*50 = 1000 times, so the efficiency increases nearly 10 times. What is more, the search parameters is much smaller than the latter, and it means that this model has fewer support vectors, more concise, and stronger generalization ability.

After the comparative analysis of these experiments, it can be seen clearly that One-Class SVM is still able to meet the industrial control systems requirements for real time, reliability, and efficiency, although parameter optimization by PSO increases the computational complexity of the detection algorithm to some extent.

At last, we also build C-SVM to compare with OCSVM through the simulation experiment. The experimental results show that the training samples accuracy of two support vector machine models can reach 100%. For the accuracy of test samples, the two types of models are able to achieve more than 90%, and this fully illustrates SVM’s advantages compared with other models. However, for the accuracy of the test samples, OCSVM is higher than traditional C-SVM, and this shows that OCSVM can overcome the shortcomings of industrial control system that the number of abnormal samples is fewer, dimension is higher and association is stronger, and it is more suitable for practical applications.

In the industrial communication network of Modbus/TCP, both the normal communication behavior and the attack behavior are based on the function code to read and write operations or to perform the corresponding command, the different attacks are performed by using Modbus commands, such as reading the device information, to rewrite the system key data, control the main station and equipment, etc. In this paper, we study intrusion detection for abnormal behavior according to function code sequence, through the abnormal value of the function code sequence of multiple data packets, the potential abnormal attack behavior is detected, and the communication data which is not in accordance with the normal function code sequence belongs to abnormal behavior data. For example, an attack behavior of reading the control information may appears a sequence of three continuous 01 function codes, which does not conform to the conventional read coil behavior and can be used to detect potential attack.

The function code 05 specifies the communication operation to write a coil value, the function code 06 is to write a register, and the function code 16 is to write multiple registers, a single function code is expressed as normal writing information behavior; however, a continuous function code sequence of 05, 06, and 16 is not a normal communication mode, which may contain a potential attack of rewriting the system key data. By using the function code sequence as input feature data, the intrusion detection system is established according to OCSVM algorithm, which can detect the potential attack in multiple packets and has a better detection performance.

### 7. CONCLUSION

According to the characteristics of industrial control system, which may have fewer abnormal data, high dimension, strong relationship, and so on, a PSO–OCSVM model with particle swarm algorithm for parameter optimization is designed in this paper. The algorithm trains the anomaly detection model with only one class of samples for the anomaly detection of communication pattern. This paper confirms that OCSVM in intrusion detection fields have many advantages, including fast and strong generalization ability, the less support vector, the simple model, and the great practical value.

Only the vector of Modbus function code is processed in this paper, not all data. This may affect the reliability of intrusion detection in a certain extent. In the further research, we will expand the related work about dimension reduction and real-time intrusion detection, and make intrusion detection model more accurate, reliable, and practical.

### ACKNOWLEDGEMENTS

This work is supported by the National Natural Science Foundation of China (Grant No. 61501447) and Independent project of Key Laboratory of Networked Control System Chinese Academy of Sciences: Research on abnormal behavior modeling, online intrusion detection and self-learning method in industrial control network. The authors would also like to acknowledge the helpful comments and suggestions of the industry control system security software group. Their efforts are greatly appreciated.

### REFERENCES


29. Maglaras LA, Jiang J, Cruz T. Integrated OCSVM mechanism for intrusion detection in SCADA systems. 
