Computers, Materials & Continua CMC, vol.63, no.3, pp.1415-1431, 2020

State-Based Control Feature Extraction for Effective Anomaly Detection in Process Industries

Ming Wan[1], Jinfang Li[1], Jiangyuan Yao[2,*], Rongbing Wang[1,3] and Hao Luo[1]

Abstract: In process industries, the characteristics of industrial activities focus on the integrality and continuity of production process, which can contribute to excavating the appropriate features for industrial anomaly detection. From this perspective, this paper proposes a novel state-based control feature extraction approach, which regards the finite control operations as different states. Furthermore, the procedure of state transition can adequately express the change of successive control operations, and the statistical information between different states can be used to calculate the feature values. Additionally, OCSVM (One Class Support Vector Machine) and BPNN (BP Neural Network), which are optimized by PSO (Particle Swarm Optimization) and GA (Genetic Algorithm) respectively, are introduced as alternative detection engines to match with our feature extraction approach. All experimental results clearly show that the proposed feature extraction approach can effectively coordinate with the optimized classification algorithms, and the optimized GA-BPNN classifier is suggested as a more applicable detection engine by comparing its average detection accuracies with the ones of PSO-OCSVM classifier.

Keywords: State-based control feature, anomaly detection, PSO-OCSVM, GA-BPNN.

1 Introduction

Different from the discrete processing, process industries focus on the essential continuity of production process, whose main purpose is to produce products through a series of successive chemical reactions or physical changes [Muller and Oehm (2019)]. Furthermore, the production facilities are orderly organized according to the technological process, and the processing sequence is fixed and invariable. Actually, process industries have broadly infiltrated into many industrial critical infrastructures, such as petrochemical, machinery, electric power, water conservancy, etc., In process industries, various control systems and computer systems have been effectively applied to monitor and control real-time statuses and technological parameters [Ge, Song, Ding et

[1] School of Information, Liaoning University, Shenyang, 110036, China.

[2] School of Computer Science & Cyberspace Security, Hainan University, Haikou, 570228, China.

[3] School of Informatics, Edinburgh University, Edinburgh, EH89AB, UK.

[*]Corresponding Author: Jiangyuan Yao. Email: yaojy@hainanu.edu.cn.

Received: 15 January 2020; Accepted: 28 February 2020.

al. (2017)], and the demands and realizations for advanced automation and networking are constantly growing. As the emerging application modes, Industrial Internet and Industry 4.0 have been widely recognized by both academia and industry, and they emphasize the deep integration between automatic control technologies and information communication technologies [Li, Yu, Deng et al. (2017); Kourtis, Kavakli and Sakellariou (2019)]. Therefore, they can provide powerful support for the digital and intelligent development of process industries.

In essence, the core infrastructure of process industries remains intelligent manufacturing-oriented control system, whose vulnerabilities have been increasingly exposed because its original self-determination situations are completely broken [Galloway and Hancke (2013); Wan, Shang and Zeng (2017)]. According to statistics, current industrial control systems are confronted with more and more serious security challenges under various outsider and insider attacks [Baybutt (2017); You, Lee, Oh et al. (2018); Xu, Tao, Yang et al. (2019)]. From Stuxnet in 2010 [Nourian and Madnick (2018)] to Triton in 2019 [Martynova and Zhang (2019)], industrial security threats have presented the obvious trends of organized, covert and persistent characteristics, which completely conform to the model of APTs (Advanced Persistent Threats) [AI-Rabiaah (2018)]. In other words, APTs have become the most popular and fatal attack patterns in industrial control systems. Especially, Industrial Internet celebrates the beautiful interconnection and interoperability of all things based on the physical network, and this innovation may actually encourage APTs' acts and accentuate their impacts. The main causes can be summarized as follows: for one thing, the interconnection and interoperability may expose more attack entrances and paths; for another, some emerging technologies may bring new security problems, for example, the virtualization vulnerabilities may become a stumbling block to the application of industrial cloud computing [Xu, Lee, Kim et al. (2018)]. In order to resolve industrial cyber threats, the researchers have started to develop industrial-oriented security solutions by combining industrial control characteristics and regular IT defense technologies. Based on the finite behaviors and stable patterns in industrial control communications, industrial anomaly detection has been regarded as a feasible way to effectively identify misbehaviors without compromising usability [Goldenberg and Wool (2013); Wan, Yao, Jing et al. (2018)]. In practice, one kind of exploring research idea can be summarized as follows: by using artificial intelligence algorithms, industrial anomaly detection can not only learn industrial communication regularities and behavior characteristics to extract the applicable features, but also design the optimized detection engines to achieve intrusion recognition with high accuracy.

It is especially interesting that feature extraction is an important target in industrial anomaly detection, because the appropriate features can not only administer to correctly describe the characteristics of various industrial activities, but also enhance the accuracy and efficiency of detection engines [Wan, Shang and Zeng (2017); Zhao and Dong (2018)]. In process industries, the characteristics of industrial activities focus on the integrality and continuity of production process. Moreover, the integrality demands that all industrial elements are orderly organized to execute the whole production process in period, and the continuity reveals that all stages of production process smoothly work without interruption. From the viewpoint of these characteristics, we propose a novel

state-based control feature extraction approach, which selects significant features from the successive control operations in one production process. In particular, this approach designs the finite control operations to different states, and the procedure of state transition can adequately express the change of successive control operations.

In this paper, we also introduce two different classification algorithms as detection engines to indirectly evaluate the proposed feature extraction approach. More specifically, these two classification algorithms are OCSVM (One Class Support Vector Machine) [Wan, Shang and Zeng (2017)] and BPNN (BP Neural Network) [Wu, Shi, Wang et al. (2019)], and PSO (Particle Swarm Optimization) and GA (Genetic Algorithm) [Pham, Malinowski and Bartczak (2011)] are chosen to optimize the key parameters of these detection engines, respectively. According to the experimental results in the Modbus/TCP control system which simulates the material synthesis process, we can draw the following conclusions: (1) the state-based control feature extraction approach can effectively coordinate with the optimized classification algorithms; (2) without considering the training process, the optimized GA-BPNN classifier is suggested as a serviceable detection engine due to its higher detection accuracy.

The main accomplishments and contributions of this paper are summarized as follows: firstly, based on FSM (Finite State Machine), we propose a novel state-based control model to analyze and characterize the integrality and continuity of control operations, and calculate the feature value by integrating the motivation coefficient with the statistical information of state transition; secondly, in order to effectively cooperate with the proposed feature extraction approach, we select OCSVM and BPNN classifiers as two representative detection engines, which are optimized to enhance their detection capabilities; thirdly, we define three practical attack types against the normal production process, and design different attack powers to compare the detection accuracies of two classifiers. In particular, the dramatic difference of our concern is that an excellent feature extraction approach not only is one significant precondition for anomaly detection, but also guarantees and improves the detection quality. In our approach, we focus on the detailed design of state-based control feature selection and calculation to address this challenge.

2 State-based control feature extraction

As stated previously, one notable advantage of process industries is that the process controls in different production stages are executed in a single uninterrupted sequence. In other words, the whole production process in process industries always completes some periodic control operations under the condition of finite states, and the change of successive control operations can reflect the corresponding production process to some extent. On this basis, we propose a novel state-based control feature extraction approach, which regards the finite control operations as different states. Furthermore, the change of successive control operations can be represented by the procedure of state transition, and the statistical information between different states can be used to calculate the feature values. The specific steps are listed as follows:

1) Initialization In process industries, each production process involves a series of successive control operations, which can achieve a combination of different functions. When one master operation station wants to control one slave PLC (Programmable Logic

Controller), the corresponding types and roles of all control operations have been defined in the function fields of industrial communication protocols. Namely, if we capture and parse industrial communication packets in chronological order, the obtained control sequence $C_i = c_i^1 c_i^2 c_i^3 \cdots c_i^k$ in the interval τ can represent the change of successive control operations in one or several production stages. As a result, we can obtain the control sequence set $C = \{C_1, C_2, C_3, \ldots, C_n\}$ in the total interval T ($T = n\tau$), and the number of control operations in each control sequence C_i ($i \in [1, n]$) is different from each other. Additionally, all control sequences involve l different functions f_l, here $l \le k$. By selecting the appropriate interval τ, each control sequence C_i can consist of l different functions, who are rearranged according to one specific production process.

2) State-based control model building Based on the control sequence set C, we further build the state-based control model by using FSM [Soewito, Vespa, Mahajan et al. (2009)]. In this model, each function f_l can be considered as a state S_l, and all states form a finite set $S = \{S_1, S_2, S_3, \ldots, S_l\}$. Therefore, the change of two successive control operations can be expressed as the transition from one state to another state, and any control sequence can be described by the state transition of multiple states. Additionally, different state transitions need to be triggered through diversified input signals in FSM. Similarly, we select the previous control operation before two successive control operations as the trigger signal, which is referred to the motivation factor in the state-based control model. For example, c_i^{j-1} can be regarded as the motivation factor of two successive control operations $c_i^j c_i^{j+1}$ in the short control sequence $c_i^{j-1} c_i^j c_i^{j+1}$ ($j \le k-1$). Fig. 1 shows the example of state transition paths in the state-based control model which associates with 7 different states. Here, S_u represents the current state, and M_{uv} represents the current motivation factor. Also, the state transition TR() can be interpreted as follows: under the action of current motivation factor M_{uv}, current state transfers from S_u to S_v. Tab. 1 shows the mathematical definitions of three key elements in the state-based control model.

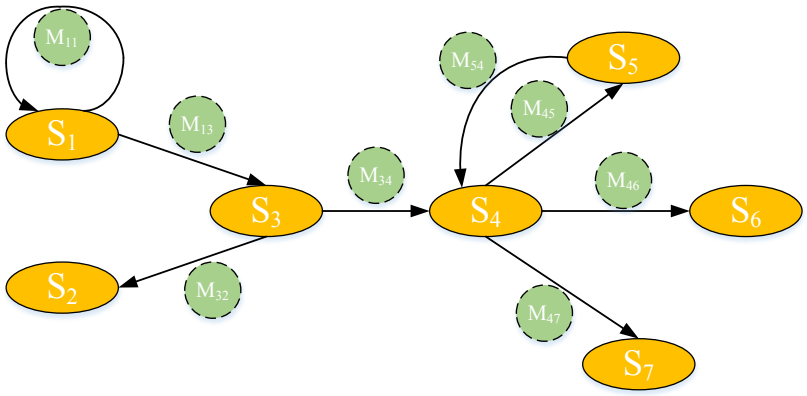

Figure 1: Example of state transition paths in the state-based control model

Table 1: Mathematical definitions of three key elements in the state-based control model

Element	Mathematical definition
c_i^j	$c_i^j \in \{f_r, \exists r \in [1,l]\}$, s.t. $\forall i \in [1,n], j \in [1,k]$
S	$S = \{S_r, \exists r \in [1,l]\}$, s.t. $S_r = f_r, \forall r \in [1,l]$
M_{uv}	$M_{uv} \in \{f_r, \exists r \in [1,l]\}$, s.t. $\mathrm{TR}(S_u, M_{uv}) = S_v, \forall u, v \in [1,l]$

3) Feature factor selection and feature value calculation According to the state transition paths, we select $M_{uv}S_uS_v$ as the feasible feature factor. More specifically, each feature factor consists of three successive control operations, in which the first control operation is viewed as the motivation factor M_{uv} and the latter two control operations represent the state transition $S_u \to S_v$ caused by the motivation factor M_{uv}. Based on the above definitions, no matter the motivation factor or the state is actually a control operation. If all control sequences involve l different functions, the maximum number of feature factors may be l^3, that is, the dimension of feature sample may reach l^3. Actually, each production process will probably not cover all feature factors, and the corresponding dimension of feature sample will be less than l^3. In the state-based control model, a simple identification method of feature factor is designed as follows: firstly, we rearrange all control sequence in the set C in chronological order; secondly, by recursively traversing the rearranged control operations, we find each different short control sequence $c_i^{j-1}c_i^jc_i^{j+1}$, which can be identified as the selected feature factor; thirdly, we can further obtain the number d of feature factors in this production process by computing the number of all short control sequences.

For each control sequence $C_i = c_i^1c_i^2c_i^3\cdots c_i^k$, we can calculate the feature value of each feature factor by

$$x = Eco \cdot H(S_u \to S_v) \tag{1}$$

Here, Eco is the motivation coefficient generated by the motivation factor, and $H(S_u \to S_v)$ is the statistical information generated by the state transition $S_u \to S_v$.

$$H(S_u \to S_v) \overset{\text{def}}{=} -P(S_u \to S_v)\log_2 P(S_u \to S_v) \tag{2}$$

Here, $P(S_u \to S_v)$ represents the probability of state transition $S_u \to S_v$ in each control sequence $C_i = c_i^1c_i^2c_i^3\cdots c_i^k$.

According to the definition of Pearson correlation coefficient, we further calculate the motivation coefficient Eco by

$$Eco \overset{\text{def}}{=} \frac{1}{n}\left\|\sum_{i=1}^{n}\frac{(I_i(M_{uv}) - \overline{I(M_{uv})})}{\delta_{IM}} \cdot \frac{(I_i(S_uS_v) - \overline{I(S_uS_v)})}{\delta_{IS}}\right\| \tag{3}$$

Here, $I_i(M_{uv})$ ($i \in [1,n]$) is the statistical self-information of motivation factor M_{uv} in

each control sequence $C_i = c_i^1 c_i^2 c_i^3 \cdots c_i^k$, and $\overline{I(M_{uv})}$ and δ_{IM} are the mean and standard deviation of $I_i(M_{uv})$, respectively. $I_i(S_u S_v)$ $(i \in [1,n])$ is the statistical self-information of two successive states $S_u S_v$ in each control sequence $C_i = c_i^1 c_i^2 c_i^3 \cdots c_i^k$, and $\overline{I(S_u S_v)}$ and δ_{IS} are the mean and standard deviation of $I_i(S_u S_v)$, respectively.

Above all, each feature can work out one feature value, and each control sequence $C_i = c_i^1 c_i^2 c_i^3 \cdots c_i^k$ can be mapped to one feature sample $X_i = (x_1^i, x_2^i, \ldots, x_d^i)$.

3 Detection engines and optimization

For the same feature samples, different detection engines may export distinct results due to their own detection characteristics. In this paper, we introduce two different classification algorithms as alternative detection engines to match with our feature extraction approach. Furthermore, the first classification algorithm is OCSVM which can be easily trained by only using normal feature samples, and the second classification algorithm is BPNN which can be specifically trained with the help of both normal and malicious feature samples. In order to obtain perfect classification effects, we choose PSO and GA to optimize the key parameters of these two classification algorithms, respectively.

3.1 OCSVM classifier optimized by PSO

Different from the traditional SVM, OCSVM can be directly applied in one type of training feature samples, which are correctly extracted from normal system or network data. By judging the attribution of observed data, the OCSVM classifier can mark the suspicious data as the abnormal type. Moreover, the general mechanism of OCSVM is described below: in order to enhance the preferable aggregation, the original feature samples $\{x_i, i = 1,2,\ldots,n\}$ need to be mapped into the high-dimensional feature space $\Phi(\bullet)$ by using the kernel function $k(x_i, x_j) = <\Phi(x_i), \Phi(x_j)>$, and an optimal hyperplane in this feature space is resolved to maximize separation between the observed feature samples and the ordinate origin, which is postulated as the only one abnormal feature sample. As shown in Eq. (4), by resolving the quadratic programming problem, OCSVM can calculate the normal vector ω and compensation factor ρ to generate the final decision function.

$$\begin{cases} \min \ \ \frac{1}{2}\|\omega\|^2 + \frac{1}{\nu r}\sum_{i=1}^{r}\xi_i - \rho \\ s.t.\ (\omega \bullet \Phi(x_i)) \geq \rho - \xi_i \ , \ \xi_i \geq 0 \ \ i = 1 \cdots r \end{cases} \Rightarrow \begin{cases} f(x) = \mathrm{sgn}(\sum_{i=1}^{r}\alpha_i k(x_i, x\ ) - \rho) \\ \rho = \sum_{i=1}^{r}\alpha_i k(x_i, x_j) \end{cases} \tag{4}$$

Here, v is the tradeoff parameter to affect the number of support vectors, and α_i is the Lagrange multiplier in Lagrange function.

In our OCSVM classifier, we introduce Gaussian kernel function to realize the nonlinear mapping of feature space, and its kernel parameter g plays an important role in the excellent hyperplane construction [Xiao, Wang and Xu (2015)]. To sum up, we employ

PSO to optimize the tradeoff parameter v and kernel parameter g, and the detailed optimization process is depicted in Fig. 2(a).

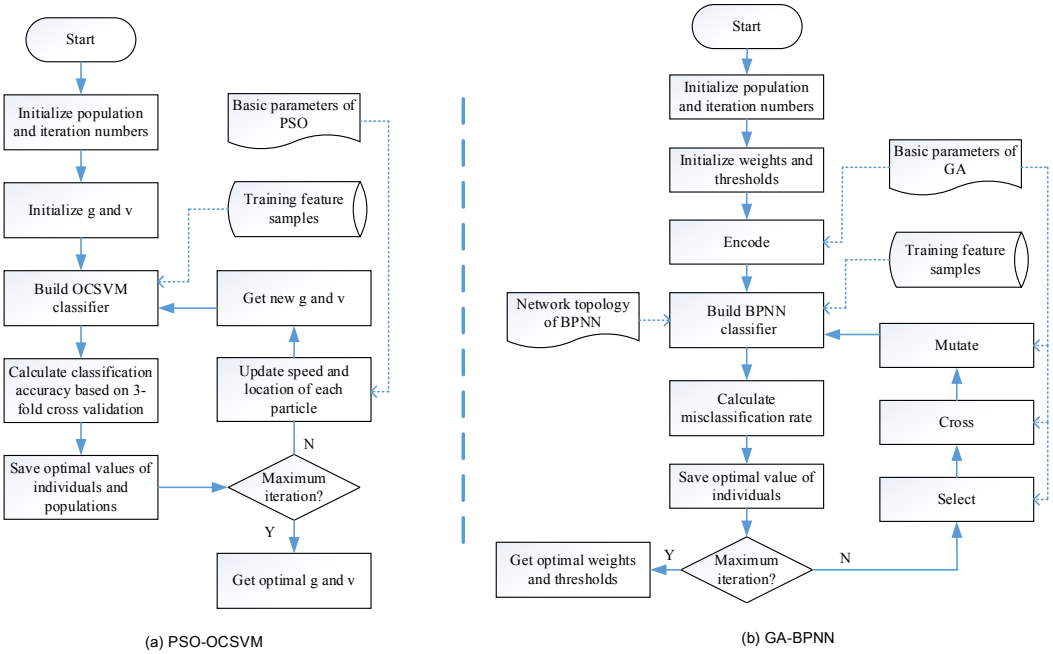

Figure 2: Detailed optimization process of two classification algorithms

3.2 BPNN classifier optimized by GA

BPNN belongs to the multilayer feedforward neural network, whose significant characteristics involve forward signal propagation and reverse error propagation. When BPNN serves as an anomaly classifier, it requires different types of training feature samples, which can improve its capability of association and prediction. Furthermore, BPNN consists of three layers: the input layer, the hidden layer and the output layer, and the neurons between every two layers possess the connection weights ω_{ij} and ω_{jk}. By setting the hidden and output thresholds Th and To, the outputs in the hidden layer and output layer can be calculated by Eq. (5).

$$\begin{cases} H(j) = f\left(\sum_{i=1}^{n} \omega_{ij} x_i - Th_j\right) \\ O(k) = \sum_{j=1}^{l} H(j)\omega_{jk} - To_k, \quad \begin{matrix} j = 1,2,\ldots,l \\ k = 1,2,\ldots,m \end{matrix} \\ f(x_i) = 1/(1+\exp^{-x_i}) \end{cases} \tag{5}$$

Here, n, l and m are the unit numbers in these three layers, and $f(\bullet)$ is the activation function of hidden layer.

In our BPNN classifier, we define the misclassification rate as BPNN's prediction error, and this error can be further used to update the parameters ω_{ij}, ω_{jk}, Th and To, which make a positive contribution during the favorable network construction. Therefore, we employ GA to optimize these parameters, and the detailed optimization process is depicted in Fig. 2(b).

4 Experimental testing and result comparison

By organically combining the proposed feature extraction approach and two detection engines, we can designate the detection accuracy as a practicable evaluation indicator. One the one hand, this indicator can contribute to developing the serviceable detection engine, which is more applicable to the proposed feature extraction approach; on the other hand, it can indirectly reflect the effectiveness of feature extraction, which embodies the appropriate level to describe the characteristics of production process in process industries. In order to achieve this goal, we build a Modbus/TCP control system to simulate the material synthesis process. As shown in Fig. 3, the production process is summarized as follows: firstly, PLC 1 opens the valves of two funnels to drop materials 1 and 2, and closes these two valves when the quantities of materials 1 and 2 reach the setting values respectively; secondly, PLC 2 switches on the conveyor belt, and materials 1 and 2 are carried into the reaction furnace; thirdly, after the material synthesis reaction, PLC 3 opens valve 3 to discharge the synthetic material 3. By means of different Modbus/TCP packets, three PLCs are managed and controlled by one operator station, and the complete cycle of production process is 30 seconds.

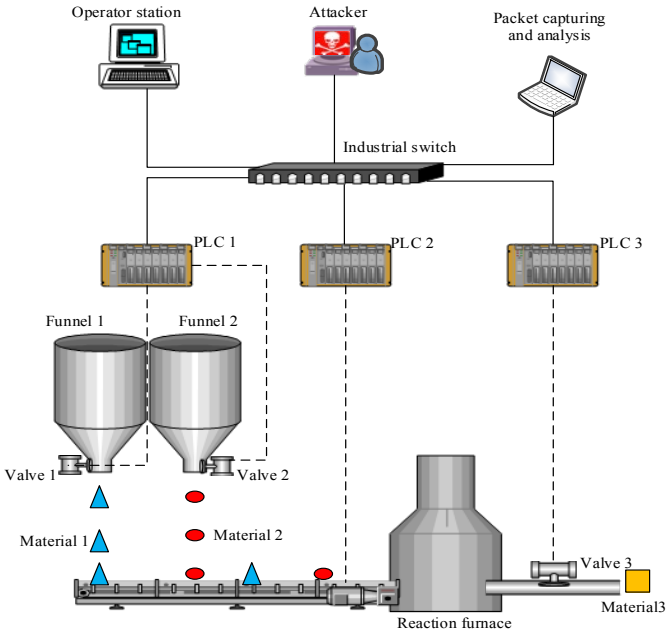

Figure 3: Modbus/TCP control system to implement the material synthesis process

4.1 Experimental data acquisition and analysis

By running this system, we capture lots of normal Modbus/TCP packets, which are divided into two parts: the first part serves as normal training data, which contains 65486 control operations during the running time of 280 minutes; the second part is regarded as normal test data, whose number of control operations is 33340 during the running time of 143 minutes. Fig. 4 shows the distribution characteristics of control operations in the normal training data. Moreover, the whole production process involves 5 different functions: 01, 03, 05, 15 and 16, which represent "Read coils", "Read multiple registers", "Write single coil", "Write multiple coils" and "Write multiple registers" in the Modbus/TCP protocol specification, respectively. From Figs. 4 (a) and 4(b) we can see that, the total number of control operations per 60 s has a tight fluctuation, and the accumulated number of each control operation presents a trend of smooth growth. In short, all of these can provide indirect evidence of the stability and periodicity of production process under the finite states. Similarly, Figs. 4 (c) and 4(d) show the average numbers and variances of different control operations per 60s, and the maximum variance for the control operation 01 is only 1.5, that is, all control operations in every production process have tiny deviations from their average numbers.

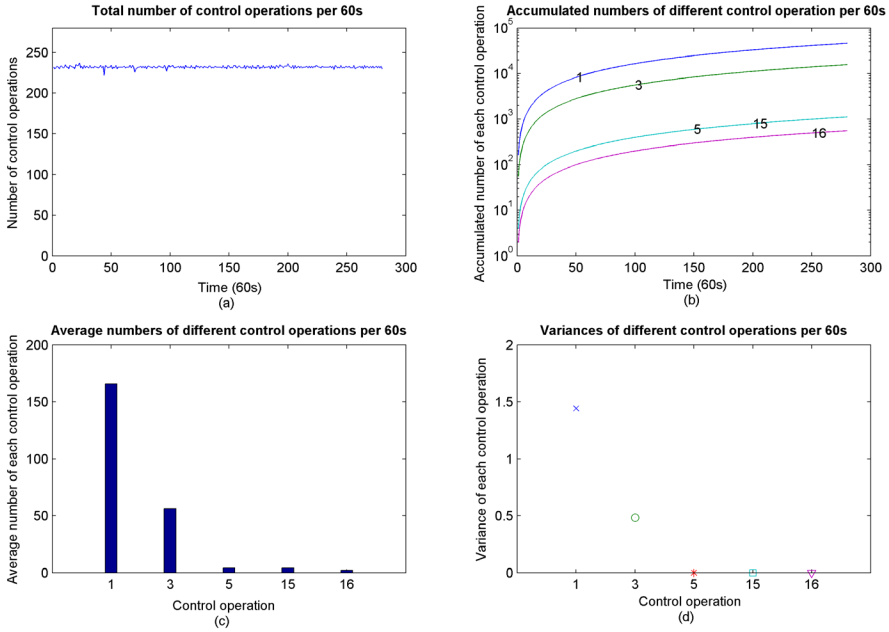

Figure 4: Distribution characteristics of control operations in the normal training data

4.2 Different attack assumptions

In order to evaluate the detection accuracy for malicious attacks, we suppose three different attack types against this system. Furthermore, the main purpose of these attacks is to destroy the normal production process by launching some imitative control operations, for example, if next control operation is changed to 05 from the normal

operation control 01 in one production stage, one industrial accident may be caused because this imitative control operation has broken the continuity of production process. Additionally, another reasonable hypothesis is that the imitative control operations only involves the above 5 different functions because incompatible control operations can be easily filtered by current industrial firewalls [Wan, Shang, Kong et al. (2017); Cheminod, Durante, Seno et al. (2018)]. Based on the network structure of simulated control system, the malicious attacker is designed to directly connect to the industrial switch, and has obtained its ownership permission. As shown in Fig. 5, the first two attack types belong to the category of MITM (Man in The Middle) attacks, and the third attack type is based on the third-party injection attack. More specifically, the detailed definitions of three attack types are interpreted as follows:

Definition 1. Continuous MITM attack The malicious attacker can hijack the normal control operations from the industrial switch, and continuously modifies some normal control operations to a chain of imitative control operations. In other words, this attack type can cause a chain of irregular control operations to appear in the normal production process.

Definition 2. Random MITM attack The malicious attacker can hijack the normal control operations from the industrial switch, and randomly modifies several normal control operations to the imitative control operations. In other words, this attack type can induce the imitative control operations to randomly spread over the normal production process.

Definition 3. Continuous injection attack As a hidden third-party adversary, the malicious attacker can launch a chain of imitative control operations, and continuously inject them into the normal control operations. In other words, this attack type can add some additional and irregular control operations into the normal production process.

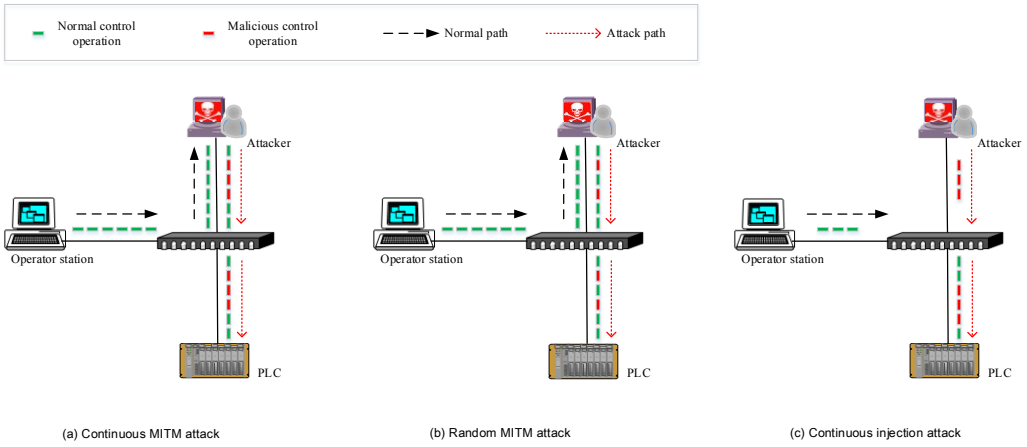

Figure 5: Description of three different attack types

4.3 Detection evaluation for PSO-OCSVM classifier

According to the proposed feature extraction approach, we acquire 280 normal training feature samples from the normal training data. Actually, the number of feature factors is only 51, and is much less than the theoretical maximum value $5^3 = 125$ due to $l = 3$. By

using normal training feature samples, we obtain an optimized PSO-OCSVM classifier, and the optimal tradeoff parameter and kernel parameter are $v = 0.0114$ and $g = 12.9090$. Furthermore, Fig. 6 depicts the changes of two fitness curves under 200 iterations, and all fitness values are computed by using 3-fold cross validation. From this figure we can see that the best value in each iteration grows fast and monotonically converges to the global optimum, which can reach 99.64%. Additionally, Fig. 7 shows the classification results for 280 normal training feature samples, and the corresponding classification accuracy can reach about 97.86%. In this figure, "1" represents the normal category, and "-1" represents the abnormal category. According to the classification results, only 6 normal feature samples are misidentified as abnormal ones, and we can conclude that this classifier has a fine ability of learning and generalization.

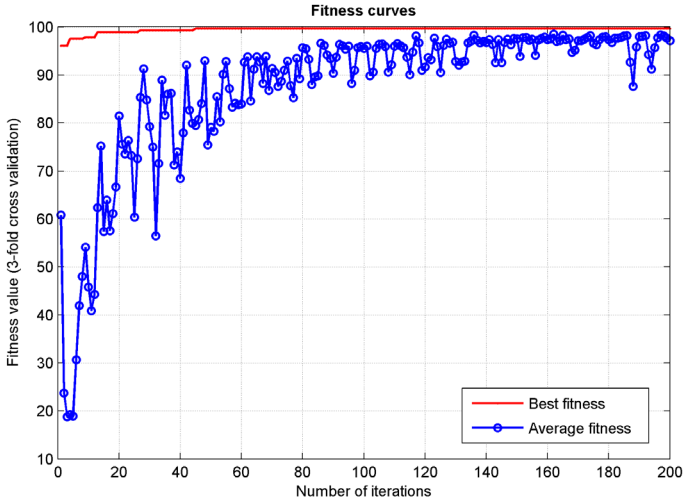

Figure 6: Changes of two fitness curves under 200 iterations

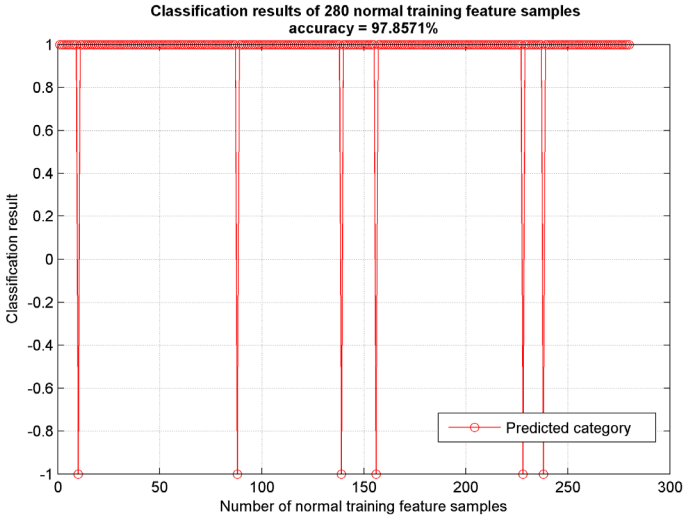

Figure 7: Classification results of 280 normal training feature samples

For 143 normal test feature samples extracted from the normal test data, we further evaluate the false classification of PSO-OCSVM classifier. Fig. 8 plots the classification results of 143 normal test feature samples, and the corresponding classification accuracy can reach 96.50%. Namely, only 5 normal feature samples are incorrectly classified as abnormal ones, and it directly proves that this classifier can ensure a low rate of false classification.

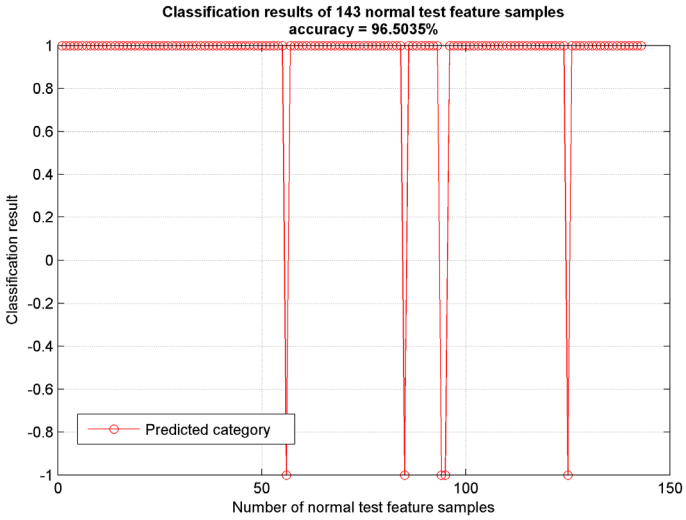

Figure 8: PSO-OCSVM's classification results of 143 normal testing feature samples

In order to evaluate the detection accuracies for three different attack types, we simulate each attack type to destroy the normal production process. For each attack type, we generate 280 malicious control sequences in one experiment, and the number of imitative control operations in each malicious control sequence is flexibly designed according to the assumed attack powers. For example, when one malicious attacker carries out the continuous injection attack, he can continuously launch 15 imitative control operations as one attack power, and the corresponding percentage in each control sequence is about 6.03%. In practice, if the malicious attacker wants to achieve a higher success probability, it is an efficient way to improve the attack power by increasing the number of imitative control operations. However, different attack powers may also have significant impacts on the detection accuracy of PSO-OCSVM classifier. As a result, we must compare the detection accuracies under different numbers of imitative control operations for each attack type. Tab. 2 shows the experimental results for three attack types, and each average detection accuracy in this table is calculated by conducting 6 different experiments. Additionally, it's worth noting that the number of imitative control operations for the random MITM attack is differently designed from the ones for another two attack types, and the causes can be briefly analyzed as follows: on the one hand, the proposed feature extraction approach is very sensitive to the random distribution of imitative control operations, that is, a tiny amount of imitative control operations can bring a significant impact on the feature value calculation; on the other hand, we focus on the trend of average detection accuracy under the incremental number of imitative control operations, and the same design for the random MITM attack may cause trouble in this

trend estimation.

From this table we can find that the optimized PSO-OCSVM classifier has a satisfying ability to detect the given attack types, and we can also summarize the following conclusions: (1) for all attack types, as the number of imitative control operations increases, the average detection accuracy of PSO-OCSVM classifier shows a trend of significant growth; (2) although the selected numbers of imitative control operations for all attack types are not the same, it remains the highest detection accuracy for the random MITM attack, because if we set the number of imitative control operations to 12, its average detection accuracy can reach 99.88% by performing additional 6 experiments; (3) based on the proposed feature extraction approach, the random distribution of imitative control operations can cause more significant changes of feature values, which can contribute to the detection accuracy of PSO-OCSVM classifier.

Table 2: PSO-OCSVM's average detection accuracies under different numbers of imitative control operations for each attack type

Continuous MITM attack		Random MITM attack		Continuous injection attack	
Number of imitative control operations	Average detection accuracy	Number of imitative control operations	Average detection accuracy	Number of imitative control operations	Average detection accuracy
12	79.82%	5	71.07%	12	70.36%
13	86.55%	6	83.93%	13	74.58%
14	91.19%	7	89.17%	14	80.95%
15	93.99%	8	95.30%	15	86.13%
16	95.24%	9	97.74%	16	90.18%
17	98.57%	10	98.81%	17	93.33%

4.4 Detection evaluation for GA-BPNN classifier

Differently, BPNN requires both normal training feature samples and malicious training feature samples, which can improve its classification capability. Based on the attack assumptions, we generate 50 malicious control sequences to extract malicious training feature samples for each attack type, and it is worth mentioning that the number of malicious training feature samples is far less than the one of normal training feature samples because the malicious attacks infrequently occur in real-world process industries. By using the above-mentioned training feature samples, we obtain an optimized GA-BPNN classifier, and Fig. 9 depicts the changes of misclassification rate under 20 iterations. Overall, the misclassification rate can obviously descend with the increasing number of iterations, and the minimal prediction error is only 0.01163. Namely, the classification accuracy for 280 normal training feature samples can approximately reach 98.84%. Similarly, we also evaluate its false classification for 143 normal test feature samples, and Fig. 10 plots the corresponding classification results. More precisely, only 2 normal feature samples are mistaken for abnormal ones, and the classification accuracy can reach about 98.60%. Compared with the PSO-OCSVM classifier, this classifier have a lower rate of false classification.

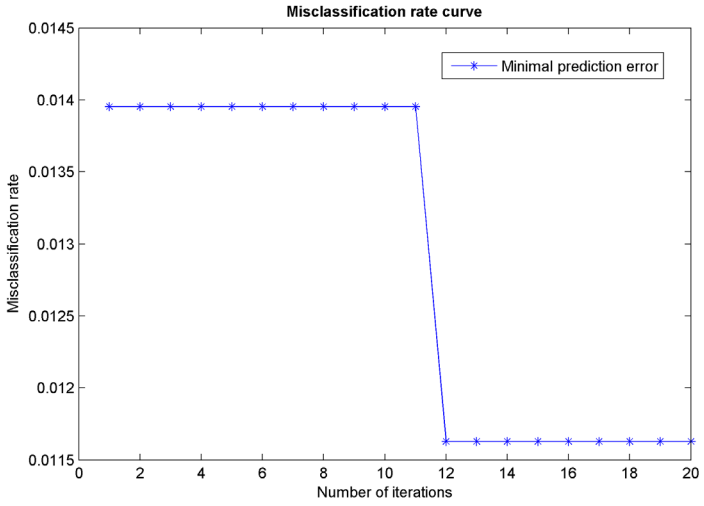

Figure 9: Changes of misclassification rate curve under 20 iterations

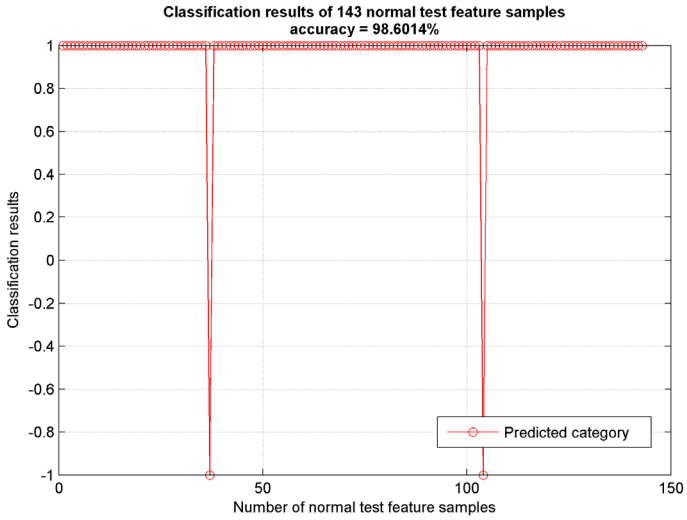

Figure 10: GA-BPNN's Classification results of 143 normal testing feature samples

Without loss of generality, we further evaluate the detection accuracies for three different attack types, and the malicious feature samples in each experiment are consistent with the ones used in the evaluation of PSO-OCSVM classifier. Tab. 3 compares the detection accuracies under different numbers of imitative control operations for each attack type. Intuitively, we can draw the similar results: (1) when the number of imitative control operations increases, the average detection accuracies for all attack types can be improved; (2) the optimized GA-BPNN classifier achieves the greatest efficiency to detect the random MITM attack, even when the number of imitative control operations is set to 12, its average detection accuracy can grow to 98.75%; (3) the proposed feature

extraction approach is more sensitive to the random MITM attack due to the random distribution of imitative control operations. Differently, by comparing the experimental results in Tabs. 2 and 3, we find that these two classifiers can present their own advantages and disadvantages: firstly, the optimized PSO-OCSVM classifier obtains the highest detection accuracy 98.81% for the random MITM attack, but its average detection accuracy under 5 imitative control operations is well below the one of GA-BPNN classifier; secondly, the optimized GA-BPNN classifier exhibits more excellent detection stability, because the change of average detection accuracies follows a relatively smooth curve; thirdly, the optimized GA-BPNN classifier has a distinct advantage to detect the continuous MITM attack and continuous injection attack, even though its average detection accuracy for the continuous MITM attack under 17 imitative control operations is slightly lower than the one of PSO-OCSVM classifier.

Table 3: GA-BPNN's average detection accuracies under different numbers of imitative control operations for each attack type

Continuous MITM attack		Random MITM attack		Continuous injection attack	
Number of imitative control operations	Average detection accuracy	Number of imitative control operations	Average detection accuracy	Number of imitative control operations	Average detection accuracy
12	92.98%	5	85.96%	12	91.13%
13	92.44%	6	89.11%	13	92.86%
14	93.63%	7	92.11%	14	94.35%
15	95.24%	8	94.58%	15	94.47%
16	96.01%	9	96.85%	16	95.72%
17	96.67%	10	97.21%	17	96.55%

Above all, the above experimental comparisons and analysis convincingly illustrate the following two points: for one thing, the state-based control feature extraction approach can not only correctly describe the characteristics of control operation in process industries, but also effectively coordinate with the optimized classification algorithms, because both of two optimized classifiers have a desirable detection capability; for another, if malicious training feature samples are sufficient and diversified, we suggest the optimized GA-BPNN classifier as a serviceable detection engine to cooperate with our feature extraction approach.

5 Conclusion

According to the integrality and continuity of production process in process industries, this paper proposes a novel state-based control feature extraction approach, which selects the finite control operations as different states to construct the feature factor. Moreover, the change of successive control operations can be represented by the procedure of state transition, and the statistical information between different states can be used to calculate the feature values. Additionally, this paper also introduces two different classification algorithms as detection engines to indirectly evaluate the proposed feature extraction approach, and these classification algorithms are optimized to the PSO-OCSVM and GA-

BPNN classifiers by using the training feature samples. By supposing three applicable attack types, we further compare the detection accuracies of these two classifiers. The experimental results show that both two classifiers have a desirable detection ability, and the average detection accuracy of GA-BPNN classifier is generally higher than the one of PSO-OCSVM classifier. In other words, the proposed feature extraction approach can effectively coordinate with the optimized classification algorithms.

Acknowledgement: The authors are grateful to the anonymous referees for their insightful comments and suggestions.

Funding Statement: This work is supported by the Program of Hainan Association for Science and Technology Plans to Youth R & D Innovation (Grant No. QCXM201910), the Natural Science Foundation of Liaoning Province (Grant No. 2019-MS-149), the Social Science Planning Foundation of Liaoning Province (Grant No. L18AGL007), the National Natural Science Foundation of China (Grant Nos. 61802092, 51704138 and 61501447), and the Scientific Research Setup Fund of Hainan University (Grant No. KYQD (ZR) 1837).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

AI-Rabiaah, S. (2018): The "Stuxnet" virus of 2010 as an example of a "APT" and its "Recent" variances. *Proceedings of 21st Saudi Computer Society National Computer Conference*, pp.1-5.

Baybutt, P. (2017): Issues for security risk assessment in the process industries. *Journal of Loss Prevention in the Process Industries*, vol. 49, part B, pp. 509-518.

Cheminod, M.; Durante, L.; Seno, L., Valenzano, A. (2018): Performance evaluation and modeling of an industrial application-layer firewall. *IEEE Transactions on Industrial Informatics*, vol. 14, no. 5, pp. 2159-2170.

Galloway, B.; Hancke, G. P. (2013): Introduction to industrial control networks. *IEEE Communications Surveys & Tutorials*, vol. 15, no. 2, pp. 860-880.

Ge, Z.; Song, Z.; Ding, S. X.; Huang, B. (2017): Data mining and analytics in the process industry: the role of machine learning. *IEEE Access*, vol. 5, pp. 20590-20616.

Goldenberg, N.; Wool, A. (2013): Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems. *International Journal of Critical Infrastructure Protection*, vol. 6, no. 2, pp. 63-75.

Kourtis, G.; Kavakli, E.; Sakellariou, R. (2019): A rule-based approach founded on description logics for Industry 4.0 smart factories. *IEEE Transactions on Industrial Informatics*, vol. 15, no. 9, pp. 4888-4899.

Li, J.; Yu, F. R.; Deng, G.; Luo, C.; Ming, Z. et al. (2017): Industrial Internet: a survey on the enabling technologies, applications, and challenges. *IEEE Communications*

Surveys & Tutorials, vol. 19, no. 3, pp. 1504-1526.

Martynova, D.; Zhang, P. (2019): An approach to encrypted fault detection of cyber-physical systems. *Proceedings of 12th Asian Control Conference*, pp. 1501-1506.

Muller, R.; Oehm, L. (2019): Process industries *vs.* discrete processing: how system characteristics affect operator tasks. *Cognition, Technology & Work*, vol. 21, no. 2, pp. 337-356.

Nourian, A.; Madnick, S. (2018): A systems theoretic approach to the security threats in cyber physical systems applied to Stuxnet. *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 1, pp. 2-13.

Pham, N.; Malinowski, A.; Bartczak, T. (2011): Comparative study of derivative free optimization algorithms. *IEEE Transactions on Industrial Informatics*, vol. 7, no. 4, pp. 592-600.

Soewito, B.; Vespa, L.; Mahajan, A.; Weng, N.; Wang, H. (2009): Self-addressable memory-based FSM: a scalable intrusion detection engine. *IEEE Network*, vol. 23, no. 1, pp. 14-21.

Wan, M.; Shang, W.; Zeng, P. (2017): Double behavior characteristics for one-class classification anomaly detection in networked control systems. *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 12, pp. 3011-3023.

Wan, M.; Shang, W.; Kong, L.; Zeng, P. (2017): Content-based deep communication control for networked control system. *Telecommunication Systems*, vol. 65, no. 1, pp. 158-168.

Wan, M.; Yao, J.; Jing, Y.; Jin, X. (2018): Event-based anomaly detection for non-public industrial communication protocols in SDN-based control systems. *Computers, Materials & Continua*, vol. 55, no. 3, pp. 447-463.

Wu, D.; Shi, H.; Wang, H.; Wang, R.; Fang, H. (2019): A feature-based learning system for Internet of Things applications. *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1928-1937.

Xiao, Y.; Wang, H.; Xu, W. (2015): Parameter selection of Gaussian kernel for one-class SVM. *IEEE Transactions on Cybernetics*, vol. 45, no. 5, pp. 941-953.

Xu, L.; Lee, J.; Kim, S. H.; Zheng, Q.; Xu, S. et al. (2018): Architectural protection of application privacy against software and physical attacks in untrusted cloud environment. *IEEE Transactions on Cloud Computing*, vol. 6, no. 2, pp. 478-491.

Xu, W.; Tao, Y.; Yang, C.; Chen, H. (2019): MSICST: multiple-scenario industrial control system testbed for security research. *Computers, Materials & Continua*, vol. 60, no. 2, pp.691-705.

You, Y.; Lee, J.; Oh, J.; Lee, K. (2018): A review of cyber security controls from an ICS perspective. *Proceedings of International Conference on Platform Technology and Service*, pp. 1-5.

Zhao, L.; Dong, X. (2018): An industrial Internet of Things feature selection method based on potential entropy evaluation criteria. *IEEE Access*, vol. 6, pp. 4608-4617.