energies

MDPI

Article

A Game Theory-Based Approach for Vulnerability Analysis of a Cyber-Physical Power System

Keren Chen [1], Fushuan Wen [2,3,*], Chung-Li Tseng [4], Minghui Chen [5], Zeng Yang [5], Hongwei Zhao [5] and Huiyu Shang [5]

[1] School of Electrical Engineering, Zhejiang University, Hangzhou 310027, China
[2] Department for Management of Science and Technology Development, Ton Duc Thang University, Ho Chi Minh City 800010, Vietnam
[3] Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City 800010, Vietnam
[4] UNSW Business School, The University of New South Wales, Sydney, NSW 2052, Australia
[5] Guangzhou Power Supply Company Limited, Guangzhou 510620, China
* Correspondence: fushuan.wen@tdtu.edu.vn

Received: 20 June 2019; Accepted: 1 August 2019; Published: 3 August 2019

Abstract: In a Cyber-Physical Power System (CPPS), the interaction between the power cyber system and the power physical system becomes more extensive and more in-depth. The failure of a cyber component could have an impact on the security and reliability of the power physical system. Existing publications have focused on the impacts of the power cyber network on the power physical network, while a general CPPS model considering the mutual impacts of these two networks is less studied. Given this background, a game-theoretic approach for a cyber-physical power system vulnerability analysis is proposed. First, a CPPS interactive model framework is structured, consisting of five types of elements: P-nodes, PP-links, C-nodes, CC-links and CP-links. The interactions among these elements are considered. On this basis, the system cascading failure under potential attacks is analyzed, followed with an optimal load curtailment operation when in an emergency. To further illustrate the system vulnerability, a bi-level optimization model under a game-theoretic framework is presented to describe the interactions between a CPPS attacker and a system defender. Optimal resource allocation by the system defender for maintaining system reliability can be obtained by solving the problem. The feasibility and effectiveness of the proposed method are demonstrated by a revised version of the IEEE 14-bus power system.

Keywords: cyber-physical power system (CPPS); vulnerability assessment; cyber-physical link; optimal load curtailment; bi-level mathematic programming

1. Introduction

A power system is one of the most complicated and delicate engineering systems in the world. Its complexity increases even more as a number of advanced devices such as distributed generators, energy storage, and a massive amount of monitoring devices are integrated into the power system. The concept of a Cyber-Physical System (CPS) was introduced to describe a next-generation engineered system covering functions of communication, computing, and control [1]. The power system integrated with monitoring devices is a typical Cyber-Physical System, and therefore forming a Cyber-Physical Power System (CPPS).

In a CPPS, each of the power, information, and communication infrastructures is governed by its own physical or logical laws. The power systems benefit from the development of information technology by both economic boost and reliability improvements [2]. The more precise and trustful the data provided by information infrastructures is, the more it increases the efficiency of the power utility [3]. By recognizing and isolating faults with higher accuracy, the CPPS is able to operate in a better manner, in terms of improved reliability [4].

However, in addition to being vulnerable to failures or attacks on a physical power network as in traditional power systems, a CPPS is also prone to malicious attacks on the cyber network. The Ukraine blackout in 2015 is a typical coordinated cyber physical attack (CCPA) case where the physical attack is masked by coordinated cyberattacks.

In the 2015 Ukraine blackout case, the attacker launched several attacks simultaneously. By using BlackEnergy 3 malware, the hackers took control of the computers in the Ukraine power system control center, and opened breakers to bring at least thirty substations off-line. Meanwhile a telephonic denial-of-service attack was launched to postpone the reports of the outage. The CCPA in this case caused power outage affecting at least 225,000 customers for several hours [5].

It is essential to build a CPPS model as the basis for research in vulnerability assessment, malicious attack detection, and optimization in CPPSs. For example, a hybrid system model is described in [6] where both a continuous power system model and a discrete information system model were integrated. There are also researches focusing on the CPS modeling for other CPS systems such as computer systems and control systems. A taxonomy for description of attacks on CPS is presented in [7,8]. A distributed unmanned aerial vehicles architecture is developed in [9] to characterize attacks and their propagation.

Based on the given literature review, this paper presents a vulnerability assessment procedure of a CPPS considering virtual cyber-physical links. The main contributions of this paper are threefold:

(1) A comprehensive CPPS interactive model framework is developed. The CPPS components are classified into five categories (i.e., physical nodes, cyber nodes, physical-physical links, cyber-cyber links, and cyber-physical links). The interaction between cyber components and physical components is discussed by analyzing the optimal load curtailment operation upon component failure.

(2) A game-theoretic bi-level optimization model for the CPPS attacker and defender is proposed. At the upper level, the defender manages the defending resources to minimize the worst-case load loss caused by the attacks. At the lower level, the attacker decides which component (or components) to attack so that the load loss could be maximized. The hierarchical interactions between the defender and the attacker are described in a game-theoretic model.

(3) The proposed model is illustrated based on a revised version of the IEEE 14-bus power system. The defender's strategy (i.e., the distribution of the defending resources) can be viewed as the relative vulnerability index among the CPPS components. This result can be further developed to calibrate the defender's decisions on the system.

The remainder of this paper is organized as follows: Section 2 describes the related work. Section 3 presents a CPPS node-link model, which considers virtual cyber-physical links. Section 4 analyzes the CPPS cascading failure under malicious attacks, followed by an optimal load curtailment operation when in an emergency. Section 5 discusses the bi-level optimization problem between the malicious attacker and the system defender. Section 6 illustrates the effectiveness of the proposed models with the simulation results. Conclusions and future work are given in Section 7.

2. Related Work

2.1. Cyber Data Attacks in CPPSs

An attack on either the power network or the cyber network will no doubt damage the power system [10]. As malicious attacks generally occur in intelligent ways, modeling attacks with accurate mathematical models is challenging. Researchers have explored some specific attacks. For example, integrity attacks on state estimation systems are studied in [11,12], where the integrity of sensor measurements could be damaged by integrity attacks. The problems of estimation and control of linear systems with several sensors hijacked by deception attacks are considered in [13]. In [14,15], false data injection attacks (FDIAs) are explored in the state estimation frameworks for power systems. Generally, FDIAs can be considered as a specific version of integrity attack, where an adversary could launch attacks to inject fake information into the measurement system of a CPPS, and eventually bypass the existing bad data detection scheme, with the knowledge of the power system configuration. In [16], a specific FDIA called a fake-acknowledge attack against a remote state estimation is considered, where the online power schedule signal from the remote estimator might be falsified by attackers. The optimal strategies for both attackers and defenders are explored with the aid of a game-theoretic framework. Denial-of-service (DoS) attacks are studied in [10] for the state estimation of CPSs where an attacker jams the wireless cyber network. DoS attacks are launched aiming to prevent information transmission between CPS components by jamming the cyber network. Interfering with the radio frequencies is a DoS attack technique that is frequently used [17,18]. In [10], the interactive decision-making process of both information transmission and attacker launching attacks is investigated by formulating a game-theoretic framework. The optimal attack strategy that maximizes the impact of DoS attacks on CPSs is explored in [18,19]. In [20], another form of attacks, i.e. replay attacks, is studied.

The coordinated cyber physical attacks (CCPAs) are also a great concern in the CPPS. It is shown in [21] that CCPAs could be detected through online tracking of the power system equivalent impedance. In [22], a single-level optimization model is constructed to identify the meters that should be protected from attacks. In [23], linear algebra and graph theory are used to develop methods for information recovery of the system under CCPAs.

2.2. Cyber-Physical Mutual Impacts Analysis

CPPS modeling normally starts with analyzing the mutual coupling effect between power networks and cyber networks. A method to solve the communication delay problem in load frequency control is proposed in [24] based on a linear matrix inequality. By modeling the information system as a feedback module, [25] proposes a cyber-based dynamical modeling approach for describing the CPPS. In [26], the cascading failures in an interdependent network are modeled, with the percolation theory of the network considered. The vulnerability of the interdependent network was assessed in [27]. The interdependency model of a power network and a cyber network is studied in [28,29] where both direct and indirect impacts of the cyber network on the power network were modeled and assessed.

3. The CPPS Interactive Model Framework

In order to consider the status of physical and cyber components in CPPS as well as their interaction, a node-link model is proposed as shown in Figure 1. The proposed model consists of five categories of components: physical nodes (P-nodes), cyber nodes (C-nodes), physical–physical links (PP-links), cyber–cyber links (CC-links), and cyber–physical links (CP-links). The detailed design of the node–link relationships in the CPPS model is shown in Figure 2. The model is demonstrated with two planes, i.e., a physical network plane at the bottom and a cyber network plane at the top.

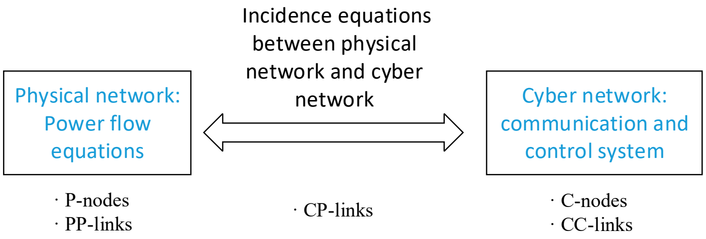
Incidence equations between physical network and cyber network
Physical network: Power flow equations
Cyber network: communication and control system
· P-nodes
· PP-links
· CP-links
· C-nodes
· CC-links

Figure 1. The node–link model in a Cyber-Physical Power System (CPPS).

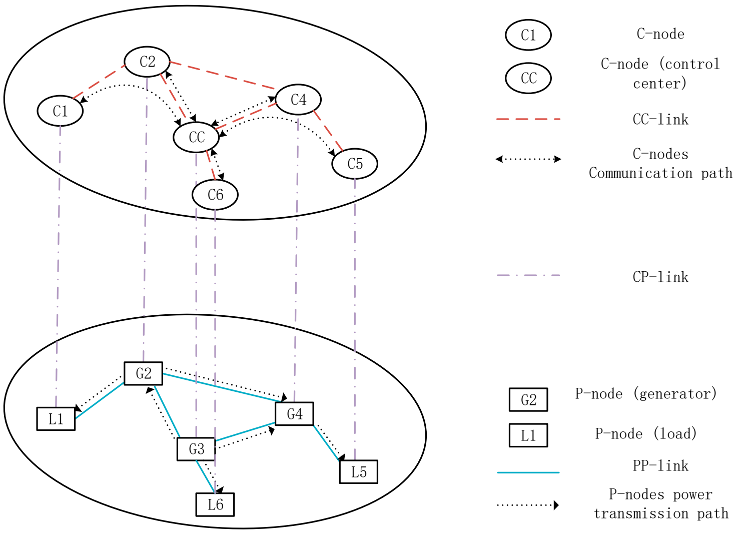

Figure 2. Node–link relationships in a CPPS.

A. P-nodes

The rectangles in the physical plane denoted with $P_1, P_2, \ldots, P_5$ are P-nodes. A P-node represents a generator, a load, or a substation. When a P-node fails, some operations might not be available. For example, if the node represents a generator, then the generator cannot adjust the power output; if the node represents a load, then the load curtailment operation is invalid.

B. PP-links

The PP-links are the transmission lines that connect the P-nodes, shown with full lines in Figure 2. When a PP-link fails, power transmission is invalid through it, and the power flow needs to be recalculated. If the power flow exceeds the line limit, further operation should be considered, such as generator output rearrangement, load curtailment, or even line tripping of the overloaded transmission lines.

C. C-nodes

The ellipses in the cyber plane atop the physical plane marked with $C_1, C_2, \ldots, C_5$ are C-nodes. Most physical components such as generators and loads are equipped with cyber components, whose main function is data acquisition and control signal transmission, such as remote terminal units (RTUs). Many cyber components exist around a P-node and they collect different types of data. In this paper the combination of all cyber components corresponding to the same P-node are simplified as one single C-node with all their functions combined. Due to this simplification, the distribution of C-nodes is considered the same as that of P-nodes, that is, every P-node is linked to a C-node, with the same topological distribution. The C-nodes are separated into two types: the control center and the cyber terminals.

The C-nodes are vulnerable to cyber-attacks. Examples of such attacks are manifold and include buffer overflow, Denial of Service (DoS), man in the middle, and many other attacks. When a C-node fails, its communication with the neighboring C-nodes is terminated, causing the failure of all CC-links connecting this node. Moreover, as mentioned above, the data acquisition and control command transmission function for the corresponding P-node are invalid, and therefore the connecting generator cannot adjust the power output, and the connecting load cannot be curtailed in emergency; that is, the P-node fails as the result of the C-node failure.

D. CC-links

C-nodes need to communicate through wired or wireless communication, which is represented as CC-links shown with dash lines connecting C-nodes in Figure 2. If a C-node is isolated, that is, unable to communicate with the control center through any CC-links, it can be considered to have failed. In Figure 2, every C-node needs to connect to the control center, and currently active communication paths are shown with dotted lines.

E. CP-links

The connection between a P-node and a C-node is denoted as a CP-link, shown with dash-dot lines in Figure 2. The physical components supply power for the local cyber components, while the cyber components collect the data such as generator power output, and adjust the physical component status. An example CP-link could be the connection between a generator and all associated RTUs, and is implemented by ports (for data collection) and electric wires (for power supply).

A CP-link brings mutual impact on both the physical side and the cyber side. If a P-node is totally out of power supply, the corresponding C-node fails due to lack of power. On the other hand, if a C-node is unable to communicate with the control center, the control command cannot reach the P-node, and some operations of this P-node might not be possible, such as load curtailment or modifying power output; therefore the P-node is considered to have failed.

The abovementioned five types of components constitute the proposed node–link model.

4. CPPS Vulnerability Analysis

4.1. External Attack and Cascading Failure

In recent years, several cases of malicious attack upon power systems have occurred in different countries. In order to maximize the damage on a power system, the attacker might choose to attack the weaker parts of the system, i.e. the parts that are more vulnerable to cyber or physical attacks. In CPPS, attacks on either the cyber side or the physical side could damage the system. In this paper, it is assumed that the attacker's target is to increase the expected energy not supplied (EENS) as much as possible, with coordinated attacks on both the physical side and the cyber side.

It is important to determine which components might be considered as the attacker's targets and what the defending strategy should be. Among the five CPPS components, a CP-link is usually an inner connection between devices and implemented by ports and electric wires for power supply, and is not an easy target for the attackers. A CC-link is usually formed with cable or a wireless connection, which is relatively reliable and more difficult to attack, while the C-nodes are easier targets for a potential attacker. In the physical subsystem, PP-links (i.e. transmission lines) are usually the most unprotected ones and hence, the vulnerable targets for destructive activities. As a result, the attacker–defender problem discussed in this paper focuses on the defending strategies against attacks on C-nodes and PP-links of a CPPS.

Suppose the attacker chooses to attack a PP-link and two C-nodes simultaneously. Because of the attack on the PP-link, the transmission line is tripped, causing a change of power flow distribution. In this case the power flow in some branches may exceed the power flow limit. The control center may try to send a control command to adjust the status of some P-nodes, which, however, may be partially blocked due to the failure of the damaged C-nodes. The generator output or load of the P-nodes connecting to the damaged C-nodes may not be adjusted, which further increases the system loss.

It can be shown from this example that the damage of either physical or cyber components could influence the other part, and deal greater damage of the system. The impacts can be summarized as follows:

(1) If a CC-link fails: both C-nodes connecting to the link should verify their connection to the control center. If a C-node loses connection to the control center, it is considered to have failed.

(2) If a CP-link fails: this causes the failure of both the C-node and the P-node connecting to it.

(3) If a PP-link fails: this influences the power flow distribution of the system, and further operations might be needed to ensure that the power flow does not exceed the line limit.

(4) If a C-node fails: all CC-links and CP-links connecting to it fail.

(5) If a P-node fails: the generator power output cannot be adjusted, and the load curtailment operation is invalid for the components represented by this failed P-node. Meanwhile the CP-link connecting to this P-node fails.

4.2. Optimal Load Curtailment Operation

The system loss can be calculated by repeatedly analyzing the impact of the aforementioned five types of component failure until the system becomes stable. When recalculating the power flow distribution, if a power line limit is exceeded, possible strategies to remedy the situation include adjusting the generator output, tripping the most seriously overloaded transmission line, and conduct load curtailment.

Based on the DC power flow model, the problem of determining the minimal load curtailment can be formulated as follows:

$$\min \sum_{i \in L} \Delta P_{L_i} \tag{1}$$

subject to

$$\sum_{i \in L} \Delta P_{L_i} = \sum_{j \in G} \Delta P_{G_j} \tag{2}$$

$$P_{L_i}^m \le P_{L_i} - \Delta P_{L_i} \le P_{L_i}^M, \forall i \in L_a \tag{3}$$

$$\Delta P_{L_i} = 0, \forall i \in L_{off} \tag{4}$$

$$P_{G_j}^m \le P_{G_j} - \Delta P_{G_j} \le P_{G_j}^M, \forall j \in G_a \tag{5}$$

$$\Delta P_{G_j} = 0, \forall j \in G_{off} \tag{6}$$

$$(P_i - \Delta P_i) - V_i \sum_{j=1}^{n} V_j B_{ij} (\theta_{ij} - \Delta\theta_{ij}) = 0, \forall i \in N \tag{7}$$

where $L = \{L_a, L_{off}\}$, $G = \{G_a, G_{off}\}$. Let L_a and L_{off}/G_a and G_{off} represent the collection of controllable/uncontrollable load/generators in the system, respectively; ΔP_{Li} and ΔP_{Gj} represent the amount of power changed at load node *i* and generator node *j*, respectively; $P_{L_i}^m$ and $P_{L_i}^M/P_{G_j}^m$ and $P_{G_j}^M$ represent the lower and upper limit of load *i*/generator *j*, respectively; P_i, ΔP_i and V_i represent the real power, change of real power, and the voltage amplitude at node *i*; θ_{ij} and $\Delta\theta_{ij}$ represent the angle difference of branch *ij* and its change; B_{ij} represents the susceptance of branch *ij* in the bus admittance matrix; *N* and *n* represent the collection of all nodes in the system and the number of nodes. The detailed descriptions for symbols used are given in the Nomenclature at the end of this paper.

The minimal load curtailment objective is given in Equation (1), subject to the power balance constraint in Equation (2), load node constraints in Equations (3) and (4), generator node constraints in Equations (5) and (6), and the branch DC power flow equation in Equation (7). The accuracy of the result can be further improved by expanding the formulations based on the AC power flow model.

5. The Attacker-Defender Game

5.1. Bi-Level Programming Problem

When facing a potential malicious attack, the power system defender should distribute the defending resources according to the importance of the components, based on the potential damage to the system if the targeted component is compromised. The defending resources include backup units, patrol frequency, protection level, etc. The more defending resources a component is distributed with, the less likely it becomes faulty under an unexpected attack. The effectiveness of the defending resources is described with probability in Equations (14) and (15).

The defending resource distribution strategy should be predetermined in the power system. Therefore, if the attacker could acquire the defending strategy, the attacking strategy would be optimized accordingly. This problem is a typical leader-follower game in which two players try to minimize their individual objective functions *F(x, y)* and *f(x, y)*, respectively, subject to a series of interdependent constraints. Therefore, this problem can be formulated as a bi-level optimization problem [30]. A bi-level optimization problem consists of two (sub-) problems, such that one of which is embedded within the other. They are referred to as the upper-level problem and the lower level problem.

A general form of a bi-level problem can be formulated as:

$$\min_{x} F(x, y^*) \tag{8}$$

subject to

$$G(x, y^*) \leq 0 \tag{9}$$

$$y^* = \arg\left\{\min_{y} f(x, y)\right\} \tag{10}$$

subject to

$$g(x, y) \leq 0 \tag{11}$$

The above bi-level problem is formed with an upper-level optimization problem in Equations (8) and (9), where the defender minimizes the potential loss, and the lower-level optimization problem Equations (10) and (11), where the attacker aims to maximize the potential loss. The defender controls the defending resources that can be distributed to PP-links and C-nodes, and the attacker decides the probabilities of different attack actions.

The objective of the upper-level optimization problem is minimized in Equation (8), subject to the constraint specified in Equation (9), and subject to the lower-level optimization objective in which the lower-level objective is minimized in Equation (10), subject to the constraint in Equation (11). Normally the upper-level and the lower-level objectives are different. However, in the defender–attacker problem discussed in this paper, the upper-level objective is the exact opposite of the lower-level one such that *f(x, y) = −F(x, y).*

5.2. Defending Resource Distribution

Assume that the attacker aims for a relatively higher success rate and chooses an attack action $a = (x_a, y_{1a}, y_{2a})$ from a set of all possible attack actions. In other words, one PP-link and two C-nodes are chosen as attack targets. The bi-level formulation for the defending resource distribution problem discussed in this paper can be written in the following form:

$$\min_{d_p, d_c} Loss = \min_{d_p, d_c} \sum_{a \in A} w_a^* R_a \tag{12}$$

subject to

$$R_a = p_{x_a} p_{y_{1a}} p_{y_{2a}} R_{(x_a, y_{1a}, y_{2a})} + p_{x_a} p_{y_{1a}} (1 - p_{y_{2a}}) R_{(x_a, y_{1a})} + p_{x_a} p_{y_{2a}} (1 - p_{y_{1a}}) R_{(x_a, y_{2a})} + p_{x_a} (1 - p_{y_{1a}})(1 - p_{y_{2a}}) R_{(x_a)} \tag{13}$$

$$p_{x_a} = 1 - \tanh(\beta_p d_{p_{x_a}}) \tag{14}$$

$$p_{y_a} = 1 - \tanh(\beta_c d_{c_{y_a}}) \tag{15}$$

$$d_{p_i} \geq 0, 0 < i \leq N_{PP} \tag{16}$$

$$d_{c_i} \geq 0, 0 < i \leq N_C \tag{17}$$

$$\sum_{i=1}^{N_{PP}} d_{p_i} = D_p \tag{18}$$

$$\sum_{i=1}^{N_C} d_{c_i} = D_c \tag{19}$$

$$w^* = \arg\left\{\max_{w} Loss\right\} \tag{20}$$

subject to

$$w_a \geq 0, \forall a \in A \tag{21}$$

$$\sum_{a \in A} w_a^* = 1 \tag{22}$$

where d_p and d_c represent the defending resources distributed to PP-links and C-nodes, respectively; R_a is the total load curtailment when attack action a is launched; w represents the attacker's mixed strategy (probability distribution) on the set of attack actions, with w_a representing the attacker's probability of taking a specific attack action a; and p_{x_a}, $p_{y_{1a}}$ and $p_{y_{2a}}$ represent the probabilities that the PP-link x_a, C-node y_{1a} and C-node y_{2a} are successfully compromised by the attacker, respectively. Furthermore, $R_{(x_a)}/R_{(x_a,y_{1a})}/R_{(x_a,y_{2a})}/R_{(x_a,y_{1a},y_{2a})}$ represent the load curtailment when components $(x_a)/(x_a,y_{1a})/(x_a,y_{2a})/(x_a,y_{1a},y_{2a})$ are successfully compromised by the attacker; β_p and β_c are the failure coefficient of the PP-links and the C-nodes, respectively; and D_p and D_c are the total defending resources for PP-links and C-nodes, respectively.

The bi-level problem is formulated in Equations (12)–(22), where Equations (12)–(19) represent the outer-level problem, and the inner optimization problem is described by Equations (20)–(22). As specified in Equation (13), after the defending resource is distributed, the load loss under a single attack strategy can be calculated by summing the weighted expected load loss of successfully breaking $(x)/(x, y_1)/(x, y_2)/(x, y_1, y_2)$. As described in Equations (14) and (15), the more defending resource a PP-link or a C-node is distributed with, the less likely it will be broken under attack. The defender has limited resource on either PP-links or C-nodes, as specified in Equations (16)–(19). The attack possibilities on different attack strategies are specified in Equations (21) and (22).

The decision variables controlled by the defender are d_p and d_c (i.e., defending resources on CPPS components). The attacker decides the mixed strategy w of different attack actions. In reality, the exact attack action to be taken by the attacker is unknown. From the defender's viewpoint, it is reasonable to assume that the attacker would launch an attack with a mixed strategy of all possible attack actions, whose probabilities are described by w.

The defender's objective in Equation (12) is to minimize the total load loss caused by the attacker's strategy, which can be determined by summing the (weighted) load loss incurred under all possible attack actions, $(x_a)/(x_a, y_{1a})/(x_a, y_{2a})/(x_a, y_{1a}, y_{2a})$, $\forall a \in A$, as specified in Equation (13). As described in Equations (14) and (15), the more defending resources a PP-link or a C-node is distributed with, the less likely it will be compromised under an attack. However, the defender has limited resources on either PP-links or C-nodes, as specified in Equations (16)–(19). The attacker has exactly the opposite objective in Equation (20), which is to maximize the expected load loss. The attack probabilities on different attacks action are specified in Equations (21) and (22).

The defender determines the strategy that minimizes the load loss under the assumption that the attacker already has the knowledge of the defending strategy. Since the defending strategy is determined before an attack happens, the defender does not minimize the load loss against any single attack action but all possible actions. That is, the optimal defending strategy in the proposed formulation minimizes the worst-case total load loss over all possible attack scenarios.

5.3. Vulnerability Assessment Procedure

The procedure of vulnerability assessment considering virtual CP-links is shown in Figure 3. It can be summarized as follows:

(1) The CPPS model is formed. The P-nodes and PP-links of the CPPS model are formed, based on the power flow model. The C-nodes and CC-links are then added, based on the one-to-one mapping rule between the P-nodes and C-nodes, and between the PP-links and CC-links, as shown in Figure 2.

(2) Choose one attack scenario of the attacker to successfully compromise the components (e.g., a PP-link/a PP-link and a C-node/a PP-link and two C-nodes), and calculate the total load loss as in Equations (1)–(7).

(3) Check whether all attack scenarios have been enumerated. If yes, go to Step 4, otherwise go to Step 2.

(4) Formulate the bi-level optimization problem as in Equations (12)–(21).

(5) The optimal defending resource distribution on the PP-links and C-nodes can be solved. Based on the result, the vulnerability of different components can be illustrated.

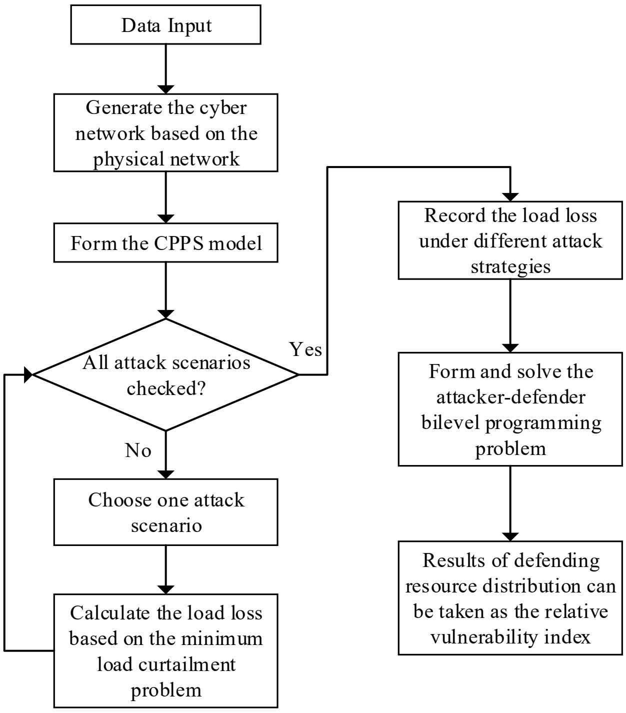
Data Input
Generate the cyber network based on the physical network
Form the CPPS model
All attack scenarios checked?
Yes
No
Choose one attack scenario
Calculate the load loss based on the minimum load curtailment problem
Record the load loss under different attack strategies
Form and solve the attacker-defender bilevel programming problem
Results of defending resource distribution can be taken as the relative vulnerability index

Figure 3. Flowchart of the CPPS vulnerability assessment procedure.

6. Case Studies

The modified IEEE 14-bus system is utilized to illustrate the proposed method in this paper, as shown in Figure 4. This system includes 14 P-nodes and 20 PP-links. Some C-nodes are added, based on the rule that every P-node is mapped to a C-node. Note that the 5th C-node is chosen as the control center. Every PP-link is mapped to a CC-link, and the CC-links form the cyber network. The configuration of the IEEE test system is extracted from MATPOWER, a MATLAB package for solving power flow problems [31]. All the experiments are simulated in MATLAB 9.5.0 (The MathWorks, Inc, Natick, MA, USA) on a DELL PC running Windows 10 with a 3.0 GHz Core i7 processor (Intel, Santa Clara, CA, USA) and 8 GB memory (Samsung, Seoul, South Korea).

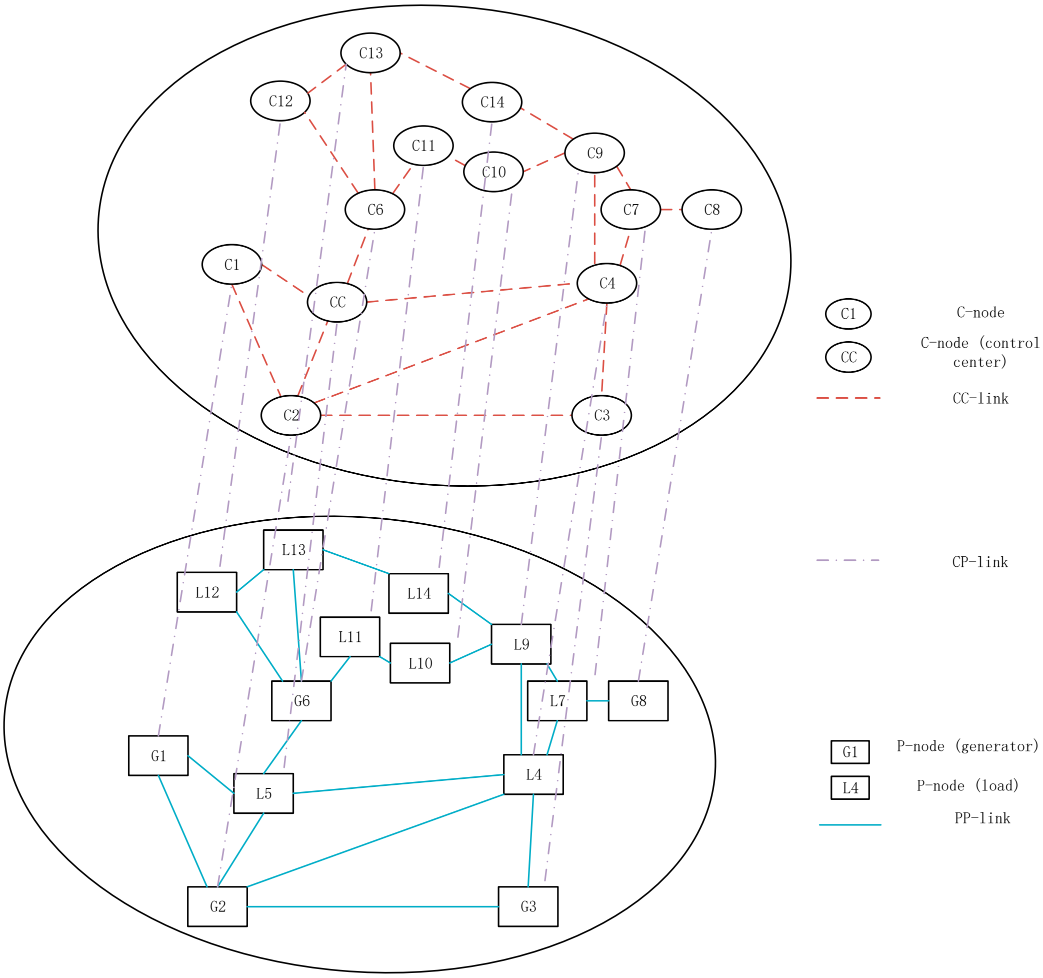

Figure 4. The modified IEEE 14-bus system.

In order to consider the impacts of a cyber-physical coordinated attack, three cases are considered:

(1) Case 1: only a PP-link is attacked, and the defender focuses on only defending PP-links;
(2) Case 2: one PP-link and one C-node are attacked, and the defender aims to defend both PP-links and C-nodes;
(3) Case 3: one PP-link and two C-nodes are attacked, as discussed previously; the defender also aims to defend both PP-links and C-nodes.

The branch power flow limit is set to be 1.3 times of the branch power flow in its initial state. After the attack, rearranging generator output is considered first. If this cannot settle the power flow off limit problem, load curtailment and line outage may be needed.

For the above three cases, up to one PP-link and two C-nodes may be compromised in each attack. In order to illustrate component vulnerability, the system loss is first calculated under the circumstance when there is no defense to attacks. That is, all components will fail once being attacked. The load loss is shown in Table 1. Among the attack actions in Table 1, PP, PP + C, PP + C + C represent Cases 1, 2, and 3 as mentioned above, respectively. The two columns with % symbols represent the extra load loss percentage of Case 2 over Case 1, and Case 3 over Case 1, respectively. Note that an attack against different C-nodes causes different results, and the results shown in Table 1 represent the worst cases among all possible scenarios.

Table 1. Load loss under different attack scenarios assuming no defense to attacks.

PP-Link	Load Loss by Different Attack Actions (MW) and the Extra Percentage (%)				
	PP (Case 1)	**PP + C (Case 2)**	**%**	**PP + C + C (Case 3)**	**%**
1-2	14.5088	14.5088	0	17.1003	**17.86**
1-5	5.4097	6.2701	15.9	6.5704	**21.46**
2-3	0	0	0	0	0
2-4	72.2991	74.5461	3.11	76.3861	5.65
2-5	21.2526	23.8454	12.20	24.7432	**16.42**
3-4	0	0	0	0	0
4-5	20.6592	21.6079	4.59	22.8152	10.44
4-7	18.1528	18.2292	0.42	18.2611	0.60
4-9	8.046	8.1913	1.81	8.238	2.39
5-6	6.3524	6.8563	7.93	7.15	12.56
6-11	9.4161	9.4161	0	9.4161	0
6-12	7.2594	7.2594	0	7.2594	0
6-13	29.325	31.976	9.04	32.2755	10.06
7-8	28.073	29.7059	5.82	30.0918	7.19
8-9	29.07	29.0721	0.0072	29.0753	0.018
9-10	6.5541	6.5541	0	6.5541	0
9-14	9.3228	9.3228	0	9.3228	0
10-11	2.7341	2.7341	0	2.7342	0.0048
12-13	0	0	0	0	0
13-14	5.756	5.756	0	5.756	0

It is obvious that an attack against different PP-links may lead to different load losses. Moreover, after a PP-link is compromised, the coordinated attack against the C-nodes is likely to cause a higher load loss. As explained in Section 3, the physical failures and cyber failures have an impact over another subsystem. As a matter of fact, in the simulation process, a C-node failure occasionally leads to communication interruption such that some physical components cannot be monitored or controlled, which causes the worse-case system load loss situation. In the worst case when the PP-link 1-5 is tripped, further attack against 2 C-nodes would cause up to 21.46% extra load loss.

Based on the knowledge of load loss under different attack actions, the defending resources are then distributed by solving the bi-level programming problem. The total amount of defending resources is set as 50% of the total number of vulnerable components. In this modified IEEE 14 bus system, there are 20 PP-links and 14 C-nodes vulnerable to malicious attacks from outsiders, and therefore we let $D_p = 10$ and $D_c = 7$. Distribution of defending resources for PP-links and C-nodes in Case 3 is shown in Table 2. The expected load loss after defending resources are distributed under different attack cases as shown in Table 3.

Table 2. Distributions of defending resources in Case 3.

PP-Link	Defending Resource	C-Node	Defending Resource
1-2	0.7126	1	0
1-5	0	2	0.0001
2-3	0	3	0
2-4	1.6066	4	0.8996
2-5	0.9401	5	0
3-4	0	6	0
4-5	0.9222	7	0
4-7	0.8445	8	0
4-9	0.3081	9	1.9131
5-6	0.1133	10	1.9394
6-11	0.4216	11	0
6-12	0.2232	12	0
6-13	1.1329	13	1.0694

Table 2. *Cont.*

PP-Link	Defending Resource	C-Node	Defending Resource
7-8	1.0954	14	1.1781
8-9	1.113		
9-10	0.1364		
9-14	0.4145		
10-11	0		
12-13	0		
13-14	0.0157		

Table 3. Expected load loss after distributions of defensive resources.

PP-Link	Load Loss by Different Attack (MW) and the Extra Percentage (%)				
	PP (Case 1)	PP + C (Case 2)	%	PP + C + C (Case 3)	%
1-2	5.642	5.6549	0.23	5.6661	**0.43**
1-5	5.4097	5.5575	2.73	5.6107	**3.72**
2-3	0	0	0	0	0
2-4	5.642	5.6549	0.23	5.6661	0.43
2-5	5.642	5.6549	0.23	5.6661	**0.43**
3-4	0	0	0	0	0
4-5	5.642	5.6549	0.23	5.6661	0.43
4-7	5.642	5.6549	0.23	5.6661	0.43
4-9	5.642	5.6549	0.23	5.6661	0.43
5-6	5.642	5.6549	0.23	5.6661	0.43
6-11	5.642	5.6549	0.23	5.6657	0.42
6-12	5.642	5.6549	0.23	5.6657	0.42
6-13	5.642	5.6549	0.23	5.6661	0.43
7-8	5.642	5.6549	0.23	5.6661	0.43
8-9	5.642	5.6549	0.23	5.6658	0.42
9-10	5.642	5.6549	0.23	5.6656	0.42
9-14	5.642	5.6549	0.23	5.6655	0.42
10-11	2.7341	2.7341	0	2.7342	0.0036
12-13	0	0	0	0	0
13-14	5.642	5.6549	0.23	5.6657	0.42

By comparing data between Tables 1 and 3, it is obvious that the existence of defending resources decreases the expected load loss. A much more exciting result from Table 3 is that in the worst case (i.e. an attack on PP-link 1-5), the coordinated attack on two C-nodes only causes 3.7% extra loss from the original 21.46%. Meanwhile, other devastating attack results (e.g., attacks on PP-links 1–2 or 2–5) are reduced from 17.86% and 16.42% to 0.43%. These results show that with well-planned cyber defending resources distributed, the extra damage to the system caused by the attacker can be reduced to a minimum level. By defending the cyber components, the CPPS vulnerability can be significantly reduced.

7. Conclusions and Future Work

As a growing number of information and communication infrastructures are applied to a modern power system, the CPPS is formed and has drawn great attention of both researchers and industry. This paper investigates the interactions between physical components and cyber components in the CPPS, and proposes a CPPS interactive model framework. Then, the interactions are considered in the system load curtailment operation under malicious attacks on both physical and cyber components. Based on this, the game theory-based attacker–defender bi-level programming problem is formulated, and the component vulnerability is examined from solving the optimal defending resource distribution. The effectiveness of this model is demonstrated by the simulation results.

The future work includes incorporating more complicated components behaviors (e.g., transmission delay in CC-links) into the developed model and considering more detailed interactions among CP-links.

Author Contributions: K.C. proposed the methodological framework and mathematical model, and performed the simulations; F.W., C.-L.T., M.C., Z.Y., H.Z., and H.S. analyzed the results, reviewed the manuscript, and provided suggestions. All authors discussed the simulation results and agreed for submission.

Funding: This work is jointly supported by National Key Research and Development Program of China (2017YFB0902900), and China Southern Power Grid Key Project (No. GZHKJXM20160035).

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

Nomenclature

P-node	Physical node
C-node	Cyber node
PP-link	Physical-physical link
CC-link	Cyber-cyber link
CP-link	Cyber-physical link
L	The collection of load in the system
L_a	The collection of controllable load in the system
L_{off}	The collection of uncontrollable load in the system
G	The collection of generators in the system
G_a	The collection of controllable generators in the system
G_{off}	The collection of uncontrollable generators in the system
ΔP_{Li}	The power changed at load i (MW)
ΔP_{Gj}	The power changed at generator j (MW)
$P_{L_i}^{m}$	The lower limit of load i (MW)
$P_{L_i}^{M}$	The upper limit of load i (MW)
$P_{G_j}^{m}$	The lower limit of generator j (MW)
$P_{G_j}^{M}$	The upper limit of generator j (MW)
P_i	The real power at node i (MW)
ΔP_i	The change of real power at node i (MW)
V_i	The voltage amplitude at node i (kV)
θ_{ij}	The angle difference of branch ij (rad)
$\Delta\theta_{ij}$	The change of angle difference of branch ij (rad)
B_{ij}	The susceptance of branch ij in the bus admittance matrix (S)
N	The collection of all nodes in the system
n	The number of nodes in the system
d_p	The defending resource distributed to PP-links
d_c	The defending resource distributed to C-nodes
a	A possible attack action
w	The attacker's weight on different attack actions
w_a	The attacker's weight on attack action a
R_a	The total load curtailment when attack action a is launched (MW)
x_a	The PP-link targeted by attack action a
y_{1a}	The first C-node targeted by attack action a
y_{2a}	The second C-node targeted by attack action a
p_{x_a}	The probability of the PP-link x_a successfully compromised by the attacker
$p_{y_{1a}}$	The probability of the first C-node y_{1a} successfully compromised by the attacker
$p_{y_{2a}}$	The probability of the second C-node y_{2a} successfully compromised by the attacker
$R_{(x_a,y_{1a},y_{2a})}$	The load curtailment when components (x_a, y_{1a}, y_{2a}) are successfully compromised by the attacker (MW)
$R_{(x_a,y_{1a})}$	The load curtailment when components (x_a, y_{1a}) are successfully compromised by the attacker (MW)

$R_{(x_a,\ y_{2a})}$	The load curtailment when components (x_a, y_{2a}) are successfully compromised by the attacker (MW)
$R_{(x_a)}$	The load curtailment when components (x_a) are successfully compromised by the attacker (MW)
β_p	The failure coefficient of PP-links
β_c	The failure coefficient of C-nodes
N_{PP}	The number of PP-links in the system
N_C	The number of C-nodes in the system
D_p	The total defending resource for PP-links
D_c	The total defending resource for C-nodes

References

1. Kim, K.D.; Kumar, P.R. Cyber-physical systems: A perspective at the centennial. *Proc. IEEE* **2012**, *100*, 1287–1308.
2. Mamo, X.; Mallet, S.; Coste, T.; Grenard, S. Distribution automation: The cornerstone for smart grid development strategy. In Proceedings of the IEEE Power & Energy Society General Meeting, Calgary, AB, Canada, 26–30 July 2009; pp. 1–6.
3. Kirschen, D.; Bouffard, F. Keeping the lights on and the information flowing. *IEEE Power Energy Mag.* **2009**, *7*, 50–60. [CrossRef]
4. Tram, H. Technical and operation considerations in using smart metering for outage management. In Proceedings of the IEEE PES Transmission and Distribution Conference and Exposition, Chicago, IL, USA, 21–24 April 2008; pp. 1–3.
5. Liang, G.; Weller, S.R.; Zhao, J.; Luo, F.; Dong, Z.Y. The 2015 ukraine blackout: Implications for false data injection attacks. *IEEE Trans. Power Syst.* **2016**, *32*, 3317–3318. [CrossRef]
6. Susuki, Y.; Koo, T.J.; Ebina, H.; Yamazaki, T.; Ochi, T.; Uemura, T.; Hikihara, T. A hybrid system approach to the analysis and design of power grid dynamic performance. *Proc. IEEE* **2012**, *100*, 225–239S. [CrossRef]
7. Yampolskiy, M.; Horvath, P.; Koutsoukos, X.D.; Xue, Y.; Sztipanovits, J. Taxonomy for description of cross-domain attacks on CPS. In Proceedings of the 2nd ACM International Conference on High Confidence Networked Systems, Philadelphia, PA, USA, 9–11 April 2013; pp. 135–142.
8. Yampolskiy, M.; Horváth, P.; Koutsoukos, X.D.; Xue, Y.; Sztipanovits, J. A language for describing attacks on cyber-physical systems. *Int. J. Crit. Infrastruct. Prot.* **2015**, *8*, 40–52. [CrossRef]
9. Petnga, L.; Xu, H. Security of unmanned aerial vehicles: dynamic state estimation under cyber-physical attacks. In Proceedings of the 2016 International Conference on Unmanned Aircraft Systems (ICUAS), Arlington, VA, USA, 7–10 June 2016; pp. 811–819.
10. Li, Y.; Shi, L.; Cheng, P.; Chen, J.; Quevedo, D.E. Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach. *IEEE Trans. Autom. Control* **2015**, *60*, 2831–2836. [CrossRef]
11. Mo, Y.; Chabukswar, R.; Sinopoli, B. Detecting integrity attacks on SCADA systems. *IEEE Trans. Control Syst. Technol.* **2014**, *22*, 1396–1407.
12. Mo, Y.; Sinopoli, B. Secure estimation in the presence of integrity attacks. *IEEE Trans. Autom. Control* **2015**, *60*, 1145–1151. [CrossRef]
13. Fawzi, H.; Tabuada, P.; Diggavi, S. Secure estimation and control for cyber-physical systems under adversarial attacks. *IEEE Trans. Autom. Control* **2014**, *59*, 1454–1467. [CrossRef]
14. Pasqualetti, F.; Carli, R.; Bullo, F. A distributed method for state estimation and false data detection in power networks. In Proceedings of the 2011 IEEE International Conference on Smart Grid Communications (SmartGridComm), Brussels, Belgium, 17–20 October 2011; pp. 469–474.
15. Mo, Y.; Garone, E.; Casavola, A.; Sinopoli, B. False data injection attacks against state estimation in wireless sensor networks. In Proceedings of the 49th IEEE Conference on Decision and Control (CDC), Atlanta, GA, USA, 15–17 December 2010; pp. 5967–5972.
16. Li, Y.; Quevedo, D.E.; Dey, S.; Shi, L. A game-theoretic approach to fake-acknowledgment attack on cyber-physical systems. *IEEE Trans. Signal Inf. Proc. Netw.* **2017**, *3*, 1–11. [CrossRef]
17. Poisel, R. *Modern Communications Jamming: Principles and Techniques*; Artech House: Norwood, MA, USA, 2011.

18. Zhang, H.; Cheng, P.; Shi, L.; Chen, J. Optimal DoS attack scheduling in wireless networked control system. *IEEE Trans. Control Syst. Technol.* **2016**, *24*, 843–852. [CrossRef]
19. Zhang, H.; Cheng, P.; Shi, L.; Chen, J. Optimal denial-of-service attack scheduling with energy constraint. *IEEE Trans. Autom. Control* **2015**, *60*, 3023–3028. [CrossRef]
20. Zhu, M.; Martínez, S. On the performance analysis of resilient networked control systems under replay attacks. *IEEE Trans. Autom. Control* **2014**, *59*, 804–808. [CrossRef]
21. Deng, R.; Zhuang, P.; Liang, H. CCPA: coordinated cyber-physical attacks and countermeasures in smart grid. *IEEE Trans. Smart Grid* **2017**, *8*, 2420–2430. [CrossRef]
22. Li, Z.; Shahidehpour, M.; Alabdulwahab, A.; Abusorrah, A. Bi-level model for analyzing coordinated cyber-physical attacks on power systems. *IEEE Trans. Smart Grid* **2016**, *7*, 2260–2272. [CrossRef]
23. Soltan, S.; Yannakakis, M.; Zussman, G. Power grid state estimation following a joint cyber and physical attack. *IEEE Trans. Control Netw. Syst.* **2018**, *5*, 499–512. [CrossRef]
24. Xin, S.; Guo, Q.; Sun, H.; Zhang, B.; Wang, J.; Chen, C. Cyber-physical modeling and cyber-contingency assessment of hierarchical control systems. *IEEE Trans. Smart Grid* **2015**, *6*, 2375–2385. [CrossRef]
25. Ilic, M.D.; Xie, L.; Khan, U.A.; Moura, J.M. Modeling of future cyber-physical energy systems for distributed sensing and control. *IEEE Trans. Syst. Man Cybern. Part A Syst. Hum.* **2010**, *40*, 825–838. [CrossRef]
26. Buldyrev, S.V.; Parshani, R.; Paul, G.; Stanley, H.E.; Havlin, S. Catastrophic cascade of failures in interdependent networks. *Nature* **2010**, *464*, 1025. [CrossRef]
27. Vespignani, A. Complex networks: The fragility of interdependency. *Nature* **2010**, *464*, 984. [CrossRef]
28. Falahati, B.; Fu, Y.; Wu, L. Reliability assessment of smart grid considering direct cyber-power interdependencies. *IEEE Trans. Smart Grid* **2012**, *3*, 1515–1524. [CrossRef]
29. Falahati, B.; Fu, Y. Reliability assessment of smart grids considering indirect cyber-power interdependencies. *IEEE Trans. Smart Grid* **2014**, *5*, 1677–1685. [CrossRef]
30. Bard, J.F. *Practical Bi-Level Optimization: Algorithms and Applications*; Springer Science & Business Media: Berlin, Germany, 2013.
31. Zimmerman, R.D.; Murillo-Sánchez, C.E.; Thomas, R.J. MATPOWER: Steady-State Operations, Planning and Analysis Tools for Power Systems Research and Education. *IEEE Trans. Power Syst.* **2011**, *26*, 12–19. [CrossRef]