Anomaly Detection Based on Zone Partition for Security Protection of Industrial Cyber-Physical Systems

Jun Yang, Chunjie Zhou, Shuanghua Yang, *Senior Member*, *IEEE*

***Abstract*—Integrating the cyber domain and physical domain for the flexibility and efficiency of supervision, management and control is the development tendency of traditional industrial systems. But, with the deep integration of these industrial cyber-physical systems, potential security hazards become severer. Anomaly detection as the front-end protective barrier plays an important role in security protection. However, traditional methods mostly focused on cyber information, without fully considering the characteristics of the physical domain, presenting some limitations. In this paper, a detectable oriented zone partition method for physical system and a zone-based anomaly detection approach are designed for industrial cyber-physical systems. In detail, an automated zone partition approach for the target of ensuring crucial system states can be represented in more than one zone is designed firstly. And then, a method of building zone function model without any prior knowledge of the physical system and analyzing the anomaly based on zone information are presented. Finally, an actual testbed is constructed to verify the effectiveness of the proposed approach. The results demonstrate that the proposed method presents a high accuracy and good real-time performance.**

***Index Terms*—Industrial cyber-physical systems, physical domain, anomaly detection, zone partition, zone function model.**

I. Introduction

THE rapid growth of information and communication technologies have prompted the traditional industrial control systems creating a tighter integration between physical process and cyberspace, and lead to the emergency of Industrial Cyber-Physical Systems (ICPSs) [1], [2]. Integrating the cyber domain and physical domain provides significantly less isolation for physical system from the outside world than predecessor systems, creating a greater vulnerabilities and cyber security problems [3]. Meanwhile, with the widely used of public networks and universal protocols, it is very convenient for attackers to access and acquire the operation right of the control systems [4]. On the other hand, as the adversarial sources, attackers try their best efforts to destroy the system defense and implement the malicious behaviors in ICPSs. Therefore, the new-type and unknown attacks emerge in endlessly, and ICPSs are faced with great threats [5]. The number of security-related incidents in ICPSs are increasing year by year according to the reports by the Industrial Control Systems Computer Emergency Readiness Team [6]. Seriously, as ICPSs have the direct connection for national economy, the safety of personnel, environment and property, once they are invaded by malicious attacks, the severity of the catastrophe would be incalculable [7], [8].

As the front-end protective barrier, intrusion detection plays an important role in security protection, and it can be classified as either signature-based or anomaly-based [9]. Signature-based methods use the database or fixed signatures to identify attacks, presenting a good result. But they are no fit for ICPSs as new-type and unknown attacks increasing rapidly. On the contrary, anomaly-based methods attempt to observe system behaviors or tendency, which show the capability of addressing the new or unfamiliar intrusions, and become a most popular method at present [10].

Unlike IT systems, both cyber domain and physical domain should be taken into account in anomaly-based detection for ICPSs. Meanwhile, the main target of cyber attacks in ICPSs is to cause a catastrophe (such as hazardous accident or production loss etc.) by manipulating and disrupting physical process [11]. And due to the feedback control loop, attacks arbitrarily acting on physical process would break down the whole system. Nevertheless, when behaviors are concealed or evidences are insufficient to determine as an anomaly in cyber domain, the attacks may be neglected if only cyber information under consideration. Therefore, physical process features are the key informations for the detection and must be taken into full consideration.

The physical system often presents a fixed model or predictable behaviors, which enables that the anomaly could be analyzed from the true physical process dynamics. These characteristics have been attracting the attention of many researchers. In many anomaly detection systems, physical system models [12], state equations [13] and statistical methods [14] were widely used to bulid the feature models of physical systems. However, models or parameters are hard to obtain in many actual systems, and the statistical data is undulate as the disturbance. On the other hand, most of existing methods do not consider that multiple sensor values and control commands are invaded simultaneously.

Zone partition is a very effective defense in security protection, because, it is hard for attacks to intrude sundry zones simultaneously when the physical system has been partitioned into multiple zones with different protection and defensive strategies [15]. Therefore, if a state could be described in multiple zones, the anomaly of the state would be detected in surviving zones. In this paper, a detectable oriented zone partition method for physical system and a zone-based anomaly detection approach are designed for ICPSs.

First, to partition the physical system into multiple zones, and ensure the crucial states could be represented in more than one zone, a causal model which includes all variables' relationship of physical system is constructed, and an automated zone partition algorithm on the basis of the causal model is proposed. Second, to accurately describe crucial states in each zone, a feedforward neural network is selected to build the zone function model. And the anomaly analysis conditions and methods are presented according to the system and zone features. Finally, the effectiveness of the proposed approach is verified through a series of experiments on an actual testbed. It is worthy to mention that, the anomaly this paper considering is caused by attacks, and for an anomaly caused by faults, it could be detected and analyzed by the mature fault diagnosis systems.

The rest of this paper is organized as follows. Section II introduces the current anomaly detection technologies in ICPSs, and the purposes of zone partition for security protection. Section III proposes a detectable oriented zone partition approach with an automated algorithm. Section IV presents an approach to analyze the anomaly in different zones. In section V, an actual testbed is built for analyzing and verifying the proposed approach, and then, the accuracy and real-time performance are discussed. The concluding remarks and future work are made in Section VI.

II. Background

A. Anomaly Detection in ICPSs

Recent years, anomaly detection both on cyber domain and physical domain have been widely studied in ICPSs. From the view of cyber domain, it mainly focused on traffic analyzing, protocol analyzing, behavior analyzing etc., with the approaches of statistics-based, model-based, machine-learning-based and so on [16]–[19]. However, there are some limitations in these methods, such as: 1) it is hard to deep parse all of the industrial protocols as the diversity and complexity. Thus, the problem of false negative and false positive are more difficult to be solved comparing with IT systems [9]; 2) the purpose of attacks is to destroy the physical object, the abnormal behaviors may not be reflected in cyber domain; and 3) the pathway of attacks is not only from the cyber network, but also from unsafe mediums., such as Stuxnet which intruded Siemens systems on the carrier of removable storage devices [20]. What's worse, once a deliberate sabotaging behavior acted on physical system, a disaster accident would happen. Therefore, it is indispensable to detect the anomaly in physical domain for ICPSs.

Statistical methods are the most widely used methods for anomaly detection in physical processes, such as *Shewhart* chart, cumulative sum (CUSUM), Exponentially Weighted Moving Average (EWMA) etc. [14]. Hu X. et al. [21] employed the hotelling's T^2 statistic to handle multivariate anomaly detection problem in control systems. Harrou F. et al. [22] integrated Principle Component Analysis (PCA) and EWMA to develop two process-monitoring detecting tools, T^2-EWMA and Q-EWMA, which exhibited an effective approach to balance the false negative rate and false positive rate. Similarly, system state equation was regarded as another useful method. Cárdenas A. et al. [12] used the system state equation to predict expected outputs, and compared it with the measured sensors' value, then CUSUM was introduced to make an anomaly analysis decision. Fabio P. et al. [23] proposed a mathematical framework for cyber-physical systems and attacks based on geometric control theory, which characterized undetectable and unidentifiable attacks perspectives. Meanwhile, according to some researches, actuators' behavior logic also was taken into account. Khalili A. and Sami A. [24] enumerated all regular behaviors of the field devices, the detection system regarded whether the system would reach the critical state as the estimation criteria. Li W. et al. [25] considered the control data were the most direct and key factors that influenced the behavior of the physical processes, and focused on control sequences to analyze the false sequential logic attacks.

But, these methods only consider that one or a few variables are anomaly. When multi-variables are invaded simultaneously, the results would be useless, and if the analyzed variables are deceived by an intelligent attacker which keeps the pace with the estimated/expected state, the anomaly could not be detected under this circumstance. Besides, the expression of system model or equation of states take a deep professional knowledge for engineers, and the parameters are hardly to know or imprecise in actual field systems.

B. Zone Partition for Security Protection

Zone partition and isolation as an effective security protection method is widely used in IT domain and ICPSs domain. *IEC62443* (one of the most important standards for industrial systems security protection) introduced a concept of "zones and conduits" for the intention of facilitating detailed risk assessment, identifying security measures requirement and protecting system safety [26]. It strongly suggested that system designers should partition the network or system into multiple physical or logical security zones and use the conduits (specific channels) to communicate among the zones. Based on this idea, Genge B. et al. [27] regarded the design of industrial systems as an integer linear programming problem, and designed a secure scheme on "zones and conduits". Gao F. et al. [28] presented a security architecture for intranet based on zone partition and isolation, and introduced a method to protect the zone border and communication depending on the ISO model. Jin Y. et al. [29] partitioned the business subsystems of military information system (MIS) into different secure domains, and proposed a MIS access control method based on security domain-oriented-administrative role-based control model to manage and control the secure domains. As a secure strategy of intrusion response, Jee J. et al. [30] controlled the communication by network control center to prevent the vicious attacks and invasions spreading to other subsystems through partitioning and isolating the intruded subsystems.

On the other hand, zone partition is also a effective and reliable approach for security or anomaly analysis. Krishnan K. [31] used an adaptive distributed algorithm to detect large-scale intrusions by partitioning sensors into multiple virtual

"computational domains" with relation graph. Yoshihiro H. et al. [32] constructed a series of cause-effect matrixs from the relationship of the field physical devices, and evaluated whether the zone partition result satisfied the detectability for cyber-attacks detection. And on the basis of it, this group [33] designed a zone partition method based on fault tree, which was constructed with the purpose of ensuring system safety, and employed PCA to detect cyber-attacks. But the detection did not rely on the partitioned zones, and zone partition method was hard to handle the conflict between partition and evaluation.

C. Architecture of Anomaly Detection for ICPSs

Architecture of the approach this paper proposed is shown in Fig. 1, and it is divided into two parts: 1) system knowledge, and 2) zone-based anomaly detection. In the first part, system feature includes the process of control, the information of field devices, and the disturbance of physical system. Zone information is the results of zone partition, and zone function model is used to describe the crucial system state in each zone. In the second part, the process consists of two processes. The first is distributed feature calculation in each zone, which addresses the filed data by filtering and feature extraction firstly, and then computes the crucial state depending on the processed data. The second is anomaly analysis. Crucial state from different zones would be compared with each other, and anomaly is recognized according to the normal conditions and the comparison results.

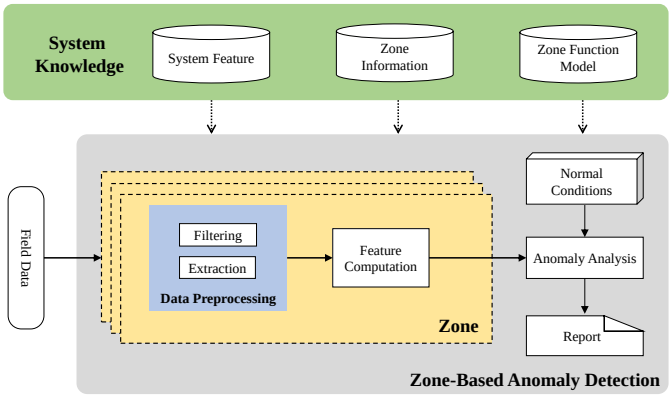

Fig. 1. Architecture of the zone-based anomaly detection for ICPSs

III. Zone Partition of Physical System for Anomaly Detection

As mentioned above, the proposed anomaly detection method is based on the crucial states which could be described in different zones. Thus, how to partition the physical system into multiple zones is the primary task. This section presents a detectable oriented zone partition method, which is based on the cause-effect relationships in physical process systems. At first, a basic causal model for a target node is introduced, and then the partitioning method based on the basic causal model is proposed.

A. Causal Model

Causal model describes the cause-effect relationships among process variables and shows the propagation of influence which has been widely used in industrial systems [34]. It is composed by nodes and directed arcs. The nodes represent the system state variables, the directed arc connecting two nodes represents the effect propagation direction, and if two adjacent nodes can affect each other, the arc should be two-way [35].

In this paper, cause model is used to express the qualitative relationships among the variables of a physical system. For a target node s (a analyzed variable), its causal model can be divided into two parts: cause nodes and effect nodes. Cause nodes are the ones which could affect s, and effect nodes are the ones which could be affected by s. Fig. 2 shows its basic structure. $\boldsymbol{c}_s = \{c_s^1, c_s^2\}$ is the cause set of s, and $\boldsymbol{e}_s = \{e_s^1, e_s^2, e_s^3\}$ is the effect set. There are both two situations for the two sets. In $\boldsymbol{c}_s$, c_s^1 can affect not only the target node s, but also another node e_s^1, but c_s^2 can only affect s. And in $\boldsymbol{e}_s$, e_s^2 will be affected only by s, but e_s^1 and e_s^3 will be affected not only by s, but also by c_s^1 and $\hat{s}$.

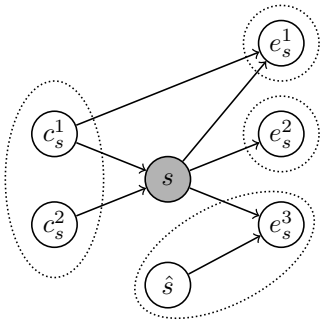

Fig. 2. The basic structure of causal model for the target node s

From the causal model, it can be qualitatively summarized that: 1) if all the states in $\boldsymbol{c}_s$ could be obtained, the state of s can be inferred; and 2) if any state in $\boldsymbol{e}_s$ could be obtained, the state of s can also be inferred. But, in Fig. 2, if the states of e_s^1 and e_s^3 need to be used for analyzing the state of s, their other cause nodes should be took into consideration. For e_s^3, as it can be affected by s and $\hat{s}$, the state of s can not be inferred only by e_s^3. In this situation, the two nodes e_s^3 and $\hat{s}$ will be regarded as an entirety in effect set, expressed as $e_s^{3'} = e_s^3 \cup \hat{s}$. But for e_s^1, as c_s^1 have already been placed in $\boldsymbol{c}_s$, c_s^1 could not be placed in $\boldsymbol{e}_s$. Finally, the corresponding cause set and effect set for the node of s are $\boldsymbol{c}_s = \{c_s^1, c_s^2\}$ and $\boldsymbol{e}_s = \{e_s^1, e_s^2, e_s^{3'}\}$.

B. Zone Partition Method

Causal model of a physical system represents the inter-relations of all the variables, and if one or part of the variables are invaded, the anomaly would be revealed from others. Detectable oriented zone partition is to separate these associated variables into multiple zones, and ensure that each zone could completely represent the states of the target nodes.

According to the qualitative summary for a causal model, for any node s, $\boldsymbol{c}_s = \{c_s^1, c_s^2, \ldots, c_s^m\}$ and $\boldsymbol{e}_s = \{e_s^1, e_s^2, \ldots, e_s^n\}$, where m and n are the number of nodes in each set, its state can be described by itself, all the elements in

$\boldsymbol{c}_s$, and each element in $\boldsymbol{e}_s$ severally. Therefore, a set named detectable-set is defined for s:

$$\boldsymbol{d}_s = \boldsymbol{c}_s \oplus \{e_s^1\} \oplus \{e_s^2\} \oplus \cdots \oplus \{e_s^n\} \oplus \{s\}, \tag{1}$$

where '$\oplus$' denotes the *minkowski sum* [36] which means that each set in the expression is regarded as a mutual independent element, such as $\boldsymbol{c}_s$, $\{e_s^1\}$, $\{s\}$ and so on, and the state of the node s can be described by any element in $\boldsymbol{d}_s$. The detectable-set for the basic structure in Fig. 2 is: $\boldsymbol{d}_s = \boldsymbol{c}_s \oplus \{e_s^1\} \oplus \{e_s^{2'}\} \oplus \{s\}$. The detectable-set for the whole system with ℓ target nodes is $\boldsymbol{d} = \{\boldsymbol{d}_{s(i)} | i = 1, 2, \ldots, \ell\}$.

Therefore, when the target node s, the set of $\boldsymbol{c}_s$, and each element in $\boldsymbol{e}_s$ are partitioned into different zones, the state of s can be observed in these zones. However, first of all, the basic function of the system must be assured, that is to say, from the view of system control, the systematic control loop should be maintained. Sensors and actuators in each control loop should be regarded as an unseparated group. A set named partner-set $\boldsymbol{p}_s$ is defined in this paper. $\boldsymbol{p}_s = \{n_1, n_2, \ldots, n_k\}$ denotes that there are k variables in the loop for controlling the state of s. The partner-sets for the whole system with κ control loops is $\boldsymbol{p} = \{\boldsymbol{p}_{s(i)} | i = 1, 2, \ldots, \kappa\}$.

Zone partition for a complex system by manual efforts is a time-consuming way. An automated partition algorithm is proposed in this paper. The principle and detailed steps of detectable oriented zone partition method are summarized in Algorithm 1, where '$\varnothing$' denotes empty set, and '$\oplus$' also represents the *minkowski sum*. First, $\boldsymbol{c}_s$, each element in $\boldsymbol{e}_s = \{e_s^1, e_s^2, \ldots, e_s^n\}$, and the target node s are partitioned into different zones; And then, merge all the zones if they overlap with the same p_s.

Algorithm 1 Zone Partition Algorithm.

In: $\boldsymbol{d} = \{\boldsymbol{d}_{s(i)} | i = 1, 2, \ldots, \ell\}$
$\boldsymbol{p} = \{\boldsymbol{p}_{s(i)} | i = 1, 2, \ldots, \kappa\}$
Out: $\boldsymbol{z} = \{\boldsymbol{z}_i | i = 1, 2, \ldots, M\}$

$x_a \leftarrow 1$
for each $\boldsymbol{d}_s$ in $\boldsymbol{d}$ **do**
  $\boldsymbol{z}' \leftarrow \varnothing, \boldsymbol{\Lambda} \leftarrow \varnothing$
  if $\boldsymbol{e}_s \neq \varnothing$ **then**
    $x_b \leftarrow$ size of $\boldsymbol{e}_s$
    for $x_c \leftarrow 1, x_b$ **do**
      $\boldsymbol{\Lambda} \leftarrow \boldsymbol{\Lambda} \oplus \{e_s^{x_c}\}$
    end for
  end if
  if $\boldsymbol{c}_s \neq \varnothing$ **then**
    $\boldsymbol{\Lambda} \leftarrow \boldsymbol{\Lambda} \oplus \boldsymbol{c}_s$
  end if
  $\boldsymbol{\Lambda} \leftarrow \boldsymbol{\Lambda} \oplus \{s\}$
  for each $\boldsymbol{p}_s$ in $\boldsymbol{p}$ **do**
    $x_b \leftarrow$ size of $\boldsymbol{\Lambda}$
    $\boldsymbol{\Theta} \leftarrow \varnothing$
    for $x_c \leftarrow 1, x_b$ **do**
      if $\boldsymbol{p}_s \cap \boldsymbol{\Lambda}(x_c) \neq \varnothing$ **then**
        $\boldsymbol{\Theta} \leftarrow \boldsymbol{\Theta} \cup \boldsymbol{\Lambda}(x_c)$
        delete $\boldsymbol{\Lambda}(x_c)$
      end if
    end for
    $\boldsymbol{z}' \leftarrow \boldsymbol{z}_{x_a} \oplus \boldsymbol{\Theta}$
  end for
  $\boldsymbol{z}' \leftarrow \boldsymbol{z}' \oplus \boldsymbol{\Lambda}$
  for each z' in $\boldsymbol{z}'$ **do**
    $\boldsymbol{z}_{x_a} \leftarrow z'$
    $x_a \leftarrow x_a + 1$
  end for
end for

According to Algorithm 1, there are more than two zones will be partitioned for any one node, the magnitude of the zone number will be huge for a complex system. Besides, a node may be partitioned into multiple zones, and intersections and contradictions may exist among the zones for different target nodes. An algorithm is designed to dispose these conflicts, shown in Algorithm 2. If there are multiple other zones overlaping with a same zone $\boldsymbol{z}_i$, $\boldsymbol{z}_i$ should be deleted. But if there is only one zone ($\boldsymbol{z}_j$) overlaping with $\boldsymbol{z}_i$, the two zones can be merged. It is worthy to mention that the terminal condition of the zone partition is no conflicts among all zones. Therefore, there are many kinds of partitioning results by this method, and it could be led to cost different resources and/or different security protection effectiveness, but it is not the focus of this paper considering.

Algorithm 2 Conflicts Disposition Algorithm.

In: $\boldsymbol{z} = \{\boldsymbol{z}_i | i = 1, 2, \ldots, M\}$
Out: $\tilde{\boldsymbol{z}}$

$\tilde{\boldsymbol{z}} \leftarrow \varnothing$, $x_a \leftarrow 1$
for $x_b \leftarrow 1, M-1$ **do**
  $\boldsymbol{\Lambda} \leftarrow \varnothing$
  for $x_c \leftarrow x_b + 1, M$ **do**
    if $\boldsymbol{z}_{x_b} \cap \boldsymbol{z}_{x_c} \neq \varnothing$ **then**
      $\boldsymbol{\Lambda} \leftarrow \boldsymbol{\Lambda} \oplus \boldsymbol{z}_{x_c}$
    end if
  end for
  $x_c \leftarrow$ size of $\boldsymbol{\Lambda}$
  if $x_c = 0$ **then**
    $\tilde{\boldsymbol{z}}_{x_a} \leftarrow \boldsymbol{z}_{x_b}$
  else if $x_c = 1$ **then**
    $\tilde{\boldsymbol{z}}_{x_a} \leftarrow \boldsymbol{\Lambda}$
  else
    delete $\boldsymbol{z}_{x_b}$
  end if
  $x_a \leftarrow x_a + 1$
end for
$\tilde{\boldsymbol{z}}_{x_a} \leftarrow \boldsymbol{z}_{x_b}$

IV. Zone-Based Anomaly Detection

The detectable oriented zone partition method mentioned above ensures that the states of the target nodes (crucial states) can be observed in multiple zones, but it can only be analyzed qualitatively. As the anomaly detection is a quantitative process, building accurate function models for the crucial states in each zone are necessary.

In this section, a method based on feedforward neural network is used to build the zone function model, and then, the conditions for anomaly analysis in each zone are proposed.

A. Zone Function Model

Generally, the function model is built by a precise expression from system modeling or multivariate fitting, which are mature techniques. However, it is hard for the engineers who are lacking in modeling knowledge. In this paper, Back-Propagation Neural Network (BP-NN) is used for zone function approximation, as its strong ability of mapping and learning without any prior knowledge of the object systems, and the capability of approximating to arbitrary continuous function, which proved by Hornik K. [37], [38].

In any zone a, for a training set $\boldsymbol{R}^a = \{\boldsymbol{I}_i^a, \boldsymbol{O}_i^a\}_{i=1}^N$, where $\boldsymbol{I}_i^a = \{x_{1i}^a, x_{2i}^a, \ldots, x_{Mi}^a\}$ is M dimensions input variables, and $\boldsymbol{O}_i^a = \{o_{1i}^a, o_{2i}^a, \ldots, o_{Ji}^a\}$ is J dimensions output variables which denote the crucial states in zone a, an expression of a three layers BP-NN with L hidden neurons for the j^{th} crucial state is given by [39]

$$\mathscr{Z}_j^a(\boldsymbol{I}_i^a) = f_j^a\Big(\sum_{\ell=1}^{L} w_{\ell j}^a \times g_l^a\big(\sum_{m=1}^{M} \omega_{m\ell}^a x_{mi}^a - \vartheta_\ell^a\big) - \theta_j^a\Big), \tag{2}$$

where g_ℓ^a is the output function of the ℓ^{th} neuron, and ϑ_ℓ^a is the corresponding threshold. θ_j^a is the output layer threshold, $\omega_{m\ell}^a$ is the weight between the input variable x_m^a and the ℓ^{th} hidden neuron, and $w_{\ell j}^a$ is the weight between the ℓ^{th} hidden neuron and the j^{th} crucial state. The training of the weight ω and w continues until mean square error falls below some threshold or tolerance level (σ), which is given by

$$E^a = \frac{1}{2}\sum_{j=1}^{J}\left(o_{ji}^a - \mathscr{Z}_j^a(\boldsymbol{I}_i^a)\right)^2 < \sigma. \tag{3}$$

Because that the unfavorable factors exist in actual systems, such as: system disturbance, sensor precision, actuator response time and so on, data extraction for training set is indispensability. Therefore, all the training sets should satisfy:

$$|\boldsymbol{I}_{i+1}^a - \boldsymbol{I}_i^a| \geq \delta^a, \quad \forall \boldsymbol{I}_i^a \subset \boldsymbol{R}^a, \tag{4}$$

and the threshold δ^a could be determined by

$$\delta^a > \max\{\boldsymbol{\zeta^a}, \nu^a\}, \tag{5}$$

where $\boldsymbol{\zeta^a} = \{\zeta_1^a, \zeta_2^a, \ldots, \zeta_M^a\}$ are the sensors' resolution, ν^a is the maximum system disturbance, which can be obtained from specifications and test. And $\boldsymbol{O}^a$ is correspondingly extracted from the sample dataset.

B. Anomaly Analysis

If a system is uninvaded, the crucial states in each zone are normal. Thus, the description for the same crucial state in any two zones should be consistent. In this paper, two basic conditions, tendency and error between any two curves, are proposed to evaluate the consistency for the description of a same crucial state. First, to inspect the consistency of tendency, cross-correlation algorithm [40] which describes the pertinence of two curves is used, which given by

$$\mathscr{R}_j^{a,b}(k,\tau^{a,b}) = \frac{\sum_{i=k-W}^{k}\mathscr{Z}_j^a(\boldsymbol{I}_i^a)\mathscr{Z}_j^b(\boldsymbol{I}_{i+\tau^{a,b}}^b)}{\sqrt{\sum_{i=k-W}^{k}\left(\mathscr{Z}_j^a(\boldsymbol{I}_i^a)\right)^2\sum_{i=k-W}^{k}\left(\mathscr{Z}_j^b(\boldsymbol{I}_{i+\tau^{a,b}}^b)\right)^2}}, \tag{6}$$

where $\mathscr{R}_j^{a,b} \in [-1,1]$ is the cross-correlation coefficient of the j^{th} crucial state in zone a and b. $\mathscr{R}_j^{a,b} = 1$ represents that the two curves is complete conformity, and $\mathscr{R}_j^{a,b} = -1$ represents that they are complete inconformity. Therefore, the value is more close to 1, the better of the pertinence. W denotes the length of sliding window. $\tau^{a,b}$ denotes the displacement between the two curves, and if the phase in zone a is ahead of zone b, then $\tau^{a,b} > 0$, otherwise $\tau^{a,b} \leq 0$. And it is a constant in one designated system. k $(k > W)$ is the calculating sequence. Normally, the cross-correlation coefficient is close to 1, but if any zone is invaded, the vaule would be dropped rapidly. However, when the two curves $\mathscr{Z}_j^a$ and $\mathscr{Z}_j^b$ are steady, the results will be only determined by the disturbance which will express a bad result. Therefore, a carrier signal is used to improve the pertinence of the original curves, which is given by

$$\mathscr{L}_j^a(\boldsymbol{I}_i^a) = \mathscr{Z}_j^a(\boldsymbol{I}_i^a)\big(1 + \alpha_j^a \sin(\omega^a i)\big), \tag{7}$$

where α_j^a $(\delta_j^a/\mathscr{Z}_j^a < \alpha_j^a < 1)$ is the carrier coefficient, and the carrier cycle ω^a is determined by the length of sliding window. Then, when system is uninvaded, the cross-correlation coefficient should satisfy

$$\min_{k\geq W}\{\mathscr{R}_j^{a,b}(k,\tau^{a,b})\} \geq \gamma_j^{a,b}, \tag{8}$$

where $\gamma_j^{a,b}$ is the minimum allowable correlation of the j^{th} crucial state between zone a and b.

The cross-correlation coefficient only reflects the tendency of the two curves, so the error $\mathscr{E}_j^{a,b}$ between the two curves which reflects the accuracy of the j^{th} crucial state also should be taken into account, which is given by

$$\mathscr{E}_j^{a,b}(k) = \left|\mathscr{Z}_j^{a,b}(\boldsymbol{I}_k^a) - \mathscr{Z}_j^{a,b}(\boldsymbol{I}_{k+\tau^{a,b}}^b)\right|, \tag{9}$$

and the errors should satisfy

$$\max_{k\geq 1}\{\mathscr{E}_j^{a,b}(k)\} \leq \varepsilon_j^{a,b}, \tag{10}$$

where $\varepsilon_j^{a,b}$ is the maximum allowable error of the j^{th} crucial state between zone a and b.

V. Experiment on Testbed

A. Introduction of Testbed

To verify the viability and assess the performance of the proposed approach, a actual testbed named Coupling Tank Control System (CTCS) is constructed firstly. As shown in Fig. 3, CTCS is a simple cyclic water supplying system among three tanks, and the level in each tank is regulated by the proportional and automatic valves. Liquidometers are placed for measuring the real-time liquid level, and in the pipeline between $1^{\#}$ and $2^{\#}$ tank, there are a flowmeter and a piezometer. The water circulation depends on motor M and pressure differential in different tanks. The main target of the system is to keep the liquid level in $1^{\#}$ and $2^{\#}$ tank stable. Besides, in CTCS, the controllers consist of PLCs, which are uniformly supervised and managed by Human Machine Interface (HMI).

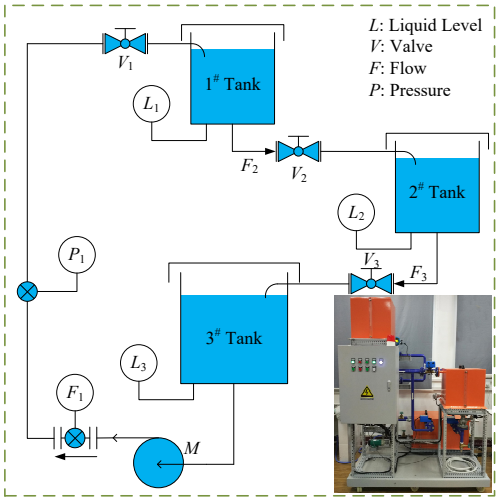

Fig. 3. Physical structure of the CTCS

In CTCS, the liquid level among the three tanks are the most important states with safety consideration. Thus, the crucial states can be defined as $\boldsymbol{d} = \{\boldsymbol{d}_{L_1}, \boldsymbol{d}_{L_2}, \boldsymbol{d}_{L_3}\}$, and its causal model is shown in Fig. 4. As F_2 and F_3 are not detectable signals, the two nodes are not taken into account.

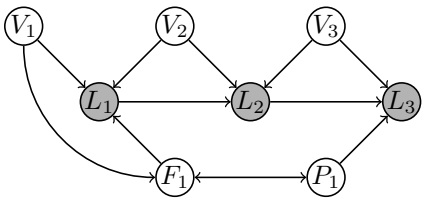

Fig. 4. The causal model of CTCS

Combining with the definition in section III-A, the elements in $\boldsymbol{d}$ are easy to be obtained, which is shown in Table I(a). Any node can not be both a cause node and a effect node for a same crucial state, thus, V_2 and V_3 are only placed in the effect sets of the two crucial states. In CTCS, the liquid level of $1^{\#}$ and $2^{\#}$ tank are the control object, so the partner-set is $\boldsymbol{p} = \{\boldsymbol{p}_{L_1}, \boldsymbol{p}_{L_2}\}$, where $\boldsymbol{p}_{L_1} = \{L_1, V_1\}$, and $\boldsymbol{p}_{L_2} = \{L_2, V_2\}$. According to the zone partition algorithms, the devices in CTCS can be partitioned into multiple zones automaticly. Because that the flow of F_1 can be observed by any one variable of $\{F_1, V_1, P_1\}$, and V_1 is located in $\boldsymbol{z}_1$, the variable of F_1 is placed in $\boldsymbol{z}_2$ finally. M is placed in $\boldsymbol{z}_1$ for the requirements of system function. The partition results are shown in Table I(b).

TABLE I. NODE SETS OF THE CAUSAL MODEL AND ZONE PARTITION RESULTS

(a) Detectable-sets

$\boldsymbol{d}_s$	$\boldsymbol{c}_s$	$\boldsymbol{e}_s$
$\boldsymbol{d}_{L_1}$	$\{F_1, V_1\}$	$\{L_2 \cup V_2\}$
$\boldsymbol{d}_{L_2}$	$\{L_1, V_2\}$	$\{L_3 \cup V_3 \cup P_1\}$
$\boldsymbol{d}_{L_3}$	$\{L_2, P_1, V_3\}$	$\varnothing$

(b) Partition Results

Zone	Nodes
$\boldsymbol{z}_1$	$\{L_1, V_1, M\}$
$\boldsymbol{z}_2$	$\{L_2, V_2, F_1\}$
$\boldsymbol{z}_3$	$\{L_3, V_3, P_1\}$

B. Experiment and Result Analysis

The purpose of this section is to illustrate the effectiveness of the proposed approach through a series of experiments on the testbed. First, to explain the advantages of zone partition, two experiments are conducted to, which are enforced on the original system and the partitioned system respectively. Then, the approximation capability and anomaly detection ability of zone function model is verifyed. And on the basis of it, the detection accuracy and real-time performance of the proposed method are discussed.

*1) **The Comparison of Original System and Partitioned System**:* A spoofing attack [9] is designed to act on the original CTCS and z_1 of the partitioned CTCS respectively, which modifies the configuration of the set point of L_1, and maintains all the measured values from PLCs to HMI at the instant of 50 in the two systems. Fig. 5 shows the level variation tendency in the two systems, and to facilitate observation, the values of the level are normalized to $[0, 1]$. After attacking, as all the states are deceived by the spoofing attack, there are a few changes in original CTCS. But, because that z_2 and z_3 is uninvaded in partitioned CTCS, the states of the variables in these zones are true, and the real state of L_1 may be able to described by the survived zones. However, it is still hard to judge whether the system is anomaly, and find out the zone where the attack is located in. Therefore, to catch the anomaly, a further analysis is necessary.

*2) **The Effectiveness of Zone Function Model for Anomaly Detection**:* There are two stages to verify the availability of the proposed method: 1) training the zone function model, and 2) verifying the detection ability. In the training stage, as the change rate of liquid level is more sensitive than the level itself, the change rates of three tanks are regarded as the training outputs. And about 3,000 datasets are synchronously collected in each zone, and some of 80% are used for training, 20% for test. Fig. 6 shows the approximation

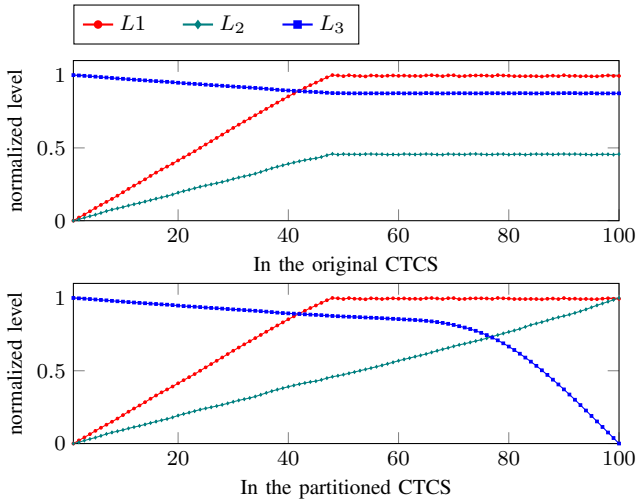

Fig. 5. The level variation tendency in the two systems

performances of the zone function models, where "measured" denotes that the vaule is calculated by the sensor's value, and "estimated" denotes that the vaule is calculated by zone function model. And the results indicate that the trained models

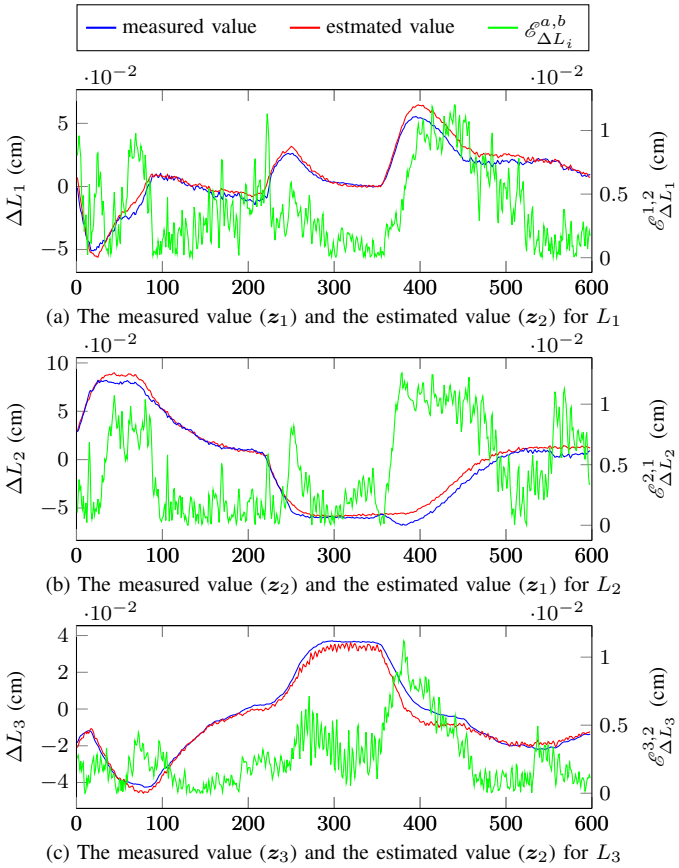

Fig. 6. The performance of zone function model in different zones

have good consistency compared with the actual states, where ΔL means the change rate, and the abscissa represents the sample sequence. Further, the thresholds of $\gamma_j^{a,b}$ and $\varepsilon_j^{a,b}$ for anomaly analysis mentioned in section IV-B can be confirmed from the results by calculating the minimum cross-correlation coefficient ($\mathscr{R}_j^{a,b}$) and the maximum error ($\mathscr{E}_j^{a,b}$) between the measured value and estimated value in different zones. The

results are shown in Table II.

TABLE II. THE PARAMETERS FOR ANOMALY ANALYSIS

$\gamma_j^{a,b}$	$\varepsilon_j^{a,b}$
$\gamma_{\Delta L_1}^{1,2} = 0.8719$	$\varepsilon_{\Delta L_1}^{1,2} = 0.0121$
$\gamma_{\Delta L_2}^{2,1} = 0.8631$	$\varepsilon_{\Delta L_2}^{2,1} = 0.0126$
$\gamma_{\Delta L_3}^{3,2} = 0.8790$	$\varepsilon_{\Delta L_3}^{3,2} = 0.0112$

Notes: $\tau = 0, W = 50$ and $\alpha = 0.005$.

Then, A spoofing attack is used to verify the detection ability of the trained model, which modifies the configuration of the set point of L_1 from 10cm to 20cm, and maintains all the measured values from PLCs to HMI at the instant of 70 in $\boldsymbol{z}_1$. Fig. 7 shows the analyzing curves of correlations and errors in different zones. While $\boldsymbol{z}_1$ is modified and deceived, the crucial states in this zone will much different compared with other zones. Thus, the values of $\mathscr{R}_{\Delta L_1}^{1,2}$, $\mathscr{E}_{\Delta L_1}^{1,2}$, $\mathscr{R}_{\Delta L_2}^{2,1}$ and $\mathscr{E}_{\Delta L_2}^{2,1}$ will beyond the normal conditions. And as the $\boldsymbol{z}_2$ and $\boldsymbol{z}_3$ are uninvaded, the valuse of $\mathscr{R}_{\Delta L_3}^{3,2}$ and $\mathscr{E}_{\Delta L_3}^{3,2}$ are in normal. Further, the anomaly is discovered at the instant of 79 by cross-correlation coefficients analysis and 76 by errors analysis, the detection time can be calculated, which is $T_d = (79-70)\cdot T_c$, where $T_c = 1s$ is the sampling period. Although it looks taking for a long time, it is not sufficient to bring any loss. Because that the valves adjusting and levels changing are a slow process, and L_1 is only changed less than 1cm during the detection time.

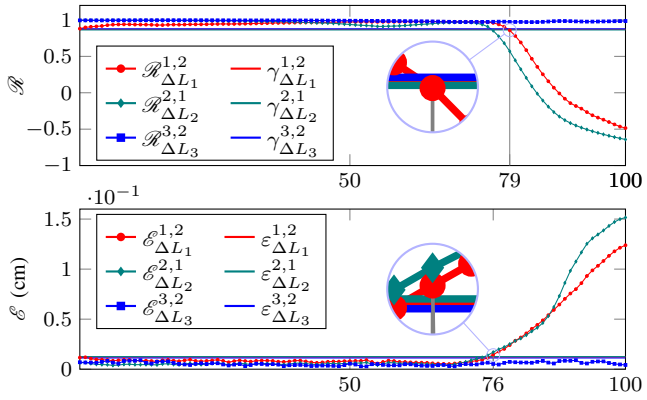

Fig. 7. The correlation and errors under spoofing attack

Meanwhile, when calculating cross-correlation coefficients, the length of sliding window (W) is a key parameter which has great influence for the results. Fig. 8 shows the calculating results on different W. It can be found that if W is too small,

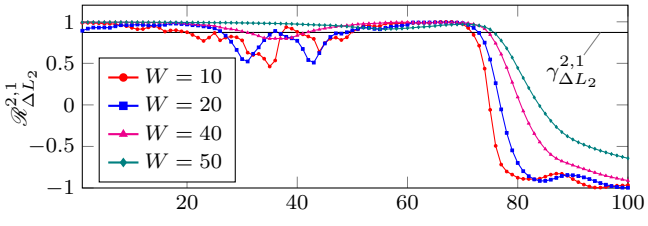

Fig. 8. The reuslts on different length of sliding window

false alarms will be appeared in normal system. With the increasing of the length, the number of false alarms will be decreased, but the time of the true alarms will be put off. Similarly, the carrier coefficient α is also a key parameter, and its selecting principle can be found in signal processing.

*3) **Detection Performance of the Proposed Approach**:* Accuracy and real-time capability are the two most important criteria for evaluating the performance of detection systems, and the four well-known metrics: False Positive Rate (FPR), False Negative Rate (FNR), Detecion Accuracy (DA) and Detecion Time (DT) are used, whose definition can be found in [9]. First, the following two factors, which are the most important reasons for influencing the detection performance, need be analyzed.

• *Analysis of Training Conditions*: Table III shows the detection performance under the different training sets with the same training parameters in BP-NN, where FP and FN denote false positive number and false negative number, and the anomaly data is collected under a spoofing attack mentioned above. Although, the metric of FNR is very low in any situations, FPR is much different. That is, false alarms appear frequently in normal system if the training sets include few operating conditions. The reason is that neural network tends to learn the zone behavior nor build accurate expression. Therefore, the more different states for training, the higher precision of the approximation at some extent.

TABLE III. PERFORMANCE ON DIFFERENT TRAINING CONDITIONS

Datasets	Normal	Anomaly	FP	FN	FPR	FNR	DA
400	431	607	350	53	81.21%	8.73%	63.43%
800	431	607	173	2	40.14%	0.33%	77.82%
1200	431	607	37	0	8.58%	0%	94.25%
2600	431	607	1	0	0.23%	0%	99.84%

Notes: the number of training sets is determined by the operating conditions.

• *Analysis of Detection Parameters*: Table IV shows the detection performance under different values of $\boldsymbol{\gamma}$ and $\boldsymbol{\varepsilon}$, where $\boldsymbol{\gamma} = \{\gamma_{\Delta L_1}^{1,2}, \gamma_{\Delta L_2}^{2,1}, \gamma_{\Delta L_3}^{3,2}\}$ and $\boldsymbol{\varepsilon} = \{\varepsilon_{\Delta L_1}^{1,2}, \varepsilon_{\Delta L_2}^{2,1}, \varepsilon_{\Delta L_3}^{3,2}\}$. The results indicate that there are some conflicts among the evaluating criteria. FPR and DA can be reduced by relaxing restrictions, but it need to increase DT. Meanwhile, FNR will arise if the detection conditions continue to be relaxed. Besides, the detection performance is more sensitvely influenced by the parameters of $\boldsymbol{\varepsilon}$ than $\boldsymbol{\gamma}$.

TABLE IV. PERFIRMANCE ON DIFFERENT DETECTION PARAMETERS

$\boldsymbol{\gamma}$	$\boldsymbol{\varepsilon}$	Normal	Anomaly	FP	FN	FPR	FNR	DA	DT
0.88	0.12	431	607	71	0	16.47%	0%	89.53%	$3.5s$
0.88	0.15	431	607	12	0	2.78%	0%	98.06%	$7.1s$
0.85	0.15	431	607	1	0	0.23%	0%	99.84%	$9.3s$
0.50	0.30	431	607	0	27	0%	4.45%	100%	$14.7s$

At last, the detection performance is discussed with attacking on different zones. And the two typical attacks: spoofing attack and tampering attack [41] are selected, where the tampering attack is to alter the value from sensors to PLCs. The results are shown in Table V. It is indicates that the approach can detect the anomaly with a high precise accuracy and real-time capability no matter which one zone is invaded. But, as discussed before, FPR can not avoid completely if FNR and long DT are unacceptable. Additionally, although there is little difference for the detection accuracy under different

TABLE V. THE ACCURACY AND REAL-TIME OF THE PROPOSED APPROACH ON CTCS

Attack Description				Dataset		Detection Performance					
Type	Param.	Normal	Modifying	Normal	Anomaly	FP	FN	FPR	FNR	DA	DT
Spoofing Attack	L_1	10cm	0cm	1195	1108	5	0	0.42%	0%	99.55%	$8.9s$
			20cm	1186	1157	8	0	0.67%	0%	99.31%	$9.1s$
	L_2	5cm	0cm	1121	865	4	0	0.36%	0%	99.54%	$9.4s$
			10cm	1053	842	0	0	0%	0%	100%	$8.5s$
Tampering Attack	L_1	any	↓ 0cm	1208	749	7	0	0.58%	0%	99.07%	$4.8s$
			↑ 20cm	1154	803	2	0	0.17%	0%	99.75%	$4.6s$
	L_2	any	↓ 0cm	1007	544	5	0	0.50%	0%	99.09%	$5.2s$
			↑ 10cm	1163	532	3	0	0.26%	0%	99.44%	$4.5s$

***DT*:** the average detection time.
***any*:** The actual value, which would be changed after the tampering attack as the control loop.
↑ expresses increasing the value smoothly, and ↓ is the opposite. The following number represents the target value.

attacks, the DT is different. Because that, the level is changed by adjusting the valves in spoofing attack which can only alter slowly, and in tampering attack, the level is changed directly. It will be longer under spoofing attack than tampering attack. But, as the magnitude of ΔL is under 10^{-2}, the actual liquid level only changes less than 1cm in any situations. In sum, from the Table V, there are three brief conclusions to be summarized: 1) attacks can be detected only if their purposes are to interpose or destroy physical process, 2) the detection time is just determined by response speed of the physical system, and the anomaly can be found before falling into hazard, and 3) each zone has the ability to catch the abnormal.

VI. Conclusion

Due to the characteristics of ICPSs, physical domain features should be fully considered in anomaly detection systems. Different from the existing ones, the proposed approach partitions the physical system into multiple zones, and detects anomaly by analyzing and matching the crucial states described in different zones whose effectiveness has been adequately proved. Meanwhile, the method of describing the crucial states avoids the problem that the model parameters are inaccurate or the system model is unknown. In detail, an automated detectable oriented zone partition method is presented firstly. Then an approach of constructing zone function model is given without any prior knowledge of the physical system. Meanwhile, the way of analyzing the anomaly is designed. At last, experiments illustrate the high accuracy and good real-time performance of the proposed approach. But, it would be invalid if all the zones are invaded simultaneously. Therefore, diversity protection strategies should be executed in different zones.

Current research work just takes the physical domain into account. An integrated intrusion detection system should synthesize the information in cyber domain, and distinguish the anomaly caused by attacks or faults. Therefore, the further work will focus on the integration of cyber information and physical feature for intrusion detection in ICPSs.

References

[1] Z. Asad, M. A. R. Chaudhry, and D. Kundur, "On the use of matroid theory for distributed cyber-physical-constrained generator scheduling in smart grid," *IEEE Trans. Ind. Electron.*, vol. 62, no. 1, pp. 299–309, 2015.

[2] P.-Y. Chen, S. Yang, and J. A. McCann, "Distributed real-time anomaly detection in networked industrial sensing systems," *IEEE Trans. Ind. Electron.*, vol. 62, no. 6, pp. 3832–3842, 2015.

[3] K. Stouffer, J. Falco, and K. Scarfone, "Guide to industrial control systems (ICS) security, SP-800-82-2011," Special Publication by National Institute of Standards and Technology (NIST), 2011.

[4] S. Ntalampiras, "Automatic identification of integrity attacks in cyber-physical systems," *Expert Syst. Appl.*, vol. 58, pp. 164–173, 2016.

[5] S. Huda, S. Miah, M. M. Hassan, R. Islam, J. Yearwood, M. Alrubaian, and A. Almogren, "Defending unknown attacks on cyber-physical systems by semi-supervised approach and available unlabeled data," *Inform. Sciences*, vol. 379, pp. 211 – 228, 2017.

[6] U. D. of Homeland Security, "ICS-CERT year in review 2015," Washington, DC, 2015.

[7] T. Novak and A. Gerstinger, "Safety-and security-critical services in building automation and control systems," *IEEE Trans. Ind. Electron.*, vol. 57, no. 11, pp. 3614–3621, 2010.

[8] B. Karabacak, S. O. Yildirim, and N. Baykal, "Regulatory approaches for cyber security of critical infrastructures: The case of turkey," *Computer Law & Security Review*, vol. 32, no. 3, pp. 526–539, 2016.

[9] C. Zhou, S. Huang, N. Xiong, S.-H. Yang, H. Li, Y. Qin, and X. Li, "Design and analysis of multimodel-based anomaly intrusion detection systems in industrial process automation," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 45, no. 10, pp. 1345–1360, 2015.

[10] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *comput. Secur.*, vol. 28, no. 1, pp. 18–28, 2009.

[11] Z.-H. Pang, G.-P. Liu, D. Zhou, F. Hou, and D. Sun, "Two-channel false data injection attacks against output tracking control of networked systems," *IEEE Trans. Ind. Electron.*, vol. 63, no. 5, pp. 3242–3251, 2016.

[12] A. A. Cárdenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry, "Attacks against process control systems: risk assessment, detection, and response," in *Proceedings of ASIACCS 2011*, pp. 355–366, 2011.

[13] G. Sabaliauskaite and A. P. Mathur, "Countermeasures to enhance cyber-physical system security and safety," in *IEEE COMPSAC 2014*, pp. 13–18, 2014.

[14] Y. Park, S. H. Baek, S.-H. Kim, and K.-L. Tsui, "Statistical process control-based intrusion detection and monitoring," *Qual. Reliab. Eng. Int.*, vol. 30, no. 2, pp. 257–273, 2014.

[15] H. Takagi, T. Morita, M. Matta, H. Moritani, T. Hamaguchi, S. Jing, I. Koshijima, and Y. Hashimoto, "Strategic security protection for industrial control systems," in *Annual Conference of SICE in Japan 2015*, pp. 986–992. IEEE, 2015.

[16] I. N. Fovino, A. Coletta, A. Carcano, and M. Masera, "Critical state-based filtering system for securing scada network protocols," *IEEE Trans. Ind. Electron.*, vol. 59, no. 10, pp. 3943–3950, 2012.

[17] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network anomaly detection: methods, systems and tools," *IEEE Commun. Surv. Tut.*, vol. 16, no. 1, pp. 303–336, 2014.

[18] D. Kang, B. Kim, J. Na, and K. Jhang, "Whitelists based multiple filtering techniques in scada sensor networks," *J. Appl. Math.*, vol. 2014, 2014.

[19] M. Mantere, M. Sailio, and S. Noponen, "Network traffic features for anomaly detection in specific industrial control system network," *Future Internet*, vol. 5, no. 4, pp. 460–473, 2013.

[20] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Secur. Priv.*, vol. 9, no. 3, pp. 49–51, 2011.

[21] X. Hu, R. Subbu, P. Bonissone, H. Qiu, and N. Iyer, "Multivariate anomaly detection in real-world industrial systems," in *IEEE IJCNN 2008*, pp. 2766–2771, 2008.

[22] F. Harrou, Y. Sun, and S. Khadraoui, "Amalgamation of anomaly-detection indices for enhanced process monitoring," *J. Loss Prevent. Proc.*, vol. 40, pp. 365–377, 2016.

[23] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Tran. Automat. Contr.*, vol. 58, no. 11, pp. 2715–2729, 2013.

[24] A. Khalili and A. Sami, "Sysdetect: a systematic approach to critical state determination for industrial intrusion detection systems using apriori algorithm," *J. Process Contr.*, vol. 32, pp. 154–160, 2015.

[25] W. Li, L. Xie, Z. Deng, and Z. Wang, "False sequential logic attack on scada system and its physical impact analysis," *comput. Secur.*, vol. 58, pp. 149–159, 2016.

[26] ANSI/ISA, "ISA 62443-3-2: (99.03.02)-2013, security for industrial automation and control systems part 3-2: Security risk assessment and system design," 2013.

[27] B. Genge, P. Haller, and I. Kiss, "Cyber-security-aware network design of industrial control systems," *IEEE Syst. J.*, pp. 1–12, 2015.

[28] G. Fuxiang, L. Sha, W. Xiaolu, and Y. Lan, "A security architecture for intranet based on security area division," in *IEEE IITSI 2010*, pp. 539–543, 2010.

[29] Y. Jin, H. Liu, L. Sun, and J. Song, "Study on security domain-oriented military information systems access control model," in *Proceedings of ISKE 2014*, pp. 849–856, 2014.

[30] J. Jee, J. Jang, I. Jo, and Y. Shin, "A network partition scheme to protect secure zone for malicious code," in *Proceedings of ICOIN 2013*, pp. 476–480, 2013.

[31] K. Krishnan, H. Luss, A. Neidhardt, and D. Shallcross, "Event-detection in sensor fields by adaptive distributed computations," in *IEEE SAS 2010*, pp. 114–118, 2010.

[32] Y. Hashimoto, T. Toyoshima, S. Yogo, M. Koike, T. Hamaguchi, S. Jing, and I. Koshijima, "Safety securing approach against cyber-attacks for process control system," *Comput. Chem. Eng.*, vol. 57, pp. 181–186, 2013.

[33] T. Morita, S. Yogo, M. Koike, T. Hamaguchi, S. Jung, I. Koshijima, and Y. Hashimoto, "Detection of cyber-attacks with zone dividing and pca." *Procedia Computer Science*, pp. 727–736, 2013.

[34] M. Iri, K. Aoki, E. O'Shima, and H. Matsuyama, "An algorithm for diagnosis of system failures in the chemical process," *Comput. Chem. Eng.*, vol. 3, no. 1, pp. 489–493, 1979.

[35] T. Hamaguchi, K. Takeda, M. Noda, and N. Kimura, "A method of designing plant alarm systems with hierarchical cause-effect model," *Proceedings of PSE 2011*, 2011.

[36] I.-K. Lee, M.-S. Kim, and G. Elber, "Polynomial/rational approximation of minkowski sum boundary curves," *Graph. Model. Im. Proc.*, vol. 60, no. 2, pp. 136 – 165, 1998.

[37] K. Hornik, M. Stinchcombe, and H. White, "Multilayer feedforward networks are universal approximators," *Neural Networks*, vol. 2, no. 5, pp. 359 – 366, 1989.

[38] K. Hornik, "Some new results on neural network approximation," *Neural Networks*, vol. 6, no. 8, pp. 1069–1072, 1993.

[39] J. Kim and S. Jung, "Implementation of the RBF neural chip with the back-propagation algorithm for on-line learning," *Appl. Soft. Comput.*, vol. 29, pp. 233 – 244, 2015.

[40] J. Luo and E. E. Konofagou, "A fast normalized cross-correlation calculation method for motion estimation," *IEEE T. Ultrason. Ferr.*, vol. 57, no. 6, pp. 1347–1357, 2010.

[41] A. Teixeira, D. Pérez, H. Sandberg, and K. H. Johansson, "Attack models and scenarios for networked control systems," in *Proceedings of HiCoNS 2012*, pp. 55–64, 2012.