Preprints of the 21st IFAC World Congress (Virtual)
Berlin, Germany, July 12-17, 2020

Intrusion Detection of Industrial Control System Based on Double-layer One-class Support Vector Machine

Wen-an Zhang * **Yinfeng Miao** * **Qi Wu** * **Li Yu** * **Xiufang Shi** *

* *College of Information Engineering, Zhejiang University of Technology, Hangzhou, 310023, P.R.China*

Abstract: In this paper, the stealthy attack detection in industrial control system (ICS) is studied, and a new detection method is proposed from the perspective of signal analysis. The method consists of a double-layer one-class support vector machine model (DL-OCSVM), where the first-layer model is the standard OCSVM, and the second-layer model is obtained by incremental learning based on the former. The wavelet decomposition is used to extract the physical characteristics of the ICS. The KKT condition and the adjacent classification interval are adopted to reduce the training samples, improving the learning rate and system scalability. In addition, the designed boundary samples are employed for incremental learning, avoiding overfitting and reducing false positives rate (FPR). The experimental results show that the proposed method has high detection rate and low FPR for stealthy attacks, and is more suitable for precision machining process.

Keywords: Industrial control systems(ICSs); intrusion detection; machine learning; one-class support vector machine (OCSVM)

1. INTRODUCTION

In recent years, the emergence and popularity of the internet of things (IOT) and cyber-pyhsical system (CPS) have greatly promoted the development of ICSs. Under the general trend of open industrial networks, the threats and risks brought by the network have become the main challenge for ICSs security. Since the stuxnet incident in 2010, ICS security events have shown an explosive growth trend. A large number of worm virus events (including Conficker, Flame, Gauss, etc), cyber espionage events, cyber extortion events and advanced persistent threat (APT) activities have posed a serious threat to the cyber security of ICSs.

At present, the issues of ICS security defense have attracted widespread attention from the industry and academia. The security protection methods of ICSs can be roughly divided into two categories: passive protection and active detection. The passive protection methods mainly adopt traditional protection technologies in the field of information security, including installing industrial firewalls, exploiting system vulnerabilities and assessing system risks. With the rapid development of computer network technology, traditional passive protection methods have been unable to cope with advanced attacks of high technology, high concealment and strong pertinence. The active detection methods based on feature matching and anomaly detection are able to achieve the real-time detection of internal and external attacks for ICSs, thus effectively remedy the shortcomings of passive protection methods. This is so-called the second line of defense for ICSs. Feng et al. (2017) developed a base-line signature database for general packages in ICS networks and used a stacked long short term memory (LSTM) network-based softmax classifier to achieve the intrusion detection for a gas pipeline SCADA system. However, the detection method based on the signature database has a high false positive rate because it cannot effectively detect unknown attacks. According to the latest report of ICS-CERT, the number of ICS security events is increasing every year, while the known tools and types of cyber attacks in ICSs are still a small part. Compared with the method based on feature matching, the method based on anomaly detection is more suitable for ICS security defense. Wang et al. (2019) discussed the opportunities and challenges of anomaly detection in industrial control network under the background of the fusion of operation technology (OT) and information communication technology (ICT), and the analysis of anomaly detection algorithm based on machine learning was carried out. Machine learning has achieved great success over the past few years, which has also been considered as one of the popular solutions for anomaly detection in industrial control networks. Classical algorithms in machine learning, such as neural networks, deep neural networks, reinforcement learning have been successfully used in ICSs security defense. On the basis of considering the effect of physical features on anomaly detection for industrial information physics systems (ICPSs), Yang et al. (2018) proposed a BP neural network-based anomaly detection method with high resolution accuracy. Wang et al. (2017) designed an anomaly detection system based on deep convolutional neural networks (CNNs) to automatically learn traffic features, thus effectively reduc-

⋆ The work was supported by the National Natural Science Foundation of China under Grant No. 61822311

ing the false positive rate. Lu et al. (2018) studied the safety control of drones and developed an anomaly detection system based on reinforcement learning to prevent the drone motor from operating at abnormal temperatures. Since the large number of hyperparameters and complicated parameter tuning in the neural networks, it is difficult to be transplanted into practical applications. As a novel small sample learning method with a profound theoretical basis, OCSVM has received extensive attention in the fields where the negative samples are difficult to be collected, such as intrusion detection, fault detection and diagnosis, etc. Li et al. (2016) used the OCSVM classifier to establish an anomaly detection system for the national grid database, and verified the effectiveness of the system by taking the user behavior data set as an example. Guo et al. (2018) verified the effectiveness of OCSVM-based anomaly detection on the spacecraft flight dataset. In addition, the successful case of building an ICS security system using OCSVM-based anomaly detection can also be found in Li et al. (2018) and Gao et al. (2016).

However, the standard OCSVM algorithm needs to be improved in terms of detection accuracy, learning rate, and system scalability. Li et al. (2018) proposed an incremental OCSVM-based (I-OCSVM) anomaly detection model, which not only improved the learning rate but also made the system more scalable. Nevertheless, the overfitting of this approach results in insensitivity to stealthy attacks. In order to improve detection of stealthy attack detection in ICSs, this paper proposes a double-layer OCSVM-based (DL-OCSVM) intrusion detection method. The advantages of adopting this method are mainly reflected in the following three points. 1) The characteristic space consists of the time-frequency information extracted by the wavelet decomposition, which can truly reflect the physical characteristics of ICSs. 2) The defined adjacent classification interval and KKT conditions reduce the training samples, which improves the learning rate and system scalability. 3) Since the sample points belonging to the adjacent classification regions and violating the KKT condition are manually marked, the overfitting is avoided and the recognition accuracy for the boundary samples is improved. The experimental results of DL-OCSVM and I-OCSVM are compared on our self-developed experimental platform of the networked multi-axis motion control system. The results show that DL-OCSVM has superior performance in detecting stealthy attacks.

The organization of this paper is as follows. The problem formulation is introduced in Section 2. The proposed intrusion detection method is shown in Section 3. The validity and superiority of the algorithm are verified in Section 4. The last section is the conclusion.

2. PROBLEM FORMULATION

Numerical control systems (NCS) is one of the common industrial control systems, the general frame diagram of the networked NCS is shown in Fig. 1. A networked NCS generally includes remote server, local controller, and servo systems. During normal operation, the local controller receives the processing instruction from the remote server and sends a control command to the servo system, while the remote server monitors the system in real time by

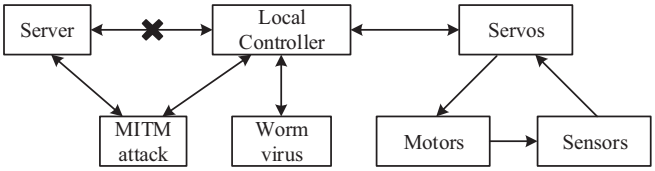


Fig. 1. Frame diagram of the networked NCS

receiving the uploaded sensor data. Without loss of generality, such industrial control systems usually have the following two types of threats. 1) Cyber attacks that occurs between the remote server and the local controller, such as man-in-the-middle (MITM) attacks. In MITM attacks, hackers implement the fake data injection attack (FDIA) by intercepting sessions between the remote server and the local controller. 2) Internal attacks that occur on the local controller, such as a worm virus. With the rapid development of computer technology, these two types of attacks have become more technical, hidden and targeted. Since the intrusion attacks have the physical characteristics of the ICS, the traditional information security-based methods become no longer applicable. Therefore, this paper focuses on signal analysis and is devoted to developing a new intrusion detection method for ICSs experiencing stealthy attacks.

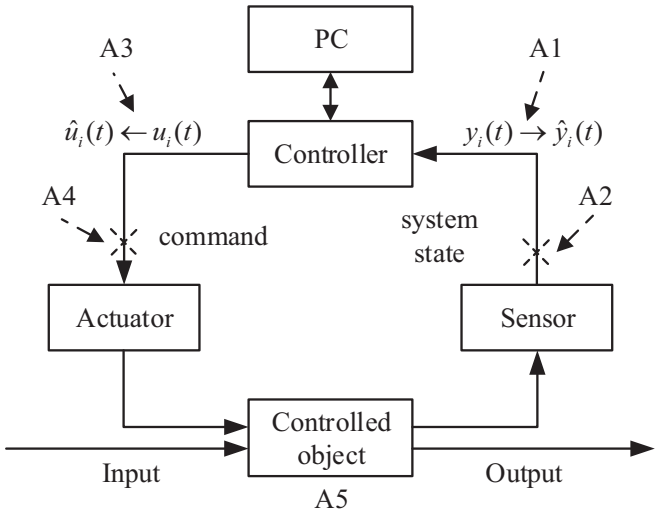


Fig. 2. The diagram of attack strategy in ICSs

Fig. 2 depicts the known attacks strategy in ICSs, where $A1$ = replacement of true sensor signals with false signals; $A2$ = disruption of sensor signals so they do not reach the controller; $A3$ = replacement of proper control signals with false signals; $A4$ = disruption of control signals so they do not reach the controlled object; $A5$ = replacement of using physical means to directly damage field devices or physical environments. As a result, $A1$ and $A3$ destroy the integrity of the data, $A2$ and $A4$ destroy the availability of the control network. As one of the FDIA strategy, the sinusoidal attack implemented at $A1$ was considered in this paper,

$$\hat{y}(t) = \begin{cases} y(t), & t \notin T \\ y(t) + w(t), & t \in T \end{cases} \tag{1}$$

$$w(t) = A(t)sin(2\pi f(t)t) \tag{2}$$

where, $y(t)$ and $\hat{y}(t)$ represent the true output and the tampered output of the system, respectively; $w(t)$ denotes a sinusoidal signal whose amplitude $A(t)$ and frequency $f(t)$ are time-varying; T is a set that includes all the moments when the system is under attack.

3. MAIN RESULTS

In this section, the derivation process and the main steps of the DL-OCSVM algorithm will be described in detail. First, time-frequency characteristics of the data set are extracted with the help of wavelet decomposition, which lays a foundation for further attack detection based on physical properties. In order to improve the learning rate and system scalability of DL-OCSVM, the KKT condition and the defined adjacent classification interval are adopted to reduce the training samples. Last but not least, the boundary samples defined in DL-OCSVM are used for incremental learning, avoiding overfitting and improving detection accuracy.

3.1 Feature extraction

Wavelet transform is an efficitive method to obtain a holonomic time-scale representation of local and transient phenomena occurring at different time scales. For time series $z(t)$, its continuous wavelet transform (CWT) can be defined as follows:

$$W_z(s,\tau) = \frac{1}{\sqrt{s}} \int_{-\infty}^{+\infty} z(t)\psi\left(\frac{t-\tau}{s}\right) dt \tag{3}$$

where ψ is a mother wavelet function, s can be interpreted as a scaling fator of $\psi(t)$, τ is used to control the temporal translation or shift of $\psi(t)$.

In practice, wavelet decomposition is an important direction of wavelet transform and is widely used in multi-resolution analysis of signals and images. As shown in Fig. 3, the time series $z(t)$ is decomposed into different resolutions (i.e. index i denotes the ith scale), while the approximate coefficients a_i and detail coefficients d_i are obtained. Thus, a non-stationary time series is able to be decomposed into stationary time series at several different scales.

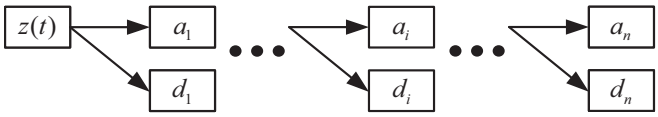


Fig. 3. Frame diagram of the wavelet decomposition

For a fixed-length digital signal, if it is shifted cyclically, its wavelet coefficient will change accordingly, that is, the wavelet coefficient without displacement invariance. Thus, the wavelet coefficient energies are used for signal characterization, providing the stealthy information in the hidden time-frequency domain. The energy of the approximate coefficient sequence $a = (a)_n$ is defined as

$$\|a\|_2 = \sum_{n=-\infty}^{+\infty} |a_n|^2 \tag{4}$$

where a_n is the approximate coefficient at the nth scale.

3.2 First layer: standard OCSVM model

According to Lang et al. (2020), the decision function of the standard OCSVM can be written as follows

$$\begin{aligned} f(x) =& sgn\left(\omega^T\phi(x_i) - \rho\right) \\ =& sgn\left(\sum_{i=1}^{n} \alpha_i K(x, x_i) - \rho\right) \end{aligned} \tag{5}$$

where ω denotes the normal vector of the classification hyperplane, x_i represents the training sample, y_i is the label of sample x_i, $f(x_i)$ is the function interval between the sample x_i and the decision boundary, $\phi(\cdot)$ is the mapping of the sample space to the characteristic space, $K(x, x_i)$ is a kernel function, ρ describes the distance from the origin to the hyperplane. According to KTT conditions, the former decision function can be rewritten as

$$y_i f(x_i) \begin{cases} > 1, & \alpha_i = 0 \\ = 1, & 0 < \alpha_i < \frac{1}{vn} \\ < 1, & \alpha_i = \frac{1}{vn} \end{cases} \tag{6}$$

where n represents the scale of the data set, $v \in (0, 1]$ is a coefficient to balance the upper bound of the negative samples in the data set, $\alpha_i \geq 0$ is the lagrange multiplier. As shown in (5), $\alpha_i = 0$ indicates that the corresponding sample is outside the classification interval; $0 < \alpha_i < 1/vn$ denotes that the corresponding sample is on the classification interval; $\alpha_i = 1/vn$ means that the corresponding sample is inside the classification interval. It can be proved that the new training sample set violating KKT condition (i.e. $\Omega = \{x_i | y_i f(x_i) < 1\}$) is most likely to change the decision boundary.

3.3 Second layer: improved OCSVM model

In incremental learning, the shape of the optimal hyperplane can be changed from the original support vector to the non-support vector, and vice versa. If only the original support vector set and the samples that violate the KKT condition are selected for re-learning, it may result in optimal hyperplane distortion and incorrect classification.

The adjacent classification interval is the maximum geometric interval between the second-layer convex hull and the decision boundary. Here, the second-layer convex hull in the sample space satisfying the KKT condition is obtained by the Graham scan method (as shown in Babu et al. (2017)). The adjacent classification interval can be wrriten as follows

$$\begin{aligned} \hat{\gamma} =& \max \gamma_i \\ =& \bar{y}_i \left(\frac{\omega}{\|\omega\|} \cdot \bar{x}_i + \frac{b}{\|\omega\|}\right) \end{aligned} \tag{7}$$

where $\bar{x}_i \in \Psi$, Ψ represents the second-layer convex hull, $\bar{y}_i$ is the label of sample $\bar{x}_i$, γ_i denotes the Euclidean distance from $\bar{x}_i$ to the decision boundary, b is the offset. Outside the decision boundary, the area within an adjacent classification interval from the decision boundary is defined as the adjacent classification region

$$\Theta = \{\tilde{x}_i | -\hat{\gamma}\|\omega\| < \tilde{y}_i(\omega \cdot \tilde{x}_i + b) < 0\} \tag{8}$$

where $\tilde{x}_i \in \Theta$, Θ represents the adjacent classification region, $\tilde{y}_i$ is the label of sample $\tilde{x}_i$. The samples that

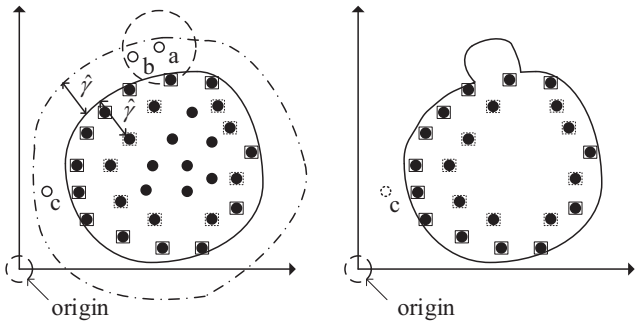
violate the KKT condition and fall into the adjacent classification region constitute a set of boundary samples, i.e. $P = \{p_i | p_i \in \Omega \cap \Theta\}$. Taking arbitrary boundary sample p_i as the center and twice the adjacent classification interval as the radius, the sphere formed is the neighborhood of the boundary sample p_i , and can be expressed as

$$\mathcal{N}_{p_i} = \{\hat{x}_i | 0 \leq \|\hat{x}_i - p_i)\|_2^2 \leq \hat{\gamma}\} \tag{9}$$

where $\hat{x}_i$ represents the point within the neighborhood of the boundary sample p_i.

3.4 Implementation of DL-OCSVM

The model training for the DL-OCSVM is depicted in Fig. 4. Samples that meet the KKT condition are marked as black, while the other points that violate the KKT condition are marked as white. The black points in the solid line frame are the vectors of first-layer convex hull, and the black points in the dotted line frame are the vectors of second-layer convex hull, as shown in Fig. 4(a). In addition, $\hat{\gamma}$ indicates the adjacent classification interval, and the area between the dotted line and the decision boundary is the adjacent classification interval region. In order to simplify the calculation and increase the model learning rate, the following two learning strategies are adopted for different boundary samples:



(a) First training (b) Second training

Fig. 4. Schematic diagram of DL-OCSVM

(1) Except for sample c, there are other boundary samples in the neighborhood of the selected boundary sample, i.e. sample a and sample b. In this case, all samples in the neighborhood of the selected boundary sample are used for the second-layer model training and are eliminated after training.
(2) The selected boundary sample is an isolated point, i.e. sample c. Then, skip this boundary sample and select the next boundary sample.

The main steps of the DL-OCSVM learning are shown in Algorithm. 1.

Algorithm 1 Framework of DL-OCSVM learning

Input: The set of positive samples X_{start};
Output: Ensemble of classifiers, E_i;

1: Extract the features of X_{start} with the help of wavelet decomposition;
2: Train the classifier E_0 of the standard OCSVM on X_{start};
3: Compute the first-layer and second-layer convex hull of X_{start} that satisfies the KKT condition with the help of Graham scan method, i.e. Φ and Ψ;
4: Compute the adjacent classification interval $\hat{\gamma}$ and define the adjacent classification region Θ;
5: Obtain the set of boundary samples P_0 with the help of Θ;
6: **while** $P_{i-1} \neq \varnothing$ **do**
7: Randomly select a sample p in P_{i-1} and construct its neighborhood $\mathcal{N}_p$ with the help of $\hat{\gamma}$. If there is not any other boundary samples in $\mathcal{N}_p$, goto step 11, else, continue;
8: Mark the set of samples Γ_i, $\Gamma_i = \mathcal{N}_p \cap (\Phi \cup \Psi \cup P_{i-1})$;
9: Train the classifier E on Γ_i;
10: Obtain ensemble of classifiers E_i, $E_i = E_{i-1} \cup E$;
11: Delete all boundary samples in the neighborhood $\mathcal{N}_p$ and reconstruct the set of boundary samples P_i for current batch. $P_i = P_{i-1} - P_{i-1} \cap \mathcal{N}_p$;
12: **end while**
13: **return** E_i;

4. EXPERIMENTAL VERIFICATION

In this section, the DL-OCSVM algorithm was tested using a self-developed physical experimental platform. As shown in Fig. 5, the experimental platform is mainly composed of the following four parts: the PC, servo system, local controller and attack kit. The PC uses the Windows 10 operating system, Intel(R) Core(TM) i5-4210M 2.6GHz processor, and 8GB of memory. The servo system consists of two ASDA-A2 high-performance communication servo drivers and two matching servo motors. The communication between the local controller and the servo system adopts the CANopen protocol, and data interaction between the PC and the local controller utilizes the Modbus/TCP protocol. The local controller is developed based on the STM32 embedded board. The attack kit implements a MITM attack by intercepting communication packets between the PC and the local controller. In addition, the human-computer interaction interface is developed based on PyQt5 and C++, which is convenient for researchers to quickly configure the experimental platform.

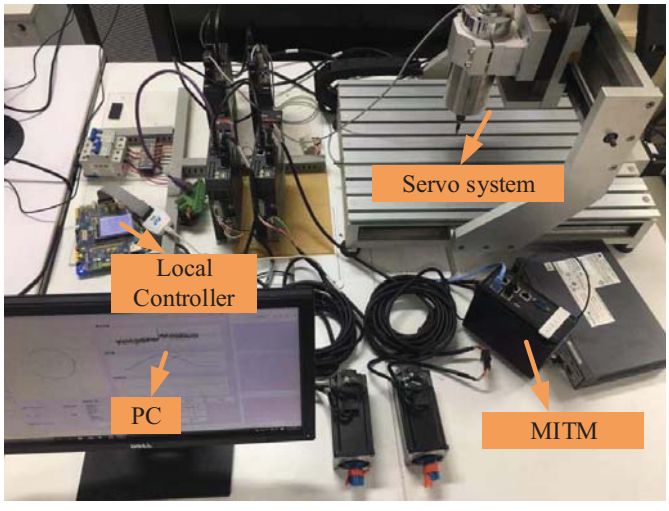


Fig. 5. Self-developed physical experimental platform

During the experiment, the system states (including speed, position and torque) are collected by the built-in sensor of the servo driver in real time, and transferred to the PC after being transferred by the embedded chip; the output control is sent to the embedded chip after being processed by the PC. The sampling frequency of the system is $100Hz$. Speed signals of the motors from a properly working system (for example, when the system is offline) were collected, and 1600 data points were randomly selected as the training set. The $db1$ wavelet was selected as the mother wavelet function. Then, the wavelet coefficient matrix was extracted by the five-layer wavelet decomposition, and the wavelet coefficients energy of the last three layers were selected as the feature data. The DL-OCSVM model was trained with the traning error $\mu = 0.01$, model complexity $\eta = 0.1$.

The indicators for evaluating the method can be written as follows

$$Precision = \frac{TP}{TP + FP} \tag{10}$$

$$Accuracy = \frac{TP + TN}{TP + FN + FP + TN} \tag{11}$$

$$Specificity = \frac{TN}{FP + TN} \tag{12}$$

$$FPR = \frac{FP}{FP + TN} \tag{13}$$

where TP indicates that the positive samples are correctly classified as normal, and TN is corresponding to the correct classification of the negative samples. FP indicates that the negative samples are falsely classified as normal, and FN is corresponding to the falsely classification of the positive samples. Note that, the expected signal from a properly working system should be defined as "positive samples", while the "negative samples" as the signal which results from the intrusion.

In order to verify the feasibility and effectiveness of the proposed detector, several test sets were designed and can be expressed as follows

$$case\ 1: w(t) = sin(2\pi t) \tag{14}$$

$$case\ 2: w(t) = log_2(t+1)sin(2\pi t) \tag{15}$$

$$case\ 3: w(t) = sin(2\pi t \cdot log_2(t+1)) \tag{16}$$

where, case 1 represents a sinusoidal attack with fixed amplitude and fixed frequency; in case 2, the amplitude is time-varying; in case 3, the frequency is time-varying. Note that, each test set consists of 1600 points, respectively. In the experiment, the system repeatedly executes the circular trajectory tracking motion with a period of $16s$ (i.e. 1600 points), and an injection is generated every three system operating cycles. For each group of tests, the duration of the experiment is 1 hour, i.e. 225 system operating cycles.

The experimental comparison results between the standard OCSVM and DL-OCSVM are shown in Table. 1. It can be seen that both the standard OCSVM and DL-OCSVM have high detection accuracy for cases 1-3. It is attributed to the use of wavelet decomposition, which is able to obtain information from both the time-domain and the frequency-domain of the signal. Compared to case 1, case 2 has a significant change in the time-domain, while case 3 has numerous peaks in the frequency-domain. As a result, case 1 has the simplest structure but is the least likely to be detected. It is worth noting that DL-OCSVM has superior performance in terms of precision and accuracy, which verifies the feasibility and effectiveness of the proposed DL-OCSVM.

Table 1. Performance comparison between standard OCSVM and DL-OCSVM

Dataset	Standard OCSVM		DL-OCSVM	
	Precision(%)	Accuracy(%)	Precision(%)	Accuracy(%)
Case 1	82.31	88.25	82.83	89.21
Case 2	93.44	95.30	93.54	96.05
Case 3	98.49	97.44	98.72	98.82

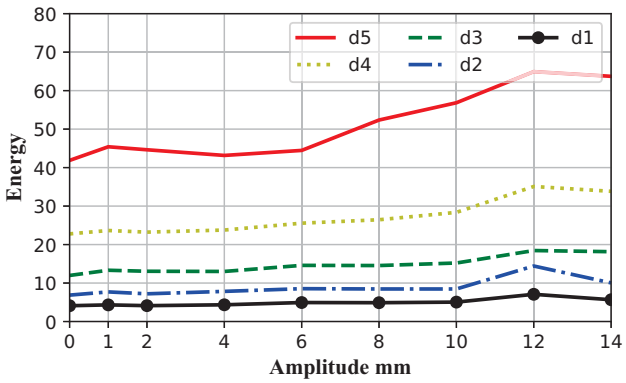


Fig. 6. The wavelet coefficient energies under different sinusoidal attacks

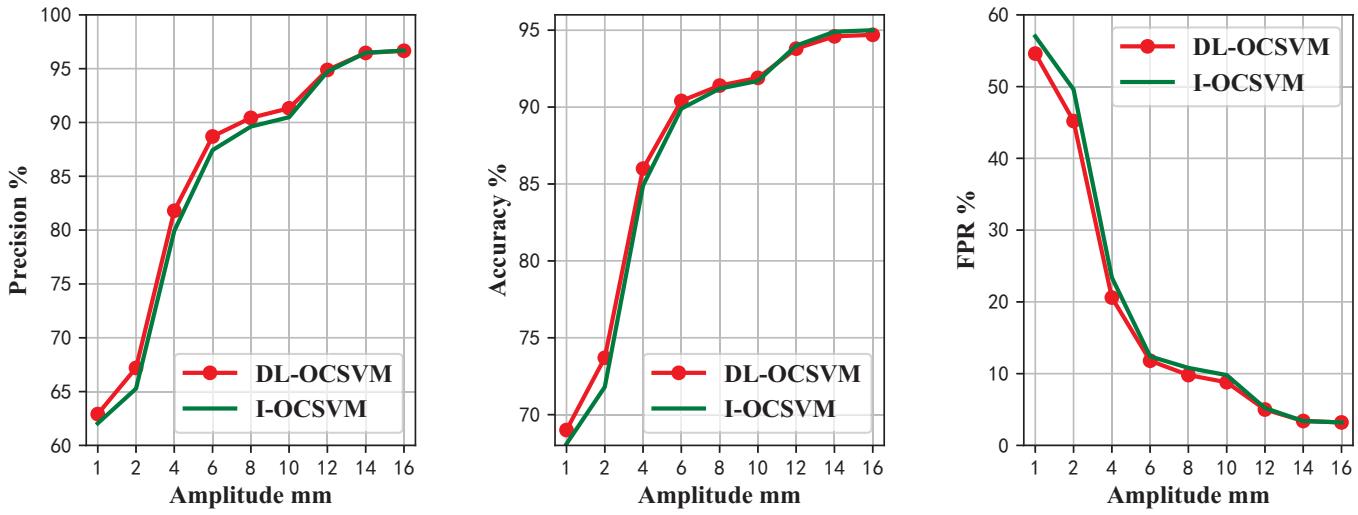
Furthermore, multiple sets of sinusoidal attacks with fixed frequency and different amplitudes are designed based on (14). The variation of wavelet coefficient energies under different amplitudes is shown in Fig. 6. We can see that, the smaller the amplitude of the attack signal is, the more hidden the attack is. The experimental comparison results between I-OCSVM and DL-OCSVM are shown in Fig. 7 and Table. 2. The horizontal axis coordinates in Fig. 7 correspond to the case 4-12, respectively. As shown in Fig. 7, the performance of DL-OCSVM and I-OCSVM are similar when the amplitude of the attack signal is large. However, the DL-OCSVM algorithm has superior performance in all the three indicators as the amplitude decreasing. Here, the normal working condition of the system is a circular trajectory tracking motion with the amplitude being 10 mm. As shown in Table. 2, the amplitudes of case 4-8 are lower than the normal case and are considered as stealthy attacks. As a result, the DL-OCSVM algorithm is more suitable for detecting the stealthy attacks in ICSs.

5. CONCLUSION

In this paper, an intrusion detection method based on DL-OCSVM is proposed to improve detection of stealthy false data injection attacks in ICSs. Compared with the standard OCSVM, the proposed approach reduces the training samples by using the adjacent classification interval and KKT conditions, thereby improving the learning rate and system scalability. In addtion, it is verified by experiments that the proposed approach performs better than the state-of-the-art approach proposed by Li et al. (2018) in detecting stealthy attacks.

Table 2. Performance comparison between I-OCSVM and DL-OCSVM

Dataset		I-OCSVM			DL-OCSVM		
Number	Characteristic	Precision(%)	Accuracy(%)	Specificity(%)	Precision(%)	Accuracy(%)	Specificity(%)
Case 4	A=1mm	62.05	68.10	43.00	62.91	69.00	45.40
Case 5	A=2mm	65.27	71.80	50.40	67.20	73.70	54.80
Case 6	A=4mm	79.93	84.90	76.60	81.80	86.02	79.40
Case 7	A=6mm	87.43	89.90	86.60	88.70	90.40	88.20
Case 8	A=8mm	89.62	91.21	89.20	90.43	91.43	90.20
Case 9	A=10mm	90.49	91.70	90.20	91.32	91.90	91.20
Case 10	A=12mm	94.72	94.00	94.80	94.88	93.80	95.00
Case 11	A=14mm	96.48	94.90	96.60	96.46	94.60	96.60
Case 12	A=16mm	96.68	95.00	96.80	96.66	94.70	96.80



(a) Precision (b) Accuracy (c) FPR

Fig. 7. Performance comparison between DL-OCSVM and I-OCSVM under different attack amplitudes

REFERENCES

A. Babu and S. Vishwanathan. Bounds for the Graham - Pollak theorem for hypergraphs. *Discrete Mathematics*, volume 342, issue 11, pages 3177–3181, 2017.

C. Feng, T. Li, and D. Chana. Multi-level anomaly detection in industrial control systems via package signatures and LSTM networks. *The 47th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Denver, CO, USA, June 2017.

X. Gao and R. Ma. Fault detection of batch process based on MSICA-OCSVM. *Chinese Control and Decision Conference (CCDC)*, Yinchuan, China, Aug. 2016.

K. Guo, D. Liu, Y. Peng, et al. Data-driven anomaly detection using OCSVM with boundary optimization. *Prognostics and System Health Management Conference*, Chongqing, China, Jan. 2018.

R.L. Lang, R.B. Lu, C.Q. Zhao, et al. Graph-based semi-supervised one class support vector machine for detecting abnormal lung sounds. *Applied Mathematics and Computation*, volume 364, pages 124487, 2020.

T. Li, Z.N. Hong, Z.Y. Liu, et al. Intrusion detection based on incremental one-class support vector machine for industrial control system. *Information and Control*, volume 47, issue 6, pages 755-760, 2018.

Y. Li, T. Zhang, Y.Y. Ma, et al. Anomaly detection of user behavior for database security audit based on OCSVM. *International Conference on Information Science and Control Engineering*, Beijing, China, Nov. 2016.

Z.A. Li and X.S. Li. Fault detection in the closed-loop system using one-class support vector machine. *IEEE 7th Data Driven Control and Learning Systems Conference (DDCLS)*, Enshi, China, Nov, 2018.

H.M. Lu, Y.J. Li, S.L. Mu, et al. Motor anomaly detection for unmanned aerial vehicles using reinforcement learning. *IEEE Internet of Things Journal*, volume 5, issue 4, pages 2315–2322, 2018.

Q. Wang, H. Chen, Y.H. Li, et al. Recent advances in machine learning-based anomaly detection for industrial control networks. *International Conference on Industrial Artificial Intelligence (IAI)*, Shenyang, China, Sep. 2019.

W. Wang, Y.Q. Sheng, J.L. Wang, et al. HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection. *IEEE Access*, volume 6, pages 1792–1806, 2017.

J. Yang, C.J. Zhou, S.H. Yang, et al. Anomaly detection based on zone partition for security protection of industrial cyber-physical systems. *IEEE Transactions on Industrial Electronics*, volume 65, issue 5, pages 4257–4267, 2018.