Received: 22 January 2022 | Revised: 18 March 2022 | Accepted: 23 March 2022

IET Energy Systems Integration

DOI: 10.1049/esi2.12068

REVIEW

Attack and defence methods in cyber-physical power system

Ting Yang[1,2] | Yuzhe Liu[2] | Wei Li[3]

[1]Key Laboratory of Smart Grid of Ministry of Education, Tianjin University, Tianjin, China

[2]School of Electrical Engineering and Automation, Tianjin University, Tianjin, China

[3]School of Computer Science, The University of Sydney, Sydney, New South Wales, Australia

Correspondence

Ting Yang, Key Laboratory of Smart Grid of Ministry of Education, Tianjin University, Tianjin 30072, China.
Email: yangting@tju.edu.cn

Funding information

National Natural Science Foundation of China, Grant/Award Number: 61971305; National Key Research and Development Program of China, Grant/Award Number: 2017YFE0132100; Natural Science Foundation of Tianjin, Grant/Award Number: 21JCZDJC00640

Abstract

With the development of digitalisation and intelligence, the power system has been upgraded from the traditional single energy transmission and conversion system to a complex cyber-physical power system (CPPS) with tightly coupled energy and information flows. The cyber-physical power system achieves the controllability and observability of the power system through ubiquitous sensing technology, advanced measurement technology, and powerful information processing technology. However, the large number of intelligent electronic device accesses and frequent information interactions in CPPS make it more vulnerable and susceptible to be attacked than any previous single structured system. Viruses and intrusions can attack the CPPS through the cyber subsystem, which in turn can deal a fatal blow to the energy supply physical system. Because of the above problems, malicious attacks against CPPS have been occurring in recent years and have generated a great deal of scholarly attention. This paper precisely focusses on this problem, by profiling the structure of CPPS and the potential threats, conducting an in-depth analysis of CPPS attack modes from the cyber and physical subsystems, and summarising the three-level security defence methods for CPPS in detail. Finally, the future technological development prospects of CPPS security research are explicitly addressed, which will provide technical support for building reliable, safe, and robust energy systems.

KEYWORDS

coordinated cyber-physical attacks, cyber-physical power system, false data injection attacks, intrusion detection, security information and event management

1 | INTRODUCTION

In recent years, with the development of computer technology, communication network, and intelligent devices, the traditional energy and power system with physical equipment as the core is gradually combined more closely with information and communication technology and gradually evolved into Cyber-Physical Power System (CPPS), which is a multi-dimensional heterogeneous system integrating control, computing and communication. The structure of CPPS is shown in Figure 1.

In CPPS, a large number of power physical devices are connected to the information and communication system through intelligent electronic devices (IEDs) to accomplish ubiquitous sensing data collection, edge computing state identification, and system regulation and control for optimal operation. Therefore, the CPPS includes complex sensing, communication, computation, and control, and covers all aspects of power system electrical energy production, transmission, distribution, and consumption etc. S. Buldyrev's research results published in Nature points out that interdependent networks are more fragile and more prone to a catastrophic cascade of failures than any single network due to existing interactive links [1]. Therefore, the CPPS faces many new challenges in protecting its physical system from inherent vulnerabilities and defending against attacks on the network system. It is particularly noteworthy that attacks against CPPS in recent years have often been launched from the cyber side and propagated through cross domains, resulting in large-scale chain failures and incidents in the power system. The first documented attack on a cyber-physical system (CPS) occurred in Siberia in 1982, where the attacker manipulated software to cause a valve to act incorrectly, ultimately leading to a pipeline explosion [2]. In 2010, the Bushehr nuclear power plant in Iran was attacked by the Stuxnet worm, which shut down its reactor

[3]. The world's first cyber attack to cause a massive power system outage occurred in 2015 when the Ukrainian power system was attacked by the BlackEnergy malware, causing power outages in more than half of the country [4]. Table 1 lists the large-scale attacks that have occurred in recent years.

From the above attacks, it can be seen that the attacks against power CPPS are mainly cyberattacks and coordinated cyber-physical attacks (CCPAs). However, the current research on CPPS attacks and defence methods is still mostly at the level of cyberattack. This paper classifies a variety of attack modes that CPPS has emerged or may face and summarises the approach to CPPS security defence in three stages: prior prediction, defence in the event, and immunity afterwards. Finally, we present the shortcomings of the current CPPS security research and provide an outlook on the future development of the technology. The study hopes to provide a reference for experts and scholars who enhance the security research of CPPS.

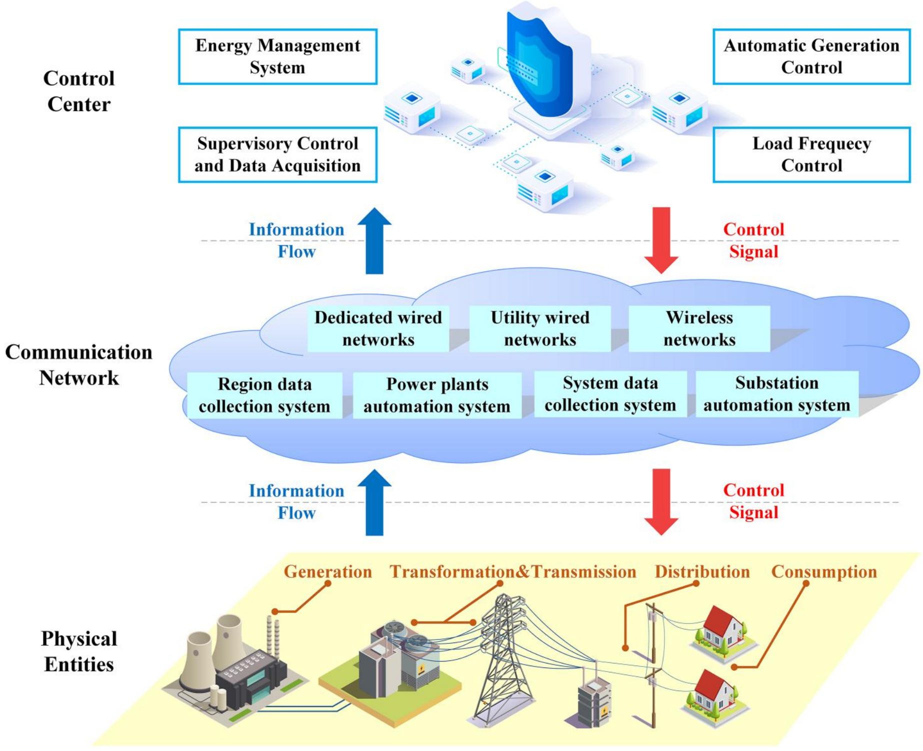

FIGURE 1 CPPS coupling structure diagram. CPPS, Cyber-Physical Power System

TABLE 1 Large-scale attacks on energy power systems

Time	Event description	Attack method
1982	Malicious manipulation to the gas transportation pipeline valve control system in Siberia led to pipeline explosion [2].	Cyber attack
2010	The control system of the Iranian nuclear power plant facility was attacked by Stuxnet worm, causing a 20% number of the centrifuges to be forced to shut down [3, 5].	Cyber attack
2013	Several industrial and energy-related companies in the United States were hit by a malware attack from dragonfly attackers, resulting in a massive energy data breach [6].	Cyber attack
2015	The BlackEnergy virus was implanted in the Ukrainian power grid information system, causing continuous tripping of transmission lines and preventing the system from restarting properly, causing 22,500 customers and half of the country outages for several hours [4, 7].	Cyber attack
2016	Israel's electricity sector suffered an unknown cyberattack that paralysed the computer systems in the electric power department for several weeks [8].	Cyber attack
2019	Venezuela's power grid suffered five consecutive rounds of attacks, including cyber, electromagnetic, and physical attacks, within 20 days, causing two consecutive widespread power outages [9, 10].	Coordinated cyber-physical attack
2020	Light S.A, a Brazilian electricity company, was attacked by the Sodinokibi malware and hacked for a ransom of $14 million, while a large amount of electricity data was locked [11, 12].	Cyber attack

The rest of this paper is organised as follows: Section 2 summarises the attack methods by classifying three possible attack modes: cyberattack, physical attack, and CCPA. Section 3 comprehensively analyses various security strategies for CPPS in three stages: prior prediction, in-person defence, and post-immunisation. Section 4 provides an outlook on the future technical development of CPPS.

2 | CYBER-PHYSICAL POWER SYSTEM ATTACK MODES AND ANALYSIS

Cyber-physical power system is a complex system that integrates communication system, control system, protection relay system, and distribution management system. The control system includes Energy Management System, Supervisory Control and Data Acquisition (SCADA) system, and so on. Under the normal operation of the system, each of the above subsystems ensures the normal operation of various power automation control components and CPPS by collecting, monitoring, and transmitting real-time operational data.

Attacks against the CPPS are malicious acts that exploit security flaws and information vulnerabilities in the physical and cyber systems to track the operational status without permission. The aim is to damage or degrade the functions and system resources of the above systems [7, 13, 14]. Typical forms of attacks against the CPPS and the role of the target are shown in Figure 2.

2.1 | Cyber attacks

The main targets of attacks on the cyber domain of CPPS are the various types of cyber terminals and communication networks scattered throughout the system. By contrast, it is more difficult to directly attack or intrude into the central control centre of CPPS because it generally has more advanced security defences.

The cyber terminals of CPPS contain a large number of sensors and information acquisition devices, including Remote Terminal Unit (RTU), Data Transfer Unit (DTU), Feeder Terminal Unit (FTU), Transformer Supervisory Terminal Unit and Phasor Measurement Unit (PMU) installed on the physical primary equipment or substation of the power system. They are responsible for the acquisition and uploading of power system voltage, current, active/reactive power, power quality data, and switchgear status [15]. The network transmission layer includes uplink/downlink communication channels and communication sub-station, such as routers or switches, which is a multi-level, multi-service complex network.

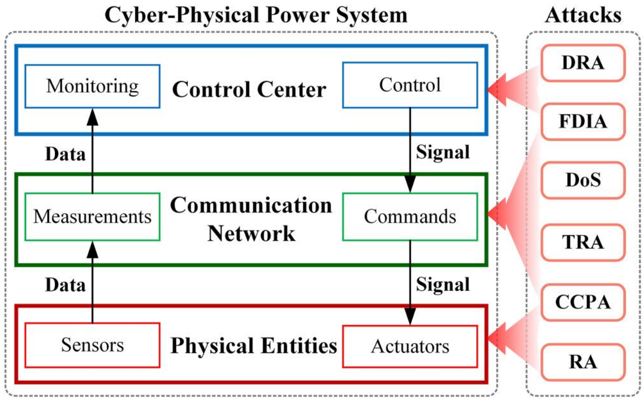

FIGURE 2 CPPS attack mode and role location. CPPS, Cyber-Physical Power System

Since the cyber terminals are the connection points between the physical devices and the cyber domain of the CPPS, most terminals exist with simple functions and are placed in publicly exposed spaces, providing attackers with convenient opportunities to compromise the CPPS system, such as through the implantation of viruses and disguised terminal damage to interfere with the data measurement function of the information terminals. For the network layer, attackers usually attack by blocking or disrupting communication channels and tampering communication data. Since the operation and control of modern power systems are more dependent on accurate and robust information data, an attack on the cyber layer would have a serious impact on the CPPS and the power system. Common attacks against CPPS cyber terminals include Time Synchronisation Attacks (TSAs), while those against the network layer include Denial of Service (DoS) attacks, Data Replay Attacks (DRAs), and False Data Injection Attacks (FDIAs) can attack at both sides.

2.1.1 | Time synchronisation attacks

As a distributed system across vast geographic space, the operation control of the power system especially relies on the time scale signals from GPS/BeiDou satellites to keep the system operation control time synchronised in different regions, such as the power flow calculation of the transmission and distribution system. The current CPPS terminals have many inherent defects, such as the Time Synchronies Device of PMU communicates using plain codes without encryption authentication mechanism. Using these flaws, TSA transmits forged satellite navigation messages to induce the CPPS cyber terminal to receive and decode the wrong synchronisation time, thus causing time deviation in the calibration data. This leads to the disruption of the Wide Area Measurement System and the power regulation and control system makes wrong control decisions, causing the system to go out of control in order to achieve the purpose of attack and destruction [16]. A method for achieving spoofed interference on satellite signals based on security code estimation and replay attacks, among others, was presented in Ref. [17]. A low-cost controller-based GPS analogue positioning software was discussed in Ref. [18], which can initiate TSA by broadcasting a forged GPS signal through several function calls. Ref. [19] presented a known combined interference strategy based on suppression and spoofing of GPS signals, capable of causing significant time jitter in the time synchronisation unit in the PMU.

In addition, actual operational system failures due to jittered synchronised time data were recorded and reported. In January 2013, due to a time data jitter caused by a malfunction in the time synchronisation device, the western China power control centre executed a power generation plant with the wrong date, resulting in the unnatural shutdown of several turbines at the hydropower plant [20]. Although this incident may not have been caused by TSAs, it demonstrates the attack potential of TSAs in CPPS. As the above analysis, unlike power equipment such as smart substations or central control master stations, there are few focussed security defence mechanisms established for PMUs and TSDs. And the time synchronisation is the basic data function for almost all monitoring and control systems in the electric power system, so TSA has a great threat to the future development of electric power systems.

2.1.2 | Denial of service attacks

Denial of Service attacks are one of the traditional attack methods against communication networks. Attackers usually launch attacks through protocol security vulnerabilities, network traffic flooding, or blocking communication channels [21]. With the development of CPPS, its communication networks are becoming more and more complex. Therefore, DoS can attack the CPPS communication network, such as the telemetry, remote signalling and remote control channels of FTU, DTU or RTU [22], which will further affect the dynamic and stable operation of the control units of the electric power system.

Figure 3 shows a typical DoS attack process. Another derivative attack from DoS is Distributed Denial of Service (DDoS) attack, which is more insidious and attacking intensity than DoS attack. Distributed Denial of Service can send overloaded traffic to the same server through multiple hosts scattered in different places, resulting in communication being broken, the service system crashing or hanging, and losing the ability to operate the power physical system.

Ref. [23] investigated the impact of DoS attacks on the stability control of Load Frequency Control (LFC) systems and proposed a new stability criterion based on the duration and frequency of DoS attacks. Ref. [24] analysed the stochastic stability of islanded microgrids under DoS attacks. Ref. [25] analysed the CPPS with multiple remote state estimation subsystems under DoS attacks and established a multi-sensor multi-channel remote state estimation model. With the construction of the new type of power systems in recent years, more diverse CPPS terminals are connected into the CPPS, which provide more handlers for DoS or DDoS attacks. Ref. [26] investigated in detail the fault ride-through capability of DC microgrids under DoS attacks. Ref. [27] investigated the impact of a smart grid connected to a large number of electric vehicles on the LFC system observers under DDoS attacks. In addition, a simulation platform was proposed in Ref. [28], in which the vulnerability of CPPS under DoS attacks can be analysed and the performance of decentralised and distributed control strategies was compared.

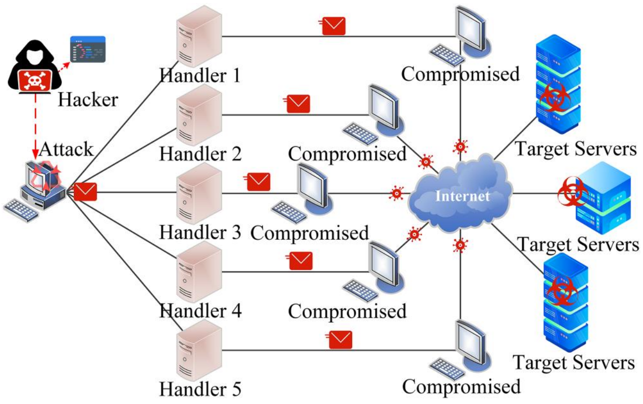

FIGURE 3 DoS attack diagram, DoS, Denial of Service

2.1.3 | Data replay attacks

Data Replay Attacks can fool the security certification system by intercepting and retransmitting certain function-specific data messages. They are mainly used in undermining the correctness of the authentication [29]. Since DRAs only need eavesdrop networks or theft authentication credentials [30], it will be more easily implemented with the more and more wireless communication applications in CPPS. Once the attacker initiates DRAs and successfully deceives the authentication system, it can directly damage the physical system by tampering with the control commands. Moreover, it also can make the control centre unable to sense the abnormal state of the power physical sub-system by replaying the false measurement data with the normal state [31]. This will cause the security defence to fail to start, resulting in more serious accidents. Therefore, some scholars have further investigated the behaviours of DRAs and the detection methods [32, 33].

2.1.4 | False data injection attacks

False Data Injection Attacks are the new type of attack methods, especially for cyber-physical coupled systems. By maliciously tampering with the measured data at the sampling terminals or the state estimation results at the control terminals, FDIAs can cause the misjudgement of the operation state of the physical power system or misoperation of the control execution. In CPPS, there is a greater threat of potential FDIAs due to the characteristics of the complex topology of the physical power system and the low redundancy of measurement data. For example, it can attack the sampled voltage, injection power, or line power flow data of the SCADA system [34], then disrupt the State Estimation (SE), and LFC of the power system [35], which lead to the SCADA system and Automatic Generation Control (AGC) system to make the wrong decision and give the wrong command, resulting in system instability [36]. False Data Injection Attacks are now one of the primary threats that seriously damage the security and reliable operation of electric power systems. Figure 4 gives a typical FDIA action process in the CPPS.

Currently, some scholars have begun to study FDIAs and its characteristics. Ref. [37] investigated various possibilities of FDIA implementations on different types of CPPS terminals. Ref. [38] presented how FDIAs can be implemented by modifying the firmware of RTUs. In analysing the impact of FDIAs on various types of controls, Ref. [39] gave an example of FDIAs by injecting false measurement data into CPPS systems and then leading to unnecessary generator rescheduling and system load shedding. Ref. [40] analysed FDIAs to AGC system, and the danger of generator frequency deviation caused by the attack was described in detail. Ref. [41] investigated FDIAs against wide-area control systems, which can lead to the inaccurate setting of the secondary voltage controller through measurement data falsification.

2.1.5 | Man-in-middle attacks

MiTMAs are indirect intrusion attacks in which an attacker hides himself between the network connections of two or more communication terminals through technical means to intercept, eavesdrop, and tamper with information in the channel, thereby compromising the confidentiality, integrity, and availability of data [42]. Unlike several of the above-mentioned network attack methods, MiTMAs are able to intercept accounts and passwords of known authentication protocols by cracking communication protocols or pointing the path to IP address devices of pre-prepared virus programs, while their whole process is more stealthy and harder to detect.

In light of MiTMAs' stealthy nature, Ref. [43] investigates the MiTMAs against CPSs under the random access protocol scheduling, where an attacker intercepts and modifies the transmitted data and then forwards them on to degrade the system performance. Ref. [44] designed and implemented multi-stage MiTM intrusions in an emulation-based CPPS testbed model to demonstrate how such attacks can cause power physical contingencies such as misguided operation and false advanced metring infrastructure. This work enables smart grid security researchers and industry to develop further detection mechanisms for inconspicuous MiTM attacks.

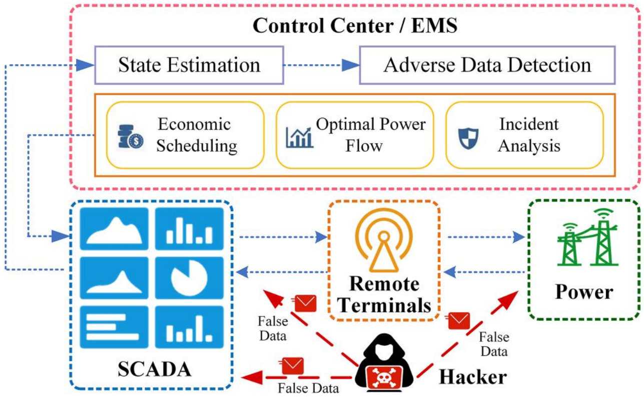

FIGURE 4 The process of FDIAs in CPPS. CPPS, cyber-physical power system; FDIAs, False Data Injection Attacks

2.2 | Physical attacks

In addition to the above-mentioned CPPS attacks launched from the cyber system by drawing on existing various Internet attack methods, there is a unique physical layer attack against CPPS, which is a type of attack that directly intrudes into the physical infrastructure of power or damages the physical system. For example, electromagnetic damage attacks using overvoltage or electromagnetic pulses can damage the electrical equipment without touching them.

Resonance Attacks (RAs) are one of the typical CPPS physical attacks, which directly target the electrical physical infrastructure. It causes abnormal frequency or rate of change of control of the power system by changing the power load or contact line signal according to a resonant source. Because the resonance is inherent of each system, RAs tamper the loads or generators' status signals that are too faint to be identified by routine detection methods [45]. The process of RAs is shown in Figure 5.

Ref. [46] represented the possibility of RA implementation through the simulation of two-area LFCs and proves that accurate RAs can have irreversible impacts on power system

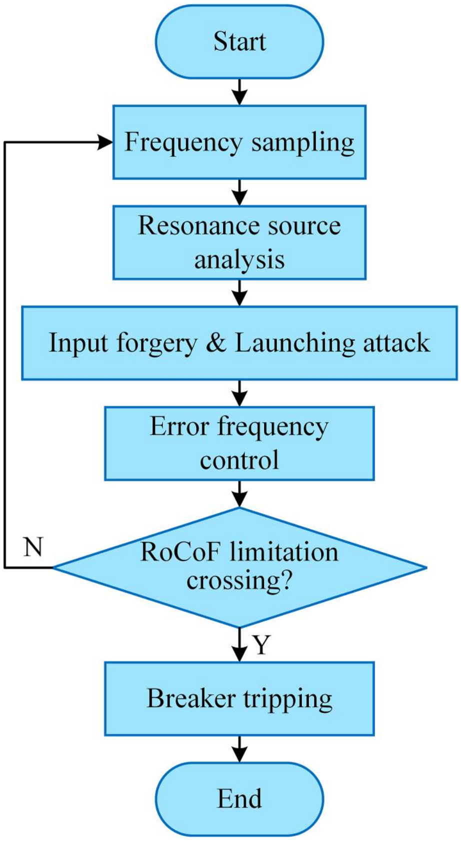
Start
Frequency sampling
Resonance source analysis
Input forgery & Launching attack
Error frequency control
RoCoF limitation crossing?
N
Y
Breaker tripping
End

FIGURE 5 Resonance Attack process

frequency control. In the work of Ref. [47], RAs on single area and multi-area LFC systems consisting of linear/non-linear terms, first-order/higher-order terms, automatic voltage regulators, and power system stabilisers were performed. The experimental results showed that RAs are capable of causing damage not only to LFC in one area but also can propagate to other interconnected areas, creating a larger scale of damage.

2.3 | Coordinated cyber-physical attacks

Since CPPS is a tightly coupled CPS, attackers naturally think of using coordinated cyber-physical attacks. Through the overlapping of two parallel domains, the attacks can cross between cyber and physical domains and form a larger scale and stronger damage than any single attack. The 2019 attack in Venezuela was a typical CCPA, which not only proved the possibility of CCPA but also demonstrated its enormous attack power and difficulty of defence.

Usually, CCPA will cover up the system failure caused by physical attack through cyberattack. The purpose of this is to delay the discovery of the failure and use the time gap to further expand or launch a larger-scale physical attack, so as to destroy the secure and stable operation of the system [48]. Figure 6 presents the flow of CCPA.

In the work of Ref. [49], it had been presented that if it is necessary to cover up false transmission line faults, the false data need to satisfy Kirchhoff Current Law and Kirchhoff Voltage Law and cunningly add the data residuals at both ends of the faulty transmission line to prevent it from being discovered by PMU. Ref. [50] presented a cooperative attack on measurement instruments in power system and its coupled communication networks. Ref. [51] designed a sparse attack strategy that can obtain the minimum attack set for the entire power grid to carry out a CCPA, even if the CPPS topology information is incomplete. In addition, there were also studies on the CCPAs against AGC and LFC system [52, 53].

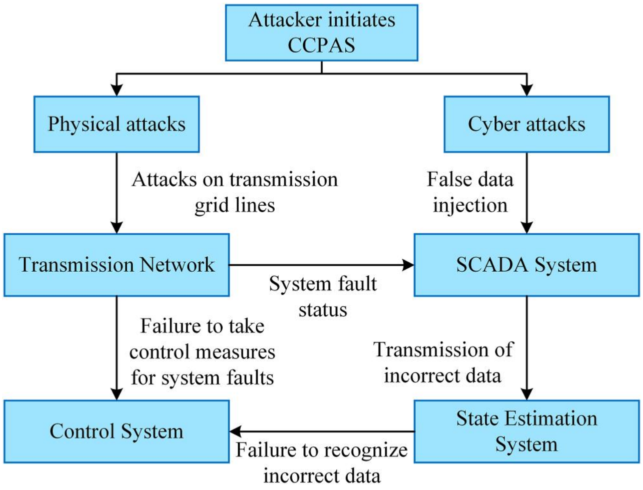

FIGURE 6 The process of coordinated cyber-physical attacks

3 | CYBER-PHYSICAL POWER SYSTEM SECURITY DEFENCE METHODS AND CLASSIFICATION

From the above analysis, it can be seen that with the technological advancement, there are more and more attacks against CPPS, showing more multi-dimensional and stealthy characteristics. To defend against various attacks, research institutions and scholars around the world have conducted in-depth research on CPPS security defence, from the cyber domain and physical domain [54], from the time dimension and the space dimension, respectively [55], and from data centric to study data availability, integrity and confidentiality [56]. As there are more and more new types of coordinated attacks against CPPS, the above classification and research cannot well summarise the previous CPPS security defence methods. This paper will study the CPPS security detection and defence methods into pre-attack, attack and post-attack according to the whole process of the periodic evolution of the attack event. Figure 7 shows the research structure of this section.

3.1 | Pre-attack security detection and defence strategy

In the face of possible attacks, any CPPS will deploy responsive security defence strategies, the primary of which is to effectively block potential attacks through identity authentication and security encryption.

3.1.1 | Security authentication and trusted access technologies

As the above analysis, with the construction of new type of electric power system, more and more IED will be connected to CPPS, including distributed renewable energy monitoring devices on the customer side, regulation device of energy storage units, and smart sensors to realise more comprehensive and detailed observability of power system. These IEDs belong to different subjects, so authentication and trusted access

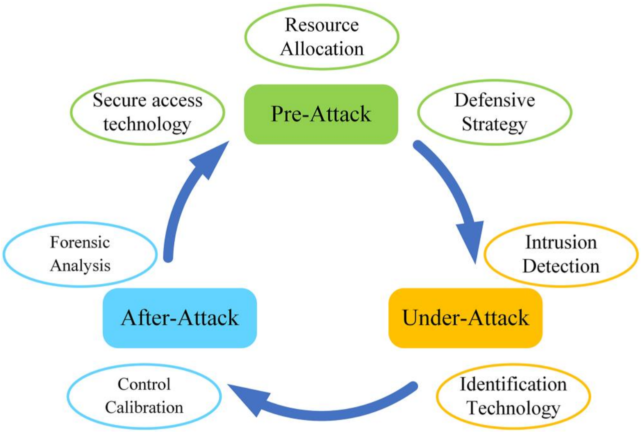

FIGURE 7 CPPS security defence phase. CPPS, Cyber-Physical Power System

technologies are necessary when the system requires a 'plug-and-play' accessing manner. At the same time, any data transmitted in CPPS should be encrypted to prevent data from being eavesdropped on or tampered. Security authentication technology is to verify whether the identity of the access object is legal, in which the object can be a consumer, a smart device or any other components connected to CPPS [57]. Authentication technology is the first line of defence of CPPS security. Some previous work is presented, such as a lightweight security authentication mechanism based on artificial intelligence Markov model prediction is proposed in Ref. [58]. A low-entropy-based shared password scheme for CPPS communication devices accessing authorisation is presented in Ref. [59]. Moreover, a blockchain-based trust consensus method for cyber terminals in zero-trust environments was proposed in Ref. [60], in which the consortium blockchain and beta distribution multiple trust evaluation mechanism was employed to enhance the reliability of the trust parameters, which can evaluate the terminal credibility and respond to multiple malicious attacks.

As a traditional method of communication security, data encryption is always used to encrypt and retransmit plaintext data to prevent attackers or eavesdroppers from obtaining important data. The methods of data encryption are mainly divided into symmetric key encryption and asymmetric key encryption. Currently, the two methods are widely used in various devices and scenarios of CPPS applications according to different requirements such as data criticality and computational complexity.

3.1.2 | Defensive strategy and resource allocation

In addition to the above effective security prevention methods, the development of defence strategies will be able to detect potential dangers, achieve early prevention of possible attacks, and optimise the allocation of defence resources.

Through the analysis and simulation of the various attacks and evaluation of system performance, the defence strategy can be effectively set up to discover the weaknesses of the current CPPS system from the attacker's perspective. And based on modelling and system extrapolation to derive the possible damage degree after the attack, the system can provide advance resource allocation deployment for the subsequent security defence of CPPS. Several attack models have been presented to simulate different attack methods, which included the parameter-weighted temporal automata evaluation models based on attack tree models [61]; the attack graphs model to simulate and quantitatively evaluate CPPS network attacks and cross-domains chain failures [62], and the models of the event-synchronous attacks and event-unsynchronous attacks on PMU measurement data [63]. In addition, a vulnerability assessment of power systems under the influence of noisy data ingestion and cyberattack was proposed in Ref. [64].

Once the attack simulation and system performance evaluation have been carried out, it is necessary to deploy defence resources based on the potential risks of the explored CPPS and improve the system defence capability.

Ref. [65] investigated the changes of key operating parameters of power systems under FDIAs and proposed a game-theoretic-based defence resource allocation method. Ref. [66] proposed a probabilistic risk analysis framework based on Bayesian adaptive networks, which can help control system to rationally allocate defence resources in resource-constrained situations. Ref. [67] proposed a co-evolutionary algorithm to obtain the optimal action set of a large-scale network equilibrium defence during the dynamic attacks. Ref. [68] modelled the attack and defence behaviours at three parts: power plant, power transmission system, and power distribution system, and then studied the different optimal defence strategy for the three parts, respectively.

The above defence strategies and resource configuration will be deployed in the CPPS system in advance through the firewall and forward and reverse isolation devices.

3.2 | Defence strategies in attack events

3.2.1 | Multi-level security line of defence approach for traditional power system and cyber-physical power system

The traditional power system enhances the safety of the system in response to faults by setting up 'three lines of defence'. The first line of defence relies on fast relay protection and effective preventive control strategies to ensure stable grid operation and normal power supply in the event of a common single fault; the second line of defence is used to ensure that the power grid can continue to maintain stable operation in case of low probability serious faults by adopting stability control devices and emergency control measures such as generator-shedding and load-shedding; the third line of defence is used to pre-instal out-of-step deregulation, frequency, and voltage emergency control devices in the system. When the power system is damaged by multiple serious accidents, these devices can be urgently started for emergency control to prevent the expansion of accidents and large-scale power outages. Coupled with the above multiple defence lines, the CPPS 'three lines of security defence' have been gradually formed. Figure 8 presents a detailed structure diagram between the two types of 'three lines of security defence'.

In CPPS, the first line of defence is used to enhance communication network planning and provide efficient routing for services, which can achieve advance prevention. It is analogous to the construction and operation planning of electric power systems to improve the capability to resist to anticipated failures; the second line of defence is used to achieve rapid recovery of the service path by network self-healing protection functions, which is analogous to the power system's emergency control strategy to quickly remove failures; the third line of defence is used to achieve system-level correction by blocking existing channels or centralising management of limited communication resources for rerouting. It will be urgently started when a serious failure cannot be

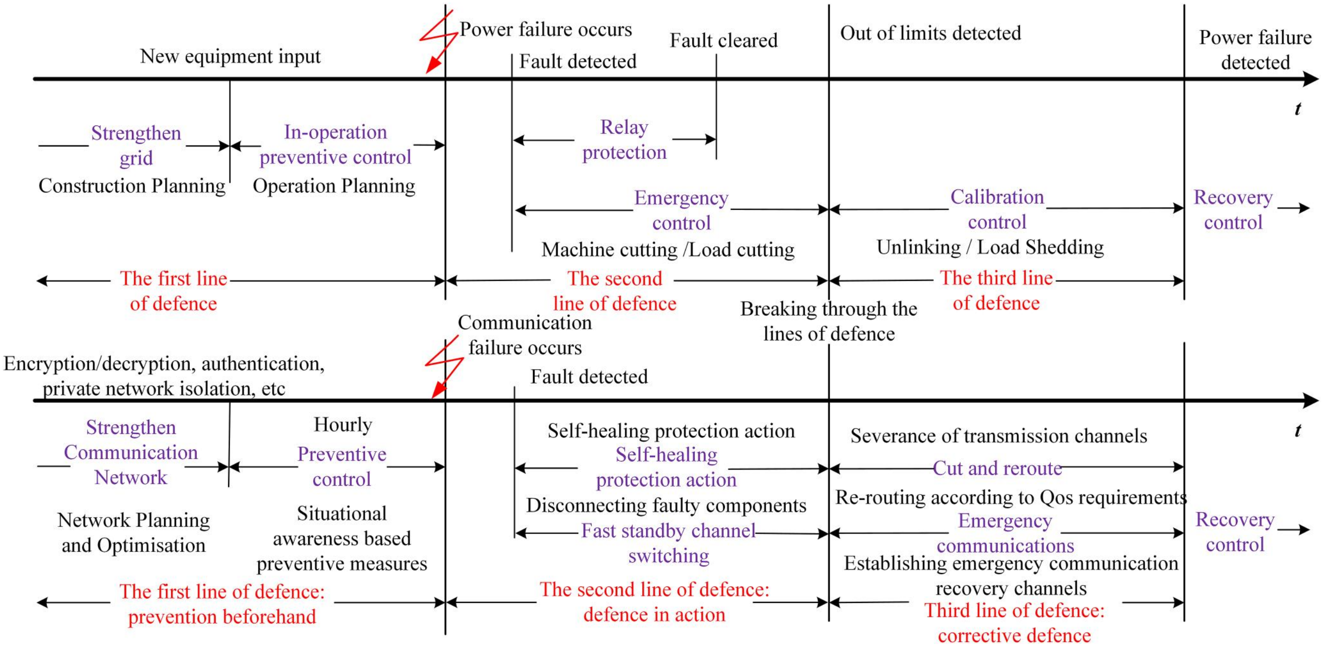
Power failure occurs
New equipment input
Fault detected
Fault cleared
Out of limits detected
Power failure detected
t
Strengthen grid
Construction Planning
In-operation preventive control
Operation Planning
Relay protection
Emergency control
Machine cutting /Load cutting
Calibration control
Unlinking / Load Shedding
Recovery control
The first line of defence
The second line of defence
The third line of defence
Breaking through the lines of defence
Communication failure occurs
Encryption/decryption, authentication, private network isolation, etc
Fault detected
t
Strengthen Communication Network
Network Planning and Optimisation
Hourly Preventive control
Situational awareness based preventive measures
Self-healing protection action
Self-healing protection action
Disconnecting faulty components
Fast standby channel switching
Severance of transmission channels
Cut and reroute
Re-routing according to Qos requirements
Emergency communications
Establishing emergency communication recovery channels
Recovery control
The first line of defence: prevention beforehand
The second line of defence: defence in action
Third line of defence: corrective defence

FIGURE 8 Traditional power grid security defences

eliminated and will spread rapidly. It is similar to the implementation of low-frequency and low-voltage load shedding or power system splitting to reduce outage loss.

Ref. [69] proposed a new algorithm to establish the main routing path and backup one during the electric power communication network planning, and then if there is any communication links' transmission performance degradation, it can automatically jump to the backup path to ensure cyber function. It achieves the function of the CPPS first defence line. The CPPS backbone network using Synchronous Digital Hierarchy (SDH) ring structure is just using the excellent feature that SDH can automatically realise 50 ms automatic return, and the CPPS second defence line of network self-healing protection is achieved. Establishing the CPPS third defence line is more complex than that of the power system because the electric power system splitting only needs to calculate the power flow, while CPPS should consider the coupling relationship between cyber and physics system. If it is necessary to block the fault evolution and cut off one of communication links, a certain number of power services will be interrupted. Therefore, if the cyber cutting surface is not unified with the physical cutting surface, it will expand the scope of power outage and aggravate the fault damage. To solve this thorny problem, Ref. [70] proposed a novel CPPS saturation defence scheme based on cyber-physical unified active cuts. It can effectively prevent the expansion of attack damage, and the stable operation of the main security area can be guaranteed.

3.2.2 | Intrusion detection and defence technology

When CPPS has been attacked, if it can accurately identify the intrusion mode and attack point in the shortest possible time, it will win the most valuable time for defence and will be able to minimise the consequences of the attack through the right defence strategies. Therefore, fast and accurate intrusion detection methods are deeply studied. It can be divided into power physical domain and information domain according to the structure of CPPS, including feature-based and bias-based methods, as shown in Figure 9.

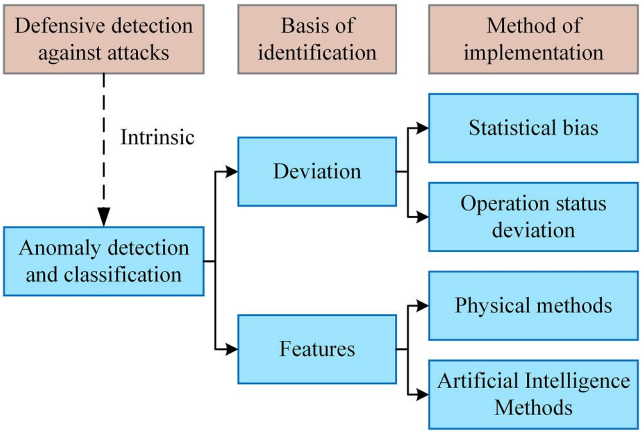
Defensive detection against attacks
Basis of identification
Method of implementation
Intrinsic
Anomaly detection and classification
Deviation
Features
Statistical bias
Operation status deviation
Physical methods
Artificial Intelligence Methods

FIGURE 9 Intrusion detection and identification technology

The detection method of power physics side mainly depends on judging whether the electrical measurement, decision action instructions and sudden changes in system operation state comply with the physical law of power system [54]. For example, bad data detection and identification based on residual detection method or spatio-temporal correlation condition constraints [71], and doubly-fed deep learning identification methods for PMU's bad data [72]. In addition, there are multi-step bad data detection algorithms for SCADA systems and FDIAs [73, 74].

The detection methods on the cyber side mainly relies on the intrusion detection in information technology, which is usually with the help of intrusion detection system (IDS) or Security Information and Event Management system to detect the addresses and network logs of cyber devices, transmission traffic or communication patterns. For example, consistency detection method or identification based on prior information is employed.

Ref. [75] found the abnormal transmission events in communication network by comparing the data sent and received by sensors and actuators. For more types of cyber-attacks, the work of Ref. [76] proposed an intrusion detection model based on whale optimisation algorithm and artificial neural network and then designed a classification intrusion detection method. Combined with electric power devices, such as smart metres and power scenarios, Ref. [77] proposed an attack detection method based on a support vector machine algorithm. For SCADA systems, an anomaly detection method based on Gaussian mixture model and Kalman filtering was designed in Ref. [78]; Ref. [79] proposed an intrusion detector-based design and a second frequency control method for possible DoS attacks on power system frequency controllers. Considering multi-area interconnected power system scenarios, Ref. [80] proposed a distributed data de-determination intrusion detection method for FDIAs. The work of Ref. [81] further considered FDIA detection methods in the scenarios where large-scale electric vehicles are connected to the power system. In addition, unlike the existing disassembled identification of each frame message, Ref. [82] proposes an artificial swarm-optimised support vector machine (ABC-SVM) anomaly traffic spectrum clustering detection method based on mixed time-frequency domain features of CPPS information streams, which greatly improves the detection speed and can accurately identify unknown attacks or intrusions because only stream transmission behaviour features are required without each data packet analysed.

In recent years, with the rapid development of artificial intelligence technology, new intrusion detection methods based on machine learning methods have been significantly improved in terms of recognition accuracy, for example, the energy Internet network attack and fraudulent transaction detection methods based on recursive neural networks and blockchain technology are used against the network attacks or fraudulent transaction in energy Internet [83], and CPPS intrusion detection methods based on preprocessing of feature volume extraction and machine learning classifiers.

The fundamental goal of CPPS defence is to ensure the operational stability of the power system, including voltage stability, frequency stability, and power angle stability. Therefore, CPPS defence methods mostly combine attack blocking and system stability control closely. By researching on targeted control strategies or designing controllers, it can maintain the system stability and minimise the impact of attacks, once an attack occurs. The present security control methods for CPPS attacks can be divided into two categories: resilient control methods and active defence control methods. Resilient control methods analyse the quantitative relationship between system performance and attack parameters based on the special attack model, use the Lyapunov function method to analyse the resilience constraints in the attack case, and then design the resilience control trigger mechanism to ensure the input state stability [84]. But this type of method is very conservative. Active defence control methods use active compensation mechanisms to cope with attacks and ensure control system performance, including predictive control methods [85], multi-channel networked control methods [86] etc.

There is also an interesting defence technique for spoofing the attacker, Honeypot Technology, which is the trap technique in network defence [87]. By arranging some network servicers, hosts or messages as bait, attackers are easily hooked to attack them. Then the attack behaviour can be captured and analysed; the tools and attack methods used by the attacker can be obtained. The honeypot technique can infer the intention and motivation of the attack, and then reinforce the system. At the same time, the honeypot technique can also consume and weaken attack resources.

3.3 | Post-attack

Whether the attack has been detected in time and blocked or has caused an incident and the system recovery is completed by reconfiguration or reboot, it should be analysed in detail and updated after the attack. For example, IDS signature, anti-virus database and security policy should be updated in time for post-attack immunisation and security defence upgrade to protect CPPS from similar attacks in the future. Forensic Analysis (FA), as a major method for post-event threat information collection and analysis forensics for attacks, includes three steps of intrusion/attack evidence collection, threat information analysis, and evidence presentation. Ref. [88] identified FDIAs on advanced metring infrastructures and trace forensics by performing FA on the data in network traffic logs. Ref. [89] proposed a digital forensic approach based on sandbox and FA technologies to analyse the historical attack data of Wide Area Monitoring Systems, Protection and Control Systems. Through the analysis of forensics and backward reinforcement to update the virus database or attack behaviour sample database for security immunity, the security defence capability is improved.

4 | CHALLENGES AND PROSPECTS

With the development of sensing, communication, and cloud-edge collaborative information processing technologies, the complexity of CPPS with tightly coupled energy flow and information flow is gradually increasing, and its security and stability directly affect the electric power system. This paper analyses and summarises the typical attack patterns and multi-dimensional defence methods of CPPS. But attack and defence must be the relationship of the spear and shield, which is a dynamic process of mutual resistance and counterbalance. New types of attacks against CPPS have never stopped emerging.

Therefore, at the end of this paper, we think about the problems that need to be deeply studied and solved in CPPS defence, so as to provide a reference for the subsequent technical development.

(1) The existing research on CPPS security are based on the attacks that have been detected or have been intercepted, but there is a lack of effective research on the identification and defence against unknown attacks. As mentioned earlier, new types of viruses and attacks against CPPS keep emerging. Therefore, rapid identification and active defence without a priori information of unknown attacks are of great significance to improve the security of CPPS.
(2) CCPA is more destructive and stealthier than any other network attacks due to the diversity of attack combinations and the difficulty of attack detection. From the recent attacks, we can also see that once a coordinated attack occurs, it will cause irreversible harm. However, there is little research on coordinated cyber-physical attacks, so the new defence methods against CCPA are the interesting topic worth exploring.
(3) With the development of the new generation of artificial intelligence technology, represented by deep learning and reinforcement learning, it has shown powerful and good application effects in the field of CPPS attack detection and security defence. Artificial intelligence algorithms are based on the big data sample libraries. So, it is greatly important to establish CPPS attack sample libraries, which can effectively improve the system's ability to quickly identify abnormal behaviour and reduce the false alarm rate. Therefore, it is necessary to establish a comprehensive information collection mechanism and a unified CPPS attack sample database. It can be collaboratively shared among countries around the world.
(4) The off-line simulation is mainly used to study the dynamic process of CPPS attack and defence. But it hardly demonstrates the complex and fast dynamic evolution of both cyber and physical sub-systems in CPPS. Therefore, it is an urgent need to establish a real experimental field, which will play an extremely important role in promoting CPPS system risk analysis, chain fault propagation, resource deployment and dynamic arming. CPPS is an independent system with numerous devices and components, including power physical equipment, electrical quantity sensing and measuring devices and communication networks, and there exists a large span of voltage levels from ±1100 kV to 110 V. The construction of the real experimental field needs to employ dynamic simulation and digital twin technologies should be studied and employed in CPPS real experimental field.

ACKNOWLEDGEMENT

This study was supported by the National Key Research and Development Program of China (2017YFE0132100), the National Natural Science Foundation of China (61971305) and the Natural Science Foundation of Tianjin (21JCZDJC00640).

CONFLICT OF INTEREST

The authors declare no conflict of interest.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are available from the corresponding author upon reasonable request.

ORCID

Ting Yang https://orcid.org/0000-0002-8863-1944

REFERENCES

1. Buldyrev, S.V., et al.: Catastrophic cascade of failures in interdependent networks. Nature. 464(7291), 1025–1028 (2010)
2. Reed, T.C.: At the Abyss: An Insider's History of the Cold War. Presidio Press (2005)
3. Chen, T.M.: Stuxnet, the real start of cyber warfare?[Editor's Note]. IEEE Network. 24(6), 2–3 (2010)
4. Liang, G., et al.: The 2015 Ukraine blackout: Implications for false data injection attacks. IEEE Trans. Power Syst. 32(4), 3317–3318 (2017)
5. Bou-Harb, E., et al.: Communication security for smart grid distribution networks. IEEE Commun. Mag. 51(1), 42–49 (2013)
6. Langill, J.T.: Defending against the dragonfly cyber security attacks, vol. 11, pp. 2015 (2014)
7. Tang, Y., et al.: Overview on cyberattacks against cyber-physical power system. Autom. Electr. Power Syst. 40(17), 59–69 (2016)
8. Steinitz: Israel's Electric Authority Hit by 'severe' Cyber-Attack. https://www.timesofisrael.com/steinitz-israels-electric-authority-hit-by-severe-cyber-attack/. 2016/01/26
9. Devanny, J., et al.: The 2019 Venezuelan blackout and the consequences of cyber uncertainty. Revista Brasileira de Estudos de Defesa. 7(2) (2020)
10. Vaz, R.: Venezuela's power grid disabled by cyberattack. Green Left Wkly. (1213), 15 (2019)
11. He, S., et al.: Detection method for Tolerable false data injection attack based on deep learning framework. In: 2020 Chinese Automation Congress (CAC) (2020)
12. Sodinokibi Ransomware Operators Hit Electrical Energy Company Light S.A. https://securityaffairs.co/wordpress/105477/cyber-crime/sodinokibi-ransomware-light-s-a.html. 2020/07/03
13. De U. S.: Smart Grid Cyber Security, vol. 3. Supportive Analyses and References (2010)
14. Stamp, J., McIntyre, A., Ricardson, B.: Reliability Impacts from Cyber Attack on Electric Power Systems. In: 2009 IEEE/PES Power Systems Conference and Exposition (2009)
15. Ye, X., et al.: Quantitative vulnerability assessment of cyber security for distribution automation systems. Energies. 8(6), 5266–5286 (2015)
16. Qian, B., et al.: Review on time synchronization attack in power system. Power Syst. Technol. 44(10), 4035–4045 (2020)
17. Humphreys, T.E.: Detection strategy for cryptographic GNSS anti-spoofing. IEEE Trans. Aero. Electron. Syst. 49(2), 1073–1090 (2013)
18. Tippenhauer, N.O., et al.: On the requirements for successful GPS spoofing attacks. In: Proceedings of the 18th ACM Conference on Computer and Communications Security, pp. 75–86 (2011)
19. Zhang, H., et al.: Review on GPS spoofing-based time synchronisation attack on power system. IET Gener., Transm. Distrib. 14(20), 4301–4309 (2020)
20. Ingram, D.M., et al.: Evaluation of precision time synchronisation methods for substation applications. In: 2012 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication Proceedings, pp. 1–6 (2012)
21. Cetinkaya, A., Ishii, H., Hayakawa, T.: An overview on denial-of-service attacks in control systems: attack models and security analyses. Entropy. 21(2), 210 (2019)
22. Wang, Y., et al.: Vulnerability analysis and countermeasures of electrical network control systems under DoS attacks. Control Decis. 32(3), 411–418 (2017)

23. ShangGuan, X., et al.: Switching system-based load frequency control for multi-area power system resilient to denial-of-service attacks. Control Eng. Pract. 107, 104678 (2021)
24. Liu, S., et al.: Stochastic stability analysis and control of secondary frequency regulation for islanded microgrids under random denial of service attacks. IEEE Trans. Ind. Inf. 15(7), 4066–4075 (2019)
25. Yuan, H., Xia, Y., Yang, H.: Resilient state estimation of cyber-physical system with Multichannel transmission under DoS attack. IEEE Trans. Syst., Man, and Cybernetics: Syst. 51(11), 6926–6937 (2021)
26. Liu, J., Lu, X., Wang, J.: Resilience analysis of DC microgrids under denial of service threats. IEEE Trans. Power Syst. 34(4), 3199–3208 (2019)
27. Hossain, M.M., Peng, C.: Observer-based event triggering $H\infty$ LFC for multi-area power systems under DoS attacks. Inf. Sci. 543, 437–453 (2021)
28. Ding, P., et al.: DoS attacks in electrical cyber-physical systems: a case study using truetime simulation tool. In: 2017 Chinese Automation Congress (CAC) (2017)
29. Cherdantseva, Y., et al.: A review of cyber security risk assessment methods for SCADA systems. Comput. Secur. 56, 1–27 (2016)
30. Mahmoud, M.S., Hamdan, M.M., Baroudi, U.A.: Modeling and control of cyber-physical systems subject to cyberattacks: a survey of recent advances and challenges. Neurocomputing. 338, 101–115 (2019)
31. Liu, K., et al.: Secure control for cyber-physical systems based on machine learning. Acta Autom. Sin. 47(6), 1273–1283 (2021)
32. Su, L., Ye, D., Zhao, X.: Static output feedback secure control for cyber-physical systems based on multisensor scheme against replay attacks. Int. J. Robust Nonlinear Control. 30(18), 8313–8326 (2020)
33. Zhao, Y., Smidts, C.: A control-theoretic approach to detecting and distinguishing replay attacks from other anomalies in nuclear power plants. Prog. Nucl. Energy. 123, 103315 (2020)
34. Liu, Y., Ning, P., Reiter, M.K.: False data injection attacks against state estimation in electric power grids. ACM Trans. Inf. Syst. Secur. 14(1), 1–33 (2011)
35. Sridhar, S., Govindarasu, M.: Model-based attack detection and mitigation for automatic generation control. IEEE Trans. Smart Grid. 5(2), 580–591 (2014)
36. Deng, R., et al.: False data injection on state estimation in power systems—attacks, impacts, and defense: a survey. IEEE Trans. Ind. Inf. 13(2), 411–423 (2016)
37. Konstantinou, C., Maniatakos, M.: Hardware-layer intelligence collection for smart grid embedded systems. J. Hardware and Syst. Security. 3(2), 132–146 (2019)
38. Konstantinou, C., Maniatakos, M.: A case study on implementing false data injection attacks against nonlinear state estimation. In: Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy (2016)
39. Chen, J., et al.: Impact analysis of false data injection attacks on power system static security assessment. J. Mod. Power Syst. Clean Energy. 4(3), 496–505 (2016)
40. Tan, R., et al.: Optimal false data injection attack against automatic generation control in power grids. In: 2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS) (2016)
41. Musleh, A.S., et al.: A prediction algorithm to enhance grid resilience toward cyberattacks in WAMCS applications. IEEE Syst. J. 13(1), 710–719 (2017)
42. Conti, M., Dragoni, N., Lesyk, V.: A survey of man in the middle attacks. IEEE Commun. Surveys and Tutorials. 18(3), 2027–2051 (2016)
43. Zhang, X., Yang, G.-H., Wasly, S.: Man-in-the-middle attack against cyber-physical systems under random access protocol. Inf. Sci. 576, 708–724 (2021)
44. Wlazlo, P., et al.: Man-in-the-middle attacks and defence in a power system cyber-physical testbed. IET Cyber-Physical Syst.: Theory & Appl. 6(3), 164–177 (2021)
45. Hammad, E., et al.: Tuning out of phase: resonance attacks. In: 2015 IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 491–496 (2015)
46. Esfahani, P.M., et al.: Cyberattack in a two-area power system: impact identification using reachability. In: Proceedings of the 2010 American Control Conference, pp. 962–967 (2010)
47. Wu, Y., et al.: Resonance attacks on load frequency control of smart grids. IEEE Trans. Smart Grid. 9(5), 4490–4502 (2017)
48. Yang, Y., et al.: Coordinated cyber-physical attacks of cyber-physical power system. Electric Power Automation Equipment. 40(2), 97–102 (2020)
49. Liu, X., et al.: Masking transmission line outages via false data injection attacks. IEEE Trans. Inf. Forensics Secur. 11(7), 1592–1602 (2016)
50. Kim, J., Tong, L.: On topology attack of a smart grid: Undetectable attacks and countermeasures. IEEE J. Sel. Area. Commun. 31(7), 1294–1305 (2013)
51. Liu, C., Liang, H., Chen, T.: Network parameter coordinated false data injection attacks against power system AC state estimation. IEEE Trans. Smart Grid. 12(2), 1626–1639 (2020)
52. He, X., Liu, X., Li, P.: Coordinated false data injection attacks in AGC system and its countermeasure. IEEE Access. 8, 194640–194651 (2020)
53. Wang, Q., et al.: Coordinated defense of distributed denial of service attacks against the multi-area load frequency control services. Energies. 12(13), 2493 (2019)
54. Tang, Y., Li, M., Wang, Q.: A review on research of cyberattacks and defense in cyber-physical power systems part two detection and protection. Autom. Electr. Power Syst. 43(10), 1–9 (2019)
55. Zhang, H., Liu, B., Wu, H.: Smart grid cyber-physical attack and defense: a review. IEEE Access. 9, 29641–29659 (2021)
56. Nejabatkhah, F., et al.: Cyber-security of smart microgrids: a survey. Energies. 14(1), 27 (2021)
57. Rawat, D.B., Bajracharya, C.: Cyber security for smart grid systems: status, challenges and perspectives. In: SoutheastCon 2015, pp. 1–6 (2015)
58. Jan, M.A., et al.: Lightweight mutual authentication and privacy-Preservation scheme for intelligent Wearable devices in Industrial-CPS. IEEE Trans. Ind. Inf. 17(8), 5829–5839 (2020)
59. Azad, M.A., et al.: Authentic caller: self-enforcing authentication in a next-generation network. IEEE Trans. Ind. Inf. 16(5), 3606–3615 (2019)
60. Yu, J., Yu, L., Yang, T.: Blockchain-based trust consensus method for power internet of Things terminal. Autom. Electr. Power Syst. 45(17), 1–10 (2021)
61. André, É., et al.: Parametric analyses of attack-fault trees. Fundam. Inf. 182(1), 69–94 (2021)
62. Wang, Y., et al.: Assessing the Harmfulness of cascading failures across space in electric cyber-physical system based on improved attack graph. Proc. Chin. Soc. Electr. Eng. 36(6), 1490–1499 (2016)
63. Kamal, M., et al.: Cyberattacks against event-based analysis in Micro-PMUs: attack models and counter measures. IEEE Trans. Smart Grid. 12(2), 1577–1588 (2020)
64. Zheng, Y., et al.: Vulnerability assessment of deep reinforcement learning models for power system topology optimization. IEEE Trans. Smart Grid. 12(4), 3613–3623 (2021)
65. Pilz, M., et al.: Security attacks on smart grid scheduling and their defences: a game-theoretic approach. Int. J. Inf. Secur. 19(4), 427–443 (2020)
66. Smith, M.D., Paté-Cornell, M.E.: Cyber risk analysis for a smart grid: how smart is smart enough? A multiarmed bandit approach to cyber security investment. IEEE Trans. Eng. Manag. 65(3), 434–447 (2018)
67. Guan, S., et al.: Colonel blotto games in network systems: models, strategies, and applications. IEEE Trans. Network Sci. Eng. 7(2), 637–649 (2019)
68. Shan, X.G., Zhuang, J.: A game-theoretic approach to modeling attacks and defenses of smart grids at three levels. Reliab. Eng. Syst. Saf. 195, 106683 (2020)
69. Zhang, T., Ji, X., Xu, W.: AHV-RPL: Jamming-resilient backup Nodes Selection for RPL-based routing in smart grid AMI networks. In: International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness (2019)
70. Ting, Y., et al.: Research on saturation defense method of power cyber-physical system based on active cut set. Proceedings of the CSEE. 42(02), 475–487 (2022)

71. Wang, C., Mu, G., Cao, Y.: A method for Cleaning power grid operation data based on Spatiotemporal correlation constraints. IEEE Access. 8, 224741–224749 (2020)
72. Gu, Y., et al.: Doubly-fed deep learning method for bad data identification in linear state estimation. J. Mod. Power Syst. Clean Energy. 8(6), 1140–1150 (2020)
73. Jolfaei, A., Kant, K.: On the silent perturbation of state estimation in smart grid. IEEE Trans. Ind. Appl. 56(4), 4405–4414 (2020)
74. Ayiad, M.M., Leite, H., Martins, H.: State estimation for Hybrid VSC based HVDC/AC: unified bad data detection integrated with Gaussian mixture model. IEEE Access. 9, 91730–91740 (2021)
75. Adepu, S., Mathur, A.: Distributed attack detection in a water treatment plant: method and case study. IEEE Trans. Dependable Secure Comput. 18(1), 86–99 (2018)
76. Haghnegahdar, L., Wang, Y.: A whale optimization algorithm-trained artificial neural network for smart grid cyber intrusion detection. Neural Comput. Appl. 32(13), 9427–9441 (2020)
77. Sun, C., et al.: Intrusion detection for cybersecurity of smart meters. IEEE Trans. Smart Grid. 12(1), 612–622 (2020)
78. Keshk, M., et al.: An integrated framework for privacy-preserving based anomaly detection for cyber-physical systems. IEEE Trans. Sustain. Computing. 6(1), 66–79 (2019)
79. Liu, S., Siano, P., Wang, X.: Intrusion-detector-dependent frequency regulation for microgrids under denial-of-service attacks. IEEE Syst. J. 14(2), 2593–2596 (2019)
80. Shi, J., et al.: Distributed data-Driven intrusion detection for sparse stealthy FDI attacks in smart grids. IEEE Trans. Circuits and Syst. II: Express Briefs. 68(3), 993–997 (2020)
81. Hu, Z., et al.: Intrusion-detector-dependent distributed Economic model predictive control for load frequency regulation with PEVs under cyberattacks. IEEE Trans. Circuits and Syst. I: Regular Papers. 68(9), 3857–3868 (2021)
82. Yang, T., et al.: WPD-ResNeSt: substation station level network anomaly traffic detection based on deep transfer learning. CSEE J. Power and Energy Syst. (2021)
83. Ferrag, M.A., Maglaras, L.: DeepCoin: A novel deep learning and blockchain-based energy exchange framework for smart grids. IEEE Trans. Eng. Manag. 67(4), 1285–1297 (2019)
84. Patel, A., Roy, S., Baldi, S.: Wide-area damping control resilience towards cyberattacks: A dynamic loop approach. IEEE Trans. Smart Grid. 12(4), 3438–3447 (2021)
85. Liu, Y., Chen, Y., Li, M.: Dynamic event-based model predictive load frequency control for power systems under cyberattacks. IEEE Trans. Smart Grid. 12(1), 715–725 (2020)
86. Yuan, H., Xia, Y.: Resilient strategy design for cyber-physical system under DoS attack over a multi-channel framework. Inf. Sci. 454, 312–327 (2018)
87. Shi, L., Li, Y., Ma, M.: Latest research progress of honeypot technology. J. Electron. Inf. Technol. 41(2), 498–508 (2019)
88. Nizam, S.A.S., et al.: Forensic analysis on false data injection attack on IoT environment. Int. J. Adv. Comput. Sci. Appl. 12(10), 265–271 (2021)
89. Iqbal, A., et al.: Identification of attack-based digital forensic evidences for WAMPAC systems. In: 2018 IEEE International Conference on Big Data (Big Data), pp. 3079–3087 (2018)

How to cite this article: Yang, T., Liu, Y., Li, W.: Attack and defence methods in cyber-physical power system. IET Energy Syst. Integr. 4(2), 159–170 (2022). https://doi.org/10.1049/esi2.12068