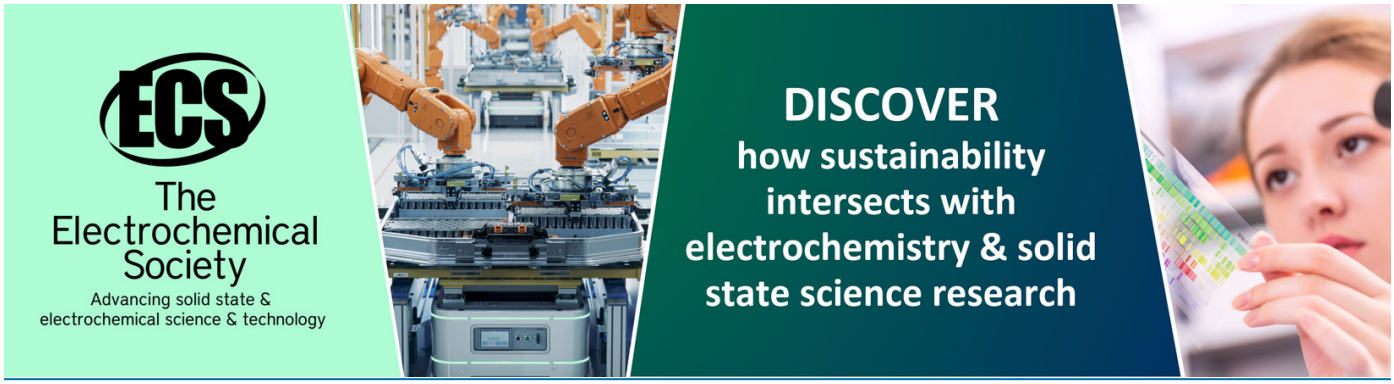
Anomaly Detection of ICS based on EB-OCSVM



IOP Conf. Series: Journal of Physics: Conf. Series **1267** (2019) 012054 doi:10.1088/1742-6596/1267/1/012054

Anomaly Detection of ICS based on EB-OCSVM

R B Zhang[1,a], L H Xia[1,b] and Y Lu[1,c]

[1]Hefei University of Technology, Hefei, Anhui

[a]zhangrb@hfut.edu.cn; [b]1428023665@qq.com; [c]luyang.hf@126.com

Abstract. Industrial process anomaly detection mechanisms have been proposed to protect industrial control system to minimize the risk of damage or loss of resources. In this paper, an one-class Support Vector Machine based extended boundary (EB-OSCVM) is used to detect anomalies in industrial multivariate time series data from a simulated Tennessee Eastman Process (TEP) with many cyber attacks. In detail, determine the change points of each process variable and capture the causality relationship between the variables based on the location and time delay of the change points. Then, by monitoring the leaf nodes in the causality graph, we can know whether the system is abnormal, it can effectively reduce the dimension of process data. The EB-OSCVM extend classification boundary of OCSVM in order to reduce the error of noise, if data is outside the boundary of EB-OCSVM, there is an anomaly. Finally, tracing the anomaly source according to causal direction. An experiment is used to verify the effectiveness of the proposed approach, the results demonstrate that the approach presents a high-accuracy solution and traces the source of anomaly correctly.

1 Introduction

The rapid growth of information and communication technologies has motivated the traditional industrial control system (ICS) to seek tighter integration between physical process and cyberspace. However, integrating the cyber and physical domain significantly reduces isolation of the physical system from the outside world, which increases their vulnerabilities and triggers a number of security problem [1,2].

Unlike information technology (IT) system, the main target of cyber-attacks on industrial control system is to cause a catastrophe by disrupting the physical process. An arbitrarily attack on the physical process would potentially cause the whole system to shut down. If only consider cyber information, the attack might be neglected when the activities are hidden or the evidence of the attack is insufficient to be identified as an anomaly in the cyber domain. Therefore, the information of relevant physical process for anomaly detection must be taken into consideration.

Different approaches have been proposed to detect anomalies in industrial physical process data, the goal of anomaly detection is find the unusual behaviors, i.e. behaviors that are not exhibited under normal operation.

Constructing a mathematical model of ICS for both physics and control dynamics can detect anomaly [3-7]. Literature [3] describes a process-oriented technology for detecting network attacks against programmable logic controllers (PLCs), using autoregressive methods to model specific process variables. Based on process attribute invariants, Urbina et al. [4-7] used Linear Dynamical State Space (LDS) to model physical processes and detect anomalies caused by network attacks. Unfortunately, creating a precise model of complex physical processes is a very challenging task, arising from the tight integration of algorithmic control and complex physical processes. It requires an

in depth understanding of the system and its implementation, which is a time consuming and cannot scale up to large and complex systems.

Most existing machine learning approaches focus on detecting anomalies in feature space, i.e., looking at data points with large deviation from normal space. These require little system knowledge and can detect a large range of attacks.

The RNN is one of the machine learning approaches used for anomaly detection in the SWaT system. However, due to the expensive training time, they only consider the first out of the six stages of the system [8]. As a follow-up work, the Deep Neural Network (DNN) and the one-class Support Vector Machine (SVM) models have been applied for anomaly detection in physical process data. All stages and attack scenarios are considered in this work. But, the DNN and one-class SVM can only detect fewer attacks [9]. Kravchik et al.[10] used a variety of deep neural networks architectures including different variants of convolutional networks to detect anomaly. The method can effectively detect the physical process anomalies of ICS and significantly superior to method in [9]. An RNN-based forecasting approach detected early anomalies in industrial multivariate time series data from a simulated Tennessee Eastman Process (TEP) with many cyber-attacks [11].

However, A significant shortcoming of the currently applied machine learning methods is that they provide little insight into the system and no explanation of detection results. All of the above articles can only detect anomalies and cannot Trace the cause of the anomaly.

In [12], a novel graphical model-based approach is proposed to learn the local behavior of a complex water treatment plant, which is used for anomaly detection. Timed automa are learned as a model of regular behaviors in sensors signal and Bayesian networks are learned to discover dependencies between sensors and actuators. It can detect cyber-attacks with high precision, and trace the cause of anomaly according to correlation between sensors and actuators. However, the method depends on the periodicity and linearity of industrial process data, and the practical industrial data usually do not satisfy.

In this work, we present a machine learning method of one-class SVM [13] based on extend boundary (EB-OCSVM) to detect attacks of Tennessee Eastman Process [14] (TEP), and trace the anomaly source. First, we use change points (CPs) to analysis causality between TEP variables and construct graph of causality. This method is suitable for both linear and non-linear system, and does not need to construct an accurate mathematical model to describe the correlation between variables. Then, obtaining normal classification boundary by training OCSVM, the boundary can be extended as anomaly detection control limit in order to reduce the error caused by noise. If process data exceeds control limit, anomaly is detected. Finally, if we capture anomaly in process data, trace the root cause of anomaly according to graph of causality.

2 Methodology

2.1 A Causal Discovery based Change Points

With the increase in scale and complexity of process operations in large industrial plants, anomaly may occur on any of the thousands of components, easily propagate along information and material flow pathways and affect other parts of the system. To determine the root cause of certain abnormality, it is important to capture the process connectivity.

In a complex industrial process, elements are not only connected to each other, they are also mutually dependent. The concept of causality has been introduced to describe the cause-effect relationships between variables or events. There are two characteristics of causality: (1) the cause occurs before the effect; (2) the cause contains information about the effect, we focus on the feature of causality that the cause occurs before the effect and the cause inevitably impel the effect to change.

2.1.1 Determination of change points. In this section, we propose a change-point detect method, determining unknown number of change points. The goal of change-point detection is to detect abrupt changes in the distribution of samples. Industrial process variables have characteristics of high delay

and high noise, even the same variable have different level of noise, so it is difficult to capture causality.

The most critical step of the proposed method is to determine change points of a given data sequence according to the change of tendency among process variables. It can be seen that a point in a data sequence with the maximum distance to a line connecting the starting and ending point of the sequence has the greatest impact on the tendency. Thus, we need to detect some special points, referred to as change points, representing the change of tendency among process variables.

First, in order to prevent that some process variables with large amplitudes erroneously play dominate roles, the proposed method preprocesses the raw data by normalizing the observations of each process variable in order to make data between 0 and 1. Given the raw data of a multivariate time series $\tilde{\mathbf{T}} = \{\tilde{\mathbf{X}}_i(n)\}$ for i=1, ..., M and n=1, ..., N, the normalized time series **T** is obtained as

$$\mathbf{T} = \{\mathbf{X}_i(n)\} = \{(\tilde{\mathbf{X}}_i(n) - \min(\tilde{\mathbf{X}}_i(n)))/(\max(\tilde{\mathbf{X}}_i(n)) - \min(\tilde{\mathbf{X}}_i(n)))\} \tag{1}$$

Where min and max denote the sample maximum and minimum value, respectively. The orthogonal distance from a point X_i to the line AB between the point X_A and X_B is defined by equation (2), namely, the distance between P and its projection on AB.

$$D_i = [(\left\|\overrightarrow{Ai}\right\|_2 \left\|\overrightarrow{AB}\right\|_2)^2 - (\overrightarrow{AB} \cdot \overrightarrow{Ai})^2]^{1/2} \Big/ \left\|\overrightarrow{AB}\right\|_2 \tag{2}$$

A potential change point P on a segment [s, e] is given by:

$$D_P = \arg\max_{s \le i \le e}^{P} \mathbf{D}_i \tag{3}$$

It can be shown that *p* is the maximum distance of the change-point location in interval [s, e]. The value D_p is tested against a threshold *Wt* in order to decide whether the null hypothesis of no change-point is rejected or not, recursively applying the above method on [s, p] and [p+1, e]. The algorithm stops in each current interval when no further change point are detected, that the obtained distance fall below threshold *Wt*.

2.1.2 Determination of threshold Wt. The *Wt* is the threshold to terminate recursive process, if *Wt* is to small, there are many false positive, and if *Wt* is to high, we will miss many change points. That is to say, a rational threshold has great influence on the determination of change point. Meanwhile, process variables have different level of noise, a fixed threshold used in different process variables is unpractical, We propose a method that can adaptively determine the threshold *Wt*.

Given a sequence T={X(i)} for s<=i<=e, s and e are start point and end point of sequence, respectively, two special indices s=1 and e=N.

(1)we calculating orthogonal distance from a point to a line connecting the starting and ending points of the sequence, obtain a change point P that makes orthogonal distance maximum. Then calculating first-order differential cumulative sum, which can represent the change of trend and the direction of change, in two segments [s, p] and [p+1, e], respectively, denoted as *sum_l* and *sum_r*. Last, we calculate the absolute value of the difference between *sum_l* and *sum_r*, denoted as *p_th*.

(2) calculating the maximum orthogonal distance of subsequence [s, p] , the process is as step (1), we can get the absolute value of the difference as *pl_th*;

(3)calculating the maximum orthogonal distance of subsequence [p+1, e], the process is as step (1), we can get the absolute value of the difference as *pr_th*;

(4) If *p_th* > *pl_th* and *p_th* > *pr_th*, then stop, otherwise, recursively applying the above method on [s, p] and [p+1, e].

Thresholds vary in the iteration process, and suitable for different levels of noise, so we can get change points without fixed threshold.

2.1.3 Causal analysis based change points. To describe the causal relationships between all the variables, a graph can be constructed with nodes denoting variables and arcs denoting their causal direction. Causality analysis provides an effective way to localize root cause of plant-wide abnormalities since a causal graph can represent the direction of anomaly propagation.

We construct a causal graph based on the number and location of change points, which can be used to reflect the causal relationship between process variables, even be used for anomaly traceability. Given variable X and Y, if X is the cause of Y, then Y must change when X changes. Since the industrial process variable has time delay and noise, the change points of Y will occur after X. If each change point of X can cause Y changes, and in the each change interval of X, the number of change points of Y remains constant, we can accept the hypothesis that X cause Y. Moreover, if Y change after X change, and X change after Y change, we can get the direction of correlation: X cause Y and Y cause X, that is to say, X and Y are mutually causal.

The change points method, a bivariate analysis, can capture a significant causality or an indirect causality. In order to distinguish direct or indirect causality between two variables, we use time delay as a rule. Given an underlying model is X->Y->Z, if the delay of X cause Z is less than the delay of Y cause Z, then we can say there is a direct causality between X and Z, otherwise, X indirectly caused Z conditioned on Y.

2.2 Anomaly Detection Based on EB-OCSVM

Recently, unsupervised machine learning was shown to be effective for detecting ICS attacks. In this paper, we apply EB-OCSVM algorithm to detect anomaly in industrial control system. The EB-OCSVM builds a model from training on normal data and then classifies test data as either normal or attack based on its classification boundary.

Physical process data of ICS has high noise, we used OCSVM to learn classification boundary and obtain label after training, then stripped noise data where label is -1 as normal data, we can get upper control limit (UCL) and lower control limit (LCL), where UCL, LCL is maximum and minimum value of normal data, respectively. Lastly, we extended control limit as the abnormal boundary of EB-OCSVM in order to reduce false positive because of strong noise, denoted by

$$UCL = UCL + \alpha \times \delta(x) \tag{4}$$

$$LCL = LCL - \alpha \times \delta(x) \tag{5}$$

Where x is normal data after noise elimination,δ is standard deviation of x, α is parameter that determine the allowable error range. So, we obtain boundary control to determine that an anomaly has occurred, i.e. if data is greater than UCL or lower than LCL, we determine that an anomaly is detected. In this work, we define α as 3.

By monitoring the leaf nodes, we can monitor the whole variables of causality graph whether is abnormal. It is reduce dimension of process data. If a leaf node is abnormal, the parent node of the leaf node should be analyzed, until the parent node of the current node is normal, so, the current node is the source of the anomaly.

3 Experiments

3.1 TEP Description

In this experiment, we used the TEP dataset [15]. TEP is a benchmark simulation model to test process control and monitoring approaches, represented in Figure 1. It was simulated at different normal modes and under cyber-attacks. The TEP has five major units: a reactor, a compressor, a separator and a stripper, the dataset contains 11 manipulated variables, 22 process measurements and 19 analyzer measurements. Our experiment focuses on reactor unit, including 4 measurements: reactor level, reactor pressure, reactor temperature, reactor cooling water temperature and 1 manipulated variable: reactor cooling water flow.

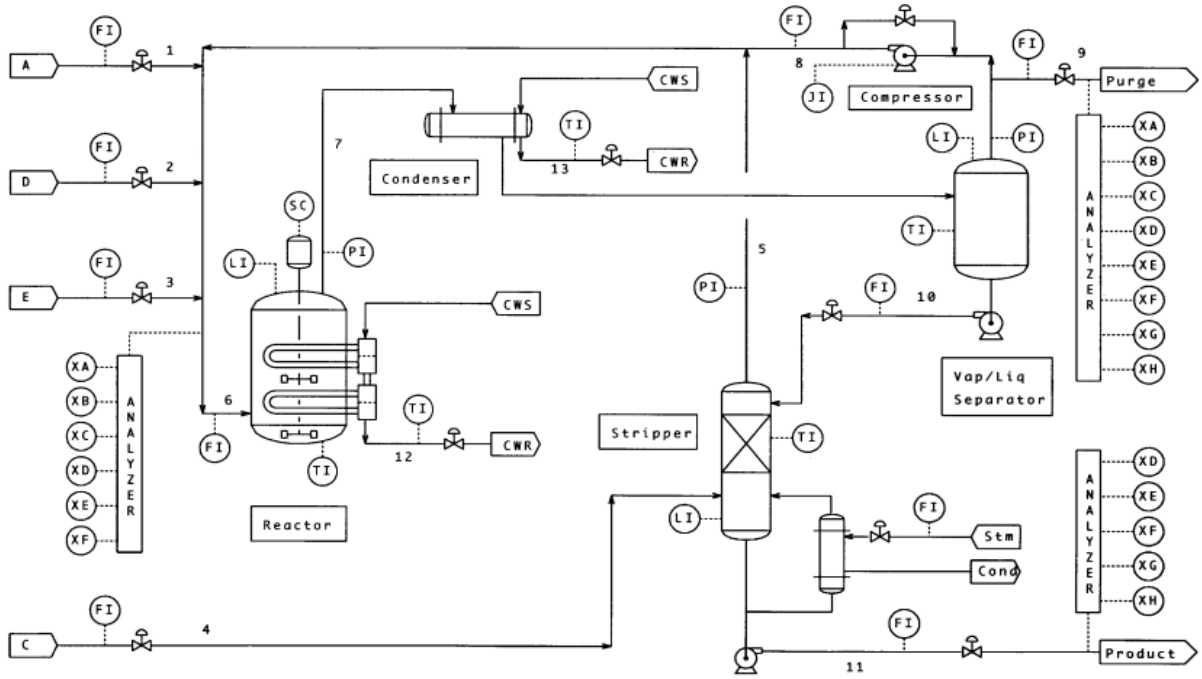
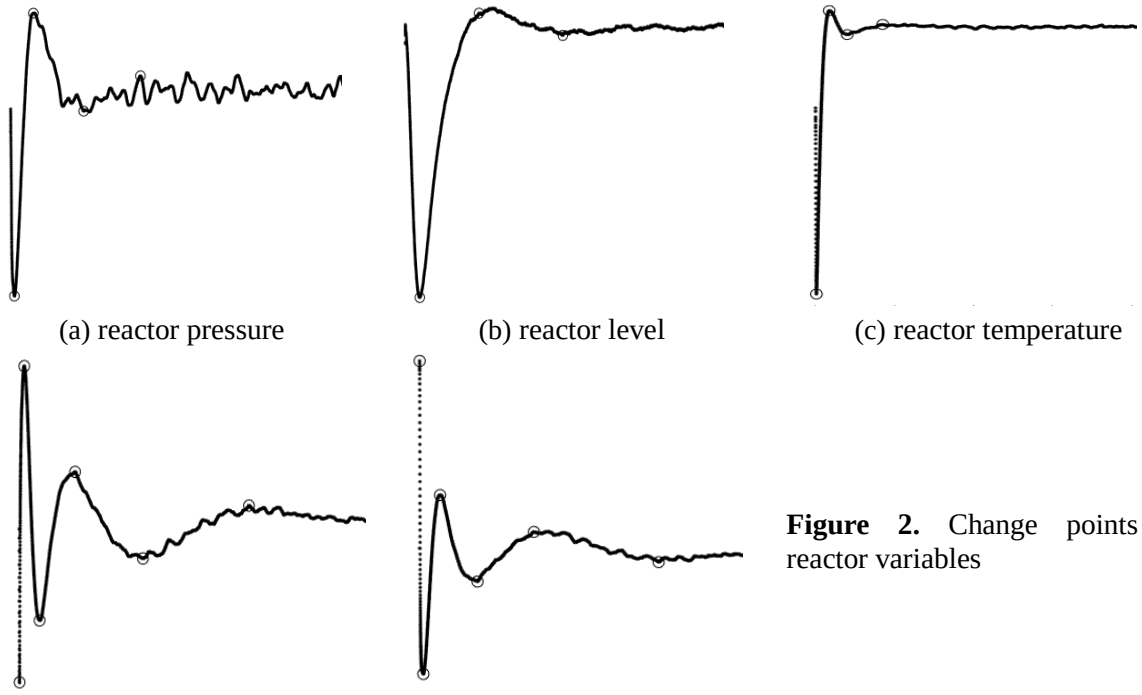


Figure 1. Tennessee Eastman Process

3.2 Causality graph based on change-points

We use change points to capture causality between reactor variables. According to experiment, we can get change points as circle points in Figure 2, as can be seen from the figure, the location of the change points are accurate.



(a) reactor pressure (b) reactor level (c) reactor temperature

(d) reactor cooling temperature (e) reactor cooling water flow

Figure 2. Change points of reactor variables

Then, analyse causality according to the number and occurrence time of change points. The occurrence time and number of change points shown in Table 1.

Table 1. Information of change points

NO	Reactor pressure	Reactor level	Reactor temperature	React cooling temperature	Reactor cooling water flow
1	292	1146	58	23	4
2	1728	5752	867	345	248
3	5548	12283	2002	1394	1348
4	9859		4245	3828	3812
5				8483	7528
6				15755	15739

First, we get a pair of variables with same number of change point: react pressure and reactor temperature, represent as A and B respectively. The change points occurs time of A takes precedence of B according chronological order, We can conclude that the change in A affects B, that is, A is cause of B denoted A->B. Similarly, the cause of reactor cooling water flow is react cooling temperature.

Next, we compare variables with different number of change points, like reactor level and react cooling temperature. The first change point of reactor level occurs at 1146, we search for the change point of react cooling temperature that is closest and greater than 1146 at 1394. By same ways, we show the results in Table 2. Calculating the number of change points of reactor cooling temperature between the previous change point and the current change point of reactor level, because of different numbers of change point, reactor level is not affect react cooling temperature and react cooling water flow. The causal relationship analysis process between other variables is as described above.

Table 2. Analyze change points of reactor level

CP of Reactor level	1146	5752	12283
CP of React cooling temperature	1394	8483	15755
Number of CP of React cooling temperature		2	1
CP of React cooling water flow	1348	7528	15739
Number of CP of React cooling water flow		2	1

Finally, for direct causality and indirect causality, we consider that the smaller the time delay is, the more direct causation is. As mentioned above, the causal graph is shown in Figure 3.

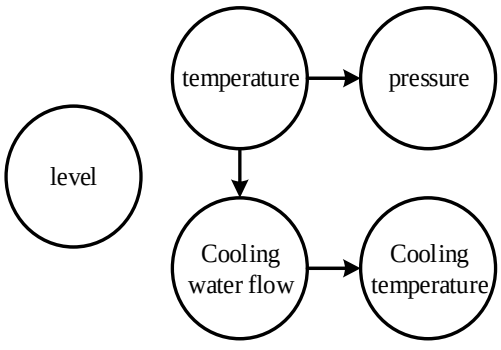


Figure 3. Causality graph of TEP reactor

3.3 Anomaly detection based on EB-OCSVM

In this paper, we use EB-OCSVM algorithm to detect anomaly, seek boundary of normal data. In order to thoroughly evaluate anomaly detection techniques, four evaluation indexes are adopt: accuracy (A), false positive rate (FPR) , false negative rate (FNR) and recall rate (R), where T represents a normal state and F represents a abnormal state. Their definitions are described as follows:

$$A=(TP+TN)/(TP+TN+FP+FN) \quad (6)$$

$$FPR=FP/(FP+TN) \quad (7)$$

$$FNR=FN/(FN+TP) \quad (8)$$

$$R=TP/(TP+FN) \quad (9)$$

There is no anomaly of reactor level, Table 3 shows the experimental results of TEP variable except reactor level.

Table 3. Effect of anomaly detection

	Reactor pressure	Reactor Temperature	React cooling Temperature	Reactor cooling water flow
A	99.93%	99.87%	98.59%	99.72%
FPR	0.06%	0.13%	1.38%	0.16%
FNR	1.7%	0%	4.77%	12%
R	98.3%	100%	95.23%	88%

It can be seen from Table 3 that EB-OCSVM-based anomaly detection method has higher accuracy and recall rate. Although the partial variable has a high false negative rate, EB-OCSVM can effectively detect process data anomalies.

3.4 Analyze the source of anomaly

In section, we obtained causality graph of reactor unit, combining with anomaly detection results, we can capture the source of the anomaly. If EB-OCSVM detect an abnormality in the reactor pressure, it needs to analyze the cause of the reactor pressure in the causality graph. If the node has an abnormality, continue to analyze the parent node of the cause node until the parent of the current variable is normal. So anomaly is generated by the current variable. Because of the cause of reactor pressure is abnormal and the cause variable does not have a parent node, the anomaly is caused by the reactor temperature.

4 Conclusion

In this paper, EB-OCSVM was proposed to detect anomaly of industrial control system process. We used change points capture causality between process variables, which change points were determined by maximum distance to a line connecting the starting and ending point of the sequence. It can obtain an unknown number of change points and be used for periodic and non-periodic systems. By analyzing the number and time delay of change points, the correlation between the variables and the causal direction are obtained. The process variable , which is the leaf node in the causal graph, were classified into normal or abnormal ones by EB-OCSVM, if there is an anomaly detected, trace the causality graph to determine the source of anomaly. The results illustrated the effectiveness of the proposed method.

REFERENCES

[1] RAVAL S, BlackEnergy a threat to Industrial Control Systems network security [J], *International Journal of Advance Research in Engineering, Science & Technology (IJA- REST)*, 2015, 2(12).

[2] LIU N, YU X H, ZHANG J H, Coordinated Cyber-attack: Inference and Thinking of In- cident on Ukrainian Power Grid[J], *Automation of Electric Power Systems*, 2016, 40(6):144-147
[3] Adepu S, Mathur A, Detecting Multi-Point Attacks in a Water Treatment System Using Intermittent Control Actions[C]// Inaugural Singapore Cyber Security R&d Conference, 2016.
[4] Adepu, S., Mathur, A., Distributed detection of single-stage multipoint cyber attacks in a water treatment plant, In: Proceedings of ACM Asia Conference on Computer and Communications Security (AsiaCCS 2016), pp. 449–460, ACM (2016).
[5] D. I. Urbina, J. A. Giraldo, A. A. Cardenas, et al, Limiting the impact of stealthy attacks on industrial control systems. In Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS), pp: 1092–1105. ACM, 2016.
[6] D. I. Urbina, J. Giraldo, A. A. Cardenas, et al, Survey and new directions for physicsbased attack detection in control systems. US Department of Commerce, National Institute of Standards and Technology, 2016.
[7] H.R.Ghaeini, et al, State-Aware Anomaly Detection for Industrial Control Systems, SAC 2018: Symposium on Applied Computing, 2018.
[8] Goh J, Adepu S, Tan M, et al, Anomaly Detection in Cyber Physical Systems Using Recurrent Neural Networks[C]// IEEE, *International Symposium on High Assurance Systems Engineering. IEEE*, 2017:140-145.
[9] J. Inoue, Y. Yamagata, Y. Chen, C. M. Poskitt, and J. Sun, Anomaly detection for a water treatment system using unsupervised machine learning, in Proc. IEEE International Conference on Data Mining Workshops (ICDMW 2017): Data Mining for Cyberphysical and Industrial Systems (DMCIS 2017). IEEE, 2017, pp.1058–1065.
[10] Moshe Kravchik, Asaf Shabtai, Detecting Cyber-attacks in Industrial Control Systems Using Convolutional Neural Networks, 2018
[11] Filonov P, Kitashov F, Lavrentyev A. RNN-based Early Cyber-Attack Detection for the Tennessee Eastman Process, ICML 2017 Time Series Workshop, 2017.
[12] Qin Lin, Sridha Adepu, Sicco Verwer, and Aditya Mathur. 2018. TABOR: A Graphical Model-based Approach for Anomaly Detection in Industrial Control Systems. (2018).
[13] Maryamsadat Hejazi , Yashwant Prasad Singh, ONE-CLASS SUPPORT VECTOR MACHINES APPROACH TO ANOMALY DETECTION, *Applied Artificial Intelligence*, 27:5, 351-366, 2013.
[14] Downs, J and Vogel, E. A plant-wide industrial process control problem, *Computers & chemical engineering*, 17(3):245–255, 1993.
[15] Tennessee Eastman Process with cyber-attacks dataset, URL: https://kas.pr/ics-research/dataset_tep_59, 2017.