Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.064402

ARTICLE

Toward Intrusion Detection of Industrial Cyber-Physical System: A Hybrid Approach Based on System State and Network Traffic Abnormality Monitoring

Junbin He[1,2], Wuxia Zhang[3], Xianyi Liu[1], Jinping Liu[2,*] and Guangyi Yang[4]

[1]Hunan Intellectual Property Protection Center, Changsha, 410006, China
[2]College of Information Science and Engineering, Hunan Normal University, Changsha, 410081, China
[3]College of Computer Science and Software Engineering, Shenzhen University, Shenzhen, 518061, China
[4]Hunan Institute of Metrology and Test, Changsha, 410018, China

*Corresponding Author: Jinping Liu. Email: ljp@hunnu.edu.cn

Received: 14 February 2025; Accepted: 03 April 2025; Published: 09 June 2025

ABSTRACT: The integration of cloud computing into traditional industrial control systems is accelerating the evolution of Industrial Cyber-Physical System (ICPS), enhancing intelligence and autonomy. However, this transition also expands the attack surface, introducing critical security vulnerabilities. To address these challenges, this article proposes a hybrid intrusion detection scheme for securing ICPSs that combines system state anomaly and network traffic anomaly detection. Specifically, an improved variation-Bayesian-based noise covariance-adaptive nonlinear Kalman filtering (IVB-NCA-NLKF) method is developed to model nonlinear system dynamics, enabling optimal state estimation in multi-sensor ICPS environments. Intrusions within the physical sensing system are identified by analyzing residual discrepancies between predicted and observed system states. Simultaneously, an adaptive network traffic anomaly detection mechanism is introduced, leveraging learned traffic patterns to detect node- and network-level anomalies through pattern matching. Extensive experiments on a simulated network control system demonstrate that the proposed framework achieves higher detection accuracy (92.14%) with a reduced false alarm rate (0.81%). Moreover, it not only detects known attacks and vulnerabilities but also uncovers stealthy attacks that induce system state deviations, providing a robust and comprehensive security solution for the safety protection of ICPS.

KEYWORDS: Industrial cyber-physical systems; network intrusion detection; adaptive Kalman filter; abnormal state monitoring; network traffic abnormality monitoring

1 Introduction

The rapid integration of advanced information technologies—such as the Industrial Internet of Things (IIoT), cloud computing, big data, and artificial intelligence—is driving an unprecedented transformation in manufacturing industries. Intelligent manufacturing has emerged as a central theme in global competition, with the Industrial Cyber-physical System (ICPS) playing a central role [1]. The advent of ICPS has driven Industrial Control Systems from traditional electromechanical architectures to interconnected, intelligent systems. While this evolution enhances automation and intelligence, it also expands the attack surface, exposing ICPS to sophisticated cybersecurity threats. The deep integration of information and physical components in ICPS means that cyberattacks on any component can propagate across the entire industrial network. Several high-profile cyberattacks have underscored these vulnerabilities. In 2013, hackers infiltrated Haifa's highway control systems, causing substantial financial losses. In December 2015, a cyberattack on Ukraine's power grid disrupted electricity for 22,500 residents. In 2017, a Chernobyl nuclear power plant in

Ukraine subway and other national facilities were infected by the NotPetya extortion virus. More recently, on 07 May 2021, a ransomware attack forced the Colonial Pipeline—the largest fuel pipeline in the United States—to shut down operations, causing widespread disruptions. These incidents highlight the urgent need for robust, adaptive, and intelligence-driven security mechanisms to protect ICPS from evolving cyber threats [2].

Traditional communication network security has been studied extensively, focusing on network anomaly-based and signature-based detection techniques [3,4]. While these methods have demonstrated effectiveness in protecting IT infrastructures, ICPS security poses unique challenges due to its distinct operational and structural characteristics [5,6].

(1) **System Integrity vs. Data Confidentiality:** Traditional communication network security primarily safeguards the confidentiality of critical data. In contrast, ICPS security prioritizes system integrity, including the physical sensory system, the information system, and the overall control system to ensure reliable operation.
(2) **Resource Constraints:** Unlike IT communication network systems with relatively ample computational resources, ICPS often operate under strict energy and processing limitations. Consequently, cybersecurity measures must enable real-time monitoring while minimizing computational overhead.
(3) **Complexity and Heterogeneity:** ICPS comprise hybrid wired-wireless networks with diverse communication protocols. The heterogeneity of controllers, sensors, and data acquisition systems across industries complicates cybersecurity. However, once deployed, ICPS configurations remain largely static.
(4) **Non-interruptible Maintenance:** Unlike IT communication network systems that can undergo periodic updates and patches, ICPS operates continuously, limiting downtime for updates. The intrusion detection of ICPSs must provide real-time threat detection and alarm, particularly identifying unknown and covert attacks.

To sum up, ICPS exhibit relatively stable traffic state with trackable system states, enabling intrusion detection through system anomaly monitoring [7]. Existing ICPS intrusion detection methods can be broadly classified into traffic anomaly-based and state anomaly-based intrusion detection technologies [8].

Traffic anomaly-based detection analyzes time-dependent node-level and network-level characteristics to identify network intrusions and classify attack types. A critical step is effective feature representation, where clustering techniques, such as K-means clustering, are commonly used. However, traditional K-means clustering suffers from initialization sensitivity, poor global search capability, and susceptibility to local optima. Evolutionary K-means (EKM) integrates genetic algorithms to optimize initialization, but its reliance on the silhouette index (SI) for clustering evaluation weakens its robustness against noise [9].

On the other hand, cyberattacks on sensors, controllers, actuators, or network transmissions can disrupt ICPS stability by altering system input-output signals. Researchers have explored fault diagnosis-inspired methodologies, such as outlier detection, for intrusion detection. Linear and nonlinear system models have been used to detect attacks, like replay attacks and denial-of-service (DoS) attacks [10]. Shinohara et al. [11] presented the optimal security investment problem as a discrete-time linear time-invariant system. These studies demonstrate that as long as not all sensors fail simultaneously, state anomaly-based intrusion detection can effectively identify small, rare, and unknown faults.

Concerning the system modeling, the commonly used method characterizes the ICPS as a linear time-varying system, with the Kalman filtering frequently employed. For instance, Pasqualetti et al. [12] and Lee et al. [13] model the ICPS attacks using a linear time-invariant system with unknown inputs and time-varying process and measurement noise. Zhang et al. [14] advanced distributed state estimation in binary sensor

networks by integrating variation Bayesian methods to handle noisy, uncertain environments. However, these methods assume known or invariant noise, making them overly reliant on prior noise statistics, which limits their applicability in dynamic ICPS environments.

To overcome the above issues, adaptive Kalman filtering models, such as Bayesian inference, maximum likelihood estimation, correction and covariance matching methods, have been explored. Among them, the Bayesian method is the most widely used [15]. For instance, Liu et al. [16] introduced an adaptive Kalman filtering method with time-varying process noise and measurement noise covariance matrix. However, these methods still assume linear time-invariant system constraints, neglecting the inherent nonlinearity of ICPS dynamics, which is critical for analyzing stability, faults, and attacks in complex industrial processes.

To capture time-varying and nonlinearity in ICPS, nonlinear ICPS modeling that adapts to process and measurement noise is essential. Many exploratory studies have been carried out. For instance, Yuan et al. [17] proposed a model-driven ICPS, leveraging an extended Kalman filter (EKF) to calibrate the empirical model with online measured data for online diagnosis and monitoring. However, this approach fails to detect covert attacks (e.g., replay attacks), which do not significantly alter measurement values.

To address the above challenges, an improved variation Bayesian-based noise covariance-adaptive nonlinear Kalman filtering (IVB-NCA-NKF) is proposed for the nonlinear system modeling of complex ICPSs. IVB-NCA-NKF can model the adaptive nonlinear time-varying system with the unknown process and measurement noise covariance matrices. It is mainly used for sensor system-related attack detection in ICPSs. To realize the overall security monitoring of networked industrial control systems, a hybrid intrusion detection framework for securing ICPSs that combines state anomaly detection of the sensor systems and the network traffic anomaly detection is proposed. The main contributions can be summarized as follows:

(1) A hybrid intrusion detection framework is proposed by combining sensor state anomaly and network traffic anomaly detection, ensuring multi-layered ICPS security from sensors to network communication systems.
(2) An IVB-NCA-NKF is proposed for modeling nonlinear time-varying ICPSs, leveraging a cluster-based sensor system model and state estimation to enable cybersecurity monitoring of large-scale distributed ICPS.
(3) An online adaptive network traffic pattern learning approach for network communication system intrusion detection is proposed, incorporating a cache-based pattern library to enhance the detection of sparse and unknown attack modes in ICPS.

The rest of this article is organized as follows. Section 2 briefly reviews the theoretical foundations of the EKF and K-means algorithm. Section 3 details the proposed hybrid intrusion detection approach. Section 4 makes extensive confirmatory and comparative experiments. Section 5 summarizes the whole article with possible extensions of this work.

2 Preliminaries

This section briefly reviews the principles of EKF and the K-Mean Algorithm.

2.1 Exended Kalman Filter (EKF)

The Kalman filter is a powerful and standard approach for state estimation. However, the standard Kalman filter is limited to linear systems, whereas most real-world systems exhibit nonlinearity, necessitating its extension to handle nonlinear dynamics. The EKF [18] is undoubtedly the most widely used nonlinear form of the standard Kalman filter. The EKF state transfer equations and observation equations can be

expressed as,

$$\mathrm{x}_k = f\left(\mathrm{x}_{k-1}, \mathrm{u}_{k-1}\right) + \mathrm{s}_k \tag{1}$$

$$\mathrm{y}_k = h\left(\mathrm{x}_k, \mathrm{u}_k\right) + \mathrm{v}_k \tag{2}$$

where $\mathrm{x}_k \in \mathbb{R}^n$ represents the system state vector, $\mathrm{u}_k \in \mathbb{R}^D$ denotes the operation vector, $\mathrm{y}_k \in \mathbb{R}^m$ stands for the observation or measurement vector; f and h are nonlinear differentiable functions representing the transfer and measurement function, respectively; s_k and v_k represent the system and measurement noises, and satisfies $\mathrm{s}_k \sim \mathcal{N}\left(\mathrm{s}_k|0, \mathbf{Q}_k\right)$, $\mathrm{v}_k \sim \mathcal{N}\left(\mathrm{v}_k|0, \mathbf{R}_k\right)$, where $\mathcal{N}\left(\mathrm{x}|\boldsymbol{\mu}, \boldsymbol{\Sigma}\right)$ stands for a multivariate normal distribution with the mean vector of $\boldsymbol{\mu}$ and variance matrix of $\boldsymbol{\Sigma}$.

Based on the Taylor's expansion, x_k in Eq. (1) can be expressed as,

$$\mathrm{x}_k = f\left(\hat{\mathrm{x}}_{k-1}, \mathrm{u}_{k-1}\right) + \mathbf{F}_{k-1}\left(\mathrm{x}_{k-1} - \hat{\mathrm{x}}_{k-1}\right) + \mathrm{s}_k \tag{3}$$

where $\hat{\mathrm{x}}_{k-1}$ is the estimation vector of the time $t-1$. Based on the Taylor expansion at the state prediction value $\hat{\mathrm{x}}_{k|k-1}$ of this round, we have,

$$\mathrm{y}_k = h\left(\hat{\mathrm{x}}_{k|k-1}, \mathrm{u}_k\right) + \mathbf{H}_k\left(\mathrm{x}_k - \hat{\mathrm{x}}_{k|k-1}\right) + \mathrm{v}_k \tag{4}$$

where $\mathbf{F}_{k-1}$ and $\mathbf{H}_k$, respectively, represent the function and the Jacobian matrix at $\hat{\mathrm{x}}_{k-1}$ and $\hat{\mathrm{x}}_{k|k-1}$.

Based on the Gaussian assumption, according to Eq. (4), under a known system state x_k, there is,

$$p\left(\mathrm{y}_k|\mathrm{x}_k, \mathrm{u}_k\right) = \mathcal{N}\left(\mathrm{y}_k|h\left(\hat{\mathrm{x}}_{k|k-1}, \mathrm{u}_k\right) + \mathbf{H}_k\left(\mathrm{x}_k - \hat{\mathrm{x}}_{k|k-1}\right), \mathbf{R}_k\right) \tag{5}$$

When x_{k-1} is known, according to Eq. (3), there is,

$$p\left(\mathrm{x}_k|\mathrm{x}_{k-1}\right) = \mathcal{N}\left(\mathrm{x}_k|f\left(\hat{\mathrm{x}}_{k-1}, \mathrm{u}_{k-1}\right) + \mathbf{F}_{k-1}\left(\mathrm{x}_{k-1} - \hat{\mathrm{x}}_{k-1}\right), \mathbf{Q}_k\right) \tag{6}$$

Kalman filter is designed to estimate x_k based on historical observations, $\mathrm{y}_{1:k}$. That is, to iteratively calculate the model parameters $\hat{\mathrm{x}}_k, \boldsymbol{\Sigma}_k$ in $p\left(\mathrm{x}_k|\mathrm{y}_{1:k}, \mathrm{u}_{1:k}\right) = \mathcal{N}\left(\mathrm{x}_k|\hat{\mathrm{x}}_k, \boldsymbol{\Sigma}_k\right)$. The main iterative steps are as follows:

(1) Estimate the state of the system at the current moment using the historical observations $\mathrm{y}_{1:k-1}$, i.e.,

$$p\left(\mathrm{x}_k|\mathrm{y}_{1:k-1}, \mathrm{u}_{1:k-1}\right) = \int p\left(\mathrm{x}_{k-1}|\mathrm{y}_{1:k-1}, \mathrm{u}_{1:k-1}\right) p\left(\mathrm{x}_k|\mathrm{x}_{k-1}\right) d\mathrm{x}_{k-1} = \mathcal{N}\left(\mathrm{x}_k|\hat{\mathrm{x}}_{k|k-1}, \boldsymbol{\Sigma}_{k|k-1}\right) \tag{7}$$

where $\hat{\mathrm{x}}_{k|k-1} = f\left(\boldsymbol{\mu}_{k-1}, \mathrm{u}_{k-1}\right)$ and $\boldsymbol{\Sigma}_{k|k-1} = \mathbf{F}_{k-1}\boldsymbol{\Sigma}_{k-1}{\mathbf{F}_{k-1}}^T + \mathbf{Q}_k$.

(2) Update $p\left(\mathrm{x}_k|\mathrm{y}_{1:k}, \mathrm{u}_{1:k}\right)$ based on the currently obtained observation vector x_k,

$$p\left(\mathrm{x}_k|\mathrm{y}_{1:k}, \mathrm{u}_{1:k}\right) \propto p\left(\mathrm{x}_k|\mathrm{y}_{1:k-1}, \mathrm{u}_{1:k-1}\right) p\left(\mathrm{y}_k|\mathrm{x}_k, \mathrm{u}_k\right) = \mathcal{N}\left(\mathrm{x}_k|\hat{\mathrm{x}}_k, \boldsymbol{\Sigma}_k\right) \tag{8}$$

where $\boldsymbol{\Sigma}_k = \left(\mathbf{I} - \mathbf{K}_k\mathbf{H}_k\right)\boldsymbol{\Sigma}_{k|k-1}$, $\hat{\mathrm{x}}_k = \hat{\mathrm{x}}_{k|k-1} + \mathbf{K}_k\left(\mathrm{y}_k - h\left(\hat{\mathrm{x}}_{k|k-1}, \mathrm{u}_k\right)\right)$, and,

$$\mathbf{K}_k \triangleq \boldsymbol{\Sigma}_{k|k-1}{\mathbf{H}_k}^T\left(\mathbf{H}_k\boldsymbol{\Sigma}_{k|k-1}{\mathbf{H}_k}^T + \mathbf{R}_k\right)^{-1} \tag{9}$$

By iterating steps (1) and (2), EKF can realize the Gaussian nonlinear dynamic system modeling.

2.2 K-Means Clustering-Based Pattern Learning

K-means clustering [19] is known as a simple and scalable pattern learning (pattern mining) method. Given a data set $X = \{\mathrm{x}_1, \mathrm{x}_2, \cdots, \mathrm{x}_N\}$, where $\mathrm{x}_i \in \mathbb{R}^D$, K-means is used to categorize X into K clusters. The pattern learning results are usually expressed by the mean vectors of the K clusters, $\{\mu_k|_{k=1,\cdots,K}\}$. To achieve the clustering results, a cluster-assigning notation of points, $r_{nk} \in \{0,1\}$, referring to that data point x_n is assigned to the cluster k if $r_{nk} = 1$, and $r_{nj} = 0$ for $j \neq k$. Thus, the K-means clustering is to minimize the following optimization objective, i.e.,

$$J = \sum_{n=1}^{N} \sum_{k=1}^{K} r_{nk} \left\| \mathrm{x}_n - \mu_k \right\|^2 \tag{10}$$

The commonly used expectation maximization (EM) algorithm can be used to address the above optimization problem. The iteration steps are as follows:

(1) **E step.** It tries to assign the optimal r_{nk} for each point based on the clustering results, $\{\mu_k|_{k=1,\cdots,K}\}$, of the last step, i.e.,

$$r_{nk} = \begin{cases} 1 \text{ if } k = \arg\min\limits_{j} \left\| \mathrm{x}_n - \mu_j \right\|^2 \\ 0 \text{ otherwise} \end{cases} \tag{11}$$

Namely, each point will be assigned to its nearest cluster.

(2) **M step.** Based on the assigned r_{nk} of each point in the E step, the clustering centers, $\{\mu_k|_{k=1,\cdots,K}\}$, can be optimized by setting the partial derivative of the optimization objective J over each clustering center be zero, i.e., $\frac{\partial J}{\partial \mu_k} = 2 \sum\limits_{n=1}^{N} r_{nk} \left(x_n - \mu_k \right) = 0$, which can be easily solved to achieve,

$$\mu_k = \frac{\sum\limits_{n=1}^{N} r_{nk} \mathrm{x}_n}{\sum\limits_{n=1}^{N} r_{nk}} \tag{12}$$

Iterating the Steps E step M until a convergent result is reached. K-mean clustering is straightforward to implement with high computational efficiency. However, the clustering results are affected greatly by the presupposed cluster number (K) and the initialized clustering centers.

Numerous studies have addressed the initialization problem in the K-means algorithm, focusing either on determining the optimal number of clusters or selecting appropriate initial cluster centers for a given cluster count. A common approach is to perform multiple clustering operations with varying cluster numbers or initial centers and then select the best results based on predefined cluster validity indices (CVIs) [20]. Arbelaitz et al. [21] conducted a comprehensive comparative study of approximately 30 CVIs, including the Dunn index, Silhouette index, and Cluster Separation (CS) measure, to evaluate clustering performance and optimize algorithm parameters. Some researchers have integrated both cluster number selection and center initialization using evolutionary algorithms. For instance, the genetic algorithm (GA) was combined with the K-mean algorithm to achieve an evolutionary K-mean (EKM) algorithm [22].

3 Proposed ICPS-Oriented Intrusion Detection Scheme

The proposed hybrid intrusion detection framework addresses cybersecurity in ICPS from two key aspects: system state anomaly detection and network traffic anomaly detection, aiming for comprehensive protection, as illustrated in Fig. 1.

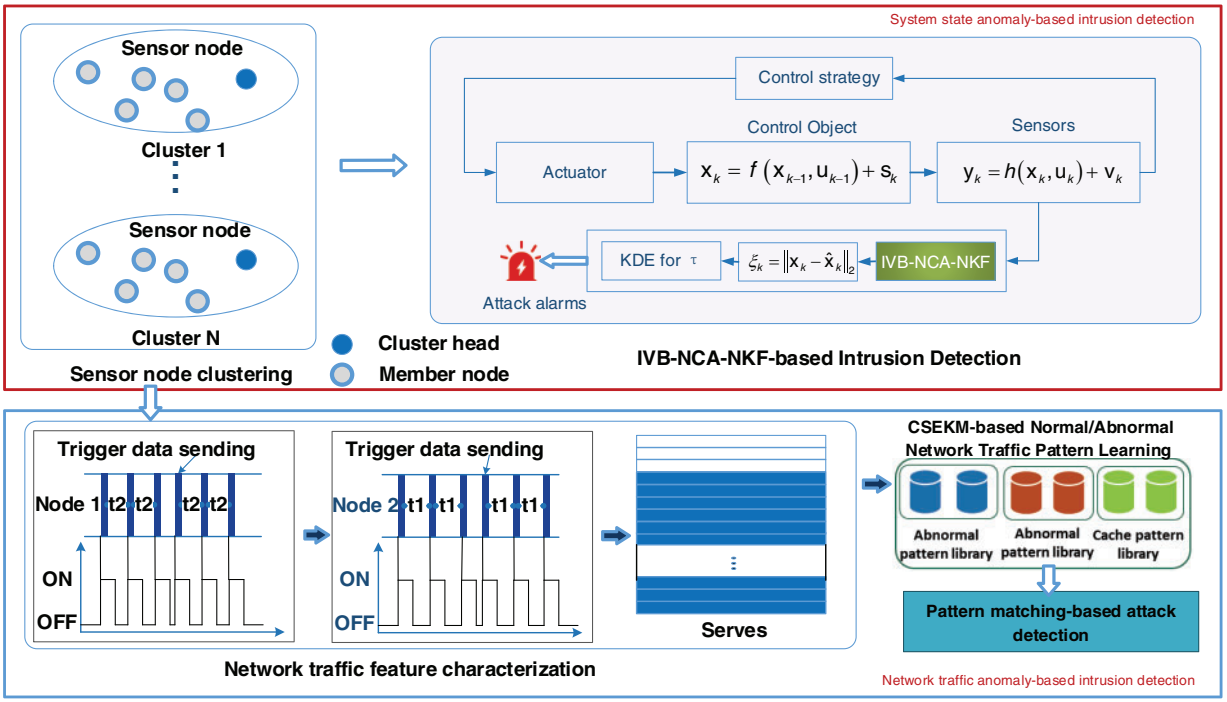

Figure 1: Intrusion detection framework

As shown in Fig. 1, the sensor system state anomaly detection model leverages data from ICPS sensor nodes for real-time anomaly monitoring. A significant system state estimation residual may indicate potential anomalies, such as sensor system attacks. To mitigate computational and communication constraints, a sensor grading strategy is adopted, clustering sensor nodes and assigning each cluster a state estimation detector for anomaly detection, thereby reducing system complexity and cost. Simultaneously, a network traffic pattern matching-based anomaly detection mechanism is introduced for network security monitoring. An improved N-Burst model is proposed to represent ICPS network traffic patterns, while an enhanced clustering stability-based evolutionary K-Means (CSEKM) algorithm is employed for network traffic pattern learning. By analyzing both node-level and system-level traffic patterns, an intrusion detector is implemented using the pattern-matching scheme.

The main detection steps can be summarized as follows:

(1) Sensor node clustering and cluster node head setting;
(2) For each sensor cluster:
  (2.1) Perform IVB-NCA-NKF to estimate the state vector x_k, measuring noise covariance matrix $\mathbf{R}_k$, and system noise covariance matrix $\mathbf{\Sigma}_{k|k-1}$;
  (2.2) Compute the system state prediction residual;
  (2.3) Determine whether an intrusion occurs based on the system residual threshold.
(3) Perform the network traffic anomaly-based intrusion detection:

(3.1) Perform N-burst model-based node-level and communication network-level traffic feature representation;
(3.2) Perform CSEKM-based Normal/Abnormal network traffic pattern learning;
(3.3) Perform pattern matching-based network intrusion detection.

3.1 Sensory System State Anomaly-Based Intrusion Detector

Sensor system anomaly-based intrusion detection are detected by analyzing the state estimation residual—the difference between the actual detected state and the estimated state—based on the proposed IVB-NCA-NKF model. To minimize transmission delays and enable distributed intrusion detection, sensor nodes are clustered [23], with each cluster assigned a detector.

3.1.1 Sensor Node Clusters

Following Sarehati's sensor clustering approach [23], controllers and their associated sensor nodes (including sensors and actuators) are grouped into clusters. Each cluster is managed by a controller as the cluster head, while the associated sensor nodes act as members. To enhance distributed attack detection, active collaboration among member nodes is employed. Sensor nodes periodically transmit local and shared information—including suspicious activity from neighboring nodes and confirmed attack warnings—to their linked nodes. The cluster head then aggregates and forwards this data to the next hop or data transfer node. A schematic representation of sensor node collaboration is shown in Fig. 2.

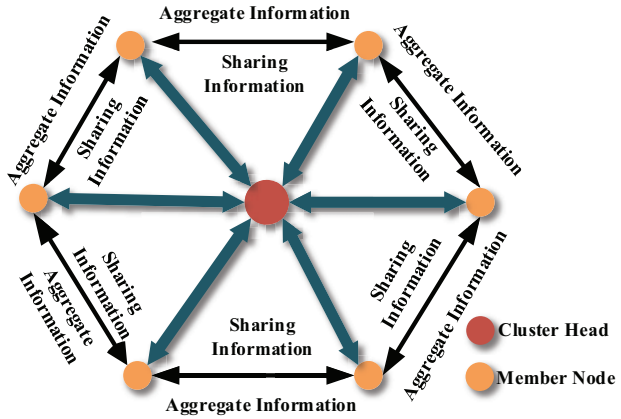

Figure 2: Collaborative work diagram of sensor node

3.1.2 IVB-NCA-NKF-Based Intrusion Detection

The proposed IVB-NCA-NKF is an optimal EKF based on the variation inference for the system modeling of unknown process and measurement noise covariance matrixes.

First of all, assuming that a nonlinear sensor system is expressed by Eqs. (1) and (2), under the Gaussian assumption, the random vector of the state, x_k, and observation, y_k, are also Gaussian, i.e.,

$$x_k|x_{k-1} \sim \mathcal{N}\left(f\left(x_{k-1}, u_{k-1}\right), \mathbf{\Sigma}_{k|k-1}\right) \tag{13}$$

$$y_k|x_k \sim \mathcal{N}\left(h\left(x_k, u_k\right), \mathbf{R}_k\right) \tag{14}$$

Although we can model the dynamic system by iterating Eqs. (7) and (8), the system noise information, $\mathbf{\Sigma}_{k|k-1}$ in (13) and the measurement noise, $\mathbf{R}_k$, in (14) are actually unknown (system noise and measurement noise are time-varying). Therefore, the classic EKF model may cause an accumulation of system estimation errors due to the inaccuracy of process and measurement noise estimation in the system modeling, results in an inaccurate system model that is far from the real system.

Chang et al. [24] have pointed out that a good solution for modeling the noise-unknown systems is to use the variation Bayesian method to measure the system state and measurement noise covariance matrices jointly. Huang et al. [25] have also extended the Kalman filter model with unknown measurement noises. The results show that the proposed method is more robust to the uncertainty factors in the process and measurement of linear dynamic systems. However, the abovementioned methods are linear system models, which are not suitable for nonlinear systems.

In this work, the linear system modeling method is extended to the nonlinear dynamic system modeling. The proposed IVB-NCA-NLKF is aimed at estimating the sensory system state, observation and process noise covariance matrixes jointly by the variation inference based on the sensor observations, i.e., to achieve a posterior probability, $p\left(\mathrm{x}_k, \mathbf{\Sigma}_{k|k-1}, \mathbf{R}_k|\mathrm{y}_{1:k}\right)$.

Since the analytic solution of the posterior, $p\left(\mathrm{x}_k, \mathbf{\Sigma}_{k|k-1}, \mathbf{R}_k|\mathrm{y}_{1:k}\right)$, is intractable, the variation Bayesian inference method is introduced to optimally approximate it, where $p\left(\mathrm{x}_k, \mathbf{\Sigma}_{k|k-1}, \mathbf{R}_k|\mathrm{y}_{1:k}\right)$ is assumed to be factorable approximately, i.e.,

$$p\left(\mathrm{x}_k, \mathbf{\Sigma}_{k|k-1}, \mathbf{R}_k|\mathrm{y}_{1:k}\right) \approx q\left(\mathrm{x}_k\right) q\left(\mathbf{\Sigma}_{k|k-1}\right) q\left(\mathbf{R}_k\right) \tag{15}$$

where $q\left(\mathrm{x}_k\right), q\left(\mathbf{\Sigma}_{k|k-1}\right), q\left(\mathbf{R}_k\right)$ should be achieved by,

$$\left\{\hat{q}\left(\mathrm{x}_k\right), \hat{q}\left(\mathbf{\Sigma}_{k|k-1}\right), \hat{q}\left(\mathbf{R}_k\right)\right\} = \arg\min\left\{\mathrm{KLD}\left(p\left(\mathrm{x}_k, \mathbf{\Sigma}_{k|k-1}, \mathbf{R}_k|\mathrm{y}_{1:k}\right) \| q\left(\mathrm{x}_k\right) q\left(\mathbf{\Sigma}_{k|k-1}\right) q\left(\mathbf{R}_k\right)\right)\right\} \tag{16}$$

where KLD stands for the Kullback–Leibler Divergenc, and $\mathrm{KLD}\left(p\left(\mathrm{x}\right) \| q\left(\mathrm{x}\right)\right) = \int p\left(\mathrm{x}\right) \log p\left(\mathrm{x}\right)/q\left(\mathrm{x}\right) d\mathrm{x}$.

Based on the variation inference, the optimal solution of Eq. (16) can be expressed as,

$$\log \hat{q}_i\left(\theta_i\right) = \mathbb{E}_{j \neq i}\left[\log p\left(\boldsymbol{\theta}, \mathrm{y}_{1:k}\right)\right], \text{where } \boldsymbol{\theta} = \left(\theta_1, \theta_2, \theta_3\right) = \left(\mathrm{x}_k, \mathbf{\Sigma}_{k|k-1}, \mathbf{R}_k\right) \tag{17}$$

To achieve $\hat{q}_i\left(\theta_i\right)$ in Eq. (17), the total probability formula, $p\left(\boldsymbol{\theta}, \mathrm{y}_{1:k}\right)$, should be achieved in advance. According to the Bayesian rule, $p\left(\boldsymbol{\theta}, \mathrm{y}_{1:k}\right) = p\left(\mathrm{x}_k, \mathbf{\Sigma}_{k|k-1}, \mathbf{R}_k, \mathrm{y}_{1:k}\right)$ can be expressed as,

$$p\left(\mathrm{x}_k, \mathbf{\Sigma}_{k|k-1}, \mathbf{R}_k, \mathrm{y}_{1:k}\right) = p\left(\mathrm{y}_{1:k-1}\right) p\left(\mathbf{R}_k|\mathrm{y}_{1:k-1}\right) . p\left(\mathbf{\Sigma}_{k|k-1}|\mathrm{y}_{1:k-1}\right) p\left(\mathrm{x}_k|\mathrm{y}_{1:k-1}, \mathbf{\Sigma}_{k|k-1}\right) . p\left(\mathrm{y}_k|\mathrm{x}_k, \mathbf{R}_k\right) \tag{18}$$

In Eq. (18), $p\left(\mathrm{x}_k|\mathrm{y}_{1:k-1}, \mathbf{\Sigma}_{k|k-1}\right)$ and $p\left(\mathrm{y}_k|\mathrm{x}_k, \mathbf{R}_k\right)$ are Gaussian density. $\mathbf{R}_k$ and $\mathbf{\Sigma}_{k|k-1}$ are the covariance matrixes of Gaussian models, whose prior distribution is known to be the Inverse-Wishart (IW) distribution [24]. By the introduction of the IW distribution, it can ensure that their posterior distribution has the same distribution form as the prior distribution, which is conducive to the probability calculation. Detailed information of IW distribution can be found in Appendix A. Briefly, these prior distributions are selected as,

$$\begin{aligned} p\left(\mathrm{x}_k|\mathrm{y}_{1:k-1}, \mathbf{\Sigma}_{k|k-1}\right) &= \mathcal{N}\left(\mathrm{x}_k|\hat{\mathrm{x}}_{k|k-1}, \mathbf{\Sigma}_{k|k-1}\right) \\ p\left(\mathrm{y}_k|\mathrm{x}_k, \mathbf{R}_k\right) &= \mathcal{N}\left(\mathrm{y}_k|\hat{\mathrm{y}}_{k|k-1}, \mathbf{R}_k\right) \\ p\left(\mathbf{R}_k|\mathrm{y}_{1:k-1}\right) &= \mathrm{IW}\left(\mathbf{R}_k|\hat{d}_{k|k-1}, \mathbf{D}_{k|k-1}\right) \\ p\left(\mathbf{\Sigma}_{k|k-1}|\mathrm{y}_{1:k-1}\right) &= \mathrm{IW}\left(\mathbf{\Sigma}_{k|k-1}|\hat{t}_{k|k-1}, \mathbf{T}_{k|k-1}\right) \end{aligned} \tag{19}$$

where $\hat{\mathrm{x}}_{k|k-1} = f\left(\hat{\mathrm{x}}_{k-1|k-1}, \mathrm{u}_{k-1}\right)$, $\hat{\mathrm{y}}_{k|k-1} = h\left(\hat{\mathrm{x}}_{k|k-1}, \mathrm{u}_k\right) + \mathbf{H}_k\left(\mathrm{x}_k - \hat{\mathrm{x}}_{k|k-1}\right)$.

By these prior distributions, we can achieve the posterior of the dynamic system state based on Formula (17). A detailed estimation procedure of $q(\mathrm{x}_k)$, $q\left(\boldsymbol{\Sigma}_{k|k-1}\right)$, $q(\mathbf{R}_k)$ is shown in Appendix B.

The state estimation residual can be computed by,

$$\xi_k = \left\|\mathrm{x}_k - \hat{\mathrm{x}}_k\right\|_2 \tag{20}$$

where $\|\cdot\|_2$ stands for the 2-norm. If the industrial control system is affected by malicious attacks, it may yield state mutation, leading to a deviation from the stable state. Thus, when ξ_k is beyond a preset threshold, τ, the system is considered to have an abnormal state or attack. The threshold value τ is generally determined by chi-square detection or by kernel density estimation of ξ_k based on a predefined confidence level.

Here below is an illustrative example to validate the performance of the proposed IVB-NCA-NKF model. Given a stochastic discrete-time nonlinear dynamic system (DC motor system) has the following state and measurement expression,

$$\begin{aligned} \begin{pmatrix} \omega_k \\ c_k \end{pmatrix} &= \begin{pmatrix} \omega_{k-1} + \left(u_{k-1} - c_{k-1}\omega_{k-1}\right) T_s/J \\ c_{k-1} \end{pmatrix} + q_k \\ y_k &= \begin{pmatrix} \omega_k \\ \left(u_k - c_k\omega_k\right)/J \end{pmatrix} + r_k \end{aligned} \tag{21}$$

where u_k represents the control value, $J = 10$, $T_s = 0.01$, and $q_k \sim \mathcal{N}(0, \mathbf{Q}_k)$, $r_k \sim \mathcal{N}(0, \mathbf{R}_k)$ are the noise vectors of the system state equation and the measurement equation, respectively, where the covariance matrixes, $\mathbf{Q}_k$, $\mathbf{R}_k$, are time-varying.

Fig. 3 presents a comparative analysis of the prediction results for the nonlinear system described in Eq. (21) using the IVB-NCA-NLKF model and traditional EKF methods. As can be seen from Fig. 3, the proposed model demonstrates higher accuracy, particularly for the step state variable. Overall, the predicted system state closely aligns with the actual state, highlighting the effectiveness of the IVB-NCA-NLKF model for nonlinear system modeling under unknown process and measurement noise conditions.

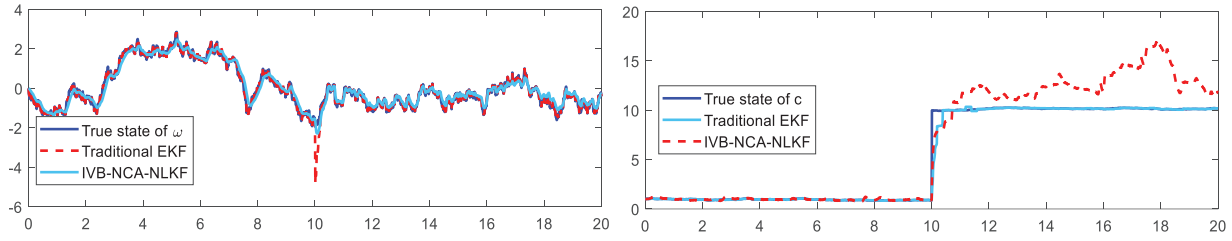

Figure 3: Example of IVB-NCA-NLKF-based nonlinear system modeling

3.2 Network Traffic Anomaly-Based Intrusion Detector

Network traffic anomaly-based intrusion detection consists of offline learning of normal and abnormal traffic patterns, followed by online anomaly detection with continuous pattern library updates. A schematic representation of this process is shown in Fig. 4.

3.2.1 Network Traffic Feature Extraction and Representation

Inspired by Huang et al.'s study [26], a N-Burst model is adopted for the network traffic representation. As described in Huang et al.'s work [26], the N-Burst model expresses an arrival process of superposition

of traffic streams from *N*-independent and statically identical ON/OFF sources. As described in Fig. 5, each ON/OFF source consists of an ON period, i.e., 1 burst, and an OFF period. A more detailed description of the N-Burst model can be found in the literature [26].

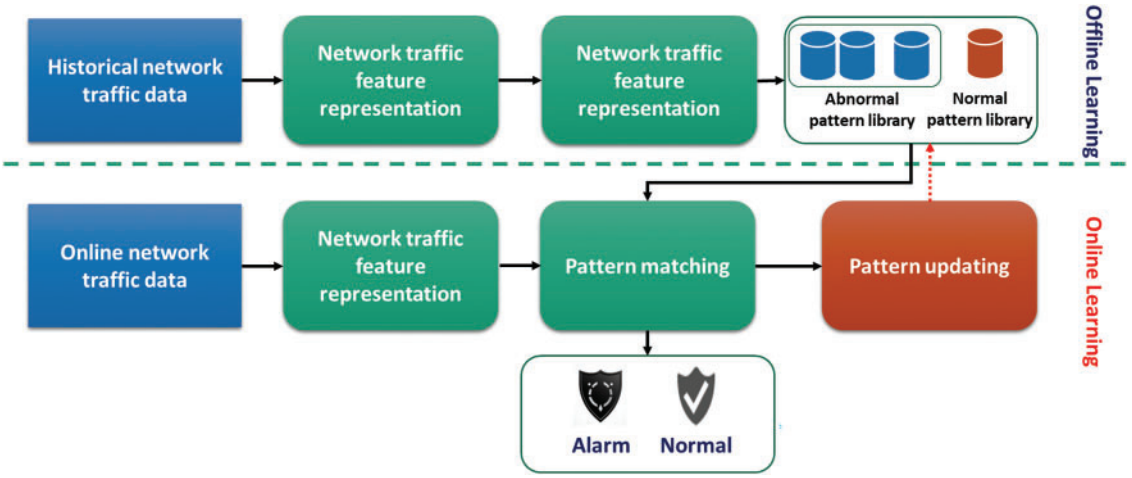

Figure 4: Network traffic anomaly detector

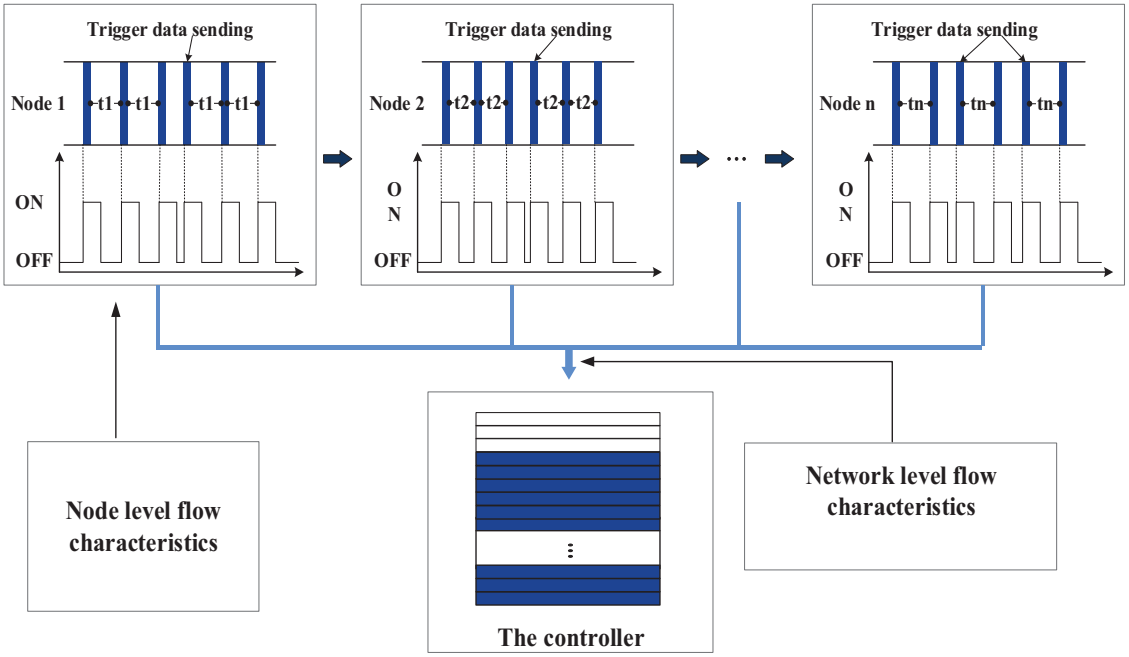

Figure 5: ON/OFF source model

In the ICPS, the ON/OFF source involves actuators and sensors. The ON stage refers to the stage in which the node transmits data, with a randomly varying duration. The OFF stage refers to the idle stage of the node, and the duration is also random. The end of each ON phase follows the previous OFF phase. When the system is running, the sensor data is collected according to the predetermined sequence and period. After a

specific event triggers data transmission, the pre-set sequence and cycle are restored, and the sensor data is collected. Due to the coupling relationship between nodes, different nodes enter the ON period according to a certain time interval. The ON/OFF model-based data feature for the network traffic representation is shown in Table 1.

Table 1: ON/OFF model-based ICPS Network traffic features

Phase	Flow	Depiction
ON (node)	$Time_{(ON)}$	Average time of ON phase
	$Trans_{(ON)}$	Average packet transmission rate in ON phase
	$Inter_{(ON)}$	Average packet transmission interval in ON phase
OFF (node)	$Time_{(OFF)}$	Average time of OFF phase
	$Trans_{(OFF)}$	Average packet transmission rate in OFF phase
	$Inter_{(OFF)}$	Average packet transmission interval in OFF stages
Idle time (node)	*Idle time*	Time interval between different sub flows
Message number (node)	*Number*	Number of traffic messages
Mean value (node)	*Average*	Average rate of achievement of total data packets
Total (network)	*Total*	Overall packet transmission rate

3.2.2 CSEKM-Based Normal/Abnormal Network Traffic Pattern Learning

The Silhouette Index (SI) is widely regarded as one of the most effective clustering validity indices (CVIs) for evaluating cluster compactness and separability [27]. However, SI is sensitive to noise, as outliers can significantly alter its values, affecting clustering results. To overcome the initialization problem of K-Means and improve the robustness, He et al. [27] introduced the clustering stability index as an alternative to SI for performance evaluation. Inspired by He's study, the CSEKM algorithm was introduced for normal/abnormal network traffic pattern learning. Using the learned pattern libraries, traffic anomalies can then be detected via pattern matching.

The main procedure of the clustering stability-based K-means model selection is to learn a set of K-means models using a set of perturbed versions of training samples and choose the minimum instability of each K-means clustering model as the final model. The clustering instability is often computed as the average distance between clusters on different perturbed training samples. However, as stated in the literature [27,28], this criterion may be misleading in the case of EKM. Besides the average distance between clusters, the other commonly used method for evaluating cluster stability is the Consensus Matrix (CM)–based approach. As suggested in Yu et al.'s study [29], the Aggregation Consensus Matrix (ACM), a modified rand index calculated based on discrete CM to evaluate clustering stability to determine K, was applicable. In this work, the ACM-based clustering stability analysis is adopted. By combining the EKM and clustering stability analysis, a CSEKM-based is adopted for the normal traffic pattern and abnormal traffic pattern learning. Detailed CSEKM algorithm steps can be found in the literature [27].

3.2.3 Pattern Matching-Based Anomaly Detection and Online Pattern Updating

Once normal and abnormal network traffic pattern libraries are established, anomaly detection via pattern matching becomes straightforward. However, the dynamic nature of ICPS networks and evolving intrusion tactics cause attack patterns to deviate from their original features, leading to new intrusion

variants. Traditional intrusion detection models, which rely on predefined intrusion characteristics, struggle to detect emerging attacks in such dynamic environments.

To enhance adaptability in dynamic ICPS network environments, an online pattern updating mechanism is incorporated into the intrusion detection model, building on our previous work [30]. The process, illustrated in Fig. 6, integrates a cache pattern library (CPL) alongside the pre-learned normal pattern library (NPL) and the abnormal pattern library (APL) to handle unforeseen or evolving network behaviors.

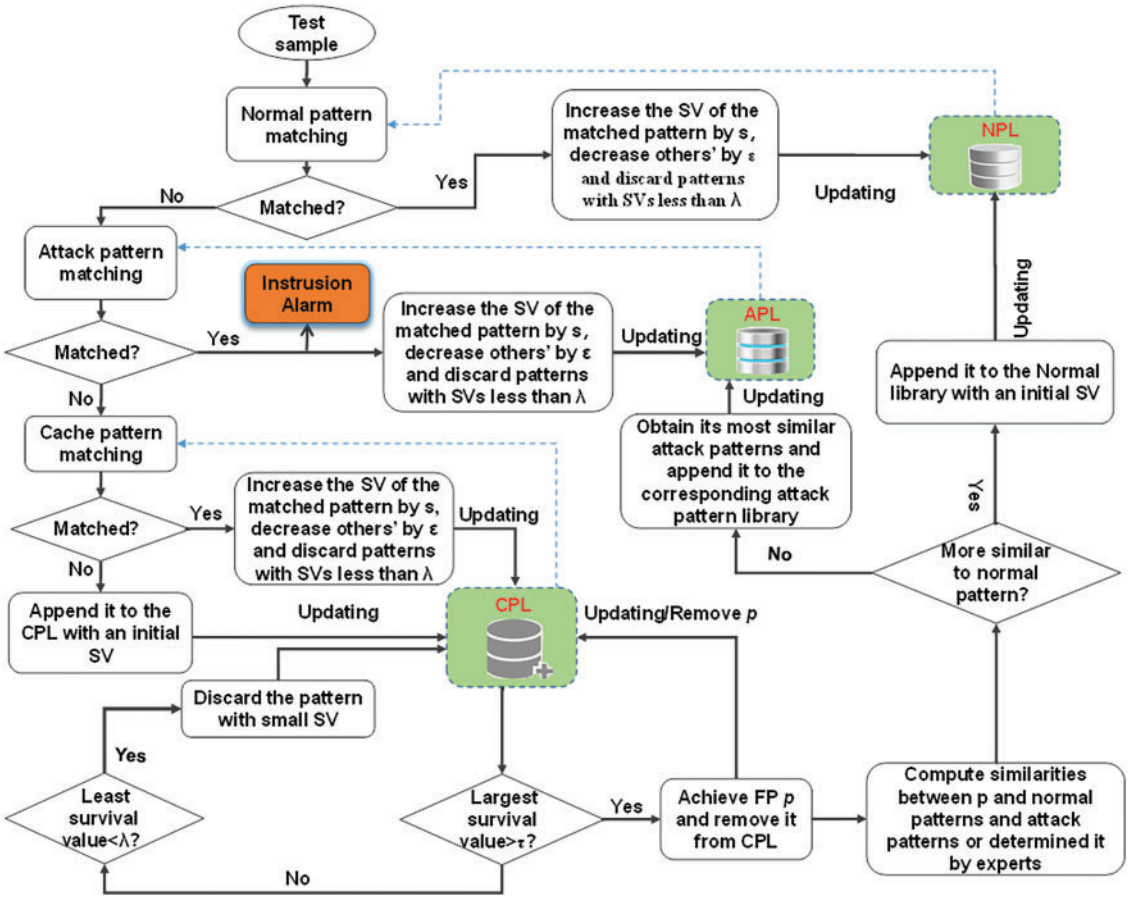

Figure 6: Pattern matching-based intrusion detection and online pattern updating

Each learned pattern in the libraries is assigned a survival value (SV) to track its activity. Patterns with SVs below a predefined threshold are discarded to maintain an updated library. Upon receiving a new network traffic instance, pattern matching is performed sequentially.

- Normal Pattern Matching: If a match is found in the NPL, the SV of the matched pattern increases by s (e.g., by 1 in experiments), while others in the NPL decrease by $\varepsilon(\ll 1)$. Patterns with SVs below the threshold (λ) are removed.
- Attack Pattern Matching: If no match is found in the NPL, the instance is checked against the APL. A successful match triggers an intrusion alarm and updates the APL similarly to the NPL.
- Cache Pattern Matching: If no match is found in either NPL or APL, the instance is compared with patterns in the CPL. A match leads to CPL updates following the same principle. If unmatched, the instance is added to the CPL with an initial confidence value (CV).

For any pattern in CPL, if its CV is larger than a high threshold (τ), this pattern can be referred as to a frequent pattern (FP). And it will perform pattern matching of the FP with NPL and APL, if it is more like to a normal pattern, the NPL will be updated accordingly. Oppositely, if the FP is more like to an abnormal pattern, the APL will be updated accordingly.

Many vector distance measurement approaches can be used for pattern matching, such as Pearson correlation coefficient, Euclidean distance, Cosine similarity, Manhattan distance, Lance Williams distance, and so on [31]. In this work, the simple cosine similarity is adopted to measure the dissimilarity of two network records, given by,

$$d(\mathrm{x},\mathrm{y}) = \frac{\mathrm{x}^T\mathrm{y}}{\|\mathrm{x}\|\,\|\mathrm{y}\|} \tag{22}$$

where x, y stands for two patterns. The smaller the value of $d(\mathrm{x},\mathrm{y})$, the smaller the angle between x and y, and the greater the similarity between x and y.

4 Experimental Validation and Result Analysis

This section details the confirmatory and comparative experiments with result discussions.

4.1 State Anomaly-Based Intrusion Detection

4.1.1 Attacking Models

Four typical and common attacks in the ICPS are considered in this work, namely, the denial of service (DoS), spoof attack, noise and scaling attacks as described in Liu et al.'s study [32]. In the following attacking model, n represents the number of sensors in the ICPS, $y_i(t)$ represents acquired value of the ith sensor at the t time, $u_i(t)$ stands for the received control signal of the sensor i at the time of t and the attacking duration is $[t_s, t_e]$.

(1) DoS

Attackers introduce attacking signals to $y_i(t)$ or control signals $u_i(t)$ to prevent the collection of correct control commands or actual sensory data by offsetting the normal signals, i.e.,

$$\hat{y}_i(t) = \begin{cases} y_i(t) & t \notin [t_s, t_e] \\ y_i(t) + a_y, a_y = -y_i(t) & t \in [t_s, t_e] \end{cases}, \quad \hat{u}_i(t) = \begin{cases} u_i(t) & t \notin [t_s, t_e] \\ u_i(t) + a_u, a_u = -u_i(t) & t \in [t_s, t_e] \end{cases} \tag{23}$$

(2) Spoof attack

The spoof attack occurs when an attacker steals historical data and replaces the current system data with the historical data in the sensory system. This is a covert intrusion that cannot be easily detected,

$$\hat{y}_i(t) = \begin{cases} y_i(t) & t \notin [t_s, t_e] \\ a_y, a_y \text{ is historical data} & t \in [t_s, t_e] \end{cases}, \quad \hat{u}_i(t) = \begin{cases} u_i(t) & t \notin [t_s, t_e] \\ a_u, a_u \text{ is historical data} & t \in [t_s, t_e] \end{cases} \tag{24}$$

(3) Noise attack

Attackers target acquisition signals $y_i(t)$ or control signals $u_i(t)$ by constructing specific noises. It can affect or even change the state of the system, leading to system fluctuation and even process faults,

$$\hat{y}_i(t) = \begin{cases} y_i(t) & t \notin [t_s, t_e] \\ y_i(t) + a_y, a_y = \omega'(t) & t \in [t_s, t_e] \end{cases}, \quad \hat{u}_i(t) = \begin{cases} u_i(t) & t \notin [t_s, t_e] \\ u_i(t) + a_u, a_u = v'(t) & t \in [t_s, t_e] \end{cases} \tag{25}$$

(4) Scaling attack

Attackers collect the sensor signal, $y_i(t)$, or control signal, $u_i(t)$, and then scale up or down them with a certain range to change the actual system state, i.e.,

$$\hat{y}_i(t) = \begin{cases} y_i(t) & t \notin [t_s, t_e] \\ a_y y_i(t) & t \in [t_s, t_e], a_y y_i(t) \in \left[y_i^{min}, y_i^{max}\right] \\ y_i^{min} & t \in [t_s, t_e], a_y y_i(t) < y_i^{min} \\ y_i^{max} & t \in [t_s, t_e], a_y y_i(t) > y_i^{max} \end{cases},$$

$$\hat{u}_i(t) = \begin{cases} u_i(t) & t \notin [t_s, t_e] \\ a_u u_i(t) & t \in [t_s, t_e], a_u u_i(t) \in \left[u_i^{min}, u_i^{max}\right] \\ u_i^{min} & t \in [t_s, t_e], a_u u_i(t) < u_i^{min} \\ u_i^{max} & t \in [t_s, t_e], a_u u_i(t) > u_i^{max} \end{cases} \tag{26}$$

4.1.2 Experimental Result Analysis

This section verifies the effectiveness of the proposed IVB-NCA-NLKF-based sensor system intrusion detection method by a numerical simulation system.

(1) Numerical system description and data preparation

Suppose the nonlinear system is expressed as follows,

$$\begin{array}{lll} y_1(t_1, t_2) = \sqrt{u(t_1)} + \sin(u(t_1)) + \varepsilon(t_2) & u(t_1) = t_1 + \sin t_1, & t_1, t_2 \geq 0 \\ y_2(t_1, t_2) = u(t_1)^2 + \cos(u(t_1)) + \varepsilon(t_2) & u(t_1) = t_1 + \cos t_1, & t_1, t_2 \geq 0 \\ y_3(t_1, t_2) = 4u(t_1) + 3u(t_1)^2 + \varepsilon(t_2) & u(t_1) = t_1 + {t_1}^2, & t_1, t_2 \geq 0 \\ y_4(t_1, t_2) = 2\cos(u(t_1)) + 3u(t_1) + \varepsilon(t_2) & u(t_1) = t_1 + 2\cos t_1, & t_1, t_2 \geq 0 \\ y_5(t_1, t_2) = \exp(u(t_1)) + 2u(t_1)^2 + \varepsilon(t_2) & u(t_1) = t_1 + \exp t_1, & t_1, t_2 \geq 0 \end{array} \tag{27}$$

where y_1, y_2, y_3, y_4, y_5 represent the five observational variables; ε is a Gaussian noise.

In the experiment, four groups of normal sample data are generated based on the system model in (27), forming four sensory clusters in the ICPS perceptual execution layer. Correspondingly, four attack modes are introduced as attack samples. These normal and attack samples constitute the initial training set, with each cluster containing 500 data samples.

Three different working modes (model 1, model 2 and model 3) are given. Each of the three modes produces 200 sets of samples as the initial training set,

$$model\,1 = \begin{cases} t_1 : Uniform(2, 1.5) \\ t_2 : Normal(0, 0.1) \end{cases} \tag{28}$$

$$model\,2 = \begin{cases} t_1 : Uniform(0, 2) \\ t_2 : Normal(0, 0.1) \end{cases} \tag{29}$$

$$model\,3 = \begin{cases} t_1 : Uniform(2, 1) \\ t_2 : Normal(0, 0.1) \end{cases} \tag{30}$$

Based on the normal working condition data, under three modes, the variables y_1, y_2, y_3, y_4, y_5 of different attack signals are introduced from the 151st sampling data to the 350th sampling data. The DoS attacks and spoof attacks are added, respectively, that is, from the 151st to 350th group, and they are considered

as samples with attack. From the 251st to the 401 sampling data, they have added the noise attack and the scaling attack, respectively.

As expressed in Eq. (20), the residual threshold τ is an important factor to the intrusion detection performance. In this work, τ is determined by crossing validation experiments. Multiple parameter values were tested. As can be seen from Fig. 7, to achieve a relatively high intrusion detection accuracy with low false alarm rate (FAR), the residual threshold $\tau = 0.8$ is a trade-off setting value. Therefore, the residual threshold was fixed as 0.8 in the following experiments.

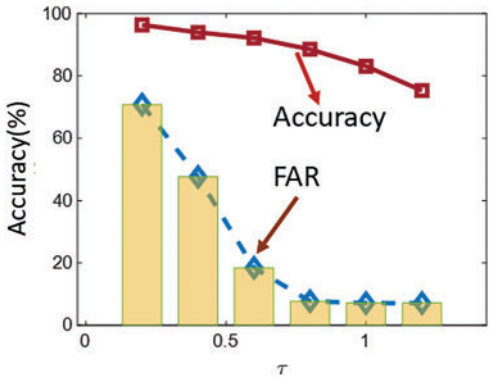

Figure 7: Effect of residual threshold τ

(2) Experimental results and discussions

Intrusion detection results of the simulated three models as described in (28) to (30) are displayed in Fig. 8. It can be seen from Fig. 8 that when attacks are introduced into the sensory system models (different clusters under each model), the system state fluctuations will occur. Though the system state fluctuations of the same attack vary under different models, they exhibit great differences between the system prediction results and the actual system state, resulting in a significant difference in the state estimation residual. By comparing the residual threshold of the system state prediction, attacks can be detected accurately.

To further analyze the effectiveness of the proposed method, the intrusion detection accuracies and FARs of different clusters under each model are listed in Fig. 9. It can be seen from Fig. 9 that although the detection accuracy and FAR of different clusters fluctuate in different models, the accuracy rates are generally over 90%, and the proposed method can achieve lower FARs for different attacks with different models. In addition, statistics of the detection performance, mean and standard deviation of the detection accuracies and FARs under different models are counted and listed in Table 2. It can be seen from Table 2 that no matter the system model, a high detection rate and lower FAR can be achieved.

Moreover, to further verify the effectiveness of IVB-NCA-NLKF, three representative and analogous methods, namely, H_∞-EKF [33], novel switching unscented Kalman filter (NS-UKF) [34], EKF and recursive last-square estimator (EKF-RLSE) [35], were used for the comparative experiment. The comparative results are listed in Table 3. As shown in Table 3, IVB-NCA-NLKF can achieve the highest detection accuracies with the lowest FAR. In addition, the proposed method can achieve relatively low standard deviation values of the detection accuracies and FAR, which means that the proposed method can achieve more stable detection results. In other words, the overall performance of the proposed method outperforms that of these comparative methods, which can realize effective intrusion detection of the sensory system.

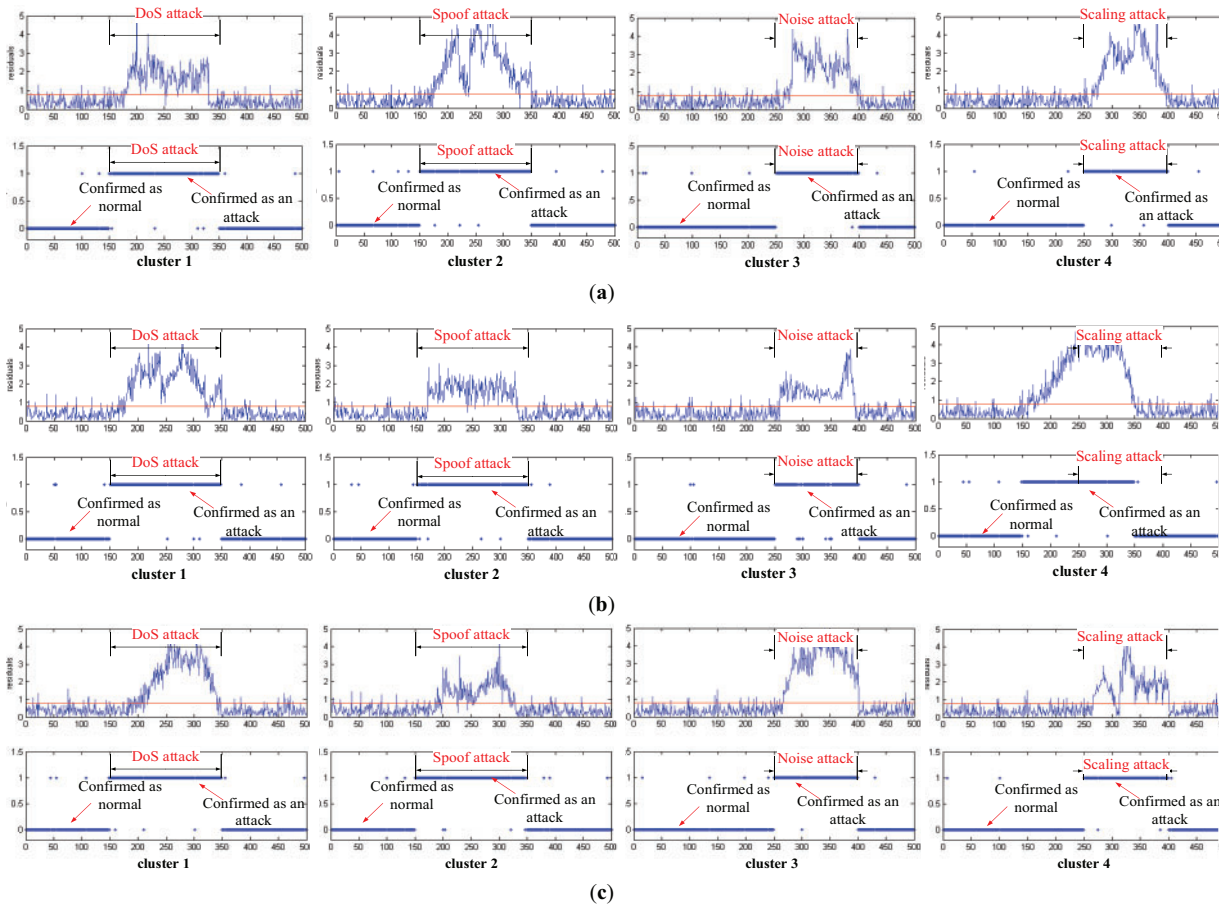

Figure 8: Experimental results of different models. (**a**) model 1; (**b**) model 2; (**c**) model 3

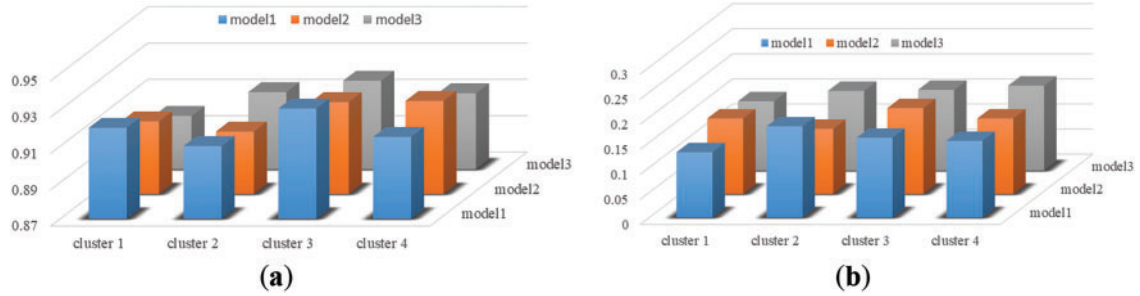

Figure 9: Detection accuracies and FAR. (**a**) Accuracies; (**b**) FAR

The IVB-NCA-NLKF method outperforms other methods due to several key advantages. First, the IVB-NCA-NLKF jointly estimates the system state, process noise, and measurement noise covariance matrices using variation inference based on sensor observations. This results in a more accurate and robust estimation of the system's state, even in the presence of uncertainties or noise in both the process and the measurements. The adoption of Bayesian inference techniques in IVB-NCA-NLKF allows for adaptive noise covariance estimation, which improves the model's ability to handle dynamic and uncertain environments. This flexibility is particularly beneficial in ICPSs, where both system dynamics and measurement noises can be highly nonlinear and unpredictable. Furthermore, the IVB-NCA-NLKF's ability to extend traditional

linear system models to nonlinear systems makes it more suitable for the intricate behaviors of ICPSs. Unlike previous linear models that may struggle with nonlinearities, the proposed method can effectively estimate the system state in more complex and realistic settings.

Table 2: Experimental results under three models of the proposed method

Models	Detection accuracy		FAR	
	Mean	Std	Mean	Std
Model 1	0.9327	0.0974	0.0026	0.0071
Model 2	0.9236	0.1135	0.0018	0.0186
Model 3	0.9193	0.1217	0.0039	0.0197

Table 3: Comparative experimental results under three models

Empirical method	Detection accuracies		FAR	
	Mean value	Std	Mean value	Std
H_∞-EKF	0.8922	0.0765	0.0137	0.0071
NS-UKF	0.8672	0.1371	0.0454	0.0186
EKF-RLSE	0.8625	0.1584	0.0669	0.0197
IVB-NCA-NLKF	0.9214	0.0212	0.0081	0.0069

4.2 Network Traffic-Based Intrusion Detection

The TrueTime toolbox (https://www.control.lth.se/research/tools-and-software/truetime/, accessed on 2 April 2025) was used to build the simulated network control system for simulating an ICPS. Detailed parameters of the simulation environment are as follows: Version-TrueTime 2.0; Operating system-Windows 10; Processor−1.99 GHz; Running memory−8 GB; Network protocol-CSMA/CD (Ethernet).

The simulated ICPS involves interference nodes, sensors, controllers and actuators, whose network structure is illustrated in Fig. 10. The simulated process system model structure is shown in Fig. 11. Some important factors of network transmission, such as data transmission delay, packet loss, and so on, will affect the system performance of the process system. By setting the interference node and acting on the whole system, various attacks are simulated. In the ICPS network system, the greater the impact on network traffic, the greater the packet loss rate, the greater the impact on system performance. When the packet loss rate reaches a certain degree, the system will no longer be stable.

Table 4 presents the normal system state and real-time data obtained from the simulation after introducing a node replication attack (NRA) at the interference node (node 1). The results show that, compared to the normal state, the average flow through the actuator (node 2) and controller (node 4) increases after the NRA attack, prolonging the ON phase and shortening the OFF phase. Moreover, the NRA attack reduces the average transmission rate of packets in the sensor node (node 3) due to bandwidth occupation. This leads to decreased transmission efficiency and an increased sensor transmission rate during the OFF phase. Although no data is sent to the controller in the OFF phase, the presence of interference nodes adds to the communication burden, further straining the system.

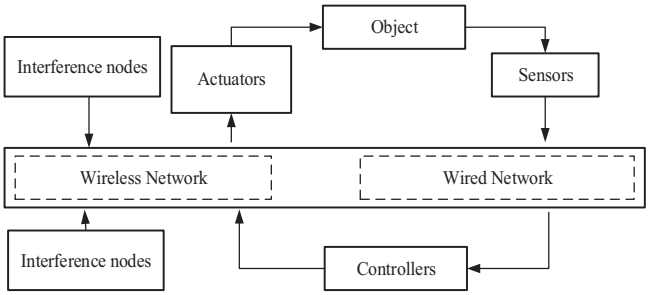

Figure 10: ICPS System block diagram

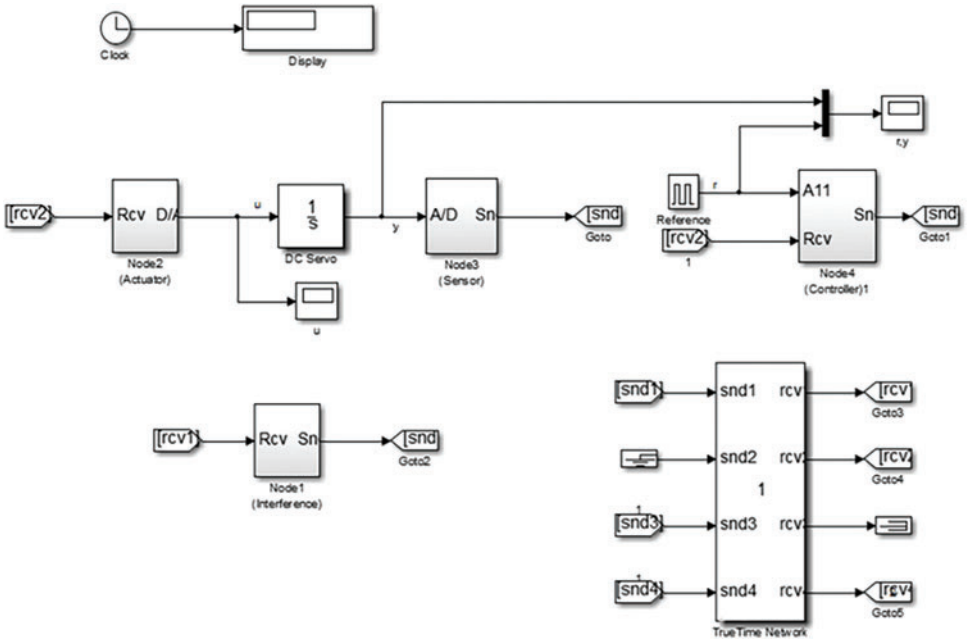

Figure 11: System simulation model

Table 4: ICPS network traffic flow

	Node	ON			OFF			*Average*	*Idle time*	*Number Total* (%)	
		Time	*Trans*	*Inter*	*Time*	*Trans*	*Inter*				
Normal	2	0.05 s	57 KB/s	0.04 s	0.77 s	0 KB/s	2.00 s	98.12%	0.58 s	18	97.97
	3	0.23 s	62 KB/s	0.01 s	0.54 s	1 KB/s	1.37 s	97.31%	0.47 s	23	
	4	0.03 s	54 KB/s	0.04 s	0.66 s	0 KB/s	2.00 s	98.49%	0.56 s	22	
NRA	1	0.15 s	36 KB/s	0.01 s	0.21 s	2 KB/s	1.21 s	87.64%	0.25 s	23	86.9
	2	0.07 s	86 KB/s	0.02 s	1.05 s	0 KB/s	2.00 s	89.71%	0.97 s	41	
	3	0.24 s	59 KB/s	0.01 s	0.61 s	3 KB/s	1.19 s	81.33%	0.68 s	23	
	4	0.06 s	87 KB/s	0.02 s	0.39 s	0 KB/s	2.00 s	88.92%	0.41 s	44	

To summarize, five common attacks, namely Man-In-The-Middle (MITM), Node Replication Attack (NRA), and Node Compromise Attack (NCA), DoS attack, and Node blocking attack, were tested to evaluate the effects of different attacks on network traffic. Experimental results are shown in Fig. 12. Fig. 12a shows the flow mode under normal conditions (no attack). Fig. 12b–d shows the network traffic flow mode after adding the corresponding attacks, respectively. It can be seen from Fig. 12 that the three attacks caused the packet loss rate of 0.1, 0.12, and 0.19, respectively, with different effects on the flow rate.

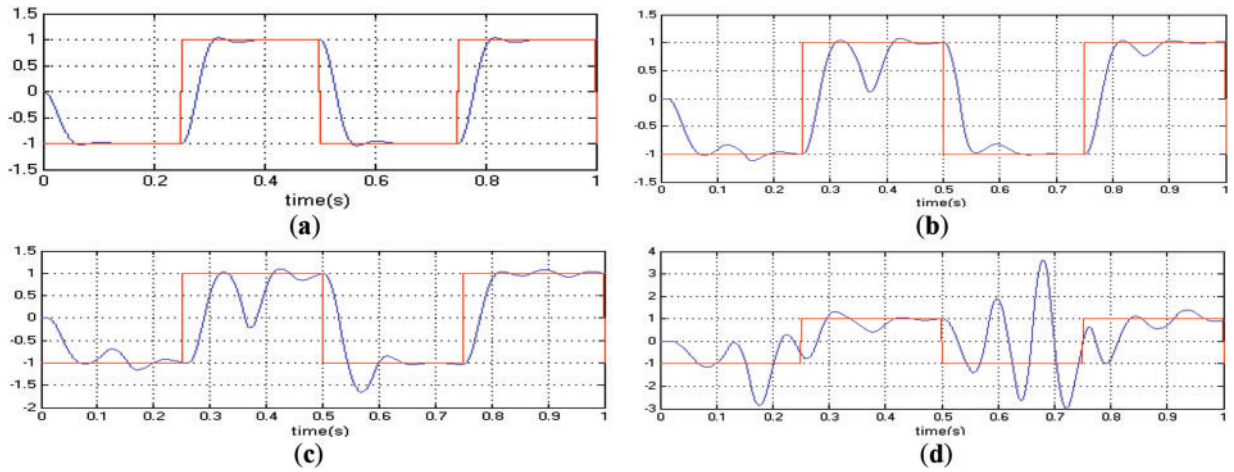

Figure 12: Impact of attacks on traffic. (a) Normal (no packet loss); (b) MITM (packet loss rate 0.1); (c) NRA (packet loss rate 0.12); (d) NCA (packet loss rate 0.19)

This experiment evaluates the detection rate and false alarm rate (FAR) of the proposed intrusion detection method, with results presented in Fig. 13. As shown, the detection rate improves as the number of training samples increases, stabilizing when the training data reaches 2000. Notably, even with fewer training samples, the model achieves a high detection rate. Additionally, the FAR decreases as training data increases, with lower FAR observed in cases of limited training data. These results demonstrate that the proposed method ensures high detection accuracy and low error rates, performing effectively even with small sample sizes.

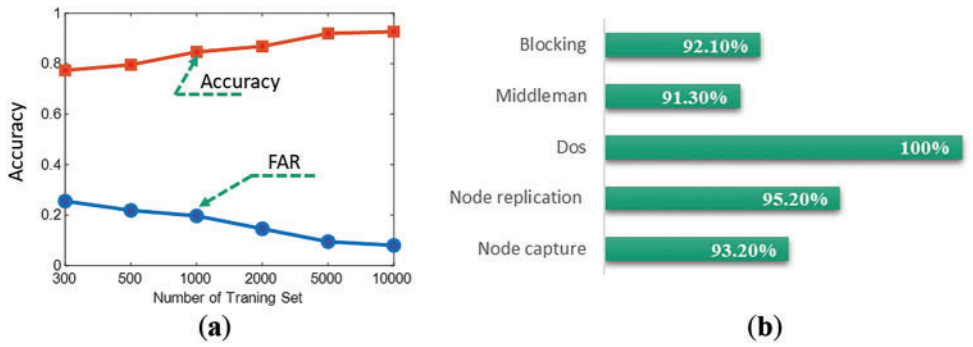

Figure 13: Relationship between detection effect and number of training sets. (a) Detection accuracy and FAR with different number of training samples; (b) Detection accuracies of different attacks

The detection results of the proposed method for different attacks are shown in Fig. 13b. As shown, the detection rates of other attacks are generally high, except in channel blocking attacks and middleman attacks because the traffic changes caused by these attacks are obvious and easy to detect. Channel-blocking attacks and middleman attacks have no great effect on traffic.

To further validate the effectiveness of the proposed intrusion detection method, some representative methods, including the CUSUM Model with Regression Strategy (CUSUM-RS) [36], Dictionary-based Compression Theory (DBCT) [37], and Hidden Semi-Markov Model (HSMM) [38], were also conducted for intrusion detection performance comparison. The detection rate (DR), FAR, and detection time (DT) are recorded as the comparison indexes. The comparative experimental results are shown in Table 5.

Table 5: Comparison of the detection performance of different methods

Data scale	CUSUM-RS [36]			DBCT [37]			HSMM [38]			Proposed		
	DR/%	FAR/%	Time/s	DR/%	FAR/%	Time/s	DR/%	FAR/%	Time/s	DR/%	FAR/%	Time/s
1000	89.22	6.47	11.53	90.68	6.44	10.42	91.65	7.23	11.03	92.06	5.26	11.79
2000	90.32	5.81	16.82	91.56	5.65	13.92	92.12	7.69	16.58	92.67	5.02	17.02
3000	91.87	5.33	19.64	92.69	5.43	16.77	92.57	5.13	17.71	93.14	4.61	19.93
4000	93.83	5.26	21.79	93.12	4.69	19.83	92.94	4.51	21.33	93.61	3.53	22.04
5000	93.96	5.20	27.02	93.49	4.51	23.49	93.47	4.24	25.43	94.22	3.12	26.89
6000	94.33	4.93	36.61	93.98	4.22	35.17	94.05	3.87	34.72	94.67	3.07	37.54
8000	94.88	4.61	41.57	94.61	4.03	40.58	94.59	3.41	41.56	95.27	2.91	42.21
10,000	95.34	4.32	69.31	95.09	3.71	68.24	95.47	3.21	69.82	96.21	2.59	69.98

Table 5 shows that the FAR of HSMM is higher than that of the proposed method. Although HSMM outperforms simple average-based schemes, it struggles to effectively differentiate between attacks and normal traffic. Its reliance on detecting spatiotemporal patterns in wake-up packet generation leads to a higher FAR. In contrast, the proposed intrusion detection method achieves higher accuracy than CUSUM-RS and DBCT. By analyzing captured data, it simultaneously extracts node-level and network-level traffic, providing a more comprehensive understanding of data characteristics and enhancing detection performance.

Beyond detection accuracy, detection efficiency is also crucial, as it directly impacts real-time performance. To ensure the real-time performance of the detection method, the detection efficiency should also be maintained at a high level. As shown in Table 5, when the sample size reaches 10,000, the detection time is only 69.98 s, demonstrating the proposed method's ability to detect attacks rapidly. While the detection time is slightly higher than that of other methods, this is due to the inclusion of CPL for dynamic network pattern learning and updating, which primarily adds time when a pattern does not match normal or abnormal cases. The system determines whether a pattern is frequent before updating the pattern library. However, given the high detection accuracy and low false alarm rate (FAR), this slight increase in detection time is negligible. Overall, the experimental results confirm that the proposed method achieves a high detection rate with relatively short detection time, proving its effectiveness for cybersecurity monitoring in ICPS networks.

5 Conclusions

To adapt to the dynamic changes of the industrial control network system environment and improve the detection effect, a hybrid ICPS-oriented intrusion detection approach is proposed. In order to detect ICPS attacks more comprehensively, intrusion detection is carried out from two aspects, i.e., the system

state anomaly monitoring and network traffic flow anomaly monitoring. Namely, an IVB-NCA-NLKF-based sensor system state anomaly detector and an online network pattern learning-based network traffic anomaly detector, are incorporated, to achieve a comprehensive cybersecurity monitoring of large-scale ICPSs. At the same time, an online pattern updating mechanism is also introduced to adjust the model automatically during the intrusion detection process to realize real-time cybersecurity monitoring. Extensive confirmatory and comparative experiments carried out by the numerical simulation system and TrueTime-based simulated network control system have demonstrated the effectiveness and superiority of the proposed method. However, the proposed ICPS security protection method in this work is based on the situation that the system is deterministic. In the current large-scale ICPS, sensors, actuators, and controllers are all likely to be dynamically added. Therefore, further work will focus on how to extend the method of this work to the system resources-dynamically changing ICPS and the real ICPSs.

Acknowledgement: Not applicable.

Funding Statement: This work is supported by the National Natural Science Foundation of China (NSFC) under grant No. 62371187 and the Hunan Provincial Natural Science Foundation of China under Grant Nos. 2024JJ8309 and 2023JJ50495.

Author Contributions: Conceptualization, Jinping Liu and Wuxia Zhang; methodology, Junbin He, Guangyi Yang and Jinping Liu; software, Wuxia Zhang and Guangyi Yang; formal analysis, Wuxia Zhang; investigation, Junbin He, Wuxia Zhang and Jinping Liu; resources, Wuxia Zhang, Guangyi Yang and Xianyi Liu; data curation, Xianyi Liu; writing—original draft preparation, Jinping Liu, Wuxia Zhang and Xianyi Liu; writing—review and editing, Jinping Liu and Wuxia Zhang; funding acquisition, Jinping Liu. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Data available on request from the authors.

Ethics Approval: Not applicable.

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

Appendix A IW Distribution

Inverse Wishart (IW) distribution, also termed inverted Wishart distribution, is a probability distribution model defined over real-valued, symmetric, positive-definite matrices. In the Bayesian estimation, it is mainly used to describe the conjugate prior distribution of the covariance matrix of multivariate normal distribution samples. The probability density of IW distribution can be expressed as [14],

$$\mathrm{IW}\left(\mathbf{R}|\lambda,\mathbf{D}\right)=\frac{|\mathbf{R}|^{-(\lambda+d+1)/2}}{Z_{\mathrm{IW}}}\exp\left\{-\frac{1}{2}\mathrm{tr}\left(\mathbf{D}\mathbf{R}^{-1}\right)\right\} \tag{A1}$$

where $\mathbf{R}$ are $d\times d$ symmetric positive definite matrices; $\mathbf{D}\in\mathbb{R}^{d\times d}$ is a symmetric positive definite matrix, also known as an inverse scale matrix; $tr\left(\cdot\right)$ means the trace of a matrix; λ stands for the degrees of freedom, and $Z_{\mathrm{IW}}=2^{\lambda d/2}\Gamma_d\left(\lambda/2\right)|\mathbf{D}|^{-\lambda/2}$, Γ_d is a d-D Gamma function.

When $\lambda>d+1$, the IW distribution has the following properties,

$$\mathbb{E}\left[\mathbf{R}\right]=\frac{\mathbf{D}}{\lambda-d-1} \tag{A2}$$

The variance of each element of $\mathbf{R}$ is,

$$\operatorname{var}\left[\mathbf{R}_{ij}\right]=\frac{(\lambda-d+1)\,\mathrm{D}_{ij}{}^{2}+(\lambda-d+1)\,\mathrm{D}_{ii}\mathrm{D}_{jj}}{(\lambda-d)\,(\lambda-d-1)^{2}\,(\lambda-d-3)} \tag{A3}$$

Given n i.i.d d-D Gaussian variables, $\mathbf{X}=[X_1,\cdots,X_n]$, drawn from the distribution of $\mathcal{N}(X|\mathbf{0},\mathbf{R})$, the conditional distribution of $p(\mathbf{R}|\mathbf{X})$ has an IW distribution of $\mathrm{IW}(\mathbf{R}|\lambda+n,\mathbf{A}+\mathbf{D})$, where $\mathbf{A}=\mathbf{X}\mathbf{X}^{T}$. Due to its conjugacy to the multivariate Gaussian, it can integrate out the covariance parameter in Gaussian by,

$$p(\mathbf{X}|\lambda,\mathbf{D})=\int p(\mathbf{X}|\mathbf{R})\,p(\mathbf{R}|\lambda,\mathbf{D})\,d\mathbf{R}=\frac{|\mathbf{R}|^{\lambda/2}\Gamma_{\lambda}\left(\frac{n+\lambda}{2}\right)}{\pi^{\frac{nd}{2}}\,|\mathbf{R}+\mathbf{A}|^{\frac{n+\lambda}{2}}\,\Gamma_{\lambda}\left(\frac{\lambda}{2}\right)} \tag{A4}$$

Appendix B Detailed $q(\mathbf{x}_k)$, $q(\mathbf{\Sigma}_{k|k-1})$, $q(\mathbf{R}_k)$ Estimation Procedure

Firstly, by the expansion of the Formula (18), we can achieve,

$$\begin{aligned}\log p\left(\mathrm{x}_k,\mathbf{\Sigma}_{k|k-1},\mathbf{R}_k,\mathrm{y}_{1:k}\right)=&-\frac{1}{2}\left(\hat{d}_{k|k-1}+m+2\right)\log|\mathbf{R}_k|-\frac{1}{2}\mathrm{tr}\left(\mathbf{D}_{k|k-1}\mathbf{R}_k{}^{-1}\right)-\\&\frac{1}{2}\left(\hat{t}_{k|k-1}+n+2\right)\log|\mathbf{\Sigma}_{k|k-1}|-\frac{1}{2}\mathrm{tr}\left(\mathbf{T}_{k|k-1}\mathbf{\Sigma}_{k|k-1}{}^{-1}\right)-\\&\frac{1}{2}\left(\mathrm{x}_k-\hat{\mathrm{x}}_{k|k-1}\right)^{T}\mathbf{\Sigma}_{k|k-1}{}^{-1}\left(\mathrm{x}_k-\hat{\mathrm{x}}_{k|k-1}\right)-\frac{1}{2}\left(\mathrm{y}_k-\hat{\mathrm{y}}_{k|k-1}\right)^{T}\mathbf{R}_k{}^{-1}\left(\mathrm{y}_k-\hat{\mathrm{y}}_{k|k-1}\right)+C_{\boldsymbol{\theta}}\end{aligned} \tag{A5}$$

where $C_{\boldsymbol{\theta}}$ represents terms that do not related to parameters, $\boldsymbol{\theta}=\left\{\mathrm{x}_k,\mathbf{\Sigma}_{k|k-1},\mathbf{R}_k\right\}$.

(1) $q(\mathbf{\Sigma}_{k|k-1})$ Estimation

Denote $\theta=\mathbf{\Sigma}_{k|k-1}$, according to the Formula (17), we can achieve,

$$\begin{aligned}\log q^{(i+1)}(\theta)=&-\frac{1}{2}\left(\hat{d}_{k|k-1}+m+2\right)\mathbb{E}^{(i)}\left[\log|\mathbf{R}_k|\right]-\frac{1}{2}\mathbb{E}^{(i)}\left[\mathrm{tr}\left(\mathbf{D}_{k|k-1}\mathbf{R}_k{}^{-1}\right)\right]-\frac{1}{2}\left(\hat{t}_{k|k-1}+n+2\right)\log|\mathbf{\Sigma}_{k|k-1}|\\&-\frac{1}{2}\mathrm{tr}\left\{\left(\mathbf{A}_k{}^{(i)}+\mathbf{T}_{k|k-1}\right)\mathbf{\Sigma}_{k|k-1}{}^{-1}\right\}-\frac{1}{2}\mathbb{E}^{(i)}\left[\left(\mathrm{y}_k-\hat{\mathrm{y}}_{k|k-1}\right)^{T}\mathbf{R}_k{}^{-1}\left(\mathrm{y}_k-\hat{\mathrm{y}}_{k|k-1}\right)\right]+C_{\boldsymbol{\theta}}\\=&\,C_{\mathbf{\Sigma}_{k|k-1}}+\frac{1}{2}\left(\hat{t}_{k|k-1}+n+2\right)\log|\mathbf{\Sigma}_{k|k-1}|-\frac{1}{2}\mathrm{tr}\left\{\left(\mathbf{A}_k{}^{(i)}+\mathbf{T}_{k|k-1}\right)\mathbf{\Sigma}_{k|k-1}{}^{-1}\right\}\end{aligned} \tag{A6}$$

where $q^{(i+1)}(\theta)$ represents the $i+1$ iteration of $q(\theta)$ estimation, and,

$$\begin{aligned}\mathbf{A}_k{}^{(i)}&=\mathbb{E}^{(i)}\left[\left(\mathrm{x}_k-\hat{\mathrm{x}}_{k|k-1}\right)\left(\mathrm{x}_k-\hat{\mathrm{x}}_{k|k-1}\right)^{T}\right]=\mathbb{E}^{(i)}\left[\begin{array}{c}\left(\mathrm{x}_k-\hat{\mathrm{x}}_k^{(i)}+\hat{\mathrm{x}}_k^{(i)}-\hat{\mathrm{x}}_{k|k-1}\right)\\\left(\mathrm{x}_k-\hat{\mathrm{x}}_k^{(i)}+\hat{\mathrm{x}}_k^{(i)}-\hat{\mathrm{x}}_{k|k-1}\right)^{T}\end{array}\right]\\&=\mathbb{E}^{(i)}\left[\left(\mathrm{x}_k-\hat{\mathrm{x}}_k^{(i)}\right)\left(\mathrm{x}_k-\hat{\mathrm{x}}_k^{(i)}\right)^{T}\right]+\left(\hat{\mathrm{x}}_k^{(i)}-\hat{\mathrm{x}}_{k|k-1}\right)\left(\hat{\mathrm{x}}_k^{(i)}-\hat{\mathrm{x}}_{k|k-1}\right)^{T}\\&=\mathbf{\Sigma}_{k|k}{}^{(i)}+\left(\hat{\mathrm{x}}_k^{(i)}-\hat{\mathrm{x}}_{k|k-1}\right)\left(\hat{\mathrm{x}}_k^{(i)}-\hat{\mathrm{x}}_{k|k-1}\right)^{T}\end{aligned} \tag{A7}$$

According to the Formulae (A6) and (A1), we can see that $q^{(i+1)}\left(\mathbf{\Sigma}_{k|k-1}\right)$ also obey an IW distribution, i.e.,

$$q^{(i+1)}\left(\mathbf{\Sigma}_{k|k-1}\right)=\mathrm{IW}\left(\mathbf{\Sigma}_{k|k-1}|\hat{t}_k^{(i+1)},\mathbf{T}_k{}^{(i+1)}\right) \tag{A8}$$

where $\hat{t}_k^{(i+1)} \triangleq \hat{t}_{k|k-1} + 1$, $\mathbf{T}_k{}^{(i+1)} \triangleq \mathbf{A}_{k|k-1}{}^{(i)} + \mathbf{T}_{k|k-1}$.

(2) $q(\mathbf{R}_k)$ Estimation

$$\begin{aligned}\log q^{(i+1)}(\mathbf{R}_k) = &-\frac{1}{2}\left(\hat{d}_{k|k-1}+m+2\right)\log|\mathbf{R}_k| - \frac{1}{2}\mathrm{tr}\left(\left(\mathbf{D}_{k|k}+\mathbf{B}_k{}^{(i)}\right)\mathbf{R}_k{}^{-1}\right) - \\ &\frac{1}{2}\left(\hat{t}_{k|k-1}+n+2\right)\mathbb{E}^{(i)}\left[\log|\boldsymbol{\Sigma}_{k|k-1}|\right] - \frac{1}{2}\mathbb{E}^{(i)}\left[\mathrm{tr}\left(\mathbf{T}_{k|k-1}\boldsymbol{\Sigma}_{k|k-1}{}^{-1}\right)\right] \\ &-\frac{1}{2}\mathbb{E}^{(i)}\left[\left(\mathrm{x}_k-\hat{\mathrm{x}}_{k|k-1}\right)^T\boldsymbol{\Sigma}_{k|k-1}{}^{-1}\left(\mathrm{x}_k-\hat{\mathrm{x}}_{k|k-1}\right)\right] + C_{\boldsymbol{\theta}} \\ = &\, C_{\mathbf{R}_k} + \frac{1}{2}\left(\hat{d}_{k|k-1}+m+2\right)\log|\mathbf{R}_k| - \frac{1}{2}\mathrm{tr}\left(\left(\mathbf{D}_{k|k-1}+\mathbf{B}_k{}^{(i)}\right)\mathbf{R}_k{}^{-1}\right)\end{aligned} \tag{A9}$$

where,

$$\begin{aligned}\mathbf{B}_k{}^{(i)} &= \mathbb{E}\left[\left(\mathrm{y}_k-\hat{\mathrm{y}}_{k|k-1}\right)\left(\mathrm{y}_k-\hat{\mathrm{y}}_{k|k-1}\right)^T\right] \\ &= \mathbb{E}\left\{\mathbb{E}\left(\mathrm{y}_k - h\left(\hat{\mathrm{x}}_{k|k-1}\right) - \mathbf{H}_k\mathrm{x}_k + \mathbf{H}_k\hat{\mathrm{x}}_{k|k-1}\right)\cdot\left(\mathrm{y}_k - h\left(\hat{\mathrm{x}}_{k|k-1}\right) - \mathbf{H}_k\mathrm{x}_k + \mathbf{H}_k\hat{\mathrm{x}}_{k|k-1}\right)^T\right\} \\ &= \mathbb{E}\left\{\mathbb{E}\left(\mathrm{y}_k - \mathbf{H}_k\mathrm{x}_{k|k}{}^{(i)} + \mathbf{H}_k\mathrm{x}_{k|k}{}^{(i)} - \mathbf{H}_k\mathrm{x}_k + \mathbf{H}_k\hat{\mathrm{x}}_{k|k-1} - h\left(\hat{\mathrm{x}}_{k|k-1}\right)\right)\cdot\right. \\ &\left.\left(\mathrm{y}_k - \mathbf{H}_k\mathrm{x}_{k|k}{}^{(i)} + \mathbf{H}_k\mathrm{x}_{k|k}{}^{(i)} - \mathbf{H}_k\mathrm{x}_k + \mathbf{H}_k\hat{\mathrm{x}}_{k|k-1} - h\left(\hat{\mathrm{x}}_{k|k-1}\right)\right)^T\right\} \\ &= \left(\mathrm{y}_k - h\left(\hat{\mathrm{x}}_{k|k-1}\right)\right)\left(\mathrm{y}_k - h\left(\hat{\mathrm{x}}_{k|k-1}\right)\right)^T + \mathbf{H}_k\boldsymbol{\Sigma}_{k|k}{}^{(i)}\mathbf{H}_k{}^T\end{aligned} \tag{A10}$$

According to the Formulae (A9) and (A1), $q^{(i+1)}(\mathbf{R}_k)$ also obeys an IW distribution, i.e.,

$$q^{(i+1)}(\mathbf{R}_k) = \mathrm{IW}\left(\mathbf{R}_k|\hat{d}_k^{(i+1)}, \hat{\mathbf{D}}_k^{(i+1)}\right) \tag{A11}$$

where $\hat{d}_k^{(i+1)} = \hat{d}_{k|k-1} + m + 1$, $\hat{\mathbf{D}}_k^{(i+1)} = \mathbf{D}_{k|k-1} + \mathbf{B}_k{}^{(i)}$.

(3) $q(\boldsymbol{x}_k)$ Estimation

$$\begin{aligned}\log q^{(i+1)}(\mathrm{x}_k) = &-\tfrac{1}{2}\left(\mathrm{x}_k-\hat{\mathrm{x}}_{k|k-1}\right)^T\mathbb{E}^{(i+1)}\left[\boldsymbol{\Sigma}_{k|k-1}{}^{-1}\right]\left(\mathrm{x}_k-\hat{\mathrm{x}}_{k|k-1}\right) - \\ &\tfrac{1}{2}\left(\mathrm{y}_k-\hat{\mathrm{y}}_{k|k-1}\right)^T\mathbb{E}^{(i+1)}\left[\mathbf{R}_k{}^{-1}\right]\left(\mathrm{y}_k-\hat{\mathrm{y}}_{k|k-1}\right) + C_{\mathrm{x}_k}\end{aligned} \tag{A12}$$

According to the first two steps, we can see that $\boldsymbol{\Sigma}_{k|k-1}$ and $\mathbf{R}_k$ all obey the IW distribution,

$$\boldsymbol{\Sigma}_{k|k-1}{}^{(i+1)} = \left\{\mathbb{E}^{(i+1)}\left[\boldsymbol{\Sigma}_{k|k-1}{}^{-1}\right]\right\}^{-1} = \frac{\mathbf{T}_k{}^{(i+1)}}{\hat{t}_k^{(i+1)} - n - 1} \tag{A13}$$

$$\mathbf{R}_k{}^{(i+1)} = \left\{\mathbb{E}^{(i+1)}\left[\mathbf{R}_k{}^{-1}\right]\right\}^{-1} = \frac{\hat{\mathbf{D}}_k^{(i+1)}}{\hat{d}_k^{(i+1)} - m - 1} \tag{A14}$$

Based on the Formula (A12), we can see that $q^{(i+1)}(\mathrm{x}_k)$ obeys a Gaussian distribution, i.e.,

$$q^{(i+1)}(\mathrm{x}_k) = \mathcal{N}\left(\mathrm{x}_k|\mathrm{x}_{k|k}{}^{(i+1)}, \boldsymbol{\Sigma}_{k|k}{}^{(i+1)}\right) \tag{A15}$$

where,

$$\boldsymbol{\Sigma}_{k|k}{}^{(i+1)} = \left(\mathbf{I} - \mathbf{K}_k{}^{(i+1)}\mathbf{H}_k\right)\boldsymbol{\Sigma}_{k|k-1}{}^{(i+1)} \tag{A16}$$

$$\hat{\mathrm{x}}_{k|k} = \hat{\mathrm{x}}_{k|k-1} + \mathbf{K}_k\left(\mathrm{y}_k - h\left(\hat{\mathrm{x}}_{k|k-1}, \mathrm{u}_k\right)\right) \tag{A17}$$

where,

$$\mathbf{K}_k{}^{(i+1)} \triangleq \boldsymbol{\Sigma}_{k|k-1}{}^{(i+1)}\mathbf{H}_k{}^T\left(\mathbf{H}_k\boldsymbol{\Sigma}_{k|k-1}{}^{(i+1)}\mathbf{H}_k{}^T + \mathbf{R}_k{}^{(i+1)}\right)^{-1} \tag{A18}$$

Given the initiation value of $\hat{\mathrm{x}}_{0|0}$, $\hat{t}_{0|0}$, $\mathbf{T}_{0|0}$, $\hat{d}_{0|0}$, $\mathbf{D}_{0|0}$ the variation Bayesian estimation of x_k, $\boldsymbol{\Sigma}_{k|k-1}$, $\mathbf{R}_k$ based on the observations can be computed by a M-step iteration compution or terminated automatically by the convergence of the estimations, Formulae (A8), (A11) and (A15).

References

1. Kayan H, Nunes M, Rana O, Burnap P, Perera C. Cybersecurity of industrial cyber-physical systems: a review. ACM Comput Surv. 2022;54(11s):1–35. doi:10.1145/3510410.
2. Chae J, Lee S, Jang J, Hong S, Park KJ. A survey and perspective on industrial cyber-physical systems (ICPS): from ICPS to AI-augmented ICPS. IEEE Trans Ind Cyber-Phys Syst. 2023;1(1):257–72. doi:10.1109/TICPS.2023.3323600.
3. Yu GF. A multi-objective decision method for the network security situation grade assessment under multi-source information. Inf Fusion. 2024;102(10):102066. doi:10.1016/j.inffus.2023.102066.
4. Kheddar H, Dawoud DW, Awad AI, Himeur Y, Khan MK. Reinforcement-learning-based intrusion detection in communication networks: a review. IEEE Commun Surv Tutor. 2024. doi:10.1109/COMST.2024.3484491.
5. Yang K, Li Q, Lin X, Chen X, Sun L. iFinger: intrusion detection in industrial control systems via register-based fingerprinting. IEEE J Sel Areas Commun. 2020;38(5):955–67. doi:10.1109/JSAC.2020.2980921.
6. Toussaint M, Krima S, Panetto H. Industry 4.0 data security: a cybersecurity frameworks review. J Ind Inf Integr. 2024;39(3):100604. doi:10.1016/j.jii.2024.100604.
7. Zhong Y, Wang Z, Shi X, Yang J, Li K. RFG-HELAD: a robust fine-grained network traffic anomaly detection model based on heterogeneous ensemble learning. IEEE Trans Inf Forensics Secur. 2024;19:5895–910. doi:10.1109/TIFS.2024.3402439.
8. Luo Y, Xiao Y, Cheng L, Peng G, Yao D. Deep learning-based anomaly detection in cyber-physical systems: progress and opportunities. ACM Comput Surv. 2021;54(5):1–36. doi:10.1145/3453155.
9. Nigro L, Cicirelli F, Pupo F. Clustering performance of an evolutionary k-means algorithm. In: Yang X, Sherratt RS, Dey N, Joshi A, editors. International Congress on Information and Communication Technology. Singapore: Springer; 2024. p. 359–69.
10. Shen S, Zhang C, Chai R, Dai L, Chai S, Xia Y. Stabilizing nonlinear model predictive control under Denial-of-Service attack via dynamic samples selection. Automatica. 2024;164(9):111591. doi:10.1016/j.automatica.2024.111591.
11. Shinohara T, Namerikawa T. Optimal security investment problem for secure state estimation on cyber-physical systems. IEEE Trans Autom Control. 2025;70(2):1244–51. doi:10.1109/TAC.2024.3451216.
12. Pasqualetti F, Dorfler F, Bullo F. Attack detection and identification in cyber-physical systems. IEEE Trans Autom Control. 2013;58(11):2715–29. doi:10.1109/TAC.2013.2266831.
13. Lee C, Shim H, Eun Y. On redundant observability: from security index to attack detection and resilient state estimation. IEEE Trans Autom Control. 2019;64(2):775–82. doi:10.1109/TAC.2018.2837107.
14. Zhang J, Wei G, Ding D, Ju Y. Distributed sequential state estimation over binary sensor networks with inaccurate process noise covariance: a variational bayesian framework. IEEE Trans Signal Inf Process Over Netw. 2025;11:1–10. doi:10.1109/TSIPN.2024.3497773.
15. Chen Y, Li W, Du Y. A novel robust adaptive Kalman filter with application to urban vehicle integrated navigation systems. Measurement. 2024;236(12):114844. doi:10.1016/j.measurement.2024.114844.

16. Liu J, Zhang W, Ma T, Tang Z, Xie Y, Gui W, et al. Toward security monitoring of industrial cyber-physical systems via hierarchically distributed intrusion detection. Expert Syst Appl. 2020;158:113578. doi:10.1016/j.eswa.2020.113578.
17. Yuan D, Luo T, Gu C, Zhu K. The cyber-physical system of machine tool monitoring: a model-driven approach with extended Kalman filter implementation. IEEE Trans Ind Inform. 2022;19(9):9576–85. doi:10.1109/TII.2022.3231422.
18. Hesar HD, Hesar AD. Adaptive dual augmented extended Kalman filtering of ECG signals. Measurement. 2025;239(7):115457. doi:10.1016/j.measurement.2024.115457.
19. Yang X, Zhao W, Xu Y, Wang CD, Li B, Nie F. Sparse K-means clustering algorithm with anchor graph regularization. Inf Sci. 2024;667(9):120504. doi:10.1016/j.ins.2024.120504.
20. Bagirov AM, Aliguliyev RM, Sultanova N. Finding compact and well-separated clusters: clustering using silhouette coefficients. Pattern Recognit. 2023;135:109144. doi:10.1016/j.patcog.2022.109144.
21. Arbelaitz O, Gurrutxaga I, Muguerza J, Pérez J, Perona II. An extensive comparative study of cluster validity indices. Pattern Recognit. 2013;46(1):243–56. doi:10.1016/j.patcog.2012.07.021.
22. Mustafi D, Sahoo G. A hybrid approach using genetic algorithm and the differential evolution heuristic for enhanced initialization of the k-means algorithm with applications in text clustering. Soft Comput. 2019;23(15):6361–78. doi:10.1007/s00500-018-3289-4.
23. Sarehati U, Mohammadreza V, Sophia AC. Sensor clustering-based approach for structural damage identification under ambient vibration—ScienceDirect. Autom Constr. 2021;121:103433. doi:10.1016/j.autcon.2020.103433.
24. Chang G, Chen C, Zhang Q, Zhang S. Variational bayesian adaptation of process noise covariance matrix in Kalman filtering. J Frankl Inst. 2021;358(7):3980–93. doi:10.1016/j.jfranklin.2021.02.037.
25. Huang Y, Zhang Y, Wu Z, Ning L, Chambers J. A novel adaptive kalman filter with inaccurate process and measurement noise covariance matrices. IEEE Trans Autom Control. 2017;63(2):594–601. doi:10.1109/TAC.2017.2730480.
26. Huang K, Zhang Q, Zhou C, Xiong N, Qin Y. An efficient intrusion detection approach for visual sensor networks based on traffic pattern learning. IEEE Trans Syst Man Cybern Syst. 2017;47(10):2704–13. doi:10.1109/TSMC.2017.2698457.
27. He Z, Yu C. Clustering stability-based evolutionary K-Means. Soft Comput. 2018;23(1):305–21. doi:10.1007/s00500-018-3280-0.
28. Silva FDS, Reis JCD, Reis MS. SERIEMA: a framework to enhance clustering stability, compactness, and separation by fusing multimodal data. In: 29th International Conference on Applications of Natural Language to Information Systems (NLDB); 2024 Jun 25–27; Turin, Italy. p. 394–408.
29. Yu Z, Wong HS, Wang H. Graph-based consensus clustering for class discovery from gene expression data. Bioinformatics. 2007;23(21):2888–96. doi:10.1093/bioinformatics/btm463.
30. Liu J, Zhang W, Tang Z, Xie Y, Ma T, Zhang J, et al. Adaptive intrusion detection via GA-GOGMM-based pattern learning with fuzzy rough set-based attribute selection. Expert Syst Appl. 2020;139(1):112845. doi:10.1016/j.eswa.2019.112845.
31. Das NR, Mukherjee I, Paul PG. An intelligent clustering framework for substitute recommendation and player selection. J Supercomput. 2023;79(15):16409–41. doi:10.1007/s11227-023-05314-z.
32. Liu T, Tian J, Wang J, Wu H, Sun L, Zhou Y, et al. Integrated security threats and defense of cyber-physical systems. Acta Autom Sin. 2019;45(1):5–24. doi:10.16383/j.aas.2018.c180461.
33. Lin C, Cheng X, Zhang H, Gong X. Estimation of center of gravity position for distributed driving electric vehicles based on combined H∞-EKF method. Energy Proc. 2016;88(1):970–7. doi:10.1016/j.egypro.2016.06.121.
34. Cui L, Wang X, Xu Y, Jiang H, Zhou J. A novel Switching Unscented Kalman Filter method for remaining useful life prediction of rolling bearing. Measurement. 2019;135:678–84. doi:10.1016/j.measurement.2018.12.028.
35. Wen S, Qi H, Niu Z, Ren Y, Wei L, Ruan L. Real-time retrieval of transient heat flux on the surface of participating medium by using the EKF-RLSE technique. Infrared Phys Technol. 2018;95(1):113–21. doi:10.1016/j.infrared.2018.10.023.
36. Haller P, Genge B, Duka AV, Duka AV. On the practical integration of anomaly detection techniques in industrial control applications. Int J Crit Infrastruct Prot. 2019;277(1):1–50.

37. Rose JD, Dhanushkkar H, Jagadishan M. A self-learning and lossless dictionary-based compression algorithm. In: 2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI); 2024 May 09–10; Chennai, India.
38. Eleftheroglou N, Galanopoulos G, Loutas T. Similarity learning hidden semi-Markov model for adaptive prognostics of composite structures. Reliab Eng Syst Saf. 2024;243:109808. doi:10.1016/j.ress.2023.109808.