eNergetics 2024
DOI: https://doi.org/10.

Original Scientific Article

A Review on Cyber Attack Detection and Defense Strategies in Cyber-Physical Power Systems

Erdem Koca[1], Musa Terkes[2], Alpaslan Demirci[3]

[1]Electrical Engineering Department of Yıldız Technical University, Istanbul, Türkiye
[2]Electrical Engineering Department of Yıldız Technical University, Istanbul, Türkiye,
https://orcid.org/0000-0002-4411-411

[3]Electrical Engineering Department of Yıldız Technical University, Istanbul, Türkiye,
https://orcid.org/0000-0002-1038-7224

[1]kocaa.erdem@gmail.com, [2]musa.terkes@yildiz.edu.tr, [3]ademirci@yildiz.edu.tr

Abstract—**Malicious cyber-attacks on efficient modern power systems based on the Internet of Energy, which are digitized and include advanced intelligence elements, coordinating complex units such as measurement, computation, execution, and communication, cause societal risks on a small or large scale. The penetration of intelligent electronic devices, simultaneous metering technology, and information communication raise vulnerability issues. Considering the possibility of large-scale attacks due to the tight coupling between the physical and cyber layers, timely detection of cyber intrusions and robustness of defenses are critical for the reliability of advanced communication network-based cyber-physical power systems (CPPS). Accordingly, this paper provides an overview of security assessment, focusing on detecting possible cyber-attacks and defense strategies that cause instability, vulnerability, and insecurity in CPPSs. A signature, anomaly and behavior-based, hybrid, AI-scale, and state observer cyber-attack detection techniques are described, and defense fundamentals in cybersecurity, such as secure authentication, encryption, trusted access and defense technologies, and resource utilization, are discussed. Developing cyber-attack detection and defense strategies that can flexibly and dynamically respond to the unique temporal and spatial characteristics of CPPS will improve the modernization of the power grid.**

Keywords - Cyber security; Cyber attack; Cyber-physical power systems; malware; Detection and defense strategies

I. INTRODUCTION

A stable and reliable power supply can be obtained using large-scale sensing measurement mechanisms, complex information communication networks, and optimizing operational processes. Recently, the traditional perception of the power system has collapsed. The scale of the cyber network has dramatically increased, and the energy internet has entered into active communication with intelligent electronic devices. Accordingly, the intersection of traditional power systems with physical equipment, information, and communication technologies, and hence cyber systems, advanced metering infrastructure, computational intelligence, and cyber-secure communication technologies form multidimensional and heterogeneous cyber-physical power systems (CPPS). Integrating control, computation, and communication functions, these structures enable smart grid technologies and the bi-directional flow of electricity and information. CPPSs improve power quality and reliability while avoiding unnecessary backup plant installation via efficient plant utilization. Enhances resilience to failures while

ISBN: xxx-xx-xxxxx-xx-x

Creative Commons Non Commercial CC BY-NC: This article is distributed under the terms of the Creative Commons Attribution-Non Commercial 4.0 License (https://creativecommons.org/licenses/by-nc/4.0/) which permits non-commercial use, reproduction and distribution of the work without further permission.

strengthening grid capacity. Promotes predictive maintenance and self-healing responses to outages. The Internet of Things has reached this point by jointly pursuing big data, cloud computing, and networking technologies. However, it should be noted that cyber system performance will significantly impact physical power system operating characteristics.

CPPSs include most functions of the unpredictable power system network, such as generation, transmission, distribution, utilization, and sale of electricity. They are dynamic and flexible to manage real-time physical power system monitoring and control and operational decisions with embedded systems. The physical layer is more governed by physical regulations and refers to the usual power systems that operate sustainably. It is also dynamic and evaluates the physical relationship of energy flow. The cyber layer is a static infrastructure and includes information and communication services, control, and embedded systems. The comparison of cyber and physical systems is described in Table I [1]. CPPSs that assess the intersection of related systems are modeled in three subcategories: connectivity, interaction, and dependency. The discrete actions of the physical and cyber systems are evaluated in the connectivity model, while their impact on each other constitutes the interaction model. The dependency model determines the level of interdependence of both systems. A connection protocol is often used for the effectiveness of communication links between heterogeneous systems. The protocol addresses heterogeneity at three levels: functional interoperability, policy regulation, and performance assurance. Functional interoperability is the intersection rather than cyber and physical integration. Policy regulation refers to the plan changes existing operators implement for economic and operational performance. In contrast, performance assurance, it addresses defense strategies against attacks and failures, control of sensitive parameters in the power system network, measurement accuracy, and data processing and analysis applicability. From another perspective, there are three levels of interaction in CPPS: first, second, and third. The relationship of components in the power system network, such as generators, transformers, and transmission lines, with the power system controller is evaluated at the first level. The information from the core components is transferred to the power system controller, and the control signal is calculated. Then, output feedback is provided to the core components for operational optimization of the power grid. A second interaction level occurs between the power system controller and the communication infrastructure. All functions of subsystems, such as sensors, actuators, interfaces, control, computation, and communication, are coordinated with the information and communication infrastructure. At the third level of interaction, the communication infrastructure interacts with the cyber system. The main and auxiliary system, main and communication server, two-way communication structure, computing stations, intelligent control application software, cyber-attack security, and defense mechanism are the sub-components of the cyber system. Operations such as load and condition forecasting, parameter optimization, voltage control, fluctuation analysis, data monitoring, model verification, and stability assessment are carried out with the cyberinfrastructure. Another view is that CPPS can be evaluated as component, communication and functional layers. The first layer consists of primary (generator, transformer, etc.), secondary (protection relay, sensor, actuator, etc.), and interconnected electrical devices. The secondary equipment collects operational information from the primary components. The communication architecture provides the coordination between all components of the power system network at the second level. Communication technologies such as the IEEE 802 series, network traffic, and routing components perform a functional process at this level. All operational information is stored and processed in the control center at the last level. Decision-making and defense mechanisms, control algorithms, master stations, web, communication and application servers, databases, and human-machine interfaces are the brains of centralized operations. Information andfunctional processes evaluate easy information exchange, coordinated interoperability, and international interface procedures, and the main station elements perform calculations.

The expansion of power system networks with increasing load demand and the growth of cyber system size has led to deploying many intelligent electronic devices (IEDs) in the network. Besides IEDs, cyber assets such as routers, Ethernet switches, and operating and business systems are also distributed in CPPS.

TABLE I. COMPARING CYBER AND PHYSICAL SYSTEMS DEPENDING ON THEIR CHARACTERISTICS

Characteristics	**Physical System**	**Cyber System**
Components	Generator, transformer, transmission line, circuit breaker, protective relay, load, etc.	Control systems, computing devices, communication networks
Nature of System	Continuous, dynamic behavior	Discrete, static behavior
Modeling	Differential-algebraic equations	Difference equations
System State	Energy flow	Information flow
Branch Model	Power grid model – energy generation, energy transmission, and energy distribution	Information flow-oriented model – data transmission, data processing, and data pool
Condition	Generation and load balance, power transmission limits	Interdependent operation balance among control, computing, and communication functions
Contingency	Physical contingency	Cyber contingency
Types of Contingencies	Line fault, generator outage, load outage, environmental effect, etc.	Cyber-attacks, communication latency, malicious control effects, etc.
Stability & Security	Power system stability & security	Networked control system stability & cyber security
Event Synchronization	Asynchronous	Synchronous

The integration of information and communication technologies (ICTs) to perform actions such as power and information flow between cyber and physical systems has occurred over time. While the digitalized electricity grid guarantees efficient operations, it is vulnerable to cyber and other attacks due to the complex interdependence between cyber and physical systems. Stability, vulnerability, reliability, and security are its main weaknesses. Vulnerabilities, especially in cyber assets, increase the risk of external threats and attacks. Since cyber-attacks may not directly damage CPPS infrastructure, assessing cyber and physical daily actions over time is essential. Cyber system failures and attacks cause most outages in electricity grids. For example, the risk of a nuclear threat emerged in 2010 when the malicious Stuxnet worm infiltrated the SCADA system of the Bushehr Nuclear Power Plant in Iran [2]. Another example occurred in 2014 when the Dragonfly team infiltrated malicious software in US and European energy companies [3]. A cyber-attack in 2015 on the Ukrainian power system infrastructure caused widespread power outages [4]. A year later, malicious software took many computers to the Israel power grid offline [5]. According to a report by the University of Cambridge, power grid outages in the US due to cyber-attacks caused an economic loss of at least 243 billion dollars [6]. Considering the relevant issues, it is mandatory to configure and optimize the cyber side rather than assessing the impacts on the physical power system in case of cyber threats to ensure the safe operation of CPPS.

Its complexity and critical functionality make it more valuable to comprehensively examine the detection and defense mechanisms that CPPSs will use against cyber-attacks. Considering the close interdependence of information, communication, and physical layers, even minor vulnerabilities can cause irreversible infrastructure damage and economic imbalances. In this case, it is necessary to know the techniques that can detect the presence of a cyber-attack and the defense mechanisms formed accordingly. The most critical elements of cyber security analysis, cyber-attack detection methods, and defense mechanisms are the main inspirations of this study. Two main interrelated problems and their solutions, which are at the center of attention of researchers interested in cyber security, are approached from a strategic and technological perspective. The CPPS phenomenon, its evolution, and modernity are described, and signature, anomaly and behavior-based, state observer, and AI-scale detection methods are discussed in a functional cost-benefit relationship. Innovations such as secure authentication, encryption and trusted access technologies are introduced to expand cybersecurity coverage at the strategic scale. Section I discusses the development of CPPS, its functional uses, and security threats, Section II explains cyber-attack detection techniques, and Section III presents the defense mechanism from a technological perspective. Section IV outlines the conclusions of the review and future directions for cybersecurity.

II. CYBER ATTACK DETECTION IN CYBER-PHYSICAL POWER SYSTEMS

Cybersecurity attack detection requires a comprehensive effort that includes data collection and analysis, real-time monitoring and response, and intervention to ensure system security. In particular, data on network traffic, system event logs, and control commands from SCADA systems, sensors and actuators, and other control devices are collected. It is directed to the pre-processing stage to make it suitable for analysis. Data analysis is initiated after preprocessing, such as cleaning, normalization, and noise reduction. Pattern recognition techniques are used to identify normal and abnormal behavior patterns, and detection algorithms are developed to identify abnormal activities. Data deviations in the analysis results represent potential attacks and defense strategies against attacks are implemented. Detailed reports on the attack are prepared concerning the actual event. The system's vulnerabilities are identified, and necessary updates and improvements are made. Such a plan can guarantee the reliability of the CPPS.

A. Cyber Attack Detection Methods

1) Signature-based methods

Signature-based method aims to detect anomalous activity in CPPS using known attack models and signatures. Its functional processes include storing attack signatures in a database and continuously comparing event logs of the system's network traffic with the stored signatures. Intrusions in the monitored environment that match the signatures stored in the database are considered attacks. Upon detection of a known attack, an alarm is triggered, and the type of attack is detected quickly and accurately. Since not every activity and network traffic in the monitored environment is evaluated and only known signatures in the database are searched, there is very little memory overhead. Although it analyzes the known threat payload, especially in system calls, the attacker's possible signature change in known attacks can easily bypass the defense strategy. On the other hand, it does not cause unnecessary actions in the system and avoids overloads in case of low false alarms, known as false positives. Overall, Fig. 1 shows the flowchart of the signature-based cyber-attack detection method [7].

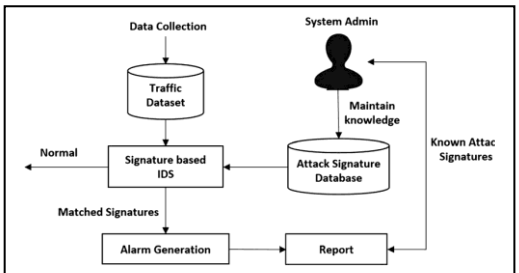


Figure 1. Flowchart of the signature-based cyber-attack detection method

Intrusion detection systems, while easier to modify and improve than distributed signatures or rules, require regular maintenance of the information they store. In addition, the method needs to constantly update itself and have an extended signature database. Data from the traffic network is sent to the signature-based detection strategy and checked for matching with the signature profile in the database. An alarm is produced if there is a match, and the generated report is sent to the system administrator as a known cyber-attack signature. The administrator retains the information and sends the cyber-attack signature to the signature-based cyber intrusion detection method.

2) Anomaly-based methods

Anomaly-based method detects cyber-attacks by learning the expected behavior of CPPS operations and monitoring abnormal deviations. The analyzer model with detection capability identifies unknown attacks or zero-day vulnerabilities without any updates to the system. It uses data collected during task-specific operations to create operational models. It is more effective than signature-based strategies in detecting new unknown cyber-attacks because it knows how the system will work periods during normal operations thanks to patterns and is not dependent on existing signatures. It obtains the learned behavior of the monitored system by comparing the activity with a baseline profile. Profiles can be fixed or have a dynamic process. Especially in dynamic profiles, extra load is added to the system as the attack detection and security profile is updated. The cyber-attack defense action shows limited performance if the attack is spread over a long period. Since the attack will be part of the profile, a defined threshold should be used, and intrusions should be detected. Fixed profiles are more effective in detecting anomalies from normal behavior. Another aspect is related to classification: techniques based on data mining, statistics, and

machine learning (ML). Statistics-based strategies are often used to detect attacks accurately. In the learning phase, statistical methods are applied to create two profiles in addition to the existing profile for intrusions whose anomaly is marked according to the base profile and the threshold settings of the monitored environment. The threshold is set based on the behavior of the monitored system. Technical anomaly monitoring in knowledge/data mining strategies is automated and increases the burden on the system [8]. It undertakes a complex duty cycle in detecting, recognizing, and classifying anomaly conditions and generates the most false positive and negative signals. However, the intensive use of memory resources should be considered. Situational or specification-based analysis to identify appropriate protocol anomalies is more aligned with ML techniques that work by analyzing system calls. On the other hand, developing a practicable and robust operational model is a comprehensive and challenging process, underscoring the complexity and importance of the task. However, the flexibility and power of artificial intelligence (AI) and ML can eliminate partial aspects of the drawback. This provides a flexible and powerful solution to ensure the system's security, and Fig. 2 illustrates the functional process of anomaly-based cyber intrusion detection [9]. A detector compares events observed in the cyber environment with the baseline profile. If the events match the baseline profile, no action is taken.

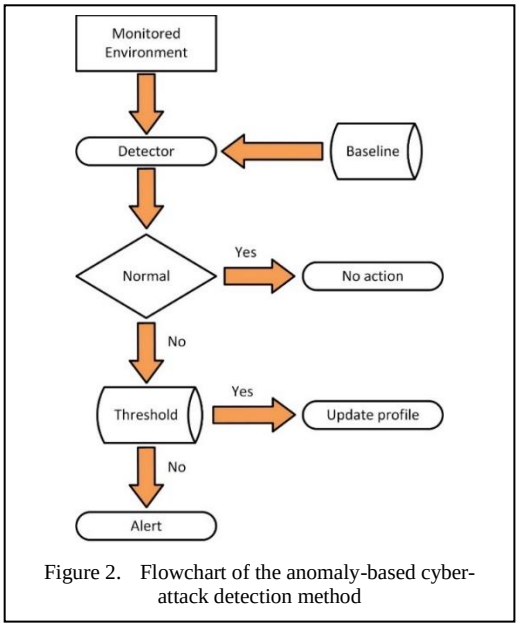


Figure 2. Flowchart of the anomaly-based cyber-attack detection method

Otherwise, the profile is updated, provided it is within acceptable threshold ranges. Understanding the difference between the two methods is crucial for network security professionals, IT professionals, and researchers. An anomaly is detected if it is outside the threshold range, triggering the alert. Activity profiles are created based on network traffic, anomalies are detected, and a report is produced. On the contrary, the signature-based method compares the signature stored in the database with the network traffic status, applies the security rule based on the threshold, and provides a report for the threat. The difference in their procedures is explained in Fig. 3 via the comparative process of signature-based and anomaly-based methods [10].

3) Behavior-based method

Behavior-based method monitors the expected behavior of CPPS components, detecting cyber-attacks from deviating behavior in normal operations. It generates behavioral profiles of system components using data from real-time monitoring. Because it dynamically considers the relationships and interactions between system components, detecting new cyberattacks in complex and challenging system operations is more effortless. However, it must accurately identify and update behavioral profiles, as potential errors can lead to high false positive rates. With continuous monitoring and real-time analysis, CPPS provides a flexible and dynamic solution for security.

Fig. 4 shows a block diagram of behavior-based cyber-attack detection [11]. The following techniques are mostly used in behavior-based detection: automated analysis using sandboxes, monitoring system calls, process monitoring, and file changes [12], and comparing registry snapshots [13]. In this way, a dataset is created by detecting behaviors and extracting features from data mining, and specific features are selected. The selected features are classified to create training and test data, and the decision-making mechanism is trained and then tested for prediction performance.

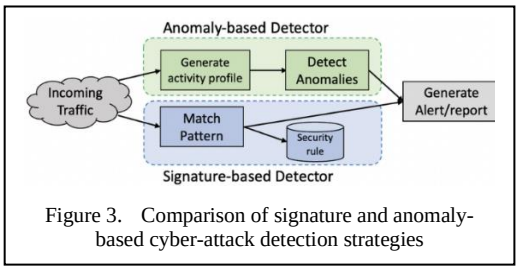


Figure 3. Comparison of signature and anomaly-based cyber-attack detection strategies

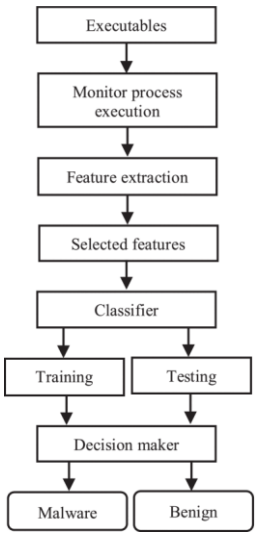


Figure 5. Flowchart of the behavior-based cyber-attack detection method

Finally, it is determined whether the behavior in cyberspace is benign or malignant.

4) Hybrid methods

Hybrid attacks reinforce the cybersecurity infrastructure and overcome the shortcomings of individual solutions by combining the advantages of two or more defense strategies to detect known and unknown intrusions. It integrates the benefits of signature and anomaly-based detection methods while detecting a more comprehensive range of attacks. It facilitates the detection of unknown attacks by learning the system's normal behavior while using updated signature models created primarily via modules to detect known attack patterns quickly and accurately. Especially for normal behavior, anomaly-based detection modules create a bidirectional approach in the known and unknown attack pool. Since signature and anomaly-based detection methods must be managed, integration and coordination issues may be encountered. However, it guarantees lower false positives and higher accuracy rates, providing a flexible, dynamic, and extended cybersecurity service for CPPSs. Responds quickly to existing threats and proactively detects new threats via real-time analysis and continuous monitoring. Fig. 5 summarizes the hybrid cyber-attack detection process [7]. The data collected from the traffic network is first directed to the signature-based cyber defense strategy. The intrusion is detected if the signature profiles in the database match the relevant situation.

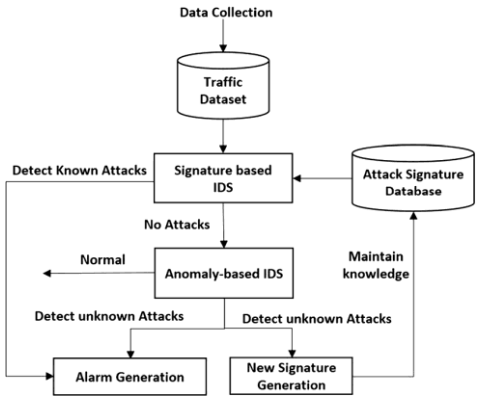


Figure 4. The procedure of the hybrid cyber-attack detection method

An anomaly-based defense strategy is activated if a signature-based method cannot detect a cyber threat. If a known attack is detected, an alert report is produced, while for unknown attacks, a new signature is created, and the attack signature database is updated.

5) AI-based methods

AI-based method is an innovative and state-of-the-art cyber-attack detection method. It detects cyberattacks by learning from large data sets and identifying complex patterns. ML methods learn the normal operational behavior of CPPS and monitor deviation in behavior. While many techniques, such as supervised, unsupervised, and deep learning, can be applied, supervised learning distinguishes between normal and abnormal situations using pre-labeled data. In contrast, unsupervised learning generates anomaly and attack detection patterns from unlabeled data. Deep learning can perform complex and detailed analyses thanks to its multi-layered structure. Finally, it has provided accurate and precise detection with its ability to continuously monitor and analyze system data and learn new types of attacks and their development over time. Due to the need for extensive and various data sets, data processing processes can take time and effort. Training and data updating for learning requires high computational power, and regular review and optimization of the model are necessary to obtain accurate results and reduce false positive rates in case of possible errors. Related techniques passively ensure cybersecurity, supporting CPPS reliability and promising future approaches [14]. Fig. 6 shows the ML-based cyber-attack detection flowchart [15].

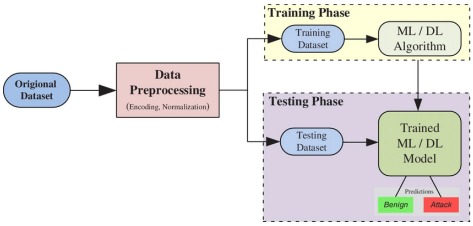


Figure 6. Flowchart of the ML-based cyber-attack detection method

There are three phases: data preprocessing, training, and testing. Data preprocessing is performed to ensure the applicability of the dataset to the algorithm and serves the purpose of coding, cleaning and normalization. The prepared data is randomly distributed into two separate classes: training and test datasets. The training data, representing 70% to 80% of the total dataset, is evaluated in the learning phase [16]. The learning times vary depending on the size of the dataset and the complexity of the proposed AI strategic model. The predictions made on the test dataset after model training according to various metrics (precision, recall, false alarm rate, true negative rate, accuracy, root mean squared error, mean absolute error, mean absolute percentage error, r^2 score, f^1 score, etc.) are briefly explained as ML techniques are discussed extensively in [15].

6) State observers

System dynamics and behavior are modeled via observers and continuously compared with real-time data. Sophisticated techniques such as Luenberger or Kalman filters are preferred as state observers to determine the current operational state and detect potential infractions.

a) Luenberger observers

It is designed to correctly estimate the actual state of CPPS in the case of linear systems. It uses designs based on modern control theory since the controlled system states can be measured. In many practical applications, measuring only a few state signals is sufficient. Theoretical applications where state vectors are known are limited, and measuring system states is costly. On the other hand, observers are used to determine state vectors. Luenberger, introduced observers and physical systems can have several delays. Especially for time-independent linear systems, one focuses on a similar point of view if the system changes without delay. Instead, in practical applications, delays occur in system states, while in fast-running systems, the time delay can be negligible. Delays are a parameter that determines the behavior of CPPS and cannot be used in delay-less system models. In single-input, single-output delayed states (SISO), and time-independent (LTI) systems, all system states can be studied using the delayed observer model, provided the system is observable. Instead of observers, sensors can perform a similar task. However, the number of sensors to be used may increase depending on the number of states, or sensors may not be utilized for every state signal since some states cannot be measured and observers are needed. Various methods are prominent in delayed-time systems. System estimation using a state vector observer is discussed in [17]. In particular, the state space for a linear and time-independent system with a single input and additional output is given by (1).

$$\begin{cases} \dot{x}(t) = A.x(t) + B.u(t) \\ y(t) = C.x(t) \end{cases} \quad (1)$$

Here $\dot{x}(t) \in \mathbb{R}^n$ is the state vector. $u(t)$ represents the input signal, and $y(t)$ represents the output signal. Equation (2) gives the state space model for time-delayed systems.

$$\begin{cases} \dot{x}(t) = A.x(t) + A_d(t-\tau) + B.u(t) \\ y(t) = C.x(t) \end{cases} \quad (2)$$

Here, A_d is the delayed state system matrix, and the objective is to estimate the system states with unknown states and delay with the help of an observer. The Luenberger observer model is defined by (3) [18].

$$\dot{\hat{x}}(t) = A.\hat{x}(t) + A_d\hat{x}(t-\tau) + L(y-\hat{y}) \quad (3)$$

Here, $\hat{x} \in \mathbb{R}^n$ is the state vector of the observer, and $\hat{y}$ is the output of the observer. $L \in \mathbb{R}^n$ is the Luenberger coefficient vector. Similarly, the Luenberger observer for delayed-time systems can be extended to the state space expression in (4). Defining the error dynamics as in (5) is necessary to stabilize the observer and system error dynamics. Moreover, the derivative of the error dynamics for use in calculations is determined as in (6). Rearranging (2) and (4), (7) is obtained.

$$\dot{\hat{x}}(t) = A.\hat{x}(t) + A_d\hat{x}(t-\tau) + L(y-\hat{y}) + B.u(t) \quad (4)$$

$$e(t) = x(t) - \hat{x}(t) \quad (5)$$

$$\dot{e}(t) = \dot{x}(t) - \dot{\hat{x}}(t) \quad (6)$$

$$\dot{e}(t) = A.x(t) + A_d x(t-\tau) - A.\hat{x}(t) - A_d \hat{x}(t-\tau) - LC(x-\hat{x}) \quad (7)$$

Due to the delay, the $e^{-\tau s}$ expression in the Laplace transform in (7) is expanded according to the Taylor series. The Laplace transform of the error dynamics is obtained as in (8) using the first two terms. The characteristic polynomial of the error dynamics is represented in its most general form by (10) using (9). Finally, cyber security operations can be performed by monitoring the observer and system state change using the computed Luenberger vector.

$$E(s) = [sI + A_d \tau s + LC - (A + A_d)]^{-1} e(0) \quad (8)$$

$$\det([sI + A_d \tau s + LC - (A + A_d)]^{-1}) = 0 \quad (9)$$

$$p(s) = s^n + a_n s^{n-1} + \ldots + a_0 \quad (10)$$

b) Kalman filter

It is a filter that can predict cyber-attack cases in systems modeled as a state space, using prior knowledge of the model, mainly input and output information. It is an idea proposed by Rudolf, a Hungarian-American mathematician and scientist working on systems theory. It is based on observation theory around a decided point of view. Minimum variance estimation or Kalman filter is the best applicable method if stochastic or random noise is available and accounted for in the system. Like traditional estimators, the Kalman filter has a filtering property that makes it a powerful and capable tool for estimating unmeasurable system states. Comparing the model prediction to the observation and scaling the difference by a multiplier known as the Kalman gain is fed back to the model as input for subsequent predictions, and its performance is determined by adjusting the gain. Especially in a low-gain state space, the filter follows the model predictions more closely and relies only on the model predictions or a single measurement. At each time step, it estimates the unknown value with its uncertainties. When the result of the subsequent measurement is observed, these estimates are updated with a weighted average, giving more weight to estimates with lower uncertainty. The Kalman filter conditions can be fitted to the problem as in (11), (12), and (13).

$$\begin{cases} x_k = A.x_{k-1} + B.u_k + w_{k-1} \\ z_k = H.x_k + \nu_k \end{cases} \quad (11)$$

$$\overbrace{\begin{aligned} \hat{x}_k^- &= A.\hat{x}_{k-1}^- + B.u_k \\ p_k^- &= A.p_{k-1}A^T + \mathbb{Q} \end{aligned}}^{\text{Prediction / Time Update}} \quad (12)$$

$$\overbrace{\begin{aligned} K_k &= p_k^-.H^T(H.p_k^-.H^T + R)^{-1} \\ \hat{x}_k &= \hat{x}_k^- + K_k(z_k - H.\hat{x}_k^-) \\ p_k &= (1 - K_k.H).p_k^- \end{aligned}}^{\text{Correction / Measurement Update}} \quad (13)$$

Analyzing these equations, the estimated value $\hat{x}_k$ of the signal x is calculated for each k using the measured value z_k. It is suitable for situations where the accuracy of the estimated value is not sure. Here again, K_k is the Kalman gain, and $\hat{x}_{k-1}^-$ is the previous state estimate of the signal. Each x_k value of the signal is calculated using (11) with a linear combination of its previous value x_{k-1} with the control signal (u_k, usually not used) and the preprocessing noise w_{k-1}. Any measurement value z_k is determined from the expression of the signal value and the measurement noise, while the parameters are considered Gaussian. A, B, and H represent the general notation of the matrices and take numerical values for most signals. Fixed assumptions can be made so the matrix operation is not performed based on changing values at each stage. When the system reliability increases, the arithmetic mean and standard deviation of the noise functions (ν_k, w_{k-1}) are estimated. While the true values are calculated with Gaussian, the Kalman filter obtains accurate estimates with suitable convergence. After the model fits the Kalman filter, the time and estimation update and the measurement adaptation and correction phases are initiated. Before the correction update, the initial raw estimation and error covariance are used. The previous state and the corresponding error covariance are estimated and used to calculate the Kalman gain in the correction phase. z_k is updated instead of the measurement; the error covariance is corrected and reassigned as input to the prediction phase.

III. Cyber Defense in Cyber-Physical Power Systems

Increasing cyber-attacks on CPPS, dominated by multidimensional and hidden features, have drawn global attention to the cyber and physical field [19]. In addition to the time and space dimension [20], data-centric defense strategies based on data availability, integrity, and confidentiality are gaining attention [21]. Due to the increased coordinated attack types, it is mandatory to study CPPS security detection and defense methods based on the periodic evolution process of the attack event: before, during, and after.

A. Pre-Cyber Attack Security Analysis and Determination of Defense Strategy

Preventing potential attacks via authentication and security encryption requires maintaining system integrity and prohibiting unauthorized access. Authenticating users or devices before they access the system will make it difficult for unauthorized persons to gain resources. Security encryption prevents unauthorized use of data and ensures the confidentiality and integrity of transmitted information.

1) Secure authentication and reliable access technologies

As each IED deals with different metering aspects and data tracking and requires "plug-and-play" access, using authentication and trusted access technologies is inevitable. Encryption is critical to ensure that any data transmitted in the system is not captured, monitored, or altered. Authentication technologies legally verify the identity of the access object, which can represent a smart device or any other equipment in the CPPS. A lightweight authentication using AI-based Markov model prediction as the first line of defense of the security mechanism is discussed in [22]. A low entropy shared password scheme is used in [23] to authorize communication devices. A blockchain-based trust reconciliation strategy for cyber terminals where there is no trust environment is discussed in [24]. Here, a multi-trust analysis mechanism is built with consortium blockchain and beta allocation, and its performance against multiple malicious attacks is verified. Data encryption encrypts plaintext data and repeats in retransmission to prevent an attacker or eavesdropper from obtaining private data. There are symmetric and asymmetric key encryption implementations, and both are widely used based on different needs, such as data criticality and computational complexity.

2) Defense strategy and resource allocation

The development of defensive strategies, in addition to technology-based security precautions, is valuable for the early prevention of potential attacks and the optimization of defense resources. Vulnerabilities of CPPS can be detected from the attacker's point of view by evaluating the performance of defense strategies via attack analysis and simulation. The possible attack potential can be extracted, and resource allocation for subsequent security defense can be made using modeling and system extrapolation. Recently, several proposals have been made to simulate different types of attacks in the presence of noise [25]. Especially noteworthy are parameter-weighted temporal automata based on the attack tree model [26], attack graph models for quantitative analysis of network attack and inter-domain chain failures [27], and synchronous or not attack models for phasor measurement unit (PMU) measurement data [28].

After the attack analysis and the performance evaluation of the system, the allocation of defense resources and the improvement of the defense capacity are necessary based on the potential risks detected. There are also examples that do not meet this condition. For instance, a game theory-based defense resource allocation strategy based on changes in the main operating parameters in the power system is developed in [29] for false data injection attacks (FDIA), which is one of the expected attack types. However, defense resources need to be allocated appropriately in constrained resource allocation. After risk analysis based on Bayesian adaptive networks, a suitable strategy for resource allocation is proposed in [30]. If the attack scope is extended to dynamic and large-scale networks, the optimal action set should be obtained by the coevolutionary algorithm to achieve operational balance [31]. Moreover, separating attack and defense behaviors into three parts, namely, power plant, transmission, and distribution system, facilitates the development of optimal defense strategies [32]. The defense strategies and resource allocation should be distributed via the firewall and forward and backward isolation devices of the CPPS.

B. Cyber Attack Detection and Defense Technology & Strategy

1) Multi-level security line of defense approach for conventional power system and CPPS

Traditional power systems usually have three lines of defense to ensure safety against faults. The first includes fast relay protection and control strategies to guarantee stable grid operation under single-phase fault conditions. In contrast, the second line of defense provides emergency control actions such as generator and load shedding against low probability but more severe faults. The last line of defense uses frequency and voltage emergency control devices, and out-of-system-step deregulation. The relevant devices for emergency control are quickly activated in the event of multiple inevitable severe faults to prevent large-scale outages. CPPS similarly has three lines of defense. However, the first line of defense aims to strengthen communication network planning and provide efficient service routing to enhance defense resilience against expected power system construction and operation failures. The second line of defense includes network and service self-healing functions and aims to address failures quickly. The third line of defense conducts system-level improvement and repair by blocking existing terminals/channels and centralizing the management of limited communication resources. The last line of defense is activated immediately in case a severe cyber threat rapidly spreads, and grid outages are mitigated by shedding low-frequency and low-voltage loads or split of the power system. However, it is necessary to plan main and backup routing paths in the power systems communication network in case of a possible communication link failure after a cyber-attack [33]. The first line of defense is functionally realized by automatically jumping to the backup path in case of a failure in the communication network. Moreover, the synchronous digital hierarchy (SDH) ring structure, which can perform automatic rotation within 50 ms, reinforces the security procedure by providing the second line of cyber defense. The first two lines of defense may not be sufficient, as the power system sectionalization only requires calculating the power flow given the complexity of the connection between cyber and physical systems. The failure evolution and, if necessary, the interruption of one of the communication links will hinder the sustainability of many power services. In addition, if the cyber and physical interrupting surfaces are not combined, the failure scope will expand. To address this increasing threat problem, an innovative CPPS saturation defense mechanism based on combined cyber-physical active interruptions is proposed in [34]. This way, safe and stable operations can be supported by minimizing the attack scope.

2) Cyber-attack detection and defense technology

The most valuable time for defense is gained, and the consequences of the attack are minimized if it can be accurately detected within a short period of the CPPS being attacked. CPPS can be structurally divided into power physical and information areas and is an ideal approach. Detection methods in the power physical area mainly evaluate whether electrical measurements, decision-making instructions, and sudden changes in the system's operating state obey physical laws [19]. In particular, the malicious data detection method developed in [35] considering spatial and temporal correlation in residual detection or condition constraints is an example of the relevant case. Another example is the double feed deep learning detection method, where the data obtained by the PMU is fed [36]. In addition, SCADA-based multi-step malicious data detection algorithm is another approach because of the FDIA threat [37], [38]. On the other hand, on the cyberspace side, cyber-attack attempts in information technologies are usually monitored with the help of an intrusion detection system (IDS) or a security information event management system (SIEM). The addresses and network logs of cyber devices are considered by attackers and used to detect transmission traffic or communication models. Consistency detection or prior knowledge-based identification strategies may be preferred in cyber defense. For instance, researchers in [39] detected anomalous transmission events in the communication network by comparing data sent and received from sensors and actuators. Besides the proposed whale optimization algorithm and neural network-based model for intrusion detection, a method for classifying attack attempts is proposed in [40]. A novel support vector machine (SVM) based attack detection model combining smart meters and power devices is developed in [41]. The performance of an anomaly-based cyber-attack detection method based on the Gaussian mixture model and

Kalman filtering is evaluated for SCADA in [42]. A second frequency control method is proposed in [43] by realizing an intrusion detector-based design for possible denial of service (DoS) attacks on the power system frequency controller instead of SCADA. On the other hand, a distributed data-based cyber-attack detection against the FDIA threat in multi-area interconnected power systems is emphasized in [44]. Considering the large-scale electric vehicles that can be connected to such systems, a more sophisticated method is needed as the attack scope of FDIA will expand [45]. Moreover, unlike decomposing every available message, CPPS information flows must be evaluated in the mixed time-frequency domain [46]. The researchers in [46] addressed the issue via an anomaly-principled traffic spectrum clustering detection method that integrates artificial swarm optimization and SVM. It is a promising method to increase the detection speed, but only the transmission behavior characteristics of the power and communication flow are needed. Therefore, attacks and infiltrations can be accurately detected without analyzing every data packet. However, AI and ML methods for fast and accurate cyber-attack detection have recently attracted attention. Recursive neural networks and blockchain technology are integrated in [47] to defend against energy internetwork attacks and illegal operations. Another method for addressing cyber infiltration attempts is to use feature volume extraction, data preprocessing, and ML classifiers. These techniques can recognize and respond faster to complex and ever-changing cyber threats.

The main objective of CPPS defense is to ensure voltage and frequency stability and power angle balance. Cyber-attack prevention and system stability control can be integrated for operational sustainability. Especially the design of control devices is a practical approach to maintain system stability. Nowadays, two security methods in attacks against CPPS are categorized: flexible control and active defense control methods. Flexible control methods analyze the system performance and attack parameters based on a specific intrusion model. At the same time, sub-functional processes such as the Lyapunov function can be used to evaluate the resilience constraints in the attack. After the analysis, a resilience control triggering mechanism is designed to ensure the stability of the input state [48], but the relevant cyber defense method follows a more conservative behavior. On the contrary, active defense control methods are based on the ideology of active compensation to prevent cyber-attacks and maintain the control system's performance. These defense mechanisms mainly adopt predictive control [49] and multi-channel networked strategies [50]. This way, the control system performance is guaranteed by responding to attacks quickly and efficiently. Apart from the predictive and multichannel strategy, Honeypot technology is an exciting defense technique that works on a trap set in the network defense to fool the attacker [51]. The attacker is baited via network service providers, hosts, or messages, and the attack behavior is detected to determine the attacker's means and attack strategy. This method can infer the attack intent and motivation and weaken the attack by consuming resources. Honeypot technology protects system resources and critical information by allowing attackers to focus on the traps instead of the system components.

IV. CONCLUSIONS

The scope of possible cyber threats has expanded by integrating cyberinfrastructure into smart power systems. This study highlights the development of modern CPPS infrastructure. It addresses the detection of cyber violations and defense mechanisms from a technological and strategic point of view within a systematic plan. The functional processes of innovative cyber-attack detection techniques based on signatures, anomalies, and behaviors, including state observers, are evaluated in a cost-benefit relationship. At the same time, a similar approach is maintained for modern AI-scale reliability schemes. Moreover, hybrid methods that overcome the vulnerabilities of individual techniques are discussed, and defense mechanisms on secure authentication, encryption, and access technologies are evaluated.

Future investigations of attack violations in CPPS communication networks and security protection modes are needed. Quantitative security procedures should be performed for fusion attack modeling and defense detection, especially by analyzing the probabilities of sequential failures caused by cyber-attacks. Qualitative differences between ordinary failures and intense attacks, real-time sustainable security analysis, and online auxiliary decision-making in cyber-attack defense should be emphasized. The

information and physically integrated layer of cyber defense and the prevention, emergency, and recovery aspects must be addressed at multiple spatial and temporal scales. Focus on technological advances such as blockchain and quantum computing to reinforce cybersecurity performance by considering the cyber characteristics of wireless measurement and monitoring networks and with the help of big data analytics. Blockchain and quantum computing, when integrated into CPPS cybersecurity frameworks, can offer security and performance advances beyond traditional methods. While blockchain is an immediately practical technology for data integrity and distributed security solutions, quantum computing can deliver more innovative solutions in the long term. Blockchain technology can be used to track and store data in the short term securely. Quantum computing can be used in the long term to achieve higher security standards and adopt quantum-based solutions to solve big data problems. However, a cyber security strategy that is both effective and cost-sustainable should be developed before investing in these two technologies, considering the suitability of the CPPS' current infrastructure and sectoral requirements. In conclusion, a functional analysis of cyber-attack methods and a good knowledge of applicable and up-to-date possible defense mechanisms are the most effective ways to deal with new cyber intrusions.

A different perspective is to carefully select both technical and operational metrics to assess the success of cybersecurity advances in CPPSs. To prioritize these advances in the short term, the industry should focus on critical infrastructure security, cost-effective solutions, human factors, threat intelligence, and standards compliance. These approaches can provide a practical roadmap to make CPPS systems more secure and sustainable. The industry can prioritize cybersecurity investments and improvements in the short term by optimizing the processes of Focusing on Securing Critical Infrastructure, Fast and Cost-Effective Solutions, Investing in Human Factors, Threat Intelligence-Based Strategies, and Facilitating Adaptation and Certification Processes.

Eventually, the scope of the study will be extended to analyze the cost-benefit relationships of different detection techniques and defense mechanisms in more detail. The practicability of the proposed methods will be evaluated considering not only the technical conditions but also the economic cost-benefit relationship. Thus, the realistic applicability of the proposed methods in practical and financial aspects will be revealed.

REFERENCES

[1] Adepu, S., & Mathur, A. (2021). Distributed Attack Detection in a Water Treatment Plant: Method and Case Study. IEEE Transactions on Dependable and Secure Computing, 18(1), 86–99. https://doi.org/10.1109/TDSC.2018.2875008

[2] Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies, 32(1). https://doi.org/10.1002/ett.4150

[3] Alsughayyir, B., Qamar, A. M., & Khan, R. (2019). Developing a Network Attack Detection System Using Deep Learning. 2019 International Conference on Computer and Information Sciences (ICCIS), 1–5. https://doi.org/10.1109/ICCISci.2019.8716389

[4] André, É., Lime, D., Ramparison, M., & Stoelinga, M. (2021). Parametric Analyses of Attack-fault Trees. Fundamenta Informaticae, 182, 69–94. https://doi.org/10.3233/FI-2021-2066

[5] Aslan, O., & Samet, R. (2017). Investigation of Possibilities to Detect Malware Using Existing Tools. 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA), 1277–1284. https://doi.org/10.1109/AICCSA.2017.24

[6] Aslan, O., & Samet, R. (2020). A Comprehensive Review on Malware Detection Approaches. IEEE Access, 8, 6249–6271. https://doi.org/10.1109/ACCESS.2019.2963724

[7] Assante, M. (2016). Confirmation of a Coordinated Attack on the Ukrainian Power Grid. 23, 1–5. ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid

[8] Ayiad, M. M., Leite, H., & Martins, H. (2021). State Estimation for Hybrid VSC Based HVDC/AC: Unified Bad Data Detection Integrated With Gaussian Mixture Model. IEEE Access, 9, 91730–91740. https://doi.org/10.1109/ACCESS.2021.3092308

[9] Azad, M. A., Bag, S., Perera, C., Barhamgi, M., & Hao, F. (2020). Authentic Caller: Self-Enforcing Authentication in a Next-Generation Network. IEEE Transactions on Industrial Informatics, 16(5), 3606–3615. https://doi.org/10.1109/TII.2019.2941724

[10] Bangui, H., Ge, M., & Buhnova, B. (2022). A hybrid machine learning model for intrusion detection in VANET. Computing, 104(3), 503–531. https://doi.org/10.1007/s00607-021-01001-0

[11] Ferrag, M. A., & Maglaras, L. (2020). DeepCoin: A Novel Deep Learning and Blockchain-Based Energy Exchange Framework for Smart Grids. IEEE Transactions on Engineering Management, 67(4), 1285–1297. https://doi.org/10.1109/TEM.2019.2922936

[12] Gu, Y., Yu, Z., Diao, R., & Shi, D. (2020). Doubly-fed Deep Learning Method for Bad Data Identification in Linear State Estimation. Journal of Modern Power

Systems and Clean Energy, 8(6), 1140–1150. https://doi.org/10.35833/MPCE.2020.000533

[13] Guan, S., Wang, J., Yao, H., Jiang, C., Han, Z., & Ren, Y. (2020). Colonel Blotto Games in Network Systems: Models, Strategies, and Applications. IEEE Transactions on Network Science and Engineering, 7(2), 637–649. https://doi.org/10.1109/TNSE.2019.2904530

[14] Haghnegahdar, L., & Wang, Y. (2020). A whale optimization algorithm-trained artificial neural network for smart grid cyber intrusion detection. Neural Computing and Applications, 32(13), 9427–9441. https://doi.org/10.1007/s00521-019-04453-w

[15] Head, T. M. (2015). Business Blackout The insurance implications of a cyber attack on the US power grid Emerging Risk Report-2015 Innovation Series SOCIETY & SECURITY Lloyd's Emerging Risk Report-2015. University of Cambridge Centre for Risk Studies. www.lloyds.com/ScenarioDesign

[16] Hu, Z., Liu, S., Luo, W., & Wu, L. (2021). Intrusion-Detector-Dependent Distributed Economic Model Predictive Control for Load Frequency Regulation With PEVs Under Cyber Attacks. IEEE Transactions on Circuits and Systems I: Regular Papers, 68(9), 3857–3868. https://doi.org/10.1109/TCSI.2021.3089770

[17] Independent Electricity System Operator. (2011). Modernizing Ontario's Electricity System : Next Steps (2nd ed., Issue May). The Ontario Smart Grid Forum. https://www.ieso.ca/

[18] Jan, M. A., Khan, F., Khan, R., Mastorakis, S., Menon, V. G., Alazab, M., & Watters, P. (2021). Lightweight Mutual Authentication and Privacy-Preservation Scheme for Intelligent Wearable Devices in Industrial-CPS. IEEE Transactions on Industrial Informatics, 17(8), 5829–5839. https://doi.org/10.1109/TII.2020.3043802

[19] Jolfaei, A., & Kant, K. (2020). On the Silent Perturbation of State Estimation in Smart Grid. IEEE Transactions on Industry Applications, 1–1. https://doi.org/10.1109/TIA.2020.2969117

[20] Kamal, M., Farajollahi, M., Nazaripouya, H., & Mohsenian-Rad, H. (2021). Cyberattacks Against Event-Based Analysis in Micro-PMUs: Attack Models and Counter Measures. IEEE Transactions on Smart Grid, 12(2), 1577–1588. https://doi.org/10.1109/TSG.2020.3029937

[21] Keshk, M., Sitnikova, E., Moustafa, N., Hu, J., & Khalil, I. (2021). An Integrated Framework for Privacy-Preserving Based Anomaly Detection for Cyber-Physical Systems. IEEE Transactions on Sustainable Computing, 6(1), 66–79. https://doi.org/10.1109/TSUSC.2019.2906657

[22] Kushner, D. (2013). The real story of stuxnet. Ieee Spectrum, 50(3), 48–53.

[23] Liu, S., Siano, P., & Wang, X. (2020). Intrusion-Detector-Dependent Frequency Regulation for Microgrids Under Denial-of-Service Attacks. IEEE Systems Journal, 14(2), 2593–2596. https://doi.org/10.1109/JSYST.2019.2935352

[24] Liu, Y., Chen, Y., & Li, M. (2021). Dynamic Event-Based Model Predictive Load Frequency Control for Power Systems Under Cyber Attacks. IEEE Transactions on Smart Grid, 12(1), 715–725. https://doi.org/10.1109/TSG.2020.3022094

[25] Mudzingwa, D., & Agrawal, R. (2012). A study of methodologies used in intrusion detection and prevention systems (IDPS). 2012 Proceedings of IEEE Southeastcon, 1–6. https://doi.org/10.1109/SECon.2012.6197080

[26] Nejabatkhah, F., Li, Y. W., Liang, H., & Reza Ahrabi, R. (2020). Cyber-Security of Smart Microgrids: A Survey. Energies, 14(1), 27. https://doi.org/10.3390/en14010027

[27] Niknami, N., Inkrott, E., & Wu, J. (2022). Towards Analysis of the Performance of IDSs in Software-Defined Networks. 2022 IEEE 19th International Conference on Mobile Ad Hoc and Smart Systems (MASS), 787–793. https://doi.org/10.1109/MASS56207.2022.00124

[28] Patel, A., Roy, S., & Baldi, S. (2021). Wide-Area Damping Control Resilience Towards Cyber-Attacks: A Dynamic Loop Approach. IEEE Transactions on Smart Grid, 12(4), 3438–3447. https://doi.org/10.1109/TSG.2021.3055222

[29] Pilz, M., Naeini, F. B., Grammont, K., Smagghe, C., Davis, M., Nebel, J.-C., Al-Fagih, L., & Pfluegel, E. (2020). Security attacks on smart grid scheduling and their defences: a game-theoretic approach. International Journal of Information Security, 19(4), 427–443. https://doi.org/10.1007/s10207-019-00460-z

[30] Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. Journal of Big Data, 7(1), 41. https://doi.org/10.1186/s40537-020-00318-5

[31] Shan, X. G., & Zhuang, J. (2020). A game-theoretic approach to modeling attacks and defenses of smart grids at three levels. Reliability Engineering & System Safety, 195, 106683. https://doi.org/10.1016/j.ress.2019.106683

[32] Shi, J., Liu, S., Chen, B., & Yu, L. (2021). Distributed Data-Driven Intrusion Detection for Sparse Stealthy FDI Attacks in Smart Grids. IEEE Transactions on Circuits and Systems II: Express Briefs, 68(3), 993–997. https://doi.org/10.1109/TCSII.2020.3020139

[33] Shi, L., Li, Y., & Ma, M. (2019). Latest research progress of honeypot technology. Journal of Electronics & Information Technology, 41(2), 498–508.

[34] Sikorski, M., & Honig, A. (2012). Practical malware analysis: the hands-on guide to dissecting malicious software. no starch press.

[35] Smith, M. D., & Pate-Cornell, M. E. (2018). Cyber Risk Analysis for a Smart Grid: How Smart is Smart Enough? A Multiarmed Bandit Approach to Cyber Security Investment. IEEE Transactions on Engineering Management, 65(3), 434–447. https://doi.org/10.1109/TEM.2018.2798408

[36] Staff, T. (2016). Steinitz: Israel's Electric Authority Hit by 'Severe'Cyber-Attack. The Times of Israel.

[37] Sun, C.-C., Sebastian Cardenas, D. J., Hahn, A., & Liu, C.-C. (2021). Intrusion Detection for Cybersecurity of Smart Meters. IEEE Transactions on Smart Grid, 12(1), 612–622. https://doi.org/10.1109/TSG.2020.3010230

[38] Symantec. (2014). Dragonfly : Cyberespionage Attacks Against Energy Suppliers - Symantec Security Response.

[39] Tang, Y., Li, M., Wang, Q., & Ni, M. (2019). A review on research of cyber-attacks and defense in cyber physical power systems part two detection and protection. Automation of Electric Power Systems, 43(10), 1–9.

[40] Trinh, H., & Aldeen, M. (1999). Estimation of linear functional states for time delay systems. 1999 European Control Conference (ECC), 3697–3702. https://doi.org/10.23919/ECC.1999.7099905

[41] Tsai, C.-F., Hsu, Y.-F., Lin, C.-Y., & Lin, W.-Y. (2009). Intrusion detection by machine learning: A review. Expert Systems with Applications, 36(10), 11994–12000. https://doi.org/10.1016/j.eswa.2009.05.029

[42] Wang, C., Mu, G., & Cao, Y. (2020). A Method for Cleaning Power Grid Operation Data Based on Spatiotemporal Correlation Constraints. IEEE Access, 8, 224741–224749. https://doi.org/10.1109/ACCESS.2020.3044051

[43] Wang, Y., Gao, K., Zhao, T., & Qiu, J. (2016). Assessing the harmfulness of cascading failures across space in electric cyber-physical system based on improved attack graph. Proceedings of the CSEE, 36(6), 1490–1499.

[44] WPD-ResNeSt: Substation station level network anomaly traffic detection based on deep transfer learning. (2021). CSEE Journal of Power and Energy Systems. https://doi.org/10.17775/CSEEJPES.2020.02850

[45] Yang, T., Yan, P., & others. (2022). Research on Saturation Defense Method of Power Cyber-physical System Based on Active Cut Set. Proceedings of the CSEE, 42(2), 12.

[46] Yohanandhan, R. V., Elavarasan, R. M., Manoharan, P., & Mihet-Popa, L. (2020). Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications. IEEE Access, 8, 151019–151064. https://doi.org/10.1109/ACCESS.2020.3016826

[47] Yu, J., Yu, L., & Yang, T. (2021). Blockchain-based trust consensus method for power internet of Things terminal. Automation of Electric Power Systems, 45(17), 1–10.

[48] Yuan, H., & Xia, Y. (2018). Resilient strategy design for cyber-physical system under DoS attack over a multi-channel framework. Information Sciences, 454–455, 312–327. https://doi.org/10.1016/j.ins.2018.04.082

[49] Zhang, H., Liu, B., & Wu, H. (2021). Smart Grid Cyber-Physical Attack and Defense: A Review. IEEE Access, 9, 29641–29659. https://doi.org/10.1109/ACCESS.2021.3058628

[50] Zhang, T., Ji, X., & Xu, W. (2022). Jamming-Resilient Backup Nodes Selection for RPL-based Routing in Smart Grid AMI Networks. Mobile Networks and Applications, 27(1), 329–342. https://doi.org/10.1007/s11036-020-01634-z

[51] Zheng, Y., Yan, Z., Chen, K., Sun, J., Xu, Y., & Liu, Y. (2021). Vulnerability Assessment of Deep Reinforcement Learning Models for Power System Topology Optimization. IEEE Transactions on Smart Grid, 12(4), 3613–3623. https://doi.org/10.1109/TSG.2021.3062700