mathematics

MDPI

Article

Research on Attack Detection of Cyber Physical Systems Based on Improved Support Vector Machine

Fengchun Liu [1,2,3,4,5], Sen Zhang [1,2,3,4,5], Weining Ma [1,2,3,4,6] and Jingguo Qu [1,2,3,4,5,*]

[1] Hebei Engineering Research Center for the Intelligentization of Iron Ore Optimization and Ironmaking Raw Materials Preparation Processes, North China University of Science and Technology, Tangshan 063210, China; lnobliu@ncst.edu.cn (F.L.); zhangsen@stu.ncst.edu.cn (S.Z.); mwn@ncst.edu.cn (W.M.)
[2] Hebei Key Laboratory of Data Science and Application, North China University of Science and Technology, Tangshan 063210, China
[3] Tangshan Intelligent Industry and Image Processing Technology Innovation Center, North China University of Science and Technology, Tangshan 063210, China
[4] The Key Laboratory of Engineering Computing in Tangshan City, North China University of Science and Technology, Tangshan 063210, China
[5] College of Science, North China University of Science and Technology, Tangshan 063210, China
[6] College of Metallurgy and Energy, North China University of Science and Technology, Tangshan 063210, China
* Correspondence: qujingguo@ncst.edu.cn

Abstract: Cyber physical systems (CPS), in the event of a cyber attack, can have a serious impact on the operating physical equipment. In order to improve the attack detection capability of CPS, an support vector machine (SVM) attacks detection model based on particle swarm optimization (PSO) is proposed. First, the box plot anomaly detection method is used to detect the characteristic variables, and the characteristic variables with abnormal distribution are discretized. Secondly, the number of attack samples was increased by the SMOTE method to solve the problem of data imbalance, and the linear combination of characteristic variables was performed on the high-dimensional CPS network traffic data using principal component analysis (PCA). Then, the penalty coefficient and the hyperparameter of the kernel function in the SVM model are optimized by the PSO algorithm. Finally, Experiments on attack detection of CPS network traffic data show that the proposed model can detect different types of attack data and has higher detection accuracy compared with general detection models.

Keywords: attack detection; cyber physical systems; data imbalance; principal component analysis; particle swarm optimization; support vector machine

MSC: 68T09; 94A16

Citation: Liu, F.; Zhang, S.; Ma, W.; Qu, J. Research on Attack Detection of Cyber Physical Systems Based on Improved Support Vector Machine. *Mathematics* **2022**, *10*, 2713. https://doi.org/10.3390/math10152713

Academic Editor: Matjaz Perc

Received: 21 June 2022
Accepted: 27 July 2022
Published: 1 August 2022

1. Introduction

CPS realizes the collaboration and integration of information systems and physical systems [1], and has been widely used in the fields of power distribution, pipeline transportation, and intelligent production [2–4]. CPS improves production quality and efficiency while also exposing security issues, the communication network as a bridge between information systems and physical systems is the key to system security. The attack detection of a communication network can effectively maintain the security of the CPS system, but it is necessary to consider the characteristics of the CPS to set up targeted attack detection methods. The continuous operation of the CPS generates a large amount of network traffic data, which can interfere with attack detection and increase computational overhead.

CPS network traffic data suffer from high dimensionality and information redundancy, which can reduce the efficiency of attack detection. Martin-Barreiro et al. mention that PCA as a popular multivariate statistical method to reduce the dimensionality of the data

matrix [5]. Zhang et al. mention that machine learning models based on hypergraph theory can represent the information in the network as low-dimensional dense real vectors, which can be effective for anomaly and attack detection [6]. Gao et al. proposed an anomaly detection model of network traffic sequences, using PCA to reduce the dimensionality of network traffic characteristic variables, then establishing an LSTM neural network to detect anomalies in traffic sequences [7]. The network traffic data generated by the CPS in real time include normal request and response data, and contain anomalous data that are under attack. There is an imbalance problem in the number of normal samples and abnormal samples [8], which causes the attack detection models to be unable to effectively extract the information of the attack samples. The common solutions to the data imbalance problem encountered in classification problems are undersampling and oversampling and combined sampling, these methods can balance the number of samples between different categories [9]. Deng et al. investigated the problem of attack detection in CPS systems and solved the problem of data imbalance by using an adversarial network to expand the rare attack samples, and verified the effectiveness of the method through experiments [10].

With the increasing openness of CPS access to the network, the diversity and concealment of cyber attacks increase the difficulty of attack detection. Ding et al. studied CPS systems from the perspective of control theory; summarized the modeling approach of CPS and the common types of network attacks as denial-of-service attacks, replay attacks and spoofing attacks; and detected network attacks by establishing a reasonable system state estimator [11]. The SVM model, as a machine learning model with a complete mathematical theory, has a wide range of applications in classification problems [12], and compared with other machine learning models, SVM has better pattern recognition in complex data sets [13]. The process data generated in real time in CPS networks have a complex structure and noise, the characteristics of the SVM model whether the model is suitable for solving the problem of identifying abnormal behavior patterns in CPS process data. PSO is an optimization algorithm driven by the intelligent population behavior of animals [14]. The PSO algorithm has the ability to quickly find the global optimal solution. Using the PSO algorithm to optimize the SVM classifier can improve the accuracy of detection, suitable for the attack detection scenario of CPS network traffic. Chen et al. investigate the problem of network intrusion detection in industrial control systems and establish a neural network model with PSO for effective detection of unknown types of abnormal traffic data [15]. Shang et al. analyzed the characteristics of network data based on Modbus industrial communication protocol and used an improved SVM model optimized by PSO to detect anomalies in the data, and the experimental results show the validity of the method [16]. Current research related to CPS network attack detection focuses on the analysis of network traffic data or on the optimization and design of detection models but, in fact, these two parts have equal importance.

Therefore, in this paper, when studying the attack detection problem of the CPS system, both the characteristics of network traffic data and the accuracy of the detection model are considered to establish the PSO-SVM attack detection model. In the rest of the paper, Section 2 investigates the composition structure of CPS, then the network characteristics of CPS are analyzed and compared with the traditional IT internet, and the attack principles of common attack types are analyzed. Section 3 describes the principle of processing CPS network traffic data and the principle of PSO-SVM model, and illustrates the flow of the model. Section 4 experiments on the proposed method using real CPS network traffic data, and shows the specific process and results of the experiments. Section 5 discusses the conclusions of this study and future research.

2. CPS Structure and Attack Detection

2.1. CPS Structure

The CPS composition structure can be divided into three levels from the functional point of view: sensing layer, network layer, and control layer [17], and the composition structure of CPS is shown in Figure 1.

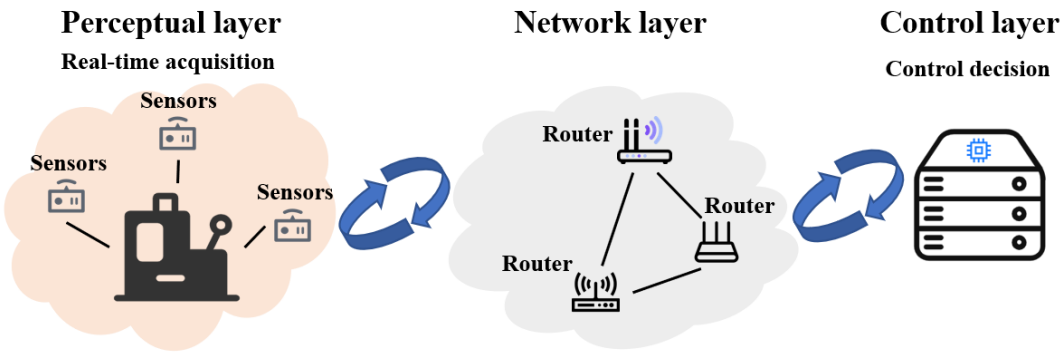

Figure 1. CPS system structure.

As shown in Figure 1, the sensing layer is the source of real-time status data of the CPS system, converting real-time status information of physical objects into digital information through various types of sensors or signal acquisition devices arranged on the physical devices. The control layer enables the CPS system to have intelligent control and decision-making capabilities, generating control commands that regulate the operational status of the CPS physical equipment through analysis and the computational processing of state data. The network layer is the bridge between the physical system and the information system, allowing real-time sent status data and control commands to be transmitted in both directions between the perceptual layer and control layer.

2.2. CPS Network

The CPS network layer is the basis for the proper operation of the CPS. The structure of the CPS network determines some differences between the CPS network and the traditional IT internet (see Table 1).

Table 1. Comparison of CPS network and traditional IT network.

Network Type	Network Structure	Type of Data to Be Transferred	Communication Protocol
CPS Network	Closed-loop network structure	Status data and control data	Industrial communication protocols
IT Internet	Many-to-one network structure	Information Data	TCP/UDP

As shown in Table 1, the CPS system uses a closed-loop network structure, and the CPS generates a large amount of high-dimensional state data as well as control command data in real time during continuous operation. Thus, the CPS network has high requirements for real time and reliability, and the diversity of the physical devices in the CPS leads to the diversity of industrial communication protocols used, and the commonly used industrial communication protocols are CANopen, EtherNet, PROFIBUS, etc. [18]. IT internet mostly uses a many-to-one client/server architecture. The function of IT internet is based on the transmission of information data (including text, language, images, video, and other information data), which has a certain tolerance for delay and allows packet retransmission after a transmission failure. In order to easily allow various communication devices to access the interconnection network for communication, the standard TCP/UDP network communication protocol is used.

2.3. CPS Attack Detection

Considering the structure and characteristics of the CPS network, attacks against the CPS network layer can seriously threaten the security of the operation of physical devices in the system. Network attacks can be divided into three categories according to the attack principle (see Table 2).

Table 2. Types of network attacks and attack principles.

Type of Attack	Attack Principle
Denial of service attacks	Sending a large number of invalid packets to the sensor channel and control channel of the CPS in a short period of time [19], resulting in the inability to respond to normal request packets and delaying or even suspending the operation of the physical device.
Replay attacks	Randomly selected packets from the packet sequence of the previous period are sent to the target device [20], disrupting the normal packet sending process and disrupting the normal operation of the physical device.
False injection attacks	Send disguised packets to the target device to enable the attacker to control the operation of the target device or obtain information of the CPS system [21,22].

As shown in Table 2, the detection of network attacks in traditional IT internet has been more thoroughly studied. The attack detection of the CPS network needs to maintain the security of the CPS network traffic and the stability of the system operation, and timely detection of abnormalities in the CPS network.

3. CPS Network Attack Detection Model

3.1. Data Pre-Processing

CPS network traffic data set $\{X_1, X_2, \cdots X_n\}$, n is the dimension of the characteristic variable. Since abnormally distributed characteristic variables can reduce the detection accuracy of the classifier, the statistical information of characteristic variables can be analyzed to understand the data distribution characteristics of each feature variable, so that characteristic variables with abnormal data distribution can be found and processed. The box plot anomaly detection method is used to discretize the characteristic variables with abnormal data distribution (as shown in Equations (1) and (2)).

$$\text{upper limit} = Q_3 + 1.5 \times (Q_3 - Q_1) \tag{1}$$

$$\text{lower limit} = Q_1 - 1.5 \times (Q_3 - Q_1) \tag{2}$$

Q_3 represents the upper quartile, while Q_1 represents the lower quartile. The sample data of the characteristic variable are coded as 0 if they are between the upper limit and lower limit, and coded as 1 if the sample data are less than the lower limit or greater than the upper limit.

Different units of each characteristic variable lead to non-comparability, which reduces the information extraction ability of the model during the training process. The normalization method can eliminate the difference in magnitude between characteristic variables (Equation (3)).

$$X_i = \frac{x_j - x_{\min}}{x_{\max} - x_{\min}} \tag{3}$$

$j \in \{1, 2, \cdots m\}$, $i \in \{1, 2, \cdots n\}$. m is the number of samples, and n is the dimensionality of the characteristic variables.

3.2. SMOTE Algorithm

The SMOTE algorithm is a method for oversampling a few sample types to solve the data imbalance problem. Synthesis of new samples is achieved by calculating the Euclidean distance between a small number of classes of samples and performing a linear interpolation operation between the samples and their k nearest neighbors [23]. The SMOTE

algorithm can avoid to some extent the overfitting problem of the classifier model during the training process caused by random oversampling.

3.3. PCA Algorithm

PCA is a multivariate statistical analysis method that analyzes the main characteristics of things [24]. The number of samples increases after SMOTE processing, which increases the computational overhead of the model training process. By linearly combining the characteristic variables to generate mutually orthogonal principal component variables, the data can be compressed to reduce the input of the classification model to improve the training efficiency while maximizing the retention of characteristic information. The calculation steps of the PCA are as follows:

1. The preprocessed data set is $\{X_1, X_2, \ldots, X_n\}$, n is the number of characteristic variables, $X_i = \{x_1, x_2, \ldots x_m\}$, m is the number of samples. Each characteristic variable is normalized $X_i = \frac{X_i - \text{mean}(X_i)}{\text{var}(X_i)}$.
2. Compute the covariance matrix $C = X^T \times X$, with T denoting the transpose of the matrix, to obtain an n-dimensional square matrix. Solve the equation $C \times \beta = \lambda\beta$ for the covariance matrix C to obtain the set of eigenvalues $\{\lambda_1, \lambda_2, \cdots, \lambda_n\}$, $(\lambda_i > \lambda_{i+1}$, $i = 1, 2, \cdots, n-1)$ and the corresponding set of eigenvectors $\{\beta_1, \beta_2, \cdots, \beta_n\}$.
3. The characteristic contribution rate of β_i is expressed as $\frac{\lambda_i}{\sum_{j=1}^{n} \lambda_j}$, and the threshold value of cumulative characteristic contribution rate is set as K. The characteristic vector set $\{\beta_1, \beta_2, \cdots, \beta_n\}$ is accumulated sequentially from the characteristic contribution rate of β_1, and the calculation stops when it is greater than or equal to K, and the subset $\{\beta_1, \beta_2, \cdots, \beta_l\}$ $(l \leq n)$ of the characteristic vector set is obtained. Compute $X \times [\beta_1\ \beta_2\ \cdots\ \beta_l]$ to get the dataset $\{PCA_1, PCA_2, \cdots, PCA_l\}$ after principal component analysis, and the dimensionality of dataset is $m \times l$.

3.4. PSO-SVM Attack Detection Model

The SVM model achieves classification by finding the decision boundary with maximum intervals between samples of different categories [25]. When there are a few outlier data will affect the decision boundary of SVM, slack variables can ignore the influence of a few outlier data, which can improve the fault tolerance of SVM model. The penalty coefficient c is used as a hyperparameter to measure the loss caused by ignoring outliers, so the selection of the penalty coefficient c can affect the accuracy of the SVM model. Many practical problems are not linearly separable, so it is difficult to find decision boundaries. Introducing kernel functions in the SVM model can map the data to a high-dimensional space and solve the problem by finding the decision boundary with the maximum interval in the high-dimensional space. RBF kernel function (Equation (4)) in which x_i and x_j are the sample vectors in the training set, $i = 1, 2, \ldots, k$, $j = 1, 2, \ldots, k$, $i \neq j$, k is the total number of samples in the train set. σ is the hyperparameter of the RBF kernel function, reflecting the range of action of the kernel function, when σ decreases the range of action of the kernel function increases. The RBF kernel function has fewer parameters, simple structure and less computational complexity, which is suitable for fast detection of network traffic. The values of penalty coefficient c and hyperparameter σ of RBF kernel function will directly affect the classification accuracy of the model. Using PSO algorithm to determine penalty coefficient c and hyperparameter σ can improve the classification accuracy of SVM model.

$$K(x_i, x_j) = \exp\left(-\frac{1}{2\sigma^2}||x_i - x_j||^2\right) \tag{4}$$

PSO achieves the objective of finding the optimal solution of the objective function in the problem space by simulating the changes in the position and flight speed of a flock of birds in nature during the feeding process. Let the number of particle swarm be m, and the particle swarm can be represented by the formula $P = \{p_1, p_2 \ldots, p_m\}$. The current position

of individual p_i ($i \in m$) can be represented by the formula $\{x_{i1}, x_{i2}, \ldots x_{in}\}$, and the current velocity can be represented by the formula $\{v_{i1}, v_{i2}, \ldots v_{in}\}$ (n represents the dimensionality of the optimization problem solution). The search effect of the particle swarm in the problem space is evaluated by the fitness value, and the velocity and position of the particles are updated according to the value of the fitness function (shown in Equations (5) and (6)). The position vector corresponding to the historical optimal fitness value of individual p_i in the search process is $p_i^{best} = \{X_{i1}, X_{i2}, \ldots, X_{im}\}$. An individual p_{global}^{best} with the global optimal fitness value is selected from the historical optimal fitness values of all individuals p_i^{best} ($i \in m$), and the corresponding position vector is the global optimal solution vector $\{X_{g1}, X_{g2}, \ldots, X_{gm}\}$.

$$v_{ij}^{t+1} = \omega v_{ij}^{t} + c_1 r_1 (X_{ij}^{t} - x_{ij}^{t}) + c_2 r_2 (X_{gj}^{t} - x_{ij}^{t}) \tag{5}$$

$$x_{ij}^{t+1} = x_{ij}^{t} + v_{ij}^{t+1} \tag{6}$$

v_{ij}^{t+1} and x_{ij}^{t+1} are the velocity and position of individual p_i at the next moment (or the next iteration); $i \in m$, $j \in n$; ω are inertia weights; c_1 and c_2 are learning factors; r_1 and r_2 are random numbers between 0 and 1; X_{ij}^{t} is the constituent element of the position vector corresponding to the current p_i^{best}; X_{gj}^{t} is the constituent element of the position vector corresponding to the current p_{global}^{best} [26].

3.5. CPS Attack Detection Flowchart

The CPS attack detection process is shown in Figure 2.

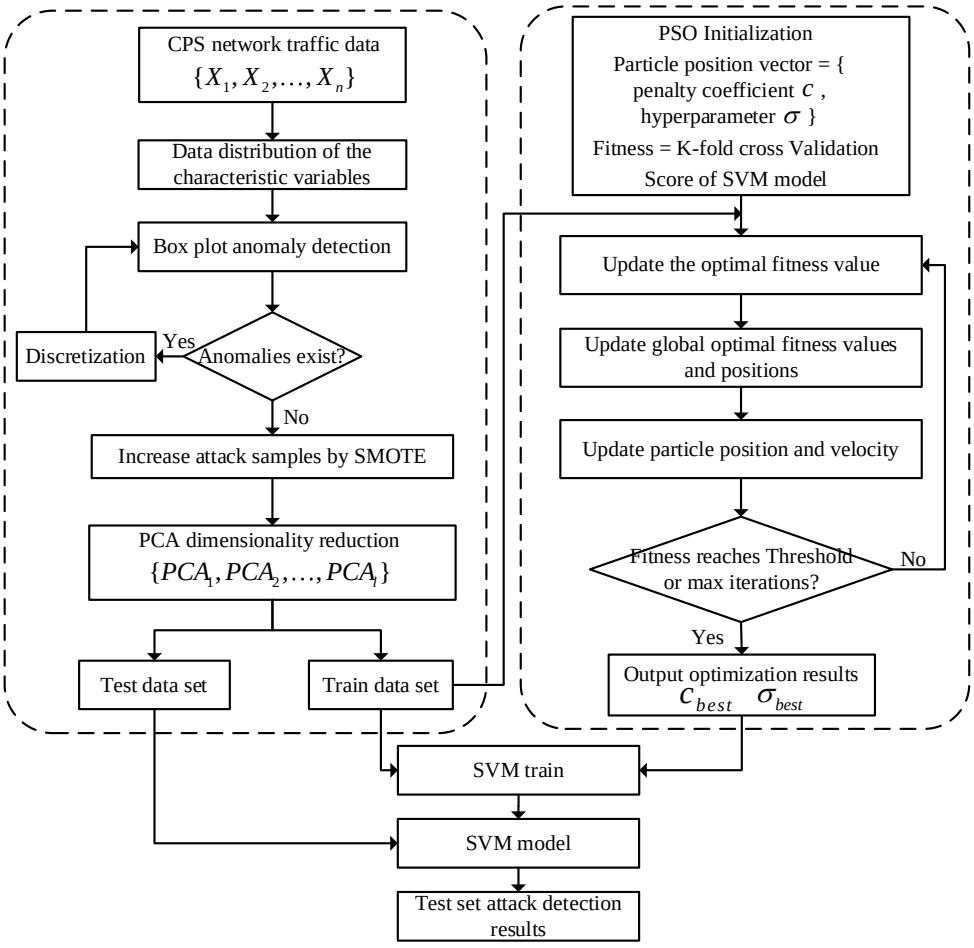

Figure 2. CPS attack detection flow chart.

As shown in Figure 2, the statistical information of the characteristic variables in the original dataset is analyzed. The characteristic variables with abnormal data distribution are discretized using the box plot anomaly detection method; the characteristic variables with normal data distribution are normalized. A small number of samples with attack types are augmented using the SMOTE algorithm, and the dataset is divided into a training set and a test set. The penalty coefficient c and the hyperparameter σ of the RBF kernel function are searched for using the PSO algorithm on the training set. The obtained globally optimal penalty coefficient c_{best}, hyperparameter σ_{best} and the data from the test set are input to the SVM model for attack detection.

4. Experiment and Analysis

The experiments in this paper were conducted on a computer with a Windows 11 operating system, AMD Ryzen 7 5800H CPU and 16.0 GB RAM. In terms of software, Anaconda 3 was used to build the Python programming environment, and Pycharm was used as the IDE.

4.1. Data Set

This paper uses network communication data collected in a natural gas pipeline control system established by Mississippi State University as the experimental data set [27]. The natural gas pipeline system collects the status data of the pipeline through sensors in real time and sends the data packets to the controller using the Modbus industrial data transmission protocol communication network, which calculates and generates control command packets based on the status data received at the current moment and sends them to the actuators for pipeline regulation through the network. The natural gas pipeline industrial control system dataset has 26 dimensions of characteristic variables and eight types of data (see Table 3).

Table 3. Data types included in the dataset.

Status Type	Abbreviations
Normal	Normal
Naïve Malicious Response Injection	NMRI
Complex Malicious Response Injection	CMRI
Malicious State Command Injection	MSCI
Malicious Parameter Command Injection	MPCI
Malicious Function Code Injection	MFCI
Denial of Service	DoS
Reconnaissance	Recon

As shown in Table 3, Normal type is the normal process data of the system; NMRI, CMRI, MSCI, MPCI, and MFCI are false injection attacks; Recon is a reconnaissance attack, and DoS is a denial of service attack. The distribution of the number of samples of each type is shown in Figure 3.

As shown in Figure 3, the above dataset contains 97,019 samples, which are about natural gas pipeline control system. However, the dataset has two serious unbalanced problems. The first problem is the imbalance between samples with normal type and samples with abnormal type. Another problem is the imbalance among samples with abnormal type, the ratio of the number of samples of CMRI type and MFCI type is 27:1. The data imbalance problem will cause the intelligent model or algorithm to be unable to effectively mine the characteristic information of a small number of sample types, resulting in the attack detection results favoring the majority of sample types.

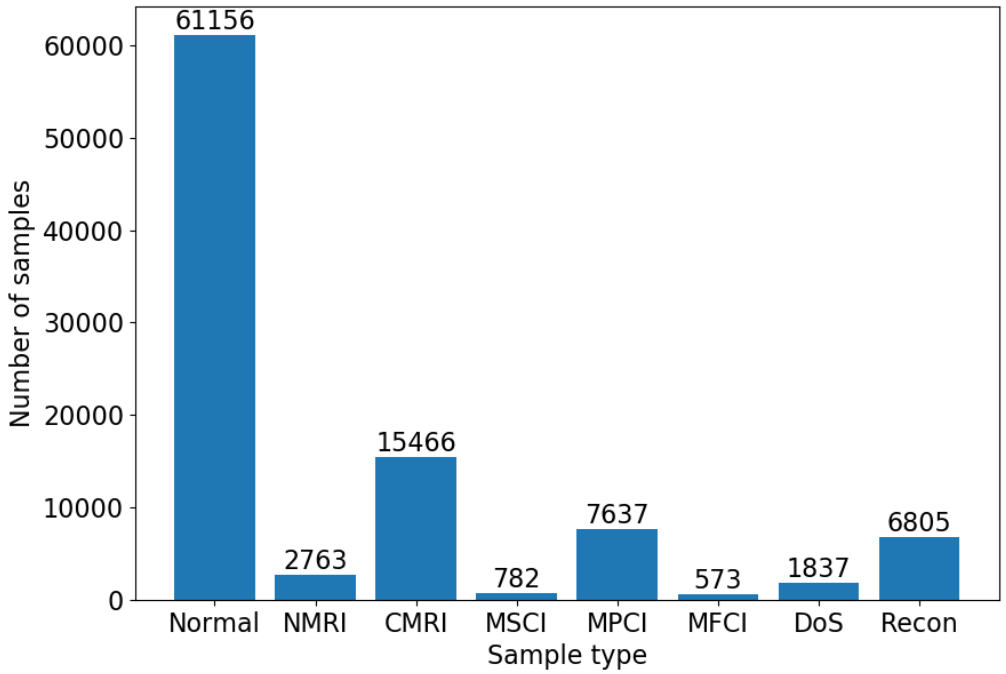

Figure 3. Distribution of the number of samples in each category.

4.2. Dataset Pre-Processing

The statistical information of the dataset reflects the basic nature of the characteristic variables, and the statistical information of the natural gas pipeline control system dataset is shown in Table 4.

Table 4. Statistical information of the data set.

Variables	Average Value	Standard Deviation	Lower Quartile	Upper Quartile
X_1	4.6	9.0	4.0	4.0
X_2	3.7	1.0	4.0	4.0
X_3	182.9	3.7	183.0	183.0
X_4	216.7	59.5	233.0	233.0
X_5	9.0	0.3	9.0	9.0
X_6	16.7	4.6	18.0	18.0
X_7	3.0	0.7	3.0	3.0
X_8	10.0	0.0	10.0	10.0
X_9	2.5	0.9	1.0	1.0
X_{10}	9.3	2.6	10.0	10.0
X_{11}	0.0	0.2	0.0	0.0
X_{12}	41.0	0.0	41.0	41.0
X_{13}	26.3	26.6	19.0	19.0
X_{14}	115.0	0.0	115.0	115.0
X_{15}	0.2	0.0	0.2	0.2
X_{16}	0.5	0.0	0.5	0.5
X_{17}	1.0	0.0	1.0	1.0
X_{18}	0.0	0.0	0.0	0.0
X_{19}	24.2	14.3	20.0	20.0
X_{20}	0.9	1.0	0.0	2.0
X_{21}	1.0	0.1	1.0	1.0
X_{22}	0.1	0.2	0.0	0.0
X_{23}	0.0	0.2	0.0	0.0
X_{24}	0.0	0.0	0.0	0.0
X_{25}	-2.8×10^{34}	1.8×10^{36}	0.2	5.3
X_{26}	1.1	0.1	1.1	1.1

From Table 4, it can be seen that characteristic variables with standard deviation of 0 do not contain valid characteristic information, so removing the characteristic variables X_8, X_{12}, X_{14}, X_{15}, X_{16}, X_{17}, X_{18}, X_{24}. The variance of characteristic variables X_1, X_{11}, X_{22}, X_{23}, X_{25} is significantly larger than the mean, which does not obey the normal distribution. The upper quartile and lower quartile of the characteristic variables are approximate, which means most of the data values of the characteristic variables are more concentrated. If directly input to the detection model is not conducive to training, and discarding the characteristic variable will reduce the training effect of the model. According to the box plot anomaly detection method using Equations (1) and (2) for discretization, the characteristic variable X_i ($i = 1, 11, 22, 23, 25$) is coded as 0 when the value of the sample data is between upper limit and lower limit, and as 1 when the value of the sample data is less than lower limit or greater than upper limit.

4.3. Sample Amplification and Dimensionality Reduction

There is an imbalance in the number of normal samples and attack samples during the continuous operation of the industrial control system, and there is also a serious imbalance in the number of samples between the types of attacks. The imbalance in the number of samples of each type will lead to the classifier not being able to effectively extract the characteristic information of a few classes of samples during the training process, resulting in training process being determined by a larger number of sample types, which directly affects the attack detection accuracy of the model. Therefore, the SMOTE algorithm is used to augment the attack types with a small number of samples, and the number of samples of each type in the dataset after the augmentation of the attack samples is shown in Table 5.

Table 5. Data set after amplification of attack type samples.

Status Type	Number of Samples after Amplification	Total
Normal	61,156	61,156
NMRI	7637	
CMRI	15,466	
MSCI	7637	
MPCI	7637	61,288
MFCI	7637	
DoS	7637	
Recon	7637	

From Table 5, we can see that the number of normal type samples is 61,156, and the total number of attack type samples after augmentation is 61,288, and the total number of attack type samples is close to the total number of normal samples, which basically eliminates the serious data imbalance problem between various types of samples.

Although balancing the number of various types of samples can improve the detection accuracy of the model, on the other hand, it is also important to consider the overhead of reducing the computational time complexity caused by the high dimensionality and redundancy of the characteristic variables. Therefore, using principal component analysis to reduce the linear combination of characteristic variables to 13 principal component variables can reduce the input dimension of the model, which in turn reduces the training time and improves the detection efficiency. The importance of the raw characteristic variables for the principal component variables was also analyzed, and the frequency distribution of the raw characteristic variables that make up the principal component variables is shown in Figure 4.

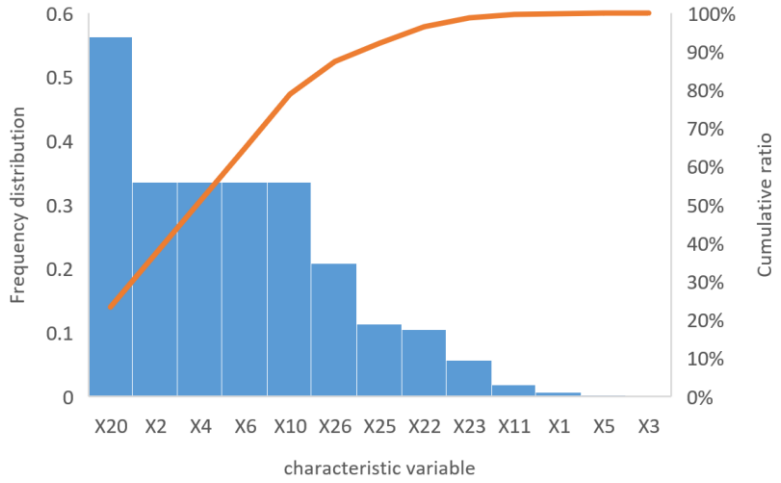

Figure 4. Frequency distribution of the original variables in PCA.

Observing Figure 4, it can be seen that the frequency distribution of the original characteristic variables is arranged in descending order, with the cumulative line located on the sub-axis marking the percentage of the total. Among them, X_{20} is the most important Variables, and the cumulative ratio of X_{20}, X_2, X_4, X_6, and X_{10} reaches 80% are the important factors that make up the principal component variables and reflect most of the information of the data set.

4.4. PSO-SVM Attack Detection

In order to make the various types of samples get sufficient training, the various types of samples are divided in the ratio of 3:1 and then combined to form the training set and the test set to avoid the situation that a certain type of samples are lost in the training set or the number of samples of a certain type is less than the samples of other types. Then the training set is disrupted to avoid overfitting. The number of samples in the delimited training set is 85,710 and the number of samples in the test set is 36,734.

The PSO algorithm is able to find the global optimal values of the hyperparameters of the RBF kernel function in the SVM model. In the process of finding the global optimal penalty coefficient c, hyperparameter σ, the fitness value of the PSO algorithm is the cross-validation score of the SVM model on the training data set when c and σ take different values. The process of the fitness value change is shown in Figure 5.

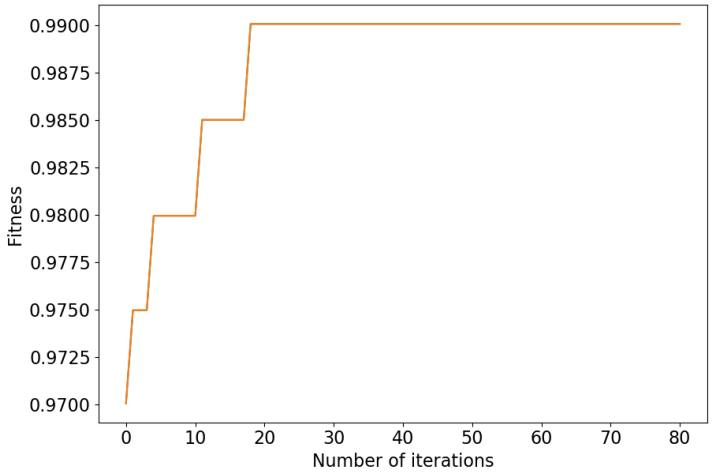

Figure 5. The fitness value of the PSO algorithm.

As shown in Figure 5, the fitness value has reached a relatively high level before the 20th iteration, indicating that the PSO algorithm has the capability of fast optimization search. The global optimal penalty coefficient c_{best} and hyperparameter σ_{best} are used as hyperparameters of the SVM, and the attack detection results obtained by using the test set as input to the SVM model are shown in Figure 6.

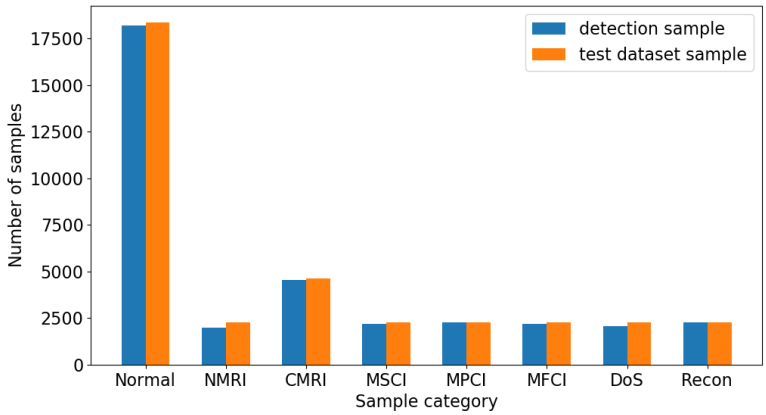

Figure 6. Detection results on the test set.

As shown in Figure 6, the PSO-SVM model has achieved good results for the detection of normal and attack samples, where the detection of various types of attack samples has also achieved good results.

4.5. Analysis and Comparison of Experimental Results

To further analyze the results, an confusion matrix is used to evaluate the attack detection results, and the confusion matrix for the test set attack detection is shown in Figure 7.

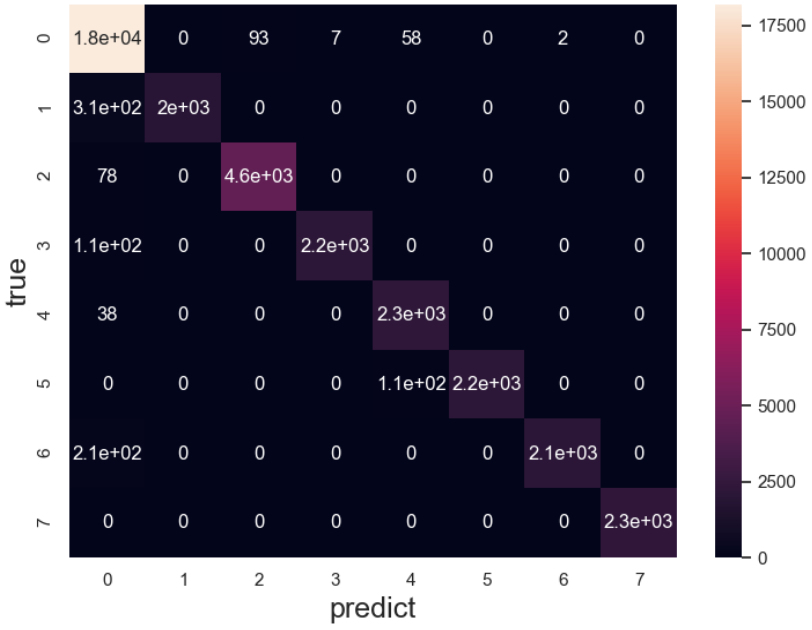

Figure 7. Confusion matrix of the test set.

From the confusion matrix of the detection results in Figure 7, it can be seen that the detection results are concentrated on the diagonal of the confusion matrix, and the detection results are less located on both sides of the diagonal, indicating that the overall

detection effect of the PSO-SVM model is good. To quantitatively measure the detection performance, Accuracy, Precision, Recall and F-Scores evaluation metrics are calculated based on the confusion matrix (Table 6).

Table 6. Evaluation indicators of attack detection results.

Sample Category	Precision (%)	Recall (%)	F-Scores (%)	Accuracy (%)
Normal	96.04	99.13	97.56	
NMRI	100.00	86.29	92.64	
CMRI	98.00	98.32	98.16	
MSCI	99.68	95.33	97.46	97.22
MPCI	92.91	98.34	95.55	
MFCI	100.00	95.02	97.45	
DoS	99.90	90.75	95.11	
Recon	100.00	100.00	100.00	
Average value	98.32	95.40	96.74	

As shown in Table 6, good detection results were achieved for each type of sample on the test set. The accuracy rate was 97.22%, and the average of the precision for all types was 98.32%, including 100% for NMRI, MFCI, and Recon. Compared with the recall rate of different types of test results, the recall rate of NMRI type was lower at 86.29%, and the average of F-Scores was 96.74%. In order to further evaluate the performance of the model, the model in this paper was compared with other algorithmic models for experiments, and the results are shown in Table 7.

Table 7. Comparison of model experiments.

Models	Accuracy (%)	Precision (%)	Recall (%)	F-Scores (%)
Model of this paper	97.22	98.32	95.40	96.74
PCA-SVM	94.61	85.14	80.86	82.41
PCA-BP	93.81	84.90	72.48	75.91
PCA-Gaussian NB	67.82	74.53	88.40	70.52

As shown in Table 7, the F-Scores of the PCA treated plain Bayesian classification model is 70.52%, indicating that the classification performance of the classifier is limited. The PCA-BP model outperforms the plain Bayesian model in each evaluation index, with F-Scores of 75.91%, indicating that the classification effect is still limited. The evaluation indexes of PCA-SVM model are better than PCA-BP model overall, while each evaluation index of this paper's model is better than PCA-SVM model, among which the F-Scores index reaches 96.74%, indicating that the classification effect of this paper's model is better than SVM model, BP model and Bayesian probability model on the test set.

5. Conclusions, Discussion and Future Research

This paper mainly studies the network attack detection model of CPS system. First, the model analyzes the statistical information of the CPS network traffic data and discretizes the characteristic variables with abnormal data distribution using the box plot anomaly detection method. Second, A small number of types of attack samples are augmented using the SMOTE method. The PCA method reduces the dimensionality of the network traffic dataset and analyzes the importance of characteristic variables. Then, the detection model uses an SVM model with RBF kernel function, the penalty coefficient of SVM model and the hyperparameter of the RBF kernel function are optimized using the PSO algorithm. Finally, experiments show that the method proposed in this paper can effectively distinguish network attack data from normal communication data, and has good detection effect on different types of network attacks as well. The method proposed in this study is able to perform attack detection on the network of CPS to protect the information security and system operation safety, which has practical application value, thus providing a reference

for the security protection of the CPS system. Since the system structure of CPS determines a high requirement for real time network communication, future research could introduce incremental learning based on the method in this paper, which can achieve online network attack detection and improve the real time performance of detection.

Author Contributions: Conceptualization, F.L.; Formal analysis, S.Z.; Investigation, S.Z.; Methodology, F.L.; Project administration, S.Z.; Supervision, J.Q.; Validation, W.M.; Writing—original draft, S.Z.; Writing—review & editing, W.M. and J.Q. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by North China University of Science and Technology Basic Research Business Funds for Provincial Universities, grant number JST2022001.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Li, R.; Xie, Y.; Li, R.; Li, L. Survey of cyber-physical systems. *J. Comput. Res. Dev.* **2012**, *49*, 1149–1161.
2. Zhao, J.; Wen, F.; Xue, Y.; Dong, Z. Modeling analysis and control research framework of cyber physical power systems. *Autom. Electr. Power Syst.* **2011**, *35*, 1–8.
3. Adedeji, K.B.; Hamam, Y. Cyber-Physical Systems for Water Supply Network Management: Basics, Challenges, and Roadmap. *Sustainability* **2020**, *12*, 9555. [CrossRef]
4. Lu, Y.; Xu, X. Resource virtualization: A core technology for developing cyber-physical production systems. *J. Manuf. Syst.* **2018**, *47*, 128–140. [CrossRef]
5. Martin-Barreiro, C.; Ramirez-Figueroa, J.A.; Cabezas, X.; Leiva, V.; Martin-Casad, A.; Galindo-Villardón, M.P. A New Algorithm for Computing Disjoint Orthogonal Components in the Parallel Factor Analysis Model with Simulations and Applications to Real-World Data. *Mathematics* **2021**, *9*, 2058. [CrossRef]
6. Zhang, L.Y.; Guo, J.F.; Wang, J.Z.; Wang, J.; Li, S.S.; Zhang, C.Y. Hypergraph and Uncertain Hypergraph Representation Learning Theory and Methods. *Mathematics* **2022**, *10*, 1921. [CrossRef]
7. Gao, Z.; Su, Y.; Ding, Y.; Liu, Y.; Wang, X.; Shen, J. Key technologies of anomaly detection using PCA-LSTM. In Proceedings of the International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, Sydney, Australia, 3–5 July 2019; Springer: Cham, Switzerland, 2019; pp. 246–254.
8. Wu, Z.; Guo, Y.; Lin, W.; Yu, S.; Ji, Y. A weighted deep representation learning model for imbalanced fault diagnosis in cyber-physical systems. *Sensors* **2018**, *18*, 1096. [CrossRef] [PubMed]
9. Li, Y.; Chai, Y.; Hu, Y.; Yin, H. Review of imbalanced data classification methods. *Control. Decis.* **2019**, *34*, 673–688. [CrossRef]
10. Deng, Z.G.; Sun, Z.W. Attack Detection Enhancement Model of Industrial Cyber Physical Systems. *Inf. Control.* **2021**, *50*, 410–418.
11. Ding, D.; Han, Q.L.; Xiang, Y.; Ge, X.; Zhang, X.M. A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing* **2018**, *275*, 1674–1683. [CrossRef]
12. Chang, C.C.; Lin, C.J. LIBSVM: A library for support vector machines. *ACM Trans. Intell. Syst. Technol.* **2011**, *2*, 1–27. [CrossRef]
13. Aruna, S.; Rajagopalan, S.P. A novel SVM based CSSFFS feature selection algorithm for detecting breast cancer. *Int. J. Comput. Appl.* **2011**, *31*, 14–20.
14. Wang, D.; Tan, D.; Liu, L. Particle swarm optimization algorithm: An overview. *Soft Comput.* **2018**, *22*, 387–408. [CrossRef]
15. Chen, W.Z.; Li, D.Z. Intrusion detection method in industrial control network combining white list filtering and neural network. *J. Comput. Appl.* **2018**, *38*, 363–369.
16. Shang, W.; Li, L.; Wan, M.; Zeng, P. Industrial communication intrusion detection algorithm based on improved one-class SVM. In Proceedings of the 2015 World Congress on Industrial Control Systems Security (WCICSS), London, UK, 14–16 December 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 21–25.
17. Ashibani, Y.; Mahmoud, Q.H. Cyber physical systems security: Analysis, challenges and solutions. *Comput. Secur.* **2017**, *68*, 81–97. [CrossRef]
18. Galloway, B.; Hancke, G.P. Introduction to industrial control networks. *IEEE Commun. Surv. Tutor.* **2012**, *15*, 860–880. [CrossRef]
19. Sun, H.; Peng, C.; Zhang, W.; Yang, T.; Wang, Z. Security-based resilient event-triggered control of networked control systems under denial of service attacks. *J. Frankl. Inst.* **2019**, *356*, 10277–10295. [CrossRef]
20. Lavrentyeva, G.; Novoselov, S.; Malykh, E.; Kozlov, A.; Kudashev, O.; Shchemelinin, V. Audio Replay Attack Detection with Deep Learning Frameworks. In Proceedings of the Interspeech, Stockholm, Sweden, 20–24 August 2017; pp. 82–86.
21. Van der Merwe, J.R.; Zubizarreta, X.; Lukčin, I.; Rügamer, A.; Felber, W. Classification of spoofing attack types. In Proceedings of the 2018 European Navigation Conference (ENC), Gothenburg, Sweden, 14–17 May 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 91–99.
22. Ding, D.; Wei, G.; Zhang, S.; Liu, Y.; Alsaadi, F. On scheduling of deception attacks for discrete-time networked systems equipped with attack detectors. *Neurocomputing* **2017**, *219*, 99–106. [CrossRef]
23. Xiang, H.Y.; Yang, Y. Survey on imbalanced data mining methods. *Comput. Eng. Appl.* **2019**, *55*, 1–16.

24. Camacho, J.; Ferrer, A. Cross-validation in PCA models with the element-wise k-fold (ekf) algorithm: Practical aspects. *Chemom. Intell. Lab. Syst.* **2014**, *131*, 37–50. [CrossRef]
25. Huang, S.; Cai, N.; Pacheco, P.P.; Narandes, S.; Wang, Y.; Xu, W. Applications of support vector machine (SVM) learning in cancer genomics. *Cancer Genom. Proteom.* **2018**, *15*, 41–51.
26. Nie, H.Y.; Li, S.M. Optimization of BP neural network combined with PID model based on PSO algorithm auto wetting control of sintering. *Metall. Ind. Autom.* **2022**, *46*, 44–53.
27. Morris, T.; Gao, W. Industrial control system traffic data sets for intrusion detection research. In Proceedings of the International Conference on Critical Infrastructure Protection, Arlington, VA, USA, 17–19 March 2014; Springer: Berlin/Heidelberg, Germany, 2014; pp. 65–78.