energies

MDPI

Article

Stability Analysis of the Cyber Physical Microgrid System under the Intermittent DoS Attacks

Rong Fu [1,*], Xiaojuan Huang [1], Jun Sun [2], Zhenkai Zhou [1], Decheng Chen [1] and Yingjun Wu [1]

[1] College of Automation, Nanjing University of Posts and Telecommunications, Nanjing 210023, China; 15150568465@163.com (X.H.); zhouzhenkai@hotmail.com (Z.Z.); chendcg@163.com (D.C.); ywu_njupt@163.com (Y.W.)

[2] NARI Group Corporation State Key Laboratory of Smart Grid Protection and Control, Nanjing 211000, China; 13585102301@139.com

* Correspondence: furong@njupt.edu.cn; Tel.: +86-25-8586-6500

Academic Editor: Paras Mandal
Received: 14 January 2017; Accepted: 9 May 2017; Published: 12 May 2017

Abstract: Recent research has demonstrated the vulnerabilities of cyber physical microgrid to different rates of denial-of-service (DoS) attacks, which send internal requests to degrade the victim's performance. However, the interaction between the attacks and the security of microgrid remains largely unknown. In this paper, we address two fundamental questions: (1) What is the impact of intermittent DoS (IDoS) attacks on the security of cyber physical microgrid and (2) how can we analyze the stability of the cyber physical microgrid under IDoS attacks? To tackle these problems, we firstly model the cyber physical microgrid system considering the IDoS attacks on the network server. Based on the model, the interaction between the cyber system and the physical system is analyzed. Then, the impacts of IDoS attacks on the security of the cyber physical microgrid system are studied. It shows that the attack may lead to the system level oscillation with the information variation during the attack period. Therefore, a risk assessment method is proposed to investigate the stability of the cyber physcial microgrid system under IDoS attacks. Lastly, the proposed methodology is verified by simulation results.

Keywords: cyber physical microgrid system; intermittent denial-of-service attack; duration stages; security analysis

1. Introduction

In a microgrid system, the computing system, communication network and electric power physical system are integrated to form a multi-dimensional and heterogeneous complex system of real-time sensing, dynamic control and information service. Microgrid system usually consists of various distributed generations (DGs), storage devices and loads. It can operate in a grid-connected mode or an island mode, and smoothly switch between the two modes [1–3]. Recently, microgrid is considered as one of the most promising forms of smart grid [4–6]. From a grid point of view, microgrids can be viewed as control entities within the power system. From the customer's point of view, microgrids and traditional low-voltage distribution networks provide heat and power requirements [7]. By aggregating loads and multiple distributed energy resources, and renewable energy sources, the microgrid system has several main advantages: increasing the energy penetration of renewable energy sources, providing better energy supply in remote areas, and balancing power at the local level [8].

The stability and security are the prerequisites and constraints of the economic optimization of the microgrid [9,10]. Since the microgrid system has various types of components and complex characteristics, it is necessary to consider more factors, such as power balance, optimization, and rated value, which may affect the stability and the security of the microgrid. The problems associated with

the inherent uncertainties such as time delays, packet losses, and cyber attacks have been extensively investigated in the microgrid [11,12]. The cyber physical security issue has attracted increasing attention. Several works indicated that the dynamic performance of frequency control was affected by communication delays [13]. In [14], security vulnerabilities and some solutions were discussed for DC microgrids. Literature [15] introduced the fact that cyber attacks on the microgrid protection systems may mimic real faults, cause component failure, and disable the communication links. Those existing cyber vulnerabilities may allow an attacker to impact the cyber physical infrastructure network [16].

Microgrids take advantage of Information and Communication Technologies (ICT) to enable enhanced system monitoring and control. In order to fully realize the operation of microgrids, it is necessary to expand the cyber network inter-connectivity so that information may flow securely between the different domains in the microgrids. In recent years, different kinds of cyber threats or cyber intrusions have become challenging issues in power systems [17]. In 2015, the Ukrainian power grid was attacked by the cyber attackers, which was considered the first cyber attack event causing power blackouts [18]. Literature [19] proposed a communication network of the SCADA (Supervisory Control and Data Acquisition) system with advanced communication technologies. They applied a trust-based intrusion detection and prevention (IDP) technology built on a monitoring, detecting, and rehabilitation (MDR) approach for cyber security analysis. By further understanding the dynamic nature of the network under cyber-attacks, literature [20] used an improved SCADA model equipped with IDP technology to enhance the cyber security of the communication network in a residential microgrid.

The National Institute of Standards and Technology (NIST) No. 7628 report has pointed out that three elements of network security are confidentiality, integrity, and availability (CIA) [21]. The cyber attacks broadly refer to the malicious attacks that destroy the CIA security target of network. The cyber attacker typically attempts to track the behavior of the communication system through exploiting the security vulnerabilities of network infrastructures. Then, the control rights of the system can be obtained without permission, which may affect the normal operation of power system.

Several models were established to analyze power system security operation under attacks, such as Petri net theory [22] and attack tree model [23]. Petri net modeling is good at a description of the attack process, as well as the relationship between the states of conversion [24]. However, the simple Petri net model is not suitable for modeling multiple concurrent attacks. A colored Petri net and the time Petri net model need to be studied further. To enhance network protection against cyber attacks, a four-way handshake mechanism was proposed to establish a secure connection in communication [25].

Cyber attacks mainly include DoS attacks, error data injection attacks, malware and virus attacks. A DoS attack is a resource-exhausting attack that exploits the flaws of network protocol/software or sends a lot of useless requests to exhaust the resources of attacked objects, so that the server or communication network cannot provide normal services [26]. In the power system, DoS attacks exist in different network layers with different types. DoS attacks may occupy the bandwidth resources and make the normal users unavailable for receiving quality services. Traditionally, DoS attacks can be easily checked by the network monitors for their high sending rates. However, there exist some kinds of intermittent DoS (IDoS) attacks that are difficult to be detected due to their low average sending rates of intermittence. The IDoS attacks, unlike the flooding-based DoS attacks, send out high-volume requests at regular intervals to occupy the normal information transmission. They occupy the communication bandwidth and disturb the information transmission.

In this paper, the cyber physical microgrid system is modeled considering an IDoS attack on the network services. The interaction between the cyber system and the physical system is analyzed. The effect on cyber physical microgrid system is studied under the IDoS attack. The cyber security of the system is investigated with the proposed risk assessment method. The cyber physical microgrid simulation results are illustrated to show the effectiveness of the theoretical analysis method.

2. IDoS Attack in a Cyber Physical Microgrid

In this section, we illustrate the impact of the IDoS attack on a cyber physical microgrid system, and analyze the system characteristics during each attack scenario. Can the physical microgrid system remain stable under the IDoS attack? What is the state of the cyber physical microgrid system under the IDoS attack?

2.1. Intermitent DoS Attack Definition

Generally, the information flows are transmitted to the control center through the network servers, then are transformed into physical energy flows through a state estimator under the measure monitors, and are then finally delivered to the corresponding circuit breakers or actuators in the microgrid system. In addition, the normal request received by the cyber network is composed of a large number of data packets transformed by acquired power voltage, power and other energy values of power nodes. These data packets are collected by a variety of smart meters in the actual microgrid operation. Once the IDoS attack is initiated, the attacker could dynamically adjust the number of normal requested service replicas through changing the arrival rate of the burst sequence pulses with ineffective requests.

In this section, an IDoS attack is defined as a burst of request queues R sent to the network server with an arrival rate γ_a over a short period of time τ. For simplifying the discussion, we assume that the IDoS attack pulse is denoted as a Dirac signal with an arrival rate γ_a and then the information request $R = \gamma_a \tau$. An IDoS attack can impulse the interval pulses, and it is supposed that the IDoS attack pulses are imposed between a period of time T. Therefore, the IDoS attack can be modeled as a sequence of a signal impulse. If the attack pulses have the same arrival rates, the IDoS attack pulses reveal like a sequence of the signals: $\gamma_a \tau \delta(t - T_k)$, where T_k is the arrival time of the kth pulse.

Considering the communication availability, we assume that the arrival rate of normal requests and attack requests are constants γ_n and γ_a, respectively. Consequently, the arrival rate of requests can be described as:

$$\gamma(t) = \begin{cases} \gamma_n & t \neq T_k \\ \gamma_a + \gamma_n & t = T_k \end{cases} \tag{1}$$

2.2. Modeling of the IDoS Attack in the Cyber Network

Figure 1 illustrates the interaction between cyber network and physical network in microgrid under an IDoS attack [27,28]. In the cyber network, the network server is modeled by three components to transmit information: the admission controller C1, the network server S1, and the feedback measurements F1. In the physical network, the microgrid system is modeled by the admission controller C2, the physical system S2 and the feedback measurements F2. The interaction operation between cyber network and physical network are mainly transmitted through the measure monitors M1 and M2. We use the controllers to adjust the error signal (e1, e2) from a set of input values (X_1, X_2) to reach the reference objectives.

We assume that the IDoS attack pulse is denoted as a Dirac signal with an arrival rate γ_a. The actual information utilization $\rho(t)$ is related to the $n(t)$, and the number of network logged requests $n(t)$ is affected by the arrival rate of information requests involving the IDoS attack pulses. When $\rho(t)$ is deviated to the desired information utilization, the admission controller is employed to adjust the utilization deviation. Therefore, the system dynamic state can be described by the information utilization $\rho(t)$, the number of the network logged requests $n(t)$ and the admission rate $\alpha(t)$ as follows:

$$\alpha(t) = K_1(\rho^* - \rho(t)) + K_2(\rho(t) - \rho(t-1)) + \alpha(t-1), \tag{2}$$

$$\rho(t) = \begin{cases} An(t) + B & if\ n(t) < \nu \\ Cn(t) + D & if\ \frac{1-D}{C} \geq n(t) \geq \nu \\ 1 & if\ n(t) > \frac{1-D}{C} \end{cases}, \tag{3}$$

where ρ^* is the utilization objective; K_1 and K_2 are proportional integral (PI) controller parameters; and A, B, C and D are the coefficients of utilization curve.

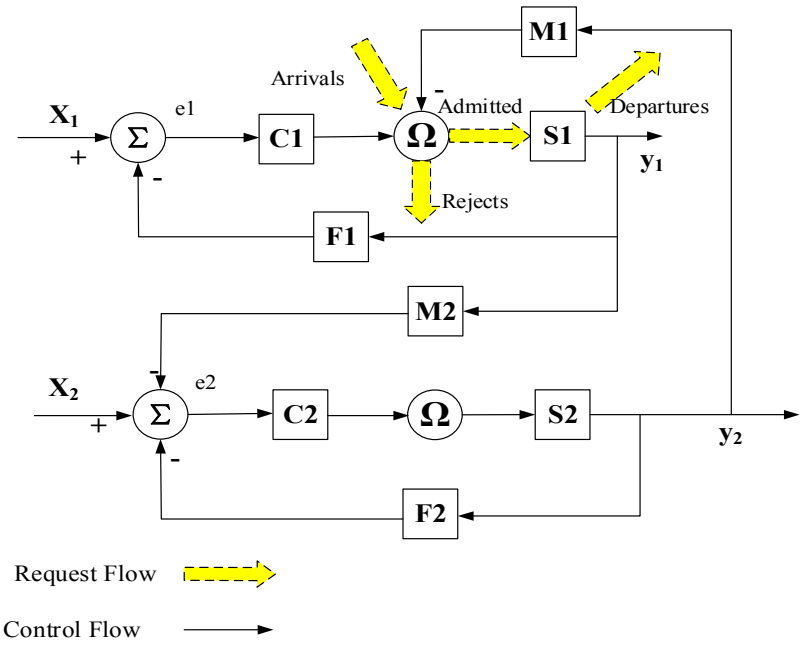

Figure 1. The interaction between the cyber network and the physical network in a microgrid.

Referring to the multiplicative-increase and multiplication-decrease policy, the number of requests admitted at time t can be given by the multiplication of admission ratio $\alpha(t)$ and the attack pulse parameter $\gamma(t)$. When an IDoS attacker transmits the intermittent pulses on the internet server, the actual information admission speed decreases, and the requests from normal users may be logged.

If $\rho(t)$ is larger than the server utilization limit ρ_0, the thrashing index w is used to multiply constant service rate index μ to represent the severity of degradation in service. Therefore, the evolution of the number of the network logged requests $n(t)$ can be expressed as:

$$n(t) = \gamma(t)\alpha(t) - \mu \times w + n(t-1). \tag{4}$$

Equations (2)–(4) show the relationship between the number of pending requests $n(t)$ and the server utilization $\rho(t)$. In the normal state, the normal information requests are $\rho^w \times t \times P_r(H/T)$ when γ equals γ_n, where H is the arrival information, P_r is the probability and ρ^w is the normal utilization in a period of time T. If there exist the attack, the actual information requests are $\rho'(t) \times t' \times P_r(H/T')$, where $\rho'(t)$ is the utilization in a period of time T'. To transmit the same information, the requests are the same as $\rho^w \times t \times P_r(H/T) = \rho'(t) \times t' \times P_r(H/T')$. Then, we can get the time value $t' = \frac{\rho^w \times t \times P_r(H/T)}{\rho'(t) \times P_r(H/T')}$. Thus, the information delay can be described as Δt as the difference between t' and t. The vulnerabilities of the cyber network under IDoS attacks are assessed when the periodic bursts of requests per second are sent over a short time duration in a period of time.

During the period of an IDoS attack pulse, the relationship of system state and the parameters of the attack is shown in Figure 2. The network server moves under different stages on the information utilization deviations when an attack pulse occurred at t = 0 s.

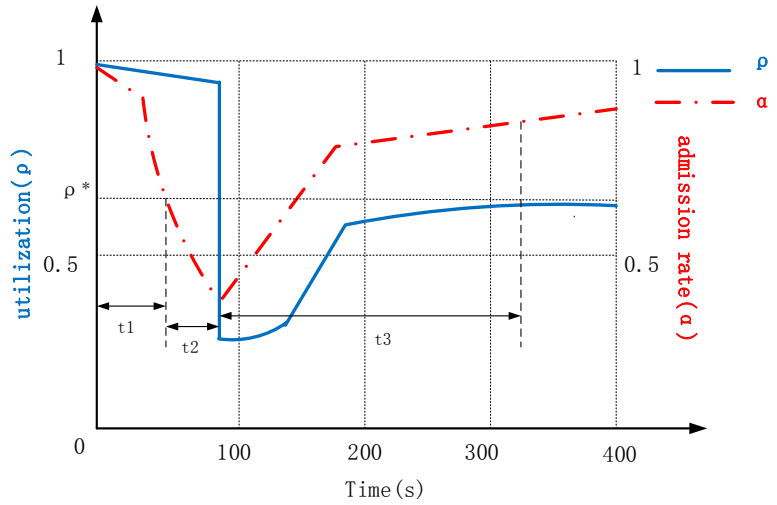

Figure 2. The duration stage of an IDoS attack pulse occurred at $t = 0$ s.

Once an attack pulse arrives, the server may move through three different stages before returning to the steady state: the arrival stage, the sustaining stage and the restoration stage. The arrival stage starts after the arrival of an IDoS attack pulse. During this stage, the utilization $\rho(t) \geq \rho^*$ and the admission rate decreases. When $\rho(t)$ is lower than ρ^*, the server enters the sustaining stage during which the admission rate keeps decreasing. In the restoration stage, the admission rate and the utilization rate restore to the steady state.

Arrival Stage: When an attack pulse arrives, the system responses from the initial state with normal utilization $\rho(t)$. The system state is characterized by the arrival rate of the requests. If $\rho(t) < \rho^*$, the controller detects the abnormal deviation and starts to control the process to interrupt this stage.

Sustaining Stage: At the beginning of this stage, because $\rho(t) < \rho^*$, $\alpha(t)$ stops decreasing and begins increasing. Consequently, $\rho(t)$ keeps on decreasing. The evolution of the system state is controlled by the admission controller. If $\rho(t)$ stops decreasing, the sustaining stage ends and then the system enters the restoration stage.

The variation of information requests lies in the system parameters and different conditions. If the pulse intermittent time is longer than the arrival stage, the controller stops attacking process, and the network sustains to recover from the network log time. If the pulse intermittent time is smaller, the network logged request decreases and the controller recovers the state automatically.

Restoration Stage: When the utilization rate stops decreasing, the system enters the restoration stage. The stage ends when the utilization reaches the desired value.

We illustrate the effect of an IDoS attack in these three stages. We use $t1$, $t2$ and $t3$ to denote the durations of these stages. Figure 2 demonstrates the admission rate's trajectory in the presence of the different kinds of IDoS attacks. If the attack duration time $\tau < t1$, a new attack pulse reaches during the arrival stage. The next attack pulse arrives, while the admission rate continues decreasing and the number of logged requests also decreases because less requests are admitted. If $\tau < t1$ holds for all of the attack pulses in extreme modes, $\alpha(t)$ will be kept at zero when the flooding-based IDoS attack occurs. Such kind of attack is not efficient because the majority of the attack requests will be detected and dropped. Therefore, the process can be continued to evolve as $t1 < \tau < t2$.

If $t1 + t2 < \tau < t1 + t2 + t3$, the next attack pulse arrives when the system is in the sustaining stage. In this case, the trajectory covers in these three stages. However, the admission rate cannot be restored to a desired one because the attack pulses occur in a short internal, which hampers the control process.

If $\tau > t1 + t2 + t3$, the evolution of the system involves all four stages: the arrival stage, the sustaining stage, the restoration stage and the steady stage. We can compute the time it takes for

the admission rate to recover and the number of rejected requests according to the above admission control model.

The contents of arrival packets are scrutinized by the Intrusion detection system (IDS) to find any suspicious activity. Most of the new IDoS attacks mimic the legitimate web service traffic, which leaves the traditional methods that are ineffective in detecting intrusions. Generally, the IDoS attacks typically last for 1 h sending ineffective requests to drop off legal internet services. Because the server may move through three different stages that have different duration times $t1$, $t2$ and $t3$ before returning to the steady state, the average rates of requests under attacks may change with intermittent pulse interval τ. If $\tau < t1$, $\alpha(t)$ will be kept at zero when the flooding-based IDoS attack occurs in extreme modes. Such kind of attack is not efficient because the majority of the attack requests will be dropped. Therefore, for a complete IDoS attack, the time interval τ satisfies $t1 + t2 < \tau < t1 + t2 + t3$.

The established microgrid model under IDoS attack illustrates the interactions between cyber network and physical network. To understand dynamic behavior that the network, in response to the erratic load, offered by legitimate requests, we tend to obtain static properties through aggregations over time scales that are long enough to hide the transients of adaptation. Therefore, the usual rate of normal requests refers to a point in time when the number of arrival requests composed of a large number of data packets are normal for the admission controller in the web server to allow a large percentage of all requests to go through. That is, the microgrid system operates in steady state.

Once the system suffers from an IDoS attack, a surge in arrival demanded requests with a short period of time would push the system into overload. This, in turn, would result in the admission controller shutting off subsequent legitimate requests for a long time. Given the fact that under overloaded conditions, the system operates in an inefficient region (e.g., due to thrashing). If the system "recovers" from the ill-effects of this unsuspected surge in demand, an attacker would simply repeat the process with intermittent time interval. Although simplistic, this behavior illustrates the exploited adaptation strategies by adversaries to reduce system stability.

Given the admission rate $\alpha(t)$ and arrival rate $\gamma(t)$ vary at time t, the number of requests admitted into a web server at time t is $m(t) = \alpha(t)\gamma(t)$, rather than the actual amount of arrival information requested $R = \gamma_a \tau$ over a short period of time τ. Considering the average service time T_S and the time on the round trip of subsequent data packets T_{RTT}, maximal simultaneous processing requests number is $[n(t) \cdot \frac{T_{RTT}}{T_S} + n(t)]$. Therefore, the boundary conditions for the impulses that could cause IDoS attacks are that:

(1) the web server reaches the maximum number of requests that can process;
(2) the intermittent stimulus impulses block the communication channel, which greatly reduces the number of legitimate requests;
(3) repeated attacks to the server over a long time make it overloaded, which causes the system oscillation due to an inefficient information transmission, i.e., communication delay.

3. Security Analysis of the Microgrid under IDoS Attacks

3.1. Modeling of the Microgrid System under IDoS Attack

The microgrid can integrate various kinds of distributed energy resources (DERs) such as photovoltaic arrays, wind turbines and batteries to supply loads more efficiently. The physical microgrid system consists of DERs, DC-AC inverters, filters and the local loads. Each DER unit supplies the loads connected on the point of common coupling (PCC) node. The integrated scheme of the cyber physical microgrid system is shown in Figure 3.

In the existing cyber physical microgrid (Figure 3), the communication requirements of the physical microgrid are supported by the network in the cyber system [29]. The data deliveries between utility grids and control centers involving fuel cell (FC), battery (BT), photovoltaic array (PV), and Load are dedicated in the independent cyber network, as shown in Figure 4. In Figure 4, smart meters S_i conduct real-time acquisition of the relevant ith DER and load nodes' power measurement data.

Formed information packets are transmitted to the control center (CC) after monitoring and processing module. These data packets are transformed into control instructions for each electrical device in the microgrid based on the real-time optimized operation target. Once the network server suffers from an IDoS attack, the information transmission channels are blocked, and the affected execution controller C_i cannot receive commands in a timely manner due to the communication delay that cause improper switch action for the breaker B_i.

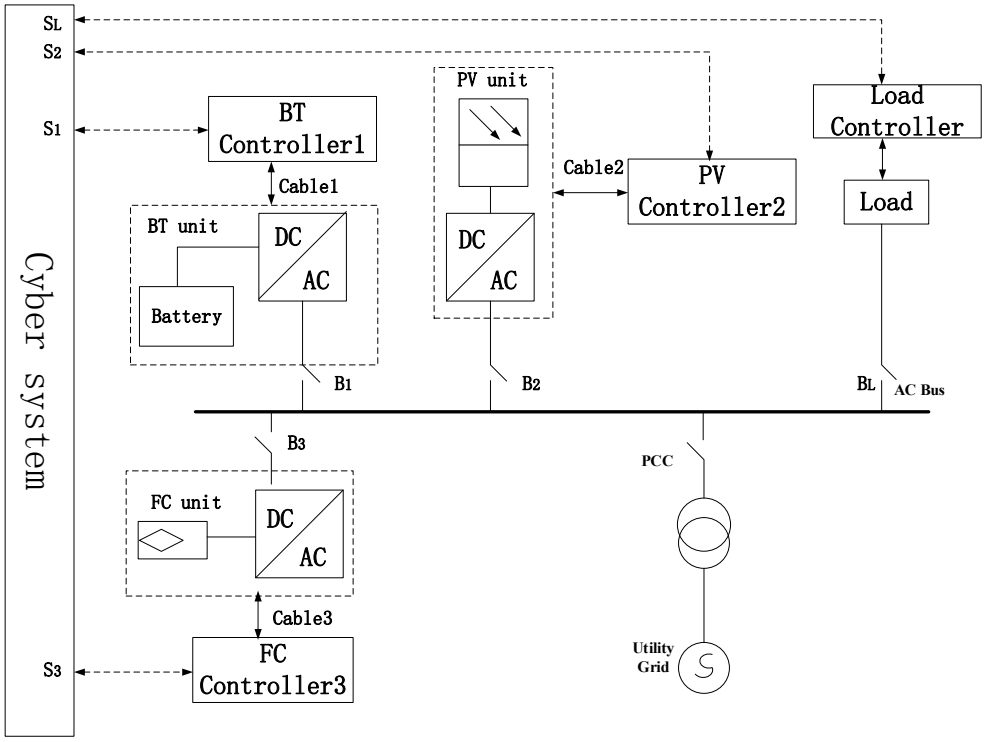

Figure 3. Integrated scheme of the cyber physical microgrid.

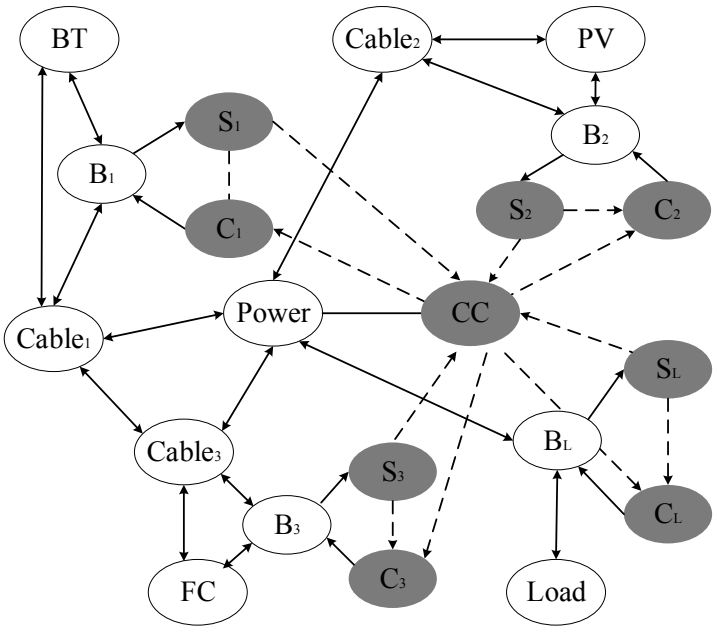

Figure 4. The network diagram of the integrated cyber physical microgrid system.

For one DER and converter transmission line (Figure 5), according to Kirchoff's voltage law and Kirchoff's current law, the following set of equations is obtained:

$$\begin{cases} \frac{di_1}{dt} = -\frac{1}{L_1}u_c + \frac{1}{L_1}u_{inv} \\ \frac{di_2}{dt} = -\frac{R}{L_2}i_2 + \frac{1}{L_2}u_c \\ \frac{du_c}{dt} = -\frac{1}{C}i_2 + \frac{1}{C}i_1 \end{cases} . \tag{5}$$

Then, the ith DER unit can be described as follows:

DER i:

$$\dot{\boldsymbol{x}}_{\boldsymbol{i}}(t) = \boldsymbol{A}_{\boldsymbol{i}}\boldsymbol{x}_{\boldsymbol{i}}(t) + \boldsymbol{B}_{\boldsymbol{i}}\boldsymbol{u}_{\boldsymbol{i}}(\mathrm{t}) + \boldsymbol{D}_{\boldsymbol{i}}\boldsymbol{w}_{\boldsymbol{i}}(t), \tag{6}$$

where $\boldsymbol{x}_{\boldsymbol{i}}(t)$ are state vectors; $\boldsymbol{u}_{\boldsymbol{i}}(t)$ are input variables; $\boldsymbol{w}_{\boldsymbol{i}}(t)$ is the disturbance transmitted from the cyber network; and $\boldsymbol{A}_{\boldsymbol{i}}$, $\boldsymbol{B}_{\boldsymbol{i}}$, and $\boldsymbol{D}_{\boldsymbol{i}}$ are the coefficient parameters.

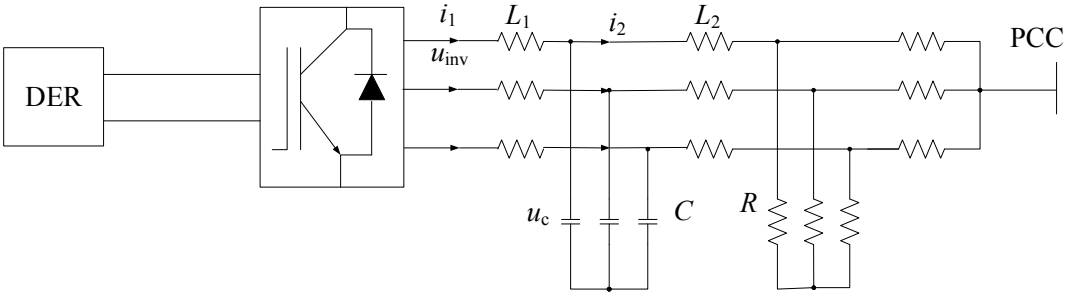

Figure 5. Structure of a DER unit.

In a microgrid system, DERs are very dispersive and loosely connected to each other, so even two adjacent DERs are generally far away. When the control signals that come from adjacent DER unit are transmitted through the transmission line, communication delay is unavoidable. Under an IDoS attack, the information effect on communication delay can vary from tens to several hundred milliseconds or more. The extensive of information error would deteriorate the device performance. If the operation of the jth DER unit is affected by the IDoS attack, the time delay should be taken into consideration.

Therefore, the ith DER unit is re-described in the following form:

DER i:

$$\dot{\boldsymbol{x}}_{\boldsymbol{i}}(t) = \widetilde{\boldsymbol{A}}_{\boldsymbol{ij}}\boldsymbol{x}_{\boldsymbol{i}}(t) + \boldsymbol{B}_{\boldsymbol{i}}\boldsymbol{u}_{\boldsymbol{i}}(t) + \boldsymbol{A}_{\boldsymbol{ij}}\boldsymbol{x}_{\boldsymbol{j}}\left(t - \tau_{ij}\right) + \widetilde{\boldsymbol{D}}_{\boldsymbol{i}}\boldsymbol{w}_{\boldsymbol{i}}(t), \tag{7}$$

where τ_{ij} is the information transmission time delay between the ith DER and the jth DER; and $\widetilde{\boldsymbol{A}}_{\boldsymbol{ij}}$ and $\widetilde{\boldsymbol{D}}_{\boldsymbol{i}}$ are the coefficient parameters when the delay-dependent controllers exist.

3.2. Risk Assessment in the Microgrid

The risk assessment method is proposed in order to evaluate the security of the cyber physical microgrid system. If the risk assessment index is violated, the operation modes of DERs need to be changed to the optimal power mode in a microgrid system.

Using the Monte Carlo simulation method, the probability stochastic process is established, and the index is calculated by probability sampling and the characteristic statistics method. Taking into account the operation parameters of the multivariate normal distribution system, the characteristics of the state probability distribution of the network are studied based on the uncertainty of the power network load and its operating parameters. Furthermore, the probability value of element failure is calculated by using the theory of Poisson distribution.

The risk assessment index and the corresponding severity are determined according to the result of the failure state of the element. The impact factor for the attack upon the system is determined by the utilization ratio and loading level. Especially, the loss of load (LOL) is quantified for a disconnected

physical node. The impact level is assigned with a ratio to the power that denotes the loss of load and total load, respectively. To determine the value P_{LOL}, we can start with the value of the physical node and gradually increase the loading level of the entire system. This process continues until the power flow diverges. We propose the calculation formula of the security risk assessment index based on the quantification principle of the risk evaluation. It can be described by

$$R = p_{vul} \times \frac{P_{LOL}}{P_{TL}}, \tag{8}$$

where p_{vul} is the possibility of the infrastructure vulnerability to transmit the cyber attacks. $\frac{P_{LOL}}{P_{TL}}$ is the quantitative potential impact on the distribution system operation caused by cyber attacks. The security risk assessment index R can reveal the security risk of the system under attacks on a smart metering node.

4. Simulation Results

We carry out extensive experiments to evaluate the IDoS attacks in the cyber system. If the physical microgrid is affected by the network logged system, the information disturbed with variable time delay is occurred. The physical microgrid system under attacks is modeled as the continuous mathematical system under variable time delays in different information routes.

The parameters are partially referred from [27]: $A = 0.00267$, $B = 0.2$, $C = 0.024$, $D = -1.4$, $\nu = 80$, $K_1 = 0.01$, $K_2 = 0.02$ and $N = 75$. The service rate μ is driven by ρ, with $\mu = 90$, $\rho^* = 0.89$, and $w = 70$. Figure 6 shows the results that we obtained. It demonstrates the trajectory of admission rate with different IDoS attack pulses.

In Figure 6a, the IDoS attack starts at time 0 second for a duration of time 40 s and repeats every $T = 50$ s. The attack occurs at the period of time between 0 and 200 s. We evaluate such an effect by launching an IDoS attack with $\gamma(t) = 2000$ requests per second and a wide range of attack periods about hundreds of seconds. It is assumed that $\gamma(t)$ requests are high enough to force the network server to decrease the utilization.

In the experiments, the attacker sends either periodic pulses or random pulses. Figure 6b illustrates that the utilization decreases in the attack period. It shows that the server has a long time to recover its admission rate and consequently takes in more normal requests. Hence, if an attacker wants to gain more profit, he would use the attack period in high intensity. It is clear that the admission rate drops to below 0.5 from its steady-state value of 0.89.

If the attack pulse time is smaller than $t1 + t2$, the trajectory of the admission rate involves mainly two stages: the sustaining stage and the restoration stage. If the $(k + 1)$th attack pulse arrives when the system is in the restoration stage, the trajectory involves the sustaining stage and the restoration stage. However, the admission rate cannot restore to the desired state during the attack period.

When the system operates normally, the IDoS attack would push the system into thrashing, causing a decline in the admission rate and hence a denial of service to the requests lasts during the dynamic periods. Under normal workload conditions, the memory utilization is normal, and the admission ratio is among 0.8–0.9. If normal requests are injected when the IDoS attack is initiated, the system is pushed into thrashing since those insignificant attack requests consume a lot of memory in the server. This inefficient period lasts during 200 s, until the admission controller recovers to admit all legitimate requests.

If the attack pulse time is between 0 to 500 s, which is longer than $t1 + t2 + t3$, the evolution of the system involves all the stages in Figure 6b, and the admission rate can reach the steady values when $\rho = \rho^*$. During the attack period, the normal requests are injected causing the same scenario to repeat. The attack request has caused denial of service for normal legitimate requests.

The utilization variation also depends on the different admission controller parameter K, as well as the degradation in the service rate μ with values w. It reflects the sensitivity of the controller to

the error eradiation. In practice, the information communication delay will slow down the controller reactions and cause vulnerability to the microgrid.

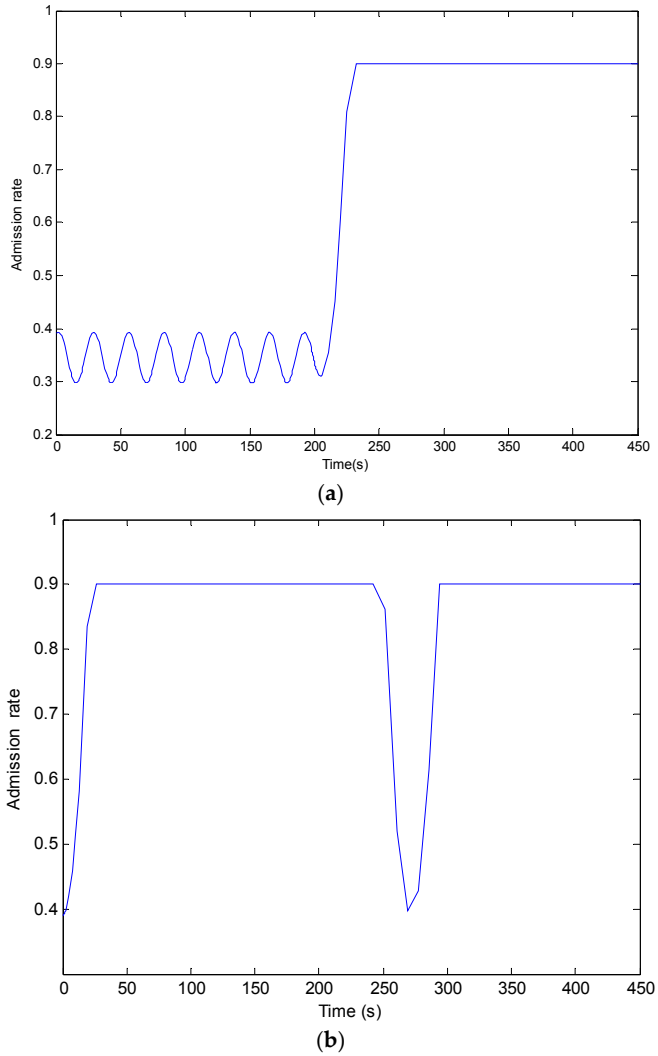

Figure 6. The variation of admission rate with different IDoS attack pulses. (**a**) $\tau < t1 + t2$; (**b**) $\tau > t1 + t2 + t3$.

The cyber physical microgrid (Figure 3) is simulated under normal operating conditions. To evaluate the performance of the microgrid, the parameters of the DERs are given in Table 1.

Table 1. The parameters of the DERs.

Name	Parameter
inductance	0.01 H
capacitance	1×10^{-6} F
resistance	0.1 Ω
PV rate output power	49 kW
Fuel cell rate output power	53 kW × 2

If the communication network is normal, the control signal can be correctly transmitted from the cyber system to the power system. The simulation results are shown in Figure 7. After a brief start-up time, the output power of each power supply tends to be stable.

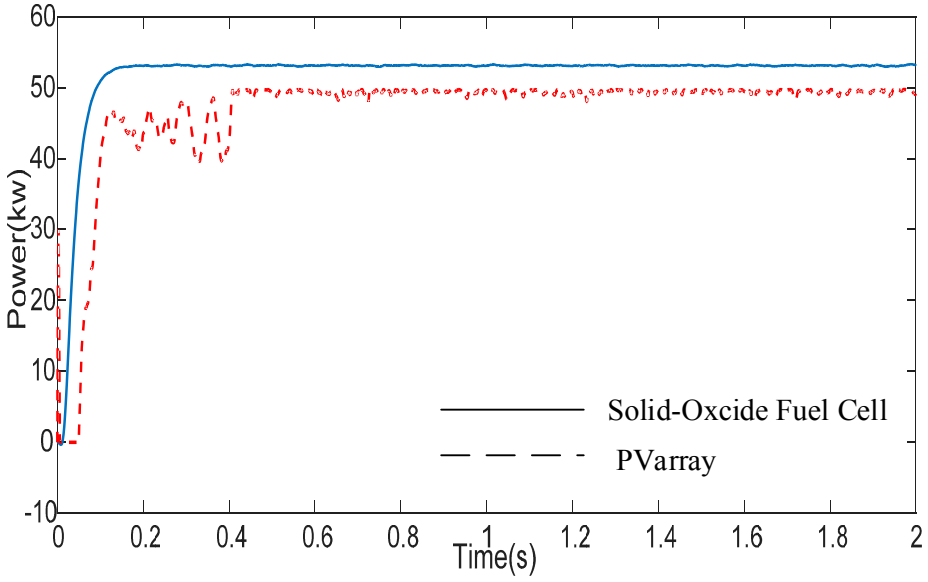

Figure 7. The output power under normal operating condition.

The simulation results illustrate the effectiveness of system analysis process. When the system is under an IDoS attack, the data packet has an oscillated loss rate, the control signal cannot be correctly transmitted to the power system. The simulation results are shown in Figure 8. The output power of the two battery packs will oscillate and become unstable.

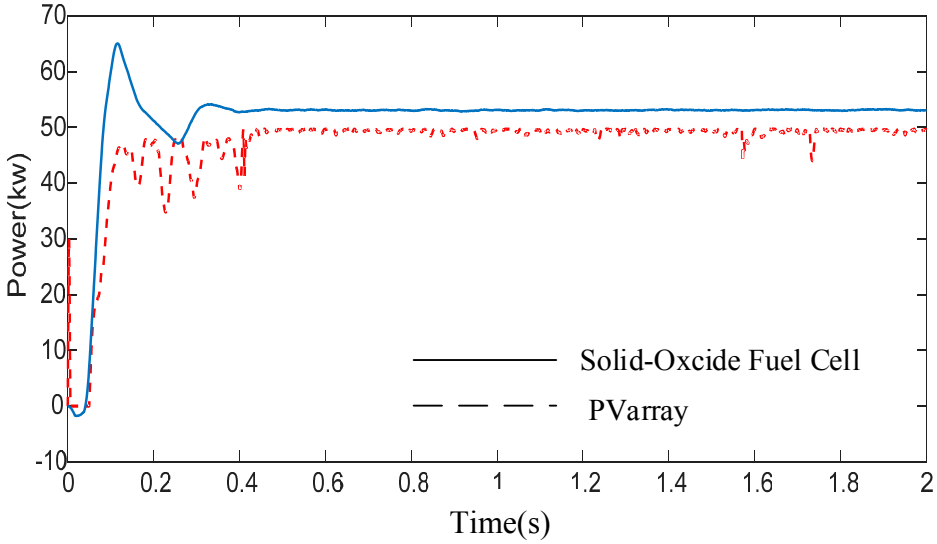

Figure 8. The output power of the two battery packs with data packet losses.

If the communication rate drops to a certain extent under the IDoS attack, the physical microgrid is affected by communication congestion. Figure 9 shows that the power system cannot receive the control signal of the information system in time, and the output power of the battery packs will oscillate and be unstable.

In order to evaluate the effect of attacks on the physical system, an improved IEEE 33 node distribution system including DERs is simulated to analyze the validity of a proposed risk assessment approach (Figure 10). More specifically, the DERs are added at the 11 and 17 nodes to supply power to the distribution lines. Moreover, the nodes 3 and 22–27 are defined as the key loads, nodes 28–31 are

treated as interruptible loads, and the rest of the load nodes are regarded as common loads. For an attacker aiming to make the system operation status available by controlling one node, the metric of p_{vul} would be the successful transmission possibility of attack information. We test the cases in which the IDoS attack impacts different nodes and calculate the risk assessment index. The simulation results are shown in Figure 11.

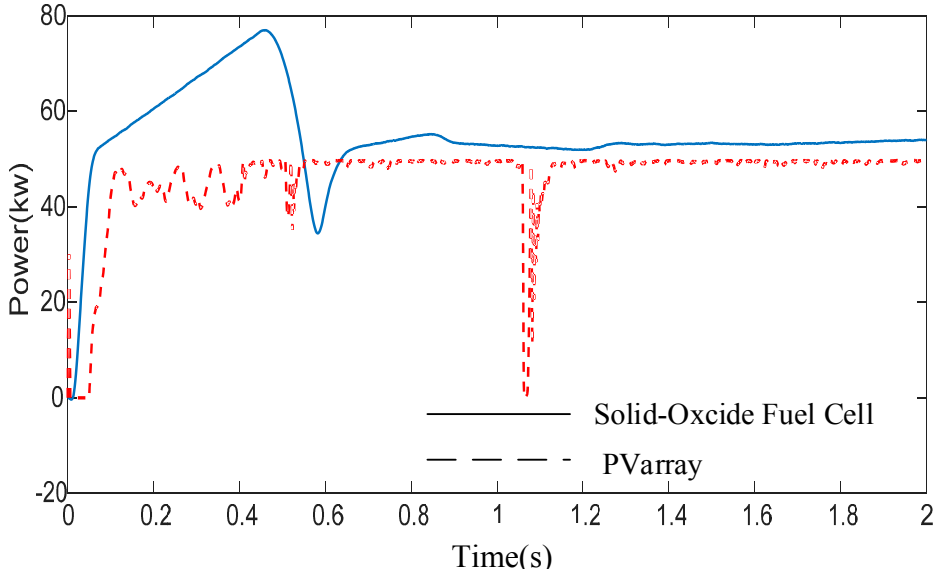

Figure 9. The output power of the two battery packs with information congestion.

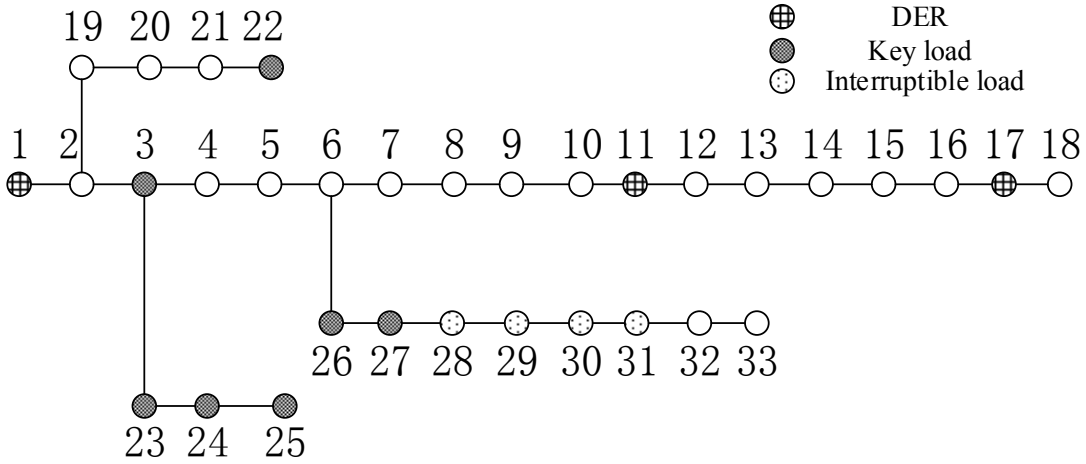

Figure 10. IEEE 33 distribution system with DER units.

The risk assessment index R reveals the node security under attacks and the aggressiveness of the attacker in Figure 11. From the distribution of results, we can obviously see that the security risk evaluation index of the DER nodes are lower than that of other load nodes. Due to the relative load node, DER nodes are configured with more perfect monitoring equipment or located in the key position of the system with more output. As the attacker generally has difficulty succeeding with the target attack, the successful delivery possibility p_{vul} is relatively low. Under the condition that the real-time load control makes the difference of load shedding smaller, the security risk index values of DER nodes are lower. With regard to load nodes, we can see an attacker whose goal is to maximize system control ability may make his target be nodes 25 or 32. Although node 25 is a key load node, it has lower importance and higher risk than other nodes for being the end of the radial structure

of the system. As node 32 is a common load node, its security is also relatively low because of its location near interruptible loads. Thus, both of them may be vulnerable to attack and result in making the stable operation of the system a higher security risk. Thus, a large index R reflects the high level of aggression.

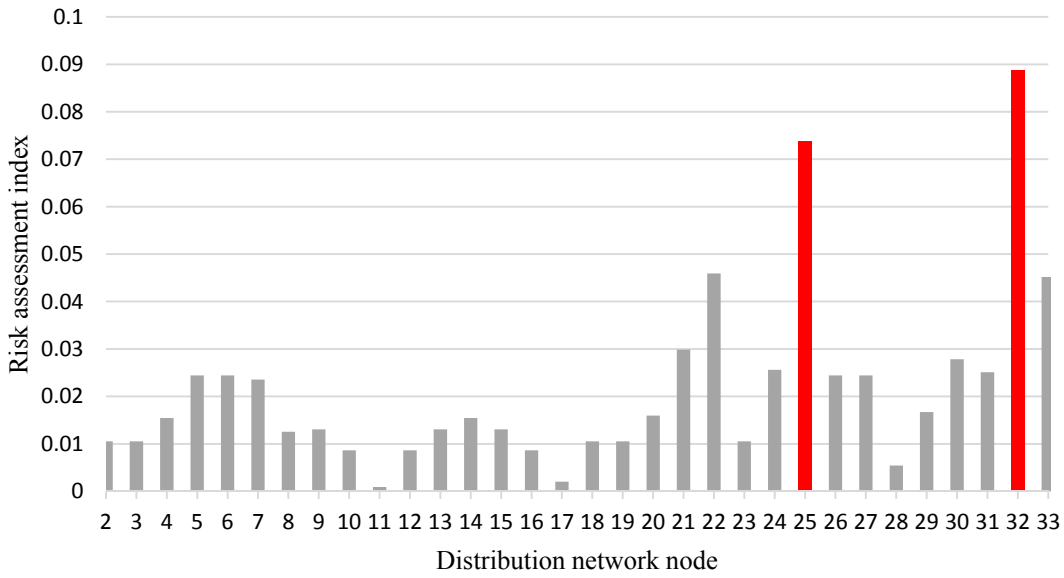

Figure 11. The security risk index in the improved IEEE 33 distribution system.

5. Conclusions

In this paper, we exposed microgrid security to IDoS attacks aiming at the physical system. Assuredly, the sustainability time of the general IDoS attack was affected by many factors, such as the individual knowledge and skills of the attackers, the strength of the security detection mechanism in the target system and the selection of potential attack points, etc. In order to more clearly explain the influence of communication delay caused by attacks on the stability of the microgrid, we assumed that the IDoS attack pulse was denoted as a Dirac function signal with an arrival rate, which is an instantaneous attack, and the arrival rate was set to be constant during each of the instances. As different stages may be affected by the duration of the attack, different IDoS attacks could cause varied degrees of communication delay on the system operation.

The impacts of the IDoS attacks were analyzed and proved to have the ability to force the system to oscillate along with the attacks. Since both the oscillation of steady state error and deviation of the desired steady state can affect the physical microgrid operation, the dynamic security of the microgrid system was analyzed under IDoS attacks. A risk assessment method of the cyber physical microgrid system was proposed in order to investigate the interactions. Finally, the experimental results were shown to verify system operating characteristics. In future work, we will research the frequency and voltage variations deeply, considering the effectiveness and the cost of the attacks.

Acknowledgments: This work has been funded by the Smart Grid Protection and Control National Key Laboratory Open Project of the NARI Group Corporation (BK217007), and the Key Project of the National Natural Science Foundation of China (61633016).

Author Contributions: Rong Fu and Jun Sun contributed to developing the ideas of this research and the IDoS attack modeling in the paper. Zhenkai Zhou, Xiaojuan Huang, Decheng Chen, and Yingjun Wu performed this research and simulated the cyber physical microgrid operations, and all of the authors involved in preparing this manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Bidram, A.; Davoudi, A. Hierarchical structure of microgrids control system. *IEEE Trans. Smart Grid* **2012**, *3*, 1963–1976. [CrossRef]
2. Guerrero, J.M.; Vasquez, J.C.; Teodoresu, R. Hierarchical control of droop-controlled AC and DC microgrids-a general approach toward standardization. *IEEE Trans. Ind. Electron.* **2011**, *58*, 158–167. [CrossRef]
3. Hu, J.F.; Zhu, J.G.; Dorrell, D.G. Model predictive control of inverters for both islanded and grid-connected operations in renewable power generations. *IET Renew. Power Gener.* **2014**, *8*, 240–248. [CrossRef]
4. Yang, X.; Song, Y.; Wang, G.; Wang, W. A comprehensive review on the development of sustainable energy strategy and implementation in China. *IEEE Trans. Sustain. Energy* **2010**, *1*, 57–65. [CrossRef]
5. Soroudi, A.; Ehsan, M.; Caire, R.; Hadjsaid, N. Possibilistic evaluation of distributed generations impacts on distribution networks. *IEEE Trans. Power Syst.* **2011**, *26*, 2293–2301. [CrossRef]
6. Liu, X.; Mohammad, S.; Cao, Y.; Wu, L. Microgrid risk analysis considering the impact of cyber attacks on solar PV ESS control systems. *IEEE Trans. Smart Grid* **2017**, *8*, 1330–1339. [CrossRef]
7. Closon, C.M.; Nehrir, M.H. Algorithms for distributed decision-making for multi-agent microgrid power management. In Proceedings of the IEEE Power and Energy Society General Meeting, Detroit, MI, USA, 24–29 July 2011; pp. 1–8.
8. Sechilariu, M.; Wang, B.C.; Locment, F. Building integrated photovoltaic system with energy storage and smart grid communication. *IEEE Trans. Ind. Electron.* **2013**, *60*, 1607–1618. [CrossRef]
9. Dou, C.X.; Liu, B. Multi-agent based hierarchical hybrid control for smart microgrid. *IEEE Trans. Smart Grid* **2013**, *4*, 771–778. [CrossRef]
10. Mohamed, F.A.; Koivo, H.N. System modeling and online optimal management of microgrid using mesh adaptive direct search. *Int. J. Electr. Power Energy Syst.* **2010**, *32*, 398–407. [CrossRef]
11. Zhang, L.; Gao, H.; Kaynak, O. Network-induced constraints in networked control systems: A survey. *IEEE Trans. Ind. Inform.* **2013**, *9*, 403–416. [CrossRef]
12. Ye, X.; Liu, S.; Liu, P.X. Modelling and stabilization of network control system with packet loss and time-varying delays. *IET Control Theory Appl.* **2010**, *4*, 1094–1100. [CrossRef]
13. Liu, S.; Wang, X.; Liu, P.X. Impact of communication delays on secondary frequency control in an islanded microgrid. *IEEE Trans. Ind. Electron.* **2015**, *62*, 2021–2031. [CrossRef]
14. Zhong, X.; Yu, L.; Brooks, R.; Venayagamoorthy, G.K. Cyber security in smart DC microgrid operations. In Proceedings of the 2015 IEEE 1st International Conference on Direct Current Microgrid, Atlanta, GA, USA, 7–10 June 2015; pp. 86–91.
15. Rahman, M.S.; Mahmud, M.A.; Oo, A.M.T. Multi-agent approach for enhancing security of protection schemes in cyber-physical energy systems. *IEEE Trans. Ind. Inform.* **2017**, *13*, 436–447. [CrossRef]
16. Robert, K.; Sheldon, F.T. Security Analysis of smart grid cyber physical infrastructures using game theoretic simulation. In Proceedings of the IEEE Symposium Series on Computational Intelligence, Cape Town, South Africa, 7–10 December 2015; pp. 455–462.
17. Meraj, T.; Sharmin, S.; Mahmud, A. Studying the impacts of cyber-attack on smart grid. In Proceedings of the 2nd International Electrical Information and Communication Technology Conference, Khulna, Bangladesh, 10–12 December 2015; pp. 461–466.
18. Lee, R.M.; Assante, M.J.; Conway, T. *Analysis of the Cyber Attack on the Ukrainian Power Grid*; Electricity Information Sharing and Analysis Center (E-ISAC): Washington, DC, USA, 18 March 2016.
19. Chalamasetty, G.K.; Mandal, P.; Tseng, B. Secure SCADA communication network for detecting and preventing cyber-attacks on power systems. In Proceedings of the 2016 Clemson University Power System Conference, Clemson, SC, USA, 8–11 March 2016; pp. 1–7.
20. Chalamasetty, G.K.; Mandal, P.; Tseng, B. SCADA framework incorporating MANET and IDP for cyber security of residential microgrid communication network. *Smart Grid Renew. Energy* **2016**, *7*, 104–112. [CrossRef]
21. Ten, C.W.; Liu, C.C.; Manimaran, G. Vulnerability assessment of cyber security for SCADA systems. *IEEE Trans. Power Syst.* **2008**, *23*, 1836–1846. [CrossRef]
22. Sun, Y.B.; Chen, Y.P.; Bai, Z. Fault diagnosis for power system using time sequence fuzzy Petri net. In Proceedings of the 3rd International Conference on Mechanical Engineering and Intelligent Systems, Yinchuan, China, 15–16 August 2015; pp. 729–735.

23. Wooi, T.C.; Govindarasu, M.; Liu, C.C. Cyber security for critical infrastructures: Attack and defense modeling. *IEEE Trans. Syst. Man Cybern.* **2010**, *40*, 853–863.
24. Chen, T.M.; Carlous, S.-A.J.; John, B. Petri net modeling of cyber-physical attacks on smart grid. *IEEE Trans. Smart Grid* **2011**, *2*, 741–749. [CrossRef]
25. Gharavi, H.; Hu, B. 4-way Handshaking protection for wireless mesh network security in smart grid. In Proceedings of the 2013 IEEE Global Communications Conference, Atlanta, GA, USA, 9–13 December 2013; pp. 790–795.
26. Srikantha, P.; Kundur, D. Denial of service attacks and mitigation for stability in cyber-enabled power grid. In Proceedings of the 2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference, Washington, DC, USA, 18–20 February 2015; pp. 1–5.
27. Guirguis, M.; Bestavros, A.; Matta, I.; Zhang, Y. Reduction of quality attacks on internet end-systems. In Proceedings of the 24th Annual Joint Conference of the IEEE Computer & Communications Societies, Miami, FL, USA, 14–17 March 2005; pp. 1362–1372.
28. Tang, Y.; Luo, X.; Qing, H.; Chang, R.K.C. Modeling the vulnerability of feedback-control based internet services to low-rate DoS Attacks. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 339–353. [CrossRef]
29. Dou, C.; Lv, M.; Zhao, T.; Ji, Y.; Li, H. Decentralised coordinated control of microgrid based on multi-agent system. *IET Gener. Transm. Distrib.* **2015**, *9*, 2474–2484. [CrossRef]