Hindawi
Complexity
Volume 2021, Article ID 6659879, 12 pages
https://doi.org/10.1155/2021/6659879

Research Article

Security Risk Analysis of Active Distribution Networks with Large-Scale Controllable Loads under Malicious Attacks

Jiaqi Liang,[1] Yibei Wu,[2] Jun'e Li,[1] Xiong Chen,[3,4,5] Heqin Tong,[3,4,5] and Ming Ni[3,4,5]

[1]*Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China*
[2]*Electric Power Research Institute of State Grid Jiangsu Electric Power Co., Ltd., Nanjing 211106, China*
[3]*NARI Group Corporation (State Grid Electric Power Research Institute), Nanjing 211106, China*
[4]*NARI Technology Co., Ltd., Nanjing 211106, China*
[5]*State Key Laboratory of Smart Grid Protection and Control, Nanjing 211106, China*

Correspondence should be addressed to Jun'e Li; jeli@whu.edu.cn

Received 23 November 2020; Revised 20 January 2021; Accepted 9 February 2021; Published 20 February 2021

Academic Editor: Xin Li

With the development of distributed networks, the remote controllability of the distributed energy objects and the vulnerability of user-side information security protection measures make distributed energy objects extremely vulnerable to malicious control by attackers. Hence, the large-scale loads may produce abnormal operation performance, such as load casting/dropping synchronously or frequent and synchronous casting and dropping, and hence, it can threaten the security and stable operation of the distribution networks. First, we analyze the security threats faced by industrial controllable load, civil controllable load, and the gains and losses of attacks on the distribution networks. Considering the factors of cyber attacks, we propose a control model and cyber attack model in active distribution networks (ADNs). And, three types of attacks that the target suffered are defined on the basis of "on" and "off" modes for control. Then, the controllable load was maliciously controlled as the research object, and a suitable scenario is selected. The impact of malicious control of the controllable load on the power supply reliability and power quality of the distribution networks are simulated and analyzed, and risk consequences for different types of attacks are provided.

1. Introduction

With the development of power grid, distributed generation (DG) provided to the distribution networks and suppling the power for surrounding users is an inevitable trend [1, 2]. Hence, the development of distributed energy storage (DES) and controllable load (CL) has greatly promoted the consumption of DG in the distribution networks. The DG, DES, and CL constitute the distributed energy objects in the ADNs. The coordinated control of distributed energy objects through the communication method greatly increases the flexibility and initiative of the distribution networks [3, 4]. However, it also introduces new security risks in the stable operation of the distribution networks. In the meantime, the development of the Internet of things (IoT) enables more and more distributed energy objects to be controlled by the users [5]. For example, DG can be owned by users or third-party companies. Smart homes are moving towards remote control via the Internet. Electric vehicle charging and discharging stations and the terminals of controllable industrial load may be physically touched by users [6]. Therefore, the vulnerability or deficiency of security measures on the user side may make distributed energy objects easier to be controlled by the attackers, which affects the security and stable operation of the distribution networks. If the DG is abnormally started or stopped due to malicious intrusion, the large-scale CLs are synchronously casted/dropped, there is frequent and synchronous casting/dropping caused by malicious controlling, or the DES has abnormal behavior because of cyber attacks, which will break the balance between the electricity supply and demand in the distribution networks. It also disrupts the security and stable operation of

the distribution networks, even causing power-grid cascading failures, collapses, and large-scale outages [7]. This impact may be amplified in ADNs with deep penetration of distributed energy objects.

With the increasing number of incidents of hostile forces attack on critical infrastructure through cyber space, it shows that the cyber attack through the intrusion of cyber space may have a serious impact on the physical system, such as the Iranian nuclear power plant uranium centrifuge damage in 2010 and the Ukrainian power grid outage in 2015 [8]. Therefore, when distributed energy objects suffer from attacks, how to ensure the security and stable operation of ADNs is an urgent problem.

The impact of cyber security risk on power grid operation has been paid more attention. Langner et al. [9] reviewed the process of malware intrusion from cyber technology layer and finally have studied the destructive effects on the physical layer. The Iranian nuclear power plant STUXNET incident is taken as an example, which illustrates the "cyber physical warfare" and related technology mechanism. The studies in [8, 10, 11] analyze the process of large-scale power-grid paralysis caused by hacker attack in Ukraine and put forward some thoughts on power-grid cyber security protection. Sun et al. [12] take the Ukrainian outage as an example and define a cyber-coordinated attack on the power system, which is characterized by devices launched from the cyber space and acting on the physical space. Dán et al. [13] pointed out that, with the development of control and communication technology, the primary power system and the secondary power system deeply interact with the cyber physical power system. When certain (some) equipment of the primary power system or the secondary power system is out of order (due to network attacks, natural disasters, etc.), the impacts caused by it are very likely to spread to the other party's network, causing cascading failure that can seriously impact the safe and stable operation of the power system and causing significant economic losses. Sridhar et al. [2] emphasize the importance of studying the potential impact of cyber attacks, and in order to ensure cyber security, it is necessary to study the cyber-physical relationship of smart grid and the possible attack paths. Rasim et al. [14] illustrate the transmission mechanism of cyber security risks in ECPS and explain the cyber security risks in ECPS and the role of cyber space in physical space with the characteristics of cross-space transmission. Dong et al. [15] analyze the attack modes on ECPS from the perspective of attackers, including attack modes and their harms selected to achieve different goals. However, this kind of research is still relatively preliminary and focuses on general issues. The specific modes of cyber security attacks and their effects on the stable operation of the power grid have not been excavated, and hence, targeted security defense strategies cannot be established. Komninos et al. [16] investigated a number of attacks on smart grid from direct load shifting to smart meter data manipulation. Specifically, in single, small-scale attacks, adversaries can control certain IoT devices, such as smart homes in the smart grid. Using their control, an adversary can induce an abnormal working state in the device, increasing the power usage of the household. In certain cases, aggressive adversaries can cause damage to the devices and their surroundings and even threaten the personal safety of users [17–20]. In terms of large-scale cyber attacks, adversaries can compromise many high-wattage IoT devices to manipulate the power demand in a larger smart grid. For example, Saleh et al. [21] demonstrated a large-scale attack model on real-world grids, using a botnet to turn on and off a large number of IoT devices synchronously, resulting in massive power fluctuations with the potential to cause a large-scale blackout.

At present, there are few studies on the risk of distributed energy objects being maliciously controlled by the attackers. In the research of distributed energy objects in distribution networks, most of the research is on DG, but little about cyber security and cyber attacks [22, 23]. Murty et al. [24] study the impact of DG connection to the distribution networks, which is mainly due to the random fluctuation of DG and has nothing to do with malicious control. Nikolaidis et al. [25] design the protection schemes of the distribution networks with DG, and these schemes are mainly based on the conventional failure of power grid, without considering cyber attacks from the cyber space. Clement-Nyns et al. [26] study the impacts of a large scale of electric vehicle power-charging connection to the distribution networks and propose intelligent charging strategies to optimize the distribution networks' operation, but the study does not consider the situation of charging stations under the cyber attacks. Munkhammar et al. [27] propose the residential electricity-consumption probability model based on residents' habits and formulate a load demand response plan so that residential loads can become participants in optimizing the operation of the distribution networks. Although this behavior may have an impact on the distribution network, unlike the load being maliciously controlled, such impact can be reduced through the policy guidance of the power company [28, 29].

It can be seen that the current research is mainly focused on the active application of communication control methods in the distribution networks, such as demand-side management (DSM), "source" and "load" optimization control, and microgrid control strategies. The security risk introduced to the distribution networks by the popularization of communication technology is seldom considered from the perspective of the attackers. The diversity of access components for the distribution networks increases the difficulty of unified management. Generally, the operating status of the distribution networks is determined by the regulation of the power grid side and the load usage of the user side. Mohsenian-Rad et al. [17] pointed out that the attacker would break the normal order of power grid load management, but this research only considered the attacks on the load management system by penetrating the cyber network and did not consider the security risk of the load being maliciously controlled. Adrian et al. [30] analyzed the risk of large-scale controllable loads in the malicious attack scenario, but they did not analyze the response characteristics of controllable loads. Zhang et al. [31] used ultrasound to activate the voice recognition system of the smart homes and

remotely manipulate voice assistants such as Siri and Hivoice in order to disrupt the distribution network operation. The studies in [30, 31] show that if the attackers can maliciously control cell phones and send turn "on"/"off" commands to smart homes successfully, it can result in a serious imbalance of the power flow in the 10 kV feeder line and bring serious security risks to the safety and stable operation of the distribution network. To sum up, there are few literature works on the impacts of cyber attacks from the user side on distribution networks.

Through the analysis of the above research status, it can be seen that there are few literature works considering the cyber security on the ADNs [32]. The large-scale access of CLs and high-permeability access of DGs are inevitable trends in the development of the distribution networks. Therefore, this paper analyzes the security threats faced by distributed energy objects in ADNs and establishes control models and attack models within ADNs. Then, we focus on this problem through analyzing the impact of large-scale CLs being maliciously controlled on the ADNs and explore abnormal operating characteristics of the ADNs caused by the CLs being maliciously controlled. Hence, this paper discovers the risks of ADNs and provides a basis for the research of ADNs' security control methods in order to help the further development of smart grids.

The rest of this paper is organized as follows: In Section 2, the security threat analysis is introduced. Section 3 considers cyber attacks with the control model, and the cyber attack model in ADNs are proposed. In Section 4, the impact of large-scale CL attacks on ADNs is analyzed. Finally, some conclusions are drawn in Section 5.

2. Security Threat Analysis

According to types of load application, CLs are divided into industrial controllable load and civil controllable load. Specifically, the industrial load is mainly controlled by the industrial control system of the load side, and the civil load is mainly controlled and used by residential users according to demand behavior.

2.1. Safety Threats to Industrial Controllable Load. Industry is of great significance in China's national economy. It is mainly engaged in large-scale production activities, and its electricity consumption accounts for about 70% of the total social electricity consumption. The scale of industrial load is very large, and the concentration ratio is very high. In fact, there is a corresponding control system, which is the industrial control system.

A typical industrial control system is shown in Figure 1, which consists of an enterprise information network, process control network, and field control network. The enterprise information network has traditional IT network attributes, such as mail sending and receiving feature, web browsing feature, enterprise resource planning (ERP), and manufacturing execution system (MES). The middle process control network is the bridge and link connecting the upper and lower layers of the network. On the one hand, it controls and dispatches the field control equipment at the bottom according to the upper-level production instructions, and on the other hand, it conducts real-time monitoring and data statistics on the production situation of the industrial site and provides information feedback for upper-level regulation. The field control network is located at the bottom of the industrial control system, which includes PLC (programmable logic controller), PAC (programmable automation controller), RTU (remote terminal unit), IED (intelligent electronic device), actuator, and other control equipment.

In the past, industrial control systems were physically isolated from external networks. The development and popularization of information communication technology (ICT) has made the field of industrial control increasingly open, and its degree of interaction with the information field has also increased. However, the internal network of the industrial control system does not perform encryption control on the data flow. Usually, as long as the user enters the internal network, any of the network equipment can be accessed, which also leads to a drop in network security [33]. In addition, because industrial control mainly considers functionality, the system behavior characteristics based on this principle and the role characteristics of behavior control personnel are more likely to become the entry point for attackers to intrude into the control system.

The requirement of industrial intelligence has promoted the development of open control systems with modular, reconfigurable, and expandable characteristics. The control network of the open control system has the opening characters. For example, the core components of the open control system are the industrial PC, which are based on the Windows-Intel platform. And, the industrial ethernet is widely used for communication between the components. At the same time, the BUS technology applies embedded systems to field control instruments [34]. In the abovementioned cases, there are loopholes in many systems, such as PC operation system, communication protocol with TCP/IP, and the embedded operation system. Meanwhile, the security protection measure of the industrial control system is mainly based on isolation from other systems, but the underlying security is more vulnerable than other information systems, and it is not subject to the information security policy of the grid management department. Therefore, the industrial controllable load is extremely vulnerable to be attacked by internal workers or external attackers [35] and this, in turn, makes the stable operation of the distribution network affected.

2.2. Security Threats to Civil Controllable Load. The civil controllable load is represented by smart homes. Smart home takes residential buildings as the platform, uses the IoT technology (including integrated wiring technology, network communication technology, and automatic control technology) to realize the interconnection of control terminals and smart homes, and realizes information exchange through the control platform. The control core of the smart home is the control platform, which is implemented by an

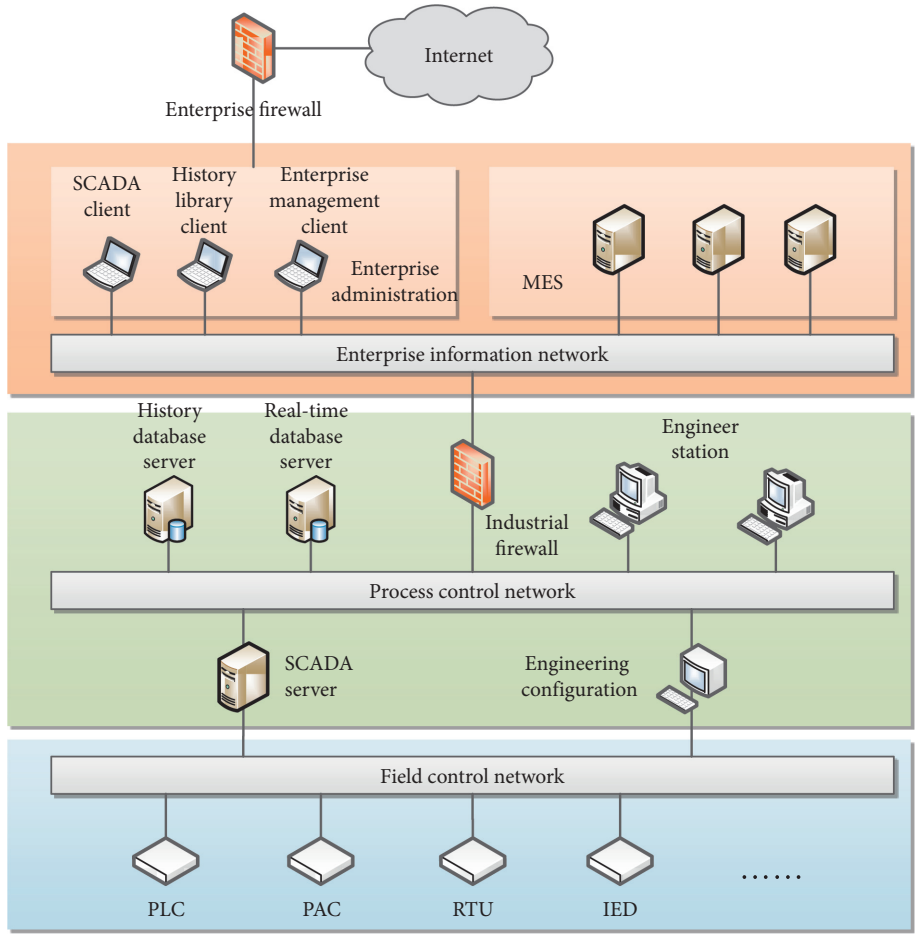

Figure 1: Industrial control system.

embedded microprocessor and can be connected to a control terminal (mobile phone or PC) via the Internet to achieve remote control. The control system of the smart home adopts a three-layer structure design [36]. As shown in Figure 2, the core is the control platform, which is implemented by an embedded microprocessor. It can be connected to the control terminal (mobile phone or PC) via the Internet for remote controlling [37]. However, the smart home control system has almost few security protection measures. According to the characteristics of network composition, the attacker has two attack paths. The first path is to use the loopholes of the embedded system, implant malicious codes into the control platform through the public network, and directly attack the internal network of the control system, to make the smart home work in an abnormal condition. The second path is to intrude the user's control terminal. At this point, the attackers implant malicious codes into smart terminals, such as mobile phones and PCs, and the terminal issues abnormal control commands to the control platform, which eventually leads to abnormal behavior of the smart homes. When the number of the maliciously controlled smart homes is large enough, it leads to the change in load of the distribution networks suddenly and it may affect the reliability of power supply and power quality.

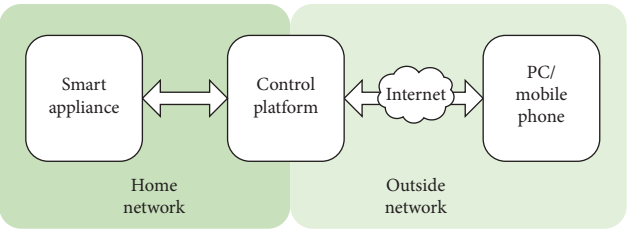

Figure 2: Smart home control system.

In summary, because the industry plays an important role in the national economy, the information security protection requirements of industrial control systems are relatively high, which leads to the cost of attacks become high accordingly. Most of the civil CLs represented by smart homes are not embedded with security mechanisms, and they can be connected to the public network with a long online time. Hence, the cost of the attack becomes extremely low, and the purpose of the attack is easy to realize. Compared with industry load, the security risk of CLs is very low. If a large-scale CL is subjected to malicious control and changes, due to the objective and unpredictable capacity, it will inevitably impact the normal operation of the distribution networks and may even cause cascading failures and

expand the scope of influence. Therefore, this paper selects CLs as the object of cyber attack for subsequent research and analysis.

3. Considering Cyber Attack with the Control Model and the Cyber Attack Model in ADNs

3.1. Control Model. The evaluation index of the distribution network includes power supply reliability, economy, security, and power quality, which are called the controlled variable and are represented by $\boldsymbol{S}$. In general, these controlled variables are determined by the electric power company, such as protection action, dispatching control, and user behavior. The connection of distributed energy objects has increased the initiative of the distribution network and promoted the development of control method diversity. Once large-scale distributed energy objects are controlled by the attackers, the dynamic balance of the distribution network may be disrupted, which can affect the normal operation of the distribution network. Attack behavior is different from normal dispatching, protection, and user behavior because it is unpredictable. Therefore, the distribution network control model with CL is shown in Figure 3, and the controlled variable is as follows:

$$S = f(g, d, u, A). \tag{1}$$

Here, g is the protection action, d isthe dispatching control, u is the normal user behavior, and A is an attack behavior.

Equation (1) is a nonlinear equation. The solution of the equation is related to the input (g, d, u, A) and the initial state of the distribution network. In the traditional distribution network, there is no attack behavior against load, and user behavior is reflected in daily life and production activities. It is a random variable that conforms to a certain law. In the meantime, the distribution network is mainly controlled by dispatching and protection action. According to the state-detection variable, the dispatching system and protection device control the distribution network, which ensures that the controlled variable S meets the requirements of the stable operation of the distribution network. In the distribution network with CLs, the added attack behavior is issued by the attackers and the distributed energy object is used as the attack object. Therefore, the DG and load dynamic balance are broken, and it is also not regulated by the power company. Finally, it may cause the controlled quantity S to deviate from the requirements of security and stable operation of the distribution network, causing safe and stable accidents.

3.2. Attack Model. The cyber attack model contains cyber element $\{M, T\}$ and physical element $P(t)$ and is defined as a double set A_u, which represents the impact mechanism of the attack from the cyber space and acts on the physical space. The attack model in which the CLs are maliciously controlled can be expressed as follows:

$$A_u = \{M, T\} \longrightarrow P(t). \tag{2}$$

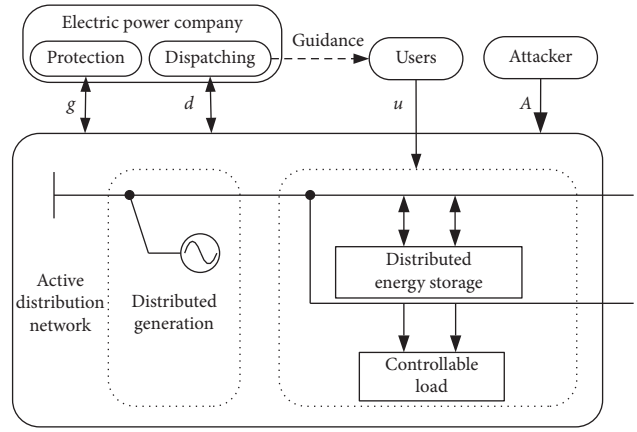

Figure 3: Distribution network control model with CLs.

Here, M is the control command, which is sent by the attackers, such as "on"/"off" represented as command M_{on}/M_{off}, namely, $M = \{M_{\text{on}}, M_{\text{off}}, \ldots\}$. Next, T is the sending time of the control command because the sending time of the cyber command has discrete characteristics, so let $T = t[n]$, where $n = 0, 1, 2, \ldots, n$, and $t[n]$ could be the sequence of time, which is sent from the control command. When large-scale CLs are maliciously controlled by cyber attacks, they are directly manifested as changes in the distribution network load. $P(t)$ is used to represent the load of the distribution network, and the symbol "$\longrightarrow$" represents the mapping relationship between the cyber attack of the information system and the load change of the power system.

Consider that after the malicious control commands are issued, some loads do not change the operating state. So the effective load control rate α is introduced; consider that the network delay and other factors may cause some control commands to be invalid and an effective attack rate β is introduced. So, $P(t)$ is composed of the normal operating load $P_0(t)$ and abnormal operating load $\Delta P(t)$. Hence, the abnormal operating load $\Delta P(t)$ can be expressed as follows:

$$\Delta P(t) = \alpha\beta P_0(t). \tag{3}$$

In this paper, we consider the abnormal operation performance of CLs, such as loads casting/dropping synchronously or frequent and synchronous casting and dropping, and based on these performances, we classify the attacks into three categories accordingly. The details are as follows.

3.2.1. Attack of Loads Casting Synchronously. At a certain point, attackers send M_{on} (synchronously "on," $M = \text{M}_{\text{on}}$) commands to massive CLs. And, attack behavior can be expressed as A_u^{I}. In the meantime, $P(t)$ increases immediately, which can be expressed as follows:

$$P(t) = P_0(t) + \Delta P(t) = P_0(t) + \alpha\beta P_0(t). \tag{4}$$

In the sequence $t[n]$ of control command-sending time, $n = 0$ is the simplest form of attack of loads casting synchronously; when $n \neq 0$, the attack is to keep sending the M_{on}

command and the ADN is kept in a high-load state for a long time.

3.2.2. Attack of Loads Dropping Synchronously. At a certain point, attackers send M_{off} (synchronously "off," $M = M_{\text{off}}$) commands to massive CLs. And, attack behavior can be expressed as A_u^{II}. In the meantime, $P(t)$ reduces immediately, which can be expressed as follows:

$$P(t) = P_0(t) - \Delta P(t) = P_0(t) - \alpha\beta P_0(t). \tag{5}$$

In the sequence $t[n]$ of control command-sending time, $n = 0$ is the simplest form of attack of loads dropping synchronously; when $n \neq 0$, the attack is to keep sending the "M_{off}" command and the ADN is kept in a low-load state for a long time.

3.2.3. Attack of Loads of Frequent and Synchronous Casting and Dropping. Attackers send M_{on} and M_{off} (frequently and synchronously "on and off," $M = M_{\text{on}}$ and M_{off}) commands periodically to massiv CLs, which leads to frequent and synchronous casting and dropping of loads. And, attack behavior can be expressed as A_u^{III}. In the meantime, $P(t)$ increases and drops frequently and synchronously. If we define M_{on} command at $t = [2i]$ and send M_{off} command, while $t = [2i + 1]$, the control command M can be expressed as follows:

$$M = \begin{cases} M_{\text{on}}, & T = [2i], \\ M_{\text{off}}, & T = t[2i + 1], \end{cases} \quad i = 0, 1, 2, \ldots, \tag{6}$$

At first, attackers send M_{on} command at $t = [2i]$ and the $P(t)$ will be increased $\alpha\beta P_0(t)$. Then, attackers send M_{off} command while $t = [2i+1]$ and $P(t)$ will be increased $\alpha\beta P_0(t)$, because CLs can be controlled by attackers. At M_{off} command, $\alpha = 1$ and $P(t)$ will be reduced to $\beta P_0(t)$.Therefore, $P(t)$ can be expressed as follows:

$$P(t) = \begin{cases} P_0(t) + \alpha\beta P_0(t), & t \in (t[2i]), \\ P_0(t) + \alpha\beta P_0(t) - \beta P_0(t), & t \in (t[2i + 1]), \end{cases} \quad i = 0, 1, 2, \ldots, \tag{7}$$

The attackers, through setting the time interval τ ($\tau = t[n] - t[n-1]$, $n = 1, 2, 3, \ldots$) in the attack command M, can change the casting and dropping frequency of CLs and lead to abnormal performance of those CLs. It may also cause problems such as resonance in serious cases.

4. Analysis on the Impact of Large-Scale CL Attacks on ADNs

The risk of the ADNs was greatly increased when the large-scale CLs were controlled by attackers, and the power quality may also be affected. The attack also resulted in abnormal power consumption of the users and damaged the power supply equipment in severe cases. Therefore, we take the impact of attacks on power quality as an example, and the 10 KV IEEE 33-bus standard distribution system was used as the study case, as shown in Figure 4. Finally, we consider a single DG connected at the end of the line and analyze the impact of the malicious attacks.

4.1. Impact of Load-Casting Attack on Power Quality. Scenario 1: node 18 of the IEEE 33-bus standard distribution system is connected to the DG, and the penetration rate is 100%. Nodes 18, 20, 25, and 30 suffered A_u^{I} attacks ($n = 0$ and $\Delta P/P_0 = 1$).

The node branch model in the ADN is shown in Figure 5. The power flow of branch b_{ij} is from node i to node j. Based on power flow calculation, the voltage of node j can be expressed as follows:

$$V_j = V_i - \Delta V = V_i - \frac{P_j R_{ij} + Q_j X_{ij}}{V_N}. \tag{8}$$

Here, ΔV is the branch voltage drop and $V_N$is the nominal voltage. P_j and Q_j are the active and reactive power of node j, respectively; R_{ij} and X_{ij} are the resistance and reactance of the branch (i, j), respectively. According to the structural parameters of the ADN and the voltage of the power supply terminal, the voltage of each node can be calculated. When the ADN suffered A_u^{I} attacks and lead to increase of the node load, the line voltage dropped very fast and the receiving terminal voltage would also be decreasing, and so low-voltage overruns may occur. According to power quality specifications, the allowable deviation of 10 kV user voltage is ±7% of the system nominal voltage.

We assume that the load is twice the normal operating state after the attacks, and $P/P_N = 0.65$ at this moment. As shown in Figure 6, we obtain the node voltage situation curves, which represent the suffered distribution network before and after the attacks. According to the analysis of the node voltage situation curves, due to the increase of the load caused by the malicious attacks, the voltage of each node has dropped and caused addition of four new low-voltage overlimit nodes, and the power quality had been dropped as well. After further calculation, when $P/P_N > 0.52$ after the attacks, which led to the increase in the low-voltage out-of-limit node number, the power quality of these nodes does not meet the standard power quality.

Compared with the attack scenario of DG connected to the standard distribution system, the attackers need to attack a large-scale CL to make the voltage deviation go beyond the standard range. In addition, the newly added low-voltage overlimit nodes are on branches that do not include DG. Because the voltage is increased by the DG, after the cyber attacks, the voltage of the nodes with DG supply branches is at the allowable range of deviation.

We compare the node voltage distribution of the suffered branch before and after the attacks with the traditional distribution network under the same type of the attack. As shown in Figure 7, the conclusions can be drawn as follows:

(1) If the power line already contains DG and not considering the off-grid status, when it is subjected to A_u^{I} attack against CLs, the DG can be leveraged to improve the power quality of the distribution network and the line is not prone to low-voltage phenomenon.

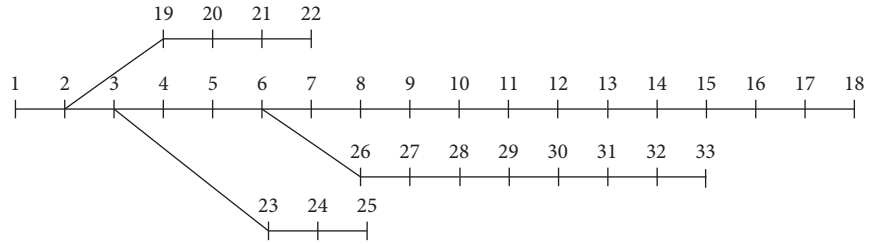

Figure 4: Diagram of IEEE 33-node standard distribution system.

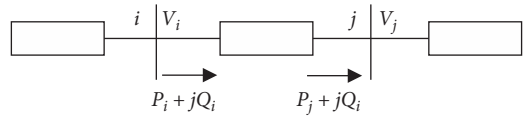

Figure 5: The node branch model.

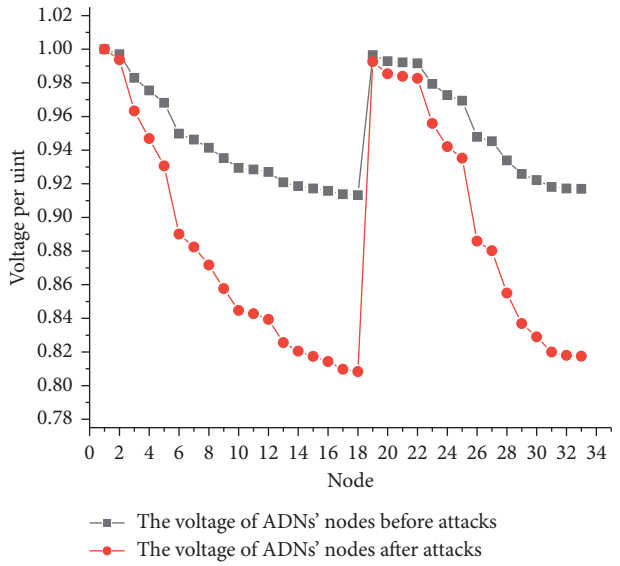

Figure 6: The voltage unit value of ADN nodes before and after A_u^{I} attack.

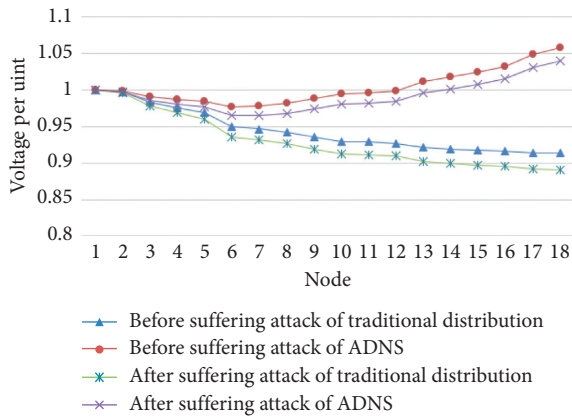

Figure 7: The voltage unit value of traditional ADN nodes before and after A_u^{I} attack.

(2) If the line contains DG and considering the off-line status, when it is subjected to A_u^{I} attack against CLs, DG may be out of operation after the attacks because of poor operation environment, and it can exacerbate voltage dropping and reduce power quality.

(3) If a DG is not connected to the power line, when it is subjected to A_u^{I} attack against CLs, the operation of the DG can be used as an adjustment strategy to improve power quality.

4.2. Impact of Load Dropping Attack on Power Quality. In the traditional distribution network, the voltage rise is caused by load dropping. However, there is only one power supply node on the power side, and it is also limited by the reference voltage. In the ADNs, DG can also provide electrical energy, if the voltage rise caused by the load dropping, it may cause high voltage to exceed the limit and reduce power quality.

Scenario 2: node 18 of the IEEE 33-bus standard distribution system is connected to the DG, and the penetration rate is 100%. Nodes 18, 20, 25, and 30 have suffered A_u^{II} attacks ($n = 0$, $\Delta P/P_0 = 1$).

In order to ensure the normal operation of the ADN, the load balance of each phase should be considered when we set up distribution lines for users. If there is load suffer due to A_u^{II} attack in this area and it is not evenly distributed on each phase line, it will cause unhomogeneous load distribution on each phase line and increases the degree of the three-phase imbalance, and while those disruptions are serious, it will also reduce the power quality.

The calculation of the three-term imbalance can be expressed as follows:

$$\varepsilon = \frac{I_2}{I_1} \times 100\%. \tag{9}$$

Here, I_1 is the effective value of the positive sequence component of the three-phase current and I_2 is the effective value of the negative sequence component of the three-phase

current. In the low-voltage power distribution system, the imbalance of the three-phase load current at the outlet of the distribution transformer should be less than 10%. For the convenience of quantification, assume that the attacked load is concentrated in one phase, that is, single phase.

In scenario 2, three-phase current on the secondary side of the transformer before and after the A_u^{II}attack is obtained through simulation, as shown in Figure 8. Before the attack, the effective value of the three-phase current $I_a = I_b = I_c = 850$ A and the degree of three-phase imbalance is 0; after the attack, the three-phase load is unbalanced, $I_a = I_b = 850$ A, and $I_c = 525$ A, and the three-phase imbalance is 14.8%. It can be seen that the three-phase balance before and after the attack exceeds the standard and the power quality does not meet the standard. Further calculation can be obtained, when single-phase $\Delta P/P_0 = 0.1$ and $\varepsilon = 10\%$. It can be obtained that when single-phase $\Delta P/P_0 > 0.1$, the three-phase imbalance degree exceeds the standard.

If the imbalance degree of three-phase voltage becomes very serious, it will increase line and transformer loss simultaneously and affect the safe operation of electrical equipment. Supplying power under unbalanced voltage conditions may easily cause the user's electrical equipment with a high-voltage one-phase connection to burn out, while the user's electrical equipment with a low-voltage one-phase connection may show abnormal work.

The suffered attack nodes dropped on a large scale in the distribution network. The voltage distribution of each node is shown in Figure 9. It can be seen that, after the A_u^{II} attacks, the voltage of each node is increasing, and the voltage per unit value of node 18 increases from 1.057 to 1.074, which has exceeded the allowable range of power quality voltage deviation and results in reduced power quality.

For the distribution network transformer, the excessive voltage not only reduced service life of transformers, but it may also cause resonance phenomena and harmonic pollution and disrupt other normally operating equipment. For electrical equipment, the excessive voltage can affect the normal operation, while the electrical equipment operated with high voltage for a long time would show reduction in service life and increase in power consumption.

To change the attack intensity, the voltage of each node is shown in Figure 10, where the corresponding attack modes from decentralized attacks to no attacks of the curve are described as follows:

(1) The decentralized attacks: all the nodes with half of the load suffered the A_u^{II} attacks

(2) The centralized large-scale attacks: nodes 18, 20, 25, and 30 of the IEEE 33-bus standard distribution system suffered A_u^{II} attacks, and it resulted in large-scale load of attacked nodes tripping from the line $P/P_N = 0$

(3) The centralized small-scale attacks: nodes 18, 20, 25, and 30 of the IEEE 33-bus standard distribution system suffered A_u^{II} attacks, and it resulted in 50% load of attacked nodes tripping from the line

(4) No attacks

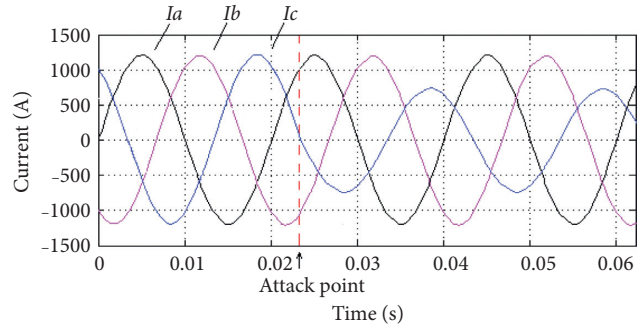

Figure 8: Three-phase current on the secondary side of the transformer before and after the A_u^{II} attack.

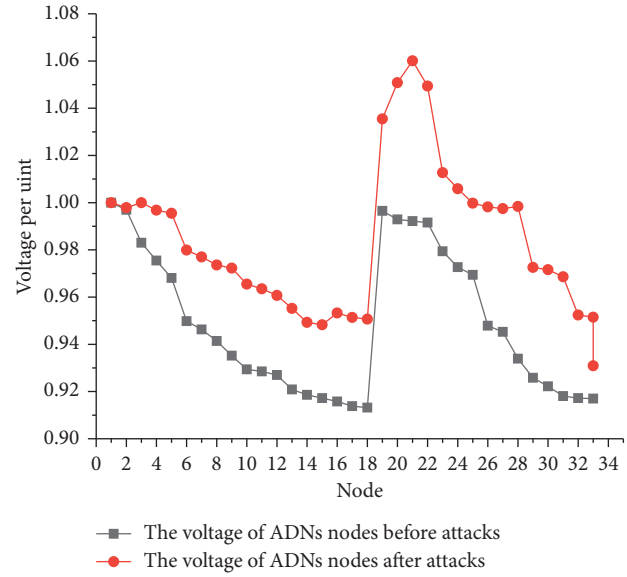

Figure 9: The voltage value of ADNs' nodes before and after A_u^{II} attack.

Among them, attack modes (1) and (2) caused the voltage to exceed the limits and reduced the power quality. Although attack mode (3) raised the node voltage, the voltage deviation index of the power quality still satisfied the specified range.

If the ADNs within a certain attack scenario, where the node 22 is connected to the DG, take this branch line as the analysis object, the voltage distribution of those nodes are shown in Figure 11. Although the node voltage increases are caused by the synchronous dropping attacks, the deviation index of the voltage still satisfied the specified range.

It can be seen that the deviation impact of A_u^{II} attacks on the load voltage of the distribution network is not only related to the attack intensity but also related to the topology of the distribution network.

4.3. Impact of Frequent Casting and Dropping of Load Attacks on Power Quality. Due to the DGs, the power system may be subjected to periodic disturbance of the load and it would cause power oscillation, that is, compelled resonance

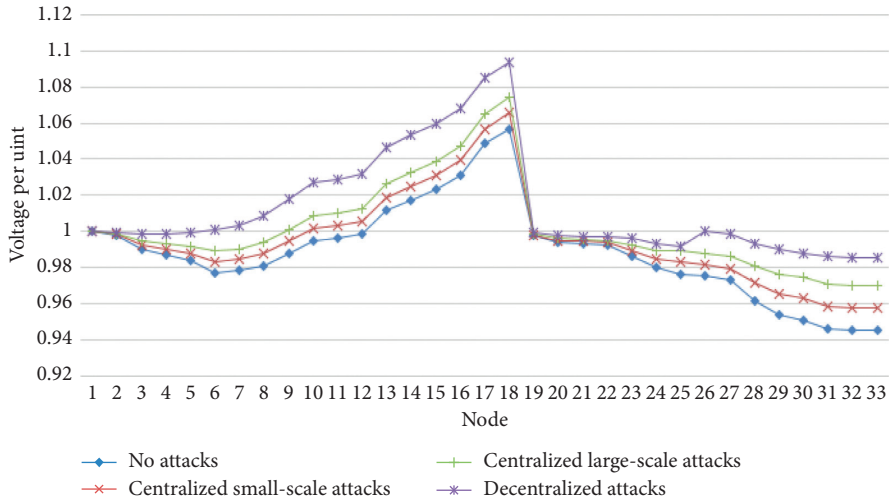

Figure 10: The voltage value of nodes before and after A_u^{II} attack under different attack modes.

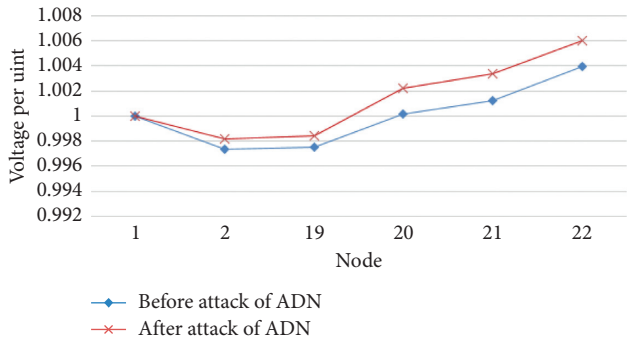

Figure 11: The partial node voltage before and after A_u^{II} attack.

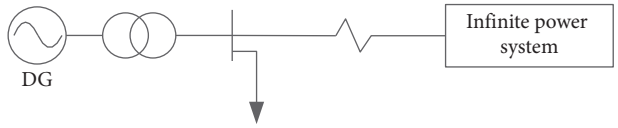

Figure 12: Single-machine (DG) infinite power system.

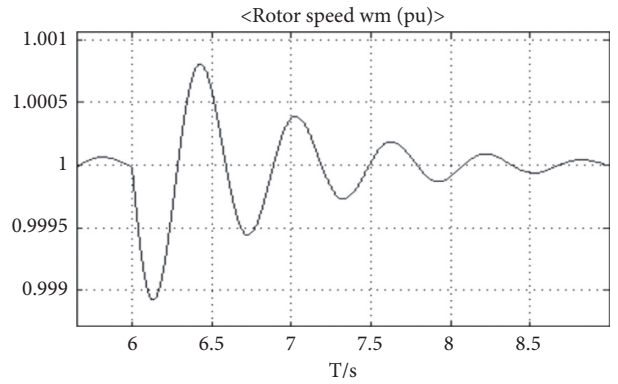

Figure 13: Rotation speed fluctuation after small disturbance.

low-frequency oscillation. The theory of compelled resonance low-frequency oscillation points out that regular small periodic disturbance in the system will cause the power oscillation. If the frequency of the disturbance is consistent with the natural frequency of the system, it will cause resonance, and the compelled oscillation amplitude of the system is the largest at this period.

Assume that the DG is directly connected to the power grid through the generator and select the connection node as a malicious attack object to construct a single-machine infinite system. As shown in Figure 12, the DG is connected into the distribution system through a 0.4 kV/10 kV booster transformer.

To cast small-scale load, while the system is running stably with light load, we can get the generator speed curve, as shown in Figure 13, and the natural oscillation frequency of the system is 1.67 Hz.

Scenario 3: the connection point of the DG suffered the A_u^{III} attack ($t[0] = 6$ s and $\Delta P/P_0 = 1$).

To change the frequency of "casting"/"dropping" of the load, while the same-scale load is attacked, we can obtain the line power curve as shown in Figure 14. When the command "on"/"off" is sent at $\tau = 0.3$ s intervals, as shown in Figure 14(a), the disturbance frequency is 1.67 Hz. When the command "on"/"off" is sent at $\tau = 0.26$ s intervals, as shown in Figure 14(b), the disturbance frequency is 1.87 Hz. When the command "on"/"off" is sent at $\tau = 0.34$ s intervals, as shown in Figure 14(c), the disturbance frequency is 1.47 Hz.

Due to the disturbance frequency being equal to the natural frequency of the system, it results in the largest amplitude of the power fluctuation; when the deviation between the disturbance frequency and the natural frequency of the system increases, the power oscillation curves can also be obtained, but the amplitude of this one is relatively small. And, the amplitude of power oscillations is also related to the scales of the attack load. Compared with Figure 14(a). While the scale of the attack load becomes 50%, the frequency of periodic disturbance is still 1.67 Hz and the oscillation amplitude becomes relatively small, as shown in Figure 15.

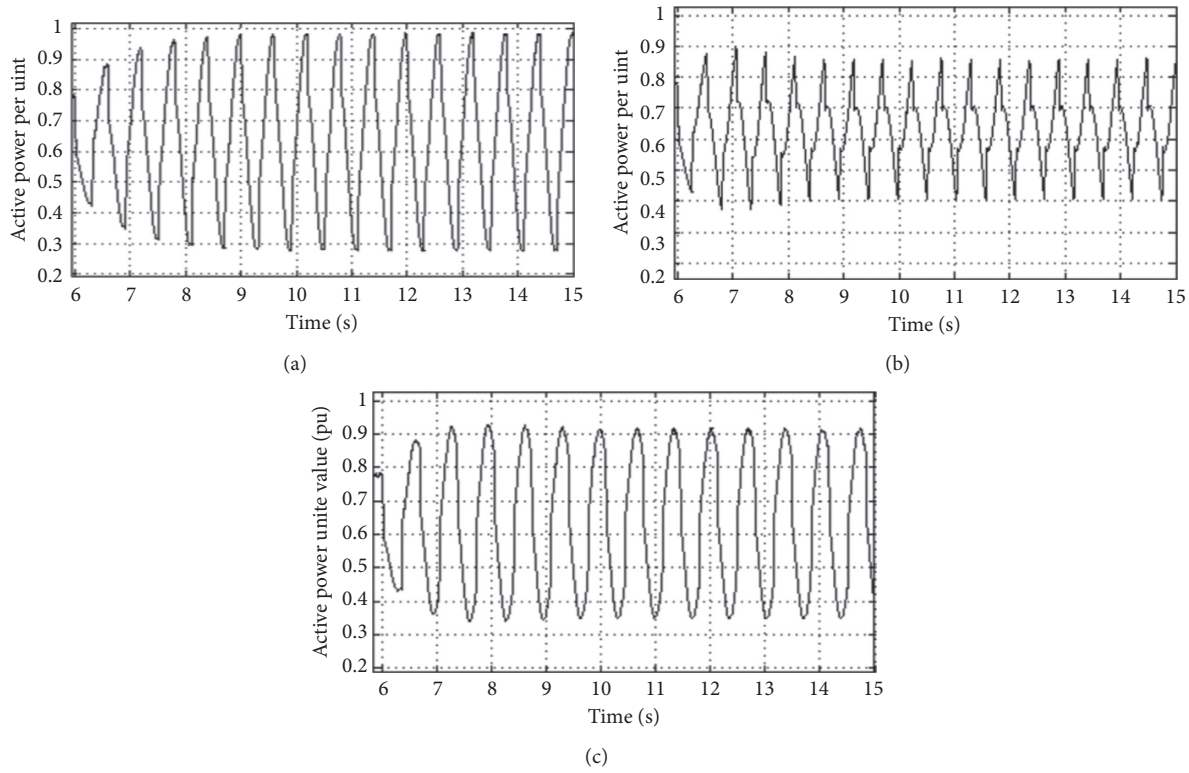

Figure 14: The active power oscillation curve of the line under different disturbance frequencies of (a) 1.67 Hz, (b) 1.87 Hz, and (c) 1.47 Hz.

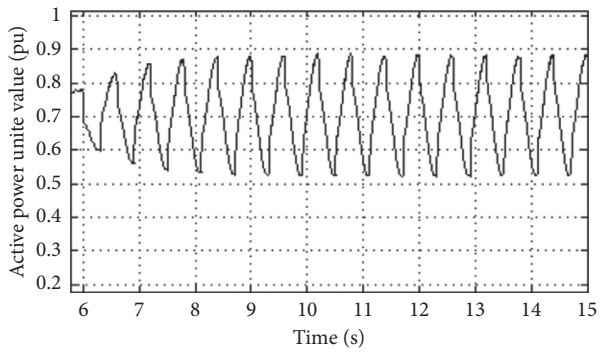

Figure 15: The active power oscillation curve of line under small-scale load attack with a disturbance frequency of 1.67 Hz.

In the traditional distribution network, the load mainly consumes electrical energy passively, and it is usually far away from the generator, with relatively scattered distribution, and it is not easy to have large-scale synchronous "casting"/"dropping". However, with the development of DG connected to the power grid and CLs, it makes the distance between the load and the generator become closer and the load would be maliciously controlled by the attackers. If the large-scale CLs are maliciously controlled and the frequency of periodic "casting" and "dropping" is close to the natural frequency of the system, it may amplify the impact of power fluctuation and affect the power quality of the distribution network.

4.4. Summary on the Influence of CLs by Malicious Control on ADNs. The power quality impact of CLs maliciously controlled by attackers on ADNs can be summarized in Table 1. Compared with the power quality of the distribution network without DG, the DG connected to the power grid can be leveraged to improve the power quality of the distribution networks, such as improving the condition of low-voltage cross-limits. However, while the CLs suffered unpredictable cyber attacks, it can result in dropping or casting of the large-scale CLs frequently and synchronously and the reliability of the distribution network is also reduced. In summary, those impacts can cause power quality problems, such as voltage deviation and voltage fluctuation, and even introduce new

Table 1: Distribution network control model with CLs.

Scenarios	Attack behaviors (A)		Risk	
	Attack object	Type of attack	Scale	
IEEE 33-bus standard distribution system	Node 18/20/25/30	A_U^{I}	$1.2 > P/P_N > 0.42$	Low-voltage exceeding limits
IEEE 33-bus standard distribution system	Node 18/20/25/30	A_U^{II}	Single-phase $\Delta P/P_0 > 0.1$	High-voltage exceeding limits
Single-machine (DG) infinite power system	DG access node	A_U^{III}	$1.2 > P/P_N > 0.5$	Power fluctuation and resonance

power quality issues (such as forced resonance at low frequencies). In addition, the impact of cyber attacks on the power supply quality of ADNs is not only related to the attack modes but also related to the topology of the distribution network (such as the connection points of DG). In order to ensure the normal operation of the ADNs, the risks introduced by cyber attacks must be considered.

5. Conclusions

The introduction of distributed energy objects and the full application of communication technologies make distribution networks face new security risks. In this paper, we analyze the security risks of industrial CLs and civil CLs in the distribution networks and compare the revenue and cost of attacks from the perspective of attackers. It can be seen that the cyber attack against civil CLs can obtain a large attack revenues with a small attack cost. Then, an ADN control model considering cyber attacks is established, and at the same time, the attack behavior model is also established. In these models, it provides a clear representation of the attack object, the attack method, and the across-space impact mechanism. Taking power quality as an example, the impacts of A_U^{I}, A_U^{II}, and A_U^{III} attacks on ADNs are analyzed. In summary, the result shows that DG connected to the power grid can improve power quality, but once large-scale CLs are suffered by cyber attacks, it may also cause power quality problems and may introduce new problems, such as low-frequency compelled oscillation.

In the future, there is still a lot of work to be done against the potential security risks of the ADNs introduced by distributed energy objects. Based on the existing research results, we can continue to study the impacts of cyber attacks against civil CL on the security and stable operation of the ADNs such as refining attack models, enriching attack scenarios, and exploring the ADN operation characteristics after the attacks. In order to provide a reference for the power grid to improve its operation control strategy and formulate user-side cyber security standards, we should fully grasp the risks introduced by the CL to the ADNs. In other words, we can refer to the ADN security risk analysis of the scenario where the CLs have suffered malicious control and carry out research on other energy objects in the ADNs as the attack object. In addition, further research on the power grid cascading failures caused by cyber attacks on distributed energy objects can provide a reference for the security and stable operation of the entire power grid.

Data Availability

The data used to support the findings of this study are currently under embargo, while the research findings are commercialized. Requests for data after publication of this article will be considered by the corresponding author.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this manuscript.

Acknowledgments

This work was supported by the Science and Technology Project of State Grid Corporation of China (Research on Cooperative Situation Awareness and Active Defense Method of Cyber-Physical Power System for Cyber Attack; no. SGJSDK00KJJS1800315).

References

[1] Q. Wang, W. Tai, Y. Tang, and M. Ni, "Review of the false data injection attack against the cyber-physical power system," *IET Cyber-Physical Systems: Theory & Applications*, vol. 4, no. 2, pp. 101–107, 2019.

[2] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, 2012.

[3] M. S. Mahmoud, M. M. Hamdan, and U. A. Baroudi, "Modeling and control of cyber-physical systems subject to cyber attacks: a survey of recent advances and challenges," *Neurocomputing*, vol. 338, no. 2, pp. 101–115, 2019.

[4] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, and A. K. Srivastava, "Analyzing the cyber-physical impact of cyber events on the power grid," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2444–2453, 2015.

[5] Y. Cai, Y. Cao, Y. Li, T. Huang, and B. Zhou, "Cascading failure analysis considering interaction between power grids and communication networks," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 530–538, 2016.

[6] F. Liang, W. Yu, X. Liu, D. Griffith, and N. Golmie, "Toward edge-based deep learning in industrial Internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4329–4341, 2020.

[7] Z. Wang, M. Rahnamay-Naeini, J. M. Abreu et al., "Impacts of operators' behavior on reliability of power grids during cascading failures," *IEEE Transactions on Power Systems*, vol. 33, no. 6, pp. 6013–6024, 2018.

[8] D. E. Whitehead, K. Owens, D. Gammel, and J. Smith, "Ukraine cyber-induced power outage: analysis and practical

mitigation strategies," in *Proceedings of the 2017 70th Annual Conference for Protective Relay Engineers (CPRE)*, pp. 1–8, College Station, TX, USA, April 2017.

[9] R. Langner, "To kill a centrifuge: a technical analysis of what Stuxnet's creators tried to achieve," Technical Report, Langner Communications, Norderstedt, Germany, 2013.

[10] J. E. Sullivan and D. Kamensky, "How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid," *The Electricity Journal*, vol. 30, no. 3, pp. 30–35, 2017.

[11] R. M. Lee, M. J. Assante, and T. Conway, *Analysis of the Cyber Attack on the Ukrainian Power Grid*, SANS Industrial Control Systems, Bethesda, MD, USA, 2016.

[12] C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: state-of-the-art," *International Journal of Electrical Power & Energy Systems*, vol. 99, no. 4, pp. 45–56, 2018.

[13] G. Dan, H. Sandberg, M. Ekstedt, and G. Bjorkman, "Challenges in power system information security," *IEEE Security Privacy*, vol. 10, no. 4, pp. 62–70, 2012.

[14] A. Rasim, I. Yadigar, and S. Lyudmila, "Cyber-physical systems and their security issues," *Computers in Industry*, vol. 100, no. 4, pp. 212–223, 2018.

[15] P. Dong, Y. Han, X. Guo, and F. Xie, "A systematic review of studies on cyber physical system security," *International Journal of Security and Its Applications*, vol. 9, no. 1, pp. 155–164, 2015.

[16] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: issues, challenges and countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1933–1954, 2014.

[17] A.-H. Mohsenian-Rad and A. Leon-Garcia, "Distributed internet-based load altering attacks against smart power grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 667–674, 2011.

[18] R. Chen, X. Li, and H. Zhong, "novel online detection method of data injection attack against dynamic state estimation in smart grid," *Neurocomputing*, vol. 344, no. 7, pp. 73–81, 2019.

[19] C. Fei, C. Patsios, P. C. Taylor, and Z. Pourmirza, "Using self-organizing architectures to mitigate the impacts of denial-of-service attacks on voltage control schemes," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 3010–3019, 2019.

[20] S. Khan, R. Khan, and A. H. Al-Bayatti, "Secure communication architecture for dynamic energy management in smart grid," *IEEE Power and Energy Technology Systems Journal*, vol. 6, no. 1, pp. 47–58, 2019.

[21] S. Saleh, M. Prateek, and P. H. Vincent, "BlackIoT: IoT botnet of high wattage devices can disrupt the power grid," in *Proceedings of the 27th {USENIX} Security Symposium ({USENIX} Security 18)*, pp. 15–32, Baltimore, MD, USA, May 2018.

[22] Z. Dong, M. Tian, and L. Ding, "A framework for modeling and structural vulnerability analysis of spatial cyber-physical power systems from an attack-defense perspective," *IEEE Systems Journal*, pp. 1–12, 2020.

[23] T. N. Boutsika and S. A. Papathanassiou, "Short-circuit calculations in networks with distributed generation," *Electric Power Systems Research*, vol. 78, no. 7, pp. 1181–1191, 2008.

[24] V. V. S. N. Murty and A. Kumar, "Optimal placement of DG in radial distribution systems based on new voltage stability index under load growth," *International Journal of Electrical Power & Energy Systems*, vol. 69, no. 3, pp. 246–256, 2015.

[25] V. C. Nikolaidis, E. Papanikolaou, and A. S. Safigianni, "A communication-assisted overcurrent protection scheme for radial distribution systems with distributed generation," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 114–123, 2016.

[26] K. Clement-Nyns, E. Haesen, and J. Driesen, "The impact of charging plug-in hybrid electric vehicles on a residential distribution grid," *IEEE Transactions on Power Systems*, vol. 25, no. 1, pp. 371–380, 2010.

[27] J. Munkhammar, P. Grahn, and J. Widén, "Quantifying self-consumption of on-site photovoltaic power generation in households with electric vehicle home charging," *Solar Energy*, vol. 97, no. 6, pp. 208–216, 2013.

[28] M. Singh, P. Kumar, and I. Kar, "A multi charging station for electric vehicles and its utilization for load management and the grid support," *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 1026–1037, 2013.

[29] M. P. Moghaddam, A. Abdollahi, and M. Rashidinejad, "Flexible demand response programs modeling in competitive electricity markets," *Applied Energy*, vol. 88, no. 9, pp. 3257–3269, 2011.

[30] D. Adrian, J. Ullrich, and E. R. Weippl, "Grid shock: coordinated load-changing attacks on power grids: the non-smart power grid is vulnerable to cyber attacks as well," in *Proceedings of the 33rd Annual Computer Security Applications Conference*, pp. 303–314, Orlando, FL, USA, September 2017.

[31] G. M. Zhang et al., "Dolphinattack: inaudible voice commands," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pp. 103–117, Dallas, TX, USA, November 2017.

[32] E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi, and C. Assi, "Communication security for smart grid distribution networks," *IEEE Communications Magazine*, vol. 51, no. 1, pp. 42–49, 2013.

[33] X. Chen, "Industrial control network information security threats and vulnerability analysis and research," *Computer Science*, vol. 39, no. 10, pp. 4188–4190, 2012.

[34] W. Knowles, D. Prince, D. Hutchison, and K. Jones, "A survey of cyber security management in industrial control systems," *International Journal of Critical Infrastructure Protection*, vol. 9, no. 1, pp. 52–80, 2015.

[35] C.-W. Disso, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Transactions on Power Systems*, vol. 23, no. 4, pp. 1836–1846, 2008.

[36] L. Sankar, S. R. Rajagopalan, S. Mohajer, and H. V. Poor, "Smart meter privacy: a theoretical framework," *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 837–846, 2013.

[37] M. Li and H.-J. Lin, "Design and implementation of smart home control systems based on wireless sensor networks and power line communications," *IEEE Transactions on Industrial Electronics*, vol. 62, no. 7, pp. 4430–4442, 2015.