electronics

MDPI

Article

Robustness of Cyber-Physical Systems against Simultaneous, Sequential and Composite Attack

Pengshuai Cui [1], Peidong Zhu [1,2,*], Peng Xun [1] and Chengcheng Shao [1]

[1] College of Computer, National University of Defense Technology, Changsha 410073, China; cuipengshuai@nudt.edu.cn (P.C.); p.xun@outlook.com (P.X.); chch.shao@outlook.com (C.S.)

[2] Department of Electronic Information and Electrical Engineering, Changsha University, Changsha 410022, China

* Correspondence: pd.zhu@outlook.com; Tel.: +86-155-0748-6081

Received: 7 August 2018; Accepted: 11 September 2018; Published: 13 September 2018

check for updates

Abstract: In this paper, a failure model of Cyber-Physical systems and an attack model are proposed. We divide the attacks into three kinds: simultaneous attack, sequential attack and composite attack. Through numerical simulations, we find that: (1) the sequential attack may bring more damage in single physical systems; (2) the coupling process of cyber system and physical systems makes it possible that sequential attack causes more damage than simultaneous attacks when the attackers only attack the cyber system; (3) with some target sets, composite attack leads to more failures than both simultaneous attack and sequential attack. The above results suggest that defenders should take all the three kinds of attacks into account when they select the critical nodes.

Keywords: robustness; cyber physical systems; simultaneous attack; sequential attack; composite attack

1. Introduction

Physical systems cover the majority of Critical Infrastructures (CIs), which are the cornerstone of social prosperity and development. The typical physical systems include power grids, transportation networks, water supply systems, medical systems, etc. The safe operation of physical systems matters a lot to the safety and stability of the society. However, system failures and malicious attacks often occur in physical systems, and it is inevitable that some components of the systems would be broken down. Robustness, which is defined as the survivability under failure or attack, is one of the most important properties of a system. In the meantime, robustness is a relative term, a system may be robust under an attack strategy but vulnerable under another attack strategy. Thus, understanding how attackers would attack the system is of great importance.

Many researchers focus on the robustness and attack strategy of physical systems, especially on the power grid. Simultaneous attack on a power grid is studied in [1], and the loss of generation power and time to reach steady-state are used to evaluate the damage to the power grid. Sequential attack on a power grid is studied in [2–5], which shows that sequential attack brings new vulnerability to the power grid. More generally, there are also researchers trying to build a universal model to describe the robustness of physical systems but not limited to the power grid, and a complex network model is used [6–8]. However, the research in [6–8] only considers the simultaneous attack but neglects the sequential attack.

In recent years, information systems are coupled with the physical systems to achieve real time monitoring and controlling. The physical systems and the information system form the Cyber-Physical Systems (CPS), which have attracted extensive attention recently [9,10]. The coupling process makes it possible to damage the physical systems through cyber systems [11–17] and makes the physical systems more vulnerable. Currently, it is difficult for both IT people and people from physical systems to understand the risk. For the former, they know little about the physical process and for the latter, they are not skilled in cyber security [18]. When we design the robustness model for the CPS, the characteristics of the cyber system and the process of physical system must be included. The existing model mainly applies to the power grid [19–21], and the universal model such as interdependent networks [22,23] can not grasp the characteristics of either cyber systems or physical systems. Thus, a new model should be built to describe the coupling CPS, which will appear in Section 2.

Meanwhile, there is little research about sequential attack on interdependent Cyber-Physical networks, which should be further studied. In addition, there are other forms of attacks that are different from simultaneous and sequential ones and we call them composite attacks. We will study the attack effect of simultaneous attack, sequential attack and composite attack, and evaluate whether the composite attack would bring new vulnerability.

The rest of the paper is organized as follows: the failure model, attack model and problem definition are given in Section 2. In Section 3, numerical simulations are conducted. At the end of the paper, the discussions and conclusions are given.

2. The Model

In this section, we propose a Cyber-Physical failure model, in which the measurement of robustness, and the cascading failure process are introduced. Then, target set, attack unit, attack tuple and attack sequence are defined.

2.1. The Failure Model of Interdependent Cyber-Physical Systems

The interdependent Cyber-Physical system containing N nodes can be divided into cyber sub-network and physical sub-network. Without loss of generality, we set that there are $N/2$ nodes in the cyber sub-network and $N/2$ nodes in the physical subnetwork, denoted by N_C and N_P. We use the one-to-one correspondence [22] to build the dependence between cyber sub-network and physical sub-network. The nodes from cyber sub-network and physical subnetwork come in pairs. For example, node c_i from a cyber sub-network and node p_i from a physical sub-network are a pair. Then, if c_i stops functioning, node p_i would stop functioning too and, if node p_i stops functioning, node c_i would fail too. In the cyber sub-network, to maintain a functional, a cyber node must (i) belong to the giant component of the cyber sub-network and (ii) meet the requirement that its support node from a physical sub-network is survival. We use the load-induced model [24] to describe the physical sub-network. The initial load $L_i(0)$ of node i is defined as:

$$L_i(0) = k_i^{\alpha}. \tag{1}$$

In Equation (1), k_i is the intra-degree of node i, and α is a tunable parameter. The capacity C_i of node i is proportional to its initial load:

$$C_i = (1+\lambda)L_i(0). \tag{2}$$

In Equation (2), λ is also a tunable parameter that represents the tolerance of the physical sub-network against attack or failure. Larger λ brings more robustness to the physical sub-network; however, larger λ also means that it will cost more when building the physical sub-network. After state s, if node i fails, its load would be redistributed to its neighbor nodes. Then, in state $s+1$, the load of its neighbor node j would become:

$$L_j(s+1) = L_j(s) + \frac{L_j(s) \times L_i(s)}{\sum_{n \in \Gamma_i} L_n(s)}. \tag{3}$$

In Equation (3), Γ_i represents the set of neighbor nodes of node i. To maintain functioning, a physical node i must meet the following conditions: (i) its load is not larger than its capacity, which means $L_i \leq C_i$; and (ii) its support node from cyber sub-network is still survival.

The attack on a Cyber-Physical system is represented by removing a fraction of nodes (how to remove the nodes will be described in Section 2.2). Generally, the physical nodes are well protected, so we assume that the removing part is all from the cyber sub-network. The ration of survival nodes to initial nodes is used to measure the robustness against attack sequence AS_i, denoted by R_{AS_i}:

$$R_{AS_i} = \frac{N'_C + N'_P}{N_C + N_P}. \tag{4}$$

In Equation (4), N'_C and N'_P are the survival nodes in the cyber sub-network and physical sub-network after being attacked. A specific example of the model is shown in Figure 1.

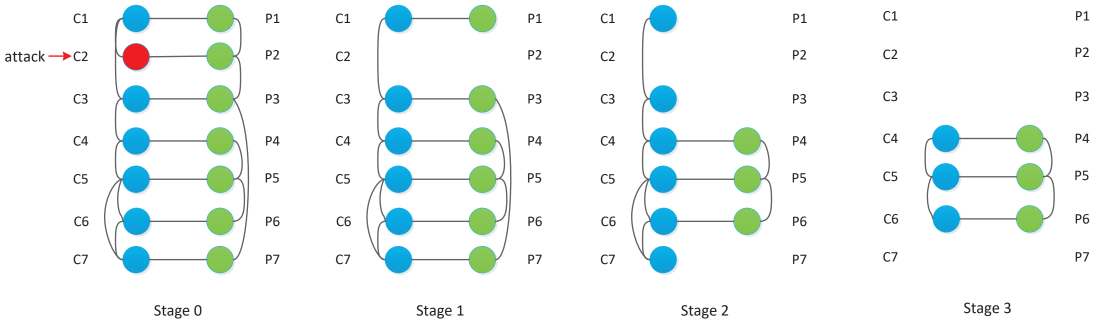


Figure 1. A specific example of the Cyber-Physical network failure model.

In Figure 1, there are 14 nodes in the Cyber-Physical network, and $N_C = N_P = 7$. The values of α and λ are 1 and 0.5, respectively. In stage 0, attackers attack node $C2$, and $C2$ fails. In stage 1, node $P2$ fails because its support node $C2$ has been failed in stage 0. In stage 2, the load of $P2$ has been redistributed to node $P1$ and $P3$; the load of $P1$ has been changed to $5/3$ and exceeds its capacity $3/2$, so node $P1$ fails; the load of $P3$ has been changed to $10/3$ and exceeds its capacity 3, so node P3 fails; then, the load of P3 has been redistributed to node P7, and the load of P7 has been changed to $13/3$ and exceeds its capacity $3/2$, so node P7 fails. In Stage 3, nodes $C1$, $C3$ and $C7$ fail because their support nodes $P1$, $P3$ and $P7$ have failed in stage 2. Finally, the interdependent Cyber-Physical sub-network reaches the stable state. Each node in the cyber sub-network belongs to the giant component and has a support node from the physical sub-network, and each node in the physical sub-network is not overloaded and has a support node from the cyber sub-network.

2.2. Attack Model

To describe our attack model clearly, the following definitions are given.

Definition 1. *Target set, denoted by T, T is a set of nodes that the attackers have the ability to attack, and all nodes in the attack set would be removed by attackers. The number of nodes in target set is denoted by T_n.*

Definition 2. *Attack unit a is the basic unit the attackers can attack, which means a specific node could be attacked and removed by attackers, and we have $a \in T$.*

Definition 3. *Attack set, denoted by $A = [a_1, a_2, \cdots, a_k]$ is a set of attack units that attackers would attack simultaneously, and $A \subset T$. $|A|$ represents the number of elements of the attack set. The attack set has the following characteristics: (i) certainty, which means for any attack unit a, either $a \in A$ or $a \notin A$; (ii) exclusion, which means for any two attack units a_i and a_j in an attack sets, $a_i \neq a_j$; (iii) disorder, for example, $[a_1, a_2, a_3] = [a_3, a_1, a_2]$.*

Definition 4. *Attack sequence, denoted by* $AS = \{A_1, A_2, \cdots, A_k\}$*, is a series of ordered attack sets. It represents the attack strategy of attackers. It has the following characteristics: (i) the most important characteristic is orderly organized, for example,* $\{A_1, A_2\} \neq \{A_2, A_1\}$*; (ii) any two attack sets in an attack sequence have no intersection, which means* $A_i \cap A_j = \emptyset$*; and (iii) an attack sequence includes all the attack units in a target set, which means* $T = \bigcup AS = A_1 \cup A_2 \cup \cdots \cup A_k$*. The attack strength of an attack sequence, denoted by* $|AS|$*, decides how many nodes would be removed from the network, obviously,* $T_n = |AS| = \sum_{n=1}^{N} |A_n|$.

Given a specific attack sequence, the attack process is as follows (see Algorithm 1).

Algorithm 1 The attack process in interdependent load-induced Cyber-Physical systems.

```
INPUT: Attack sequence $AS = \{A_1, A_2, \cdots A_n\}$
OUTPUT: $R_{AS}$
Set $N'_C = N_C$, $N'_P = N_P$
for $i = 0 \rightarrow n$ do
    for $j = 1 \rightarrow |A_i|$ do
        fail $a_j$, $N'_C = N'_C - 1$
    end for
    changetag=true
    while changetag==true do
        changetag=false
        for $l = 1 \rightarrow N_C$ do
            if node $c_l$ is survival & $c_l \notin GP$ then
                fail $c_l$, $N'_C = N'_C - 1$, changetag=true
            end if
        end for
        for $l = 1 \rightarrow N_C$ do
            if node $c_l$ is survival & its support node has been failed then
                fail $c_l$, $N'_C = N'_C - 1$, changetag=true
            end if
        end for
        redistribute the load according to Equation (4)
        for $l = 1 \rightarrow N_P$ do
            if node $p_l$ is survival & its load exceed its capacity then
                fail $p_l$, $N'_P = N'_P - 1$, changetag=true
            end if
        end for
        for $l = 1 \rightarrow N_P$ do
            if node $l$ is survival & its support node has been failed then
                fail $p_l$, $N'_P = N'_P - 1$, changetag=true
            end if
        end for
    end while
end for
return $R_{AS} = (N'_C + N'_P)/(N_C + N_P)$
```

In a initial stage, obtain the attack sequence $AS = \{A_1, A_2 \cdots A_n\}$, set $N'_C = N_C, N'_P = N_P, i = 1$;

Step 1: Fail all the nodes in attack set A_i, and set $N'_C = N'_C - |A_i|$;

Step 2: Find the giant components of a cyber sub-network, check all the nodes in the cyber-subnetwork, and fail the nodes that do not belong to the giant component. When one node is removed, set $N'_C = N'_C - 1$;

Step 3: Check all nodes in the cyber-subnetwork, and fail the nodes whose support nodes have failed. When one node fails, set $N'_P = N'_P - 1$;

Step 4: Check all the nodes in the physical sub-network, fail all the nodes whose loads exceed their capacities, and redistribute the loads according to Equation (3). When one node is removed, set $N'_P = N'_P - 1$;

Step 5: Check all nodes' physical-subnetworks, and fail the nodes whose support nodes have been failed. When one node fails, set $N'_P = N'_P - 1$;

Step 6: If there have been any nodes that failed in Step 2–Step 5, go to Step 2.

Step 7: $i = i + 1$; if $i <= n$, go to Step 1;

Step 8: Evaluate the robustness, return $R_{AS} = (N'_C + N'_P)/(N_C + N_P)$.

2.3. Problem Definition

Given a specific target set, if attacking simultaneously brings large damage to the network, these nodes in the target set would be considered as critical nodes and well protected. However, for some target sets [2], the network is robust under simultaneous attack but vulnerable under sequential attack in the power grid, so the defender should also consider these nodes that are removed sequentially as critical ones. In this paper, we try to answer the following questions: (1) whether the sequential attack would cause larger damage with some target sets in a more universal model, for example, load-induced model; (2) whether the sequential attack causes new vulnerability in an interdependent Cyber-Physical network when the attack can be only on a cyber subnetwork; (3) whether the following attack sequences exist, which are not sequential attacks and simultaneous attacks but would cause more damage. If these attack sequences exist, it means that some critical nodes are ignored, which should be realized by the defenders. First, we define the conception of simultaneous attack and sequential attack; in fact, they are only two special attack sequences:

Definition 5. *Simultaneous attack, denoted by AS_{si} in an attack sequence, there is only one attack set, such as $\{[a^1, a^2 \cdots a^n]\}$.*

Definition 6. *Sequential attack, denoted by AS_{se} in an attack sequence, in each set, there is only one attack unit, such as $\{[a^1], [a^2] \cdots [a^n]\}$.*

For a given target set who has n attack units, there are $f(n)$ kinds of attack sequences, and we have:

$$f(n) = \sum_{n^1=1}^{n} \sum_{n^2=1}^{n-n^1} \cdots \sum_{n^s=1}^{n-(n^1+n^2+\cdots+n^{s-1})} C_n^{n^1} \times C_{n-n^1}^{n^2} \cdots \times C_{n-(n^1+n^2+\cdots+n^{s-1})}^{n^s}. \tag{5}$$

Thus, for a given n, there are many kinds of attack sequences. For example, $f(4) = 81$ and $f(5) = 541$. There are many other attack sequences besides the sequential attack and simultaneous attack. The question 3 can be expressed as:

$$\begin{cases} R_{AS_i} < R_{AS_j}, \\ \bigcup AS_i = \bigcup AS_j = T, \\ AS_i \neq AS_{si}, \\ AS_j \neq AS_{se}. \end{cases} \tag{6}$$

3. Numerical Simulations and Analysis

This section is divided into three parts: first, we check whether the sequential attack can cause more damage than simultaneous attack in a load-induced network; then, whether the sequential attack can bring more damage than a simultaneous attack in an interdependent Cyber-Physical network is evaluated; finally, we find new vulnerability in some attack sequences, which are neither sequential attack nor simultaneous attack.

3.1. Sequential Attack against Single Physical Networks

To check the attack effect of a sequential attack on single physical networks, we use the IEEE-39 bus [25] to do the simulations. Each bus is treated as a node and each transmission line is treated as a link. The structure of IEEE-39 bus network is shown in Figure 2. In the simulations, $\lambda = 0.6$ and $\alpha = 1$. The attack process on a single physical network is shown in Figure 3.

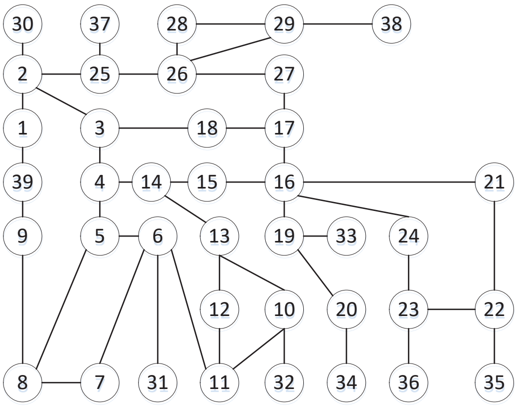


Figure 2. The IEEE 39bus as a network.

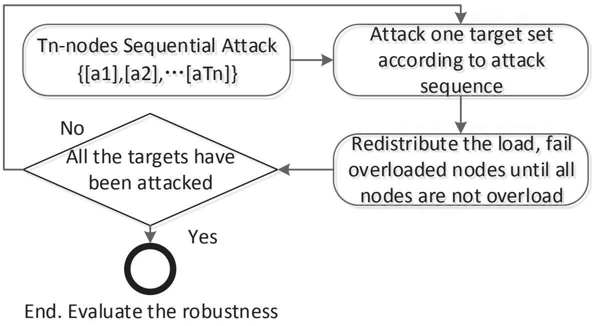

Tn-nodes Sequential Attack
{[a1],[a2],⋯[aTn]}
Attack one target set according to attack sequence
Redistribute the load, fail overloaded nodes until all nodes are not overload
All the targets have been attacked
No
Yes
End. Evaluate the robustness

Figure 3. Flow chart of the sequential attack process in a load-induced Cyber-Physical system.

The results are shown in Tables 1 and 2. With the target sets in Table 1, a simultaneous attack would cause more damage. For example, if the attackers use attack sequence {[12,11]}, none of the nodes would survive against the attack; however, if the attackers use the attack sequence {[12],[11]}, 37 nodes would survive against the attack. The results shown in Table 1 meet most people's expectations: it would cost more to attack simultaneously, so it can surely cause more damage. With the situation that attack sequence {[12,11]} causes more damage, node 11 and node 12 will be considered as critical nodes and well protected.

Table 2 shows the target sets with whom the sequential attack would cause more damage. For example, with attack sequence {[7,8]}, there are 37 nodes surviving the attack; however, with attack sequence {[7],[8]}, none would survive. These attack sequences bring new vulnerability. Only taking simultaneous attacks into account, node 7 and node 8 are not critical nodes and won't be well protected, but attackers can attack them sequentially and cause dramatic damage.

We should notice that the target sets in Table 1 or Table 2 are only small parts of all target sets. There are 39 nodes in the network, so there are $C_{39}^{2} = 741$ different kinds of target sets. In total, the former comprises 1.75% and the latter comprises 3.64%. We also do simulations with BA networks that are randomly generated, and the results imply that in these networks there also exist target sets with which sequential attack would cause more damage.

Table 1. Target sets with whom a simultaneous attack would cause more damage.

Attack Sequence	Survival Nodes	Attack Sequence	Survival Nodes
{[2,3]}	0	{[2],[3]}	1
{[6,5]}	0	{[6],[5]}	1
{[6,11]}	0	{[6],[11]}	1
{[10,11]}	0	{[10],[11]}	1
{[10,13]}	0	{[10],[13]}	1
{[12,11]}	0	{[12],[11]}	37
{[18,3]}	0	{[18],[3]}	37
{[18,17]}	0	{[18],[17]}	37
{[20,34]}	0	{[20],[34]}	37
{[22,21]}	0	{[22],[21]}	37
{[22,23]}	0	{[22],[23]}	1
{[23,22]}	0	{[23],[22]}	1
{[23,24]}	0	{[23],[24]}	37

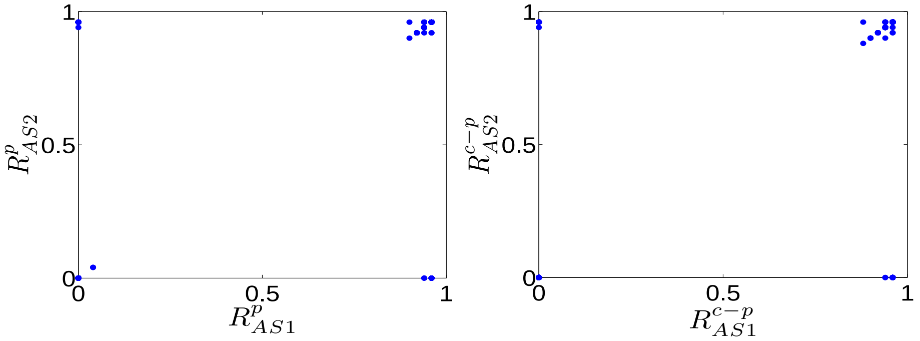
Table 2. Target sets with whom sequential attack would cause more damage.

Attack Sequence	Survival Nodes	Attack Sequence	Survival Nodes
{[1,2]}	1	{[1],[2]}	0
{[3,4]}	37	{[3],[4]}	3
{[4,3]}	37	{[4],[3]}	1
{[4,14]}	37	{[4],[14]}	0
{[5,4]}	37	{[5],[4]}	0
{[7,6]}	1	{[7],[6]}	0
{[7,8]}	37	{[7],[8]}	0
{[8,7]}	37	{[8],[7]}	0
{[12,13]}	34	{[12],[13]}	0
{[13,12]}	34	{[13],[12]}	0
{[13,14]}	37	{[13],[14]}	0
{[14,4]}	37	{[14],[4]}	0
{[14,13]}	37	{[14],[13]}	0
{[15,14]}	37	{[15],[14]}	0
{[15,16]}	10	{[15],[16]}	0
{[17,16]}	10	{[17],[16]}	0
{[17,27]}	37	{[17],[27]}	0
{[19,16]}	34	{[19],[16]}	3
{[20,19]}	36	{[20],[19]}	1
{[21,16]}	33	{[21],[16]}	0
{[24,16]}	32	{[24],[16]}	0
{[25,26]}	37	{[26],[25]}	1
{[26,25]}	37	{[26],[25]}	3
{[27,26]}	3	{[27],[26]}	0
{[28,29]}	1	{[28],[29]}	0
{[29,26]}	35	{[29],[26]}	1
{[30,2]}	37	{[30],[2]}	0
{[31,6]}	37	{[31],[6]}	0
{[32,10]}	37	{[32],[10]}	0
{[35,22]}	37	{[35],[22]}	0
{[36,23]}	37	{[36],[23]}	0
{[38,29]}	37	{[38],[29]}	0

3.2. Sequential Attack in Interdependent Cyber Physical System

In this subsection, we would mainly focus on two questions: (i) in the Cyber-Physical system, whether the target sets exist with whom sequential attack would cause more damage; and (ii) if the target sets exist, are they one-to-one corresponding to the single physical subnetwork? According to the model we propose in Section 2, we design the following simulations. An interdependent network with $n = 100$ is constructed, and the cyber subnetwork and physical subnetwork have the same size($N^C = N^P = 50$). The two subnetworks are generated by the algorithm proposed by Barabasi et al. [26], so the two subnetworks are scale-free and follow power-law distribution $P(k) = 2m^2k^{-s}$. In the simulations, $s = 3$ and we set $m = 2$. There are two targets in the attack sets, so $T_n = 2$, and there are $C_{50}^2 = 1225$ different target sets. Two attack sequences—sequential attack and simultaneous attack—are tested.

First, we construct a single physical network, set $\lambda = 0.5$ and $\alpha = 1$, and record the subnetwork's structure and initial state. The robustness of the single physical subnetwork under simultaneous attack and sequential attack is shown in Figure 4a. Then, we build an interdependent Cyber-Physical network, and the structure of the physical subnetwork is the same as the structure of a single physical network we build before, and we also set $\lambda = 0.5$ and $\alpha = 1$. The robustness of the interdependent Cyber-Physical network is shown in Figure 4b. We could see from the two figures that the results are similar but also have differences.



(**a**) Robustness of single physical subnetwork (**b**) Robustness of interdependent network

Figure 4. Robustness under simultaneous attack and sequential attack. Each point is the robustness under simultaneous attack and sequential attack with the same target set. $AS2$ represents the sequential attack and $AS1$ represents the simultaneous attack. Figure 4a shows the robustness of a single physical network under different attack sequences; Figure 4b shows the robustness of interdependent Cyber-Physical network under different attack sequences.

In the single physical network, sequential attacks would cause more damage with 19 target sets and simultaneous attack could cause more damage with 35 target sets. While in interdependent Cyber-Physical systems, sequential attacks would cause more damage with 28 target sets and simultaneous attack would cause more damage with 28 target sets. We could find, with the coupling process, that the number of target sets for which a sequential attack would cause more damage is increasing, while the number of the target sets for which a simultaneous attack would cause more damage is decreasing.

We make a brief analysis here for the phenomenon. During the above case, we could find 39 target sets in interdependent Cyber-Physical systems with which a sequential attack would cause more damage, and we could find 18 of them that are the correspondence of the target sets in single physical systems. For example, in interdependent Cyber-Physical systems, attack sequence {[26],[31]} causes more damage than attack sequence {[26,31]}. While in single physical systems, the attack sequence {[13],[21]} causes more damage than attack sequence {[13,21]}. Node 26 in the cyber subnetwork and node 13 in the physical subnetwork are a pair and node 31 in the cyber subnetwork and node 21 in the physical subnetwork are a pair.

3.3. Composite Attack in Interdependent Cyber-Physical Systems

With the number of targets in attack sets increasing, there are many attack sequences besides simultaneous attack and sequential attack. For example, according to Equation (5), when T_n = 3, we could get:

$$f(3) = C_3^1 \times C_2^1 \times C_1 3^1 + C_3^1 \times C_2^1 + C_3^2 \times C_1^1 + C_3^1 = 13. \tag{7}$$

Thus, there are 13 kinds of combinations, and the specific combinations are as follows:

$AS1 : \{[i,j,k]\}$; $AS2 : \{[i],[j],[k]\}$; $AS3 : \{[i],[k],[j]\}$; $AS4 : \{[j],[i],[k]\}$; $AS5 : \{[j],[k],[i]\}$; $AS6 : \{[k],[i],[j]\}$; $AS7 : \{[k],[j],[i]\}$; $AS8 : \{[i],[j,k]\}$; $AS9 : \{[j],[i,k]\}$; $AS10 : \{[k],[i,j]\}$; $AS11 : \{[i,j],k]\}$; $AS12 : \{[i,k],j]\}$; $AS13 : \{[k,j],i]\}$.

We could find during the 13 combinations that one of them is simultaneous attack and six of them are sequential attacks. We call the rest of them the composite attack. In the simulations, an interdependent Cyber-Physical network is built with all configuration parameters the same as the interdependent Cyber-Physical network we construct in Section 3.2. The robustness under sequential attack versus the robustness under simultaneous attack is shown in Figure 5a–f and we could see that some sequential attacks can cause more damage than simultaneous attack. The robustness under composite attack versus robustness under simultaneous attack is shown in Figure 5g–l, and we could also find that some composite attacks can cause more damage than simultaneous attack.

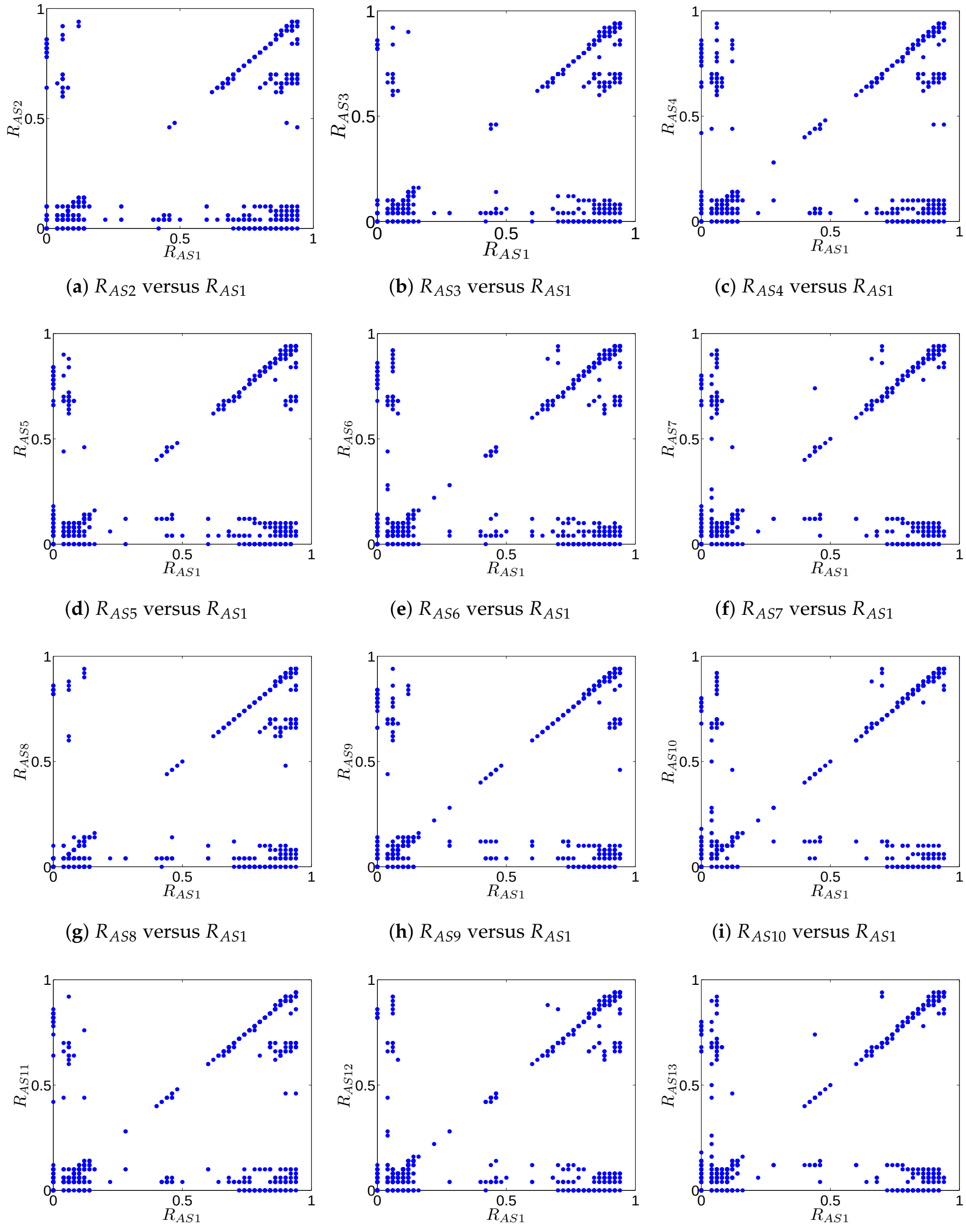
We also compare the robustness under sequential attack and composite attack. There are six kinds of sequential attacks and six kinds of composite attacks. If we compare each one, there would be 36 comparisons. For simplicity, we only take R_{AS8} versus R_{AS2} and R_{AS11} versus R_{AS2} for examples. The results are shown in Figure 6. From Figure 6a,b, we could get that some composite attacks can cause more damage than sequential attack with the same target sets.

From the above simulations, we could get that there exist target sets with whom sequential attacks would cause more damage than simultaneous attack, so sequential attack must be considered when the defenders select the critical nodes in Cyber-Physical systems. There are target sets with whom composite attack would cause more damage than simultaneous attack, and there are target sets with whom composite attack can cause more damage than sequential attacks, but if there are no target sets with whom composite attacks would cause larger damages than both sequential attack and simultaneous attack, it is not necessary to consider the composite attack when the defenders select the critical nodes.

Many numerical simulations are done to check whether these target sets exist, and the results tell us the answer is yes though they are really rare. In one case, we find a composite attack whose damage effect is that all nodes fail; however, with another composite attack, sequential attack and simultaneous attack, at least 80% of all nodes survive. Thus, composite attack must be considered by defenders.

We should notice that the "best attack sequences" are not always composite attack. During many cases, sometimes the "best attack sequences" are sequential attack or simultaneous attack. We can not come to the conclusion that one kind of attack sequence is better than the other attack sequence. The target sets, network structure, λ and α all decide which attack sequence would cause larger damage with the same target set. We can only reach the conclusion that new attack sequences cause new vulnerability, which should be considered by the defenders.

Many simulations are conducted with different parameters to verify whether the conclusions are general. Different values of m, α and λ are used. The results we get are different, but the conclusions hold with different parameters. The source code and data of the above simulations are offered as open source supplementary materials [27] to this manuscript. Readers can use them to verify our conclusions or make further study.



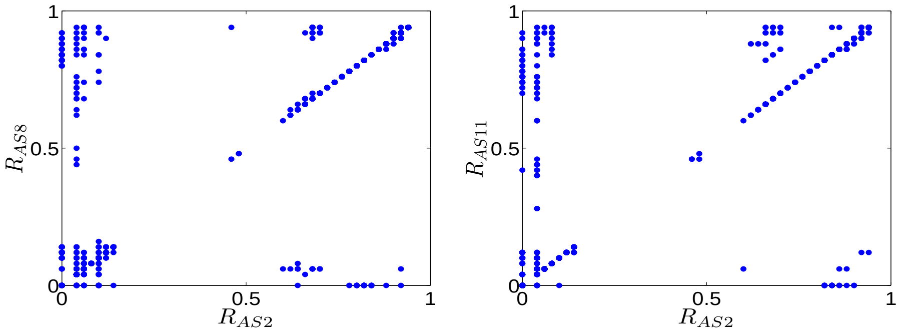
(**a**) R_{AS2} versus R_{AS1} (**b**) R_{AS3} versus R_{AS1} (**c**) R_{AS4} versus R_{AS1}

(**d**) R_{AS5} versus R_{AS1} (**e**) R_{AS6} versus R_{AS1} (**f**) R_{AS7} versus R_{AS1}

(**g**) R_{AS8} versus R_{AS1} (**h**) R_{AS9} versus R_{AS1} (**i**) R_{AS10} versus R_{AS1}

(**j**) R_{AS11} versus R_{AS1} (**k**) R_{AS12} versus R_{AS1} (**l**) R_{AS13} versus R_{AS1}

Figure 5. Robustness of an interdependent Cyber-Physical network under different attack sequences with the same target sets. AS1 represents the simultaneous attack. AS2–AS7 represent sequential attacks. AS7–AS13 are composite attacks.



(**a**) network *A*

(**b**) network *B*

Figure 6. Robustness of interdependent Cyber-Physical network under different attack sequences with same target sets. R_{AS8} represents the robustness under attack sequence $AS8$, R_{AS11} represents the robustness under attack sequence $AS11$, and R_{AS2} represents the robustness under attack sequence $AS2$.

4. Discussions

Our model cannot apply to all Cyber-Physical systems and there are limitations for the systems: first, the cyber system and physical system should depend on each other; second, the physical system is load-induced, and the load would be redistributed after a physical node's failures; third, the attack targets are cyber nodes, while in some cases, attackers may prefer attacking physical edges; finally, the number of survival nodes should be used to measure the robustness of systems. A Cyber-Physical system meeting all the limitations can use our model to simulate its robustness, and all we need to do is just adjust the parameters in our model.

We suggest that the following changes may be needed while building the model for other types of systems: first, the dependency relation may be changed; second, the physical process in physical systems may be changed; third, the attack targets may be changed; finally, the measurement of robustness may be changed.

In our model, with some target sets, the sequential attack causes more damage than simultaneous attack, and with some target sets, composite attack causes more damage than both sequential attack and simultaneous attack. However, how to find these target sets is still a research field that needs to be researched. In Section 3.1, we find that most nodes in target sets with which sequential attack causes more damage are neighbors; in Section 3.1, we find half of the target sets are the correspondence of target sets in single physical systems; these may be a clue to find the target sets with which sequential attack would cause more damage in interdependent Cyber-Physical networks and could be verified later. However, there are no clues on how to find target sets with which composite attack would cause more damage than both simultaneous attack and sequential attack.

In Section 3.1, there are only 3.64% target sets with which sequential attack would cause more damage in a single physical network; in Section 3.2, there are only 2.29% target sets with which sequential attack would cause more damage in interdependent Cyber-Physical network; in Section 3.3, the target sets with which the composite attack effect are better than both sequential attack and simultaneous attack are more rare. In some cases, these target sets do not even exist. However, we still suggest that the defenders consider the sequential attack and composite attack when selecting the critical nodes. It is very dangerous when the attackers find an attack sequence with which they can bring vast damage on the network, while the defenders ignore these nodes because their simultaneous failure can only bring limited damages.

We also suggest that the defenders take the composite attack as a priority, not because composite attack is more advanced than sequential attack or simultaneous attack. In fact, it is hard to tell which is better. For some target sets, one kind of attack sequence may cause more damage. For other target sets, another attack sequence may cause more damage. We suggest the composite attack as priority, because it comprises the majority of all attack sequences. If there are four nodes in target sets, this means $T_n = 4$. Then, there are $f(4) = 81$ kinds of attack sequences, and one of them is simultaneous attack and 24 of them are sequential attacks, so there are 56 kinds of composite attacks. When $T_n = 5$, 420 attack sequences of 521 total attack sequences are composite attacks. Thus, with T_n increasing, the composite attack takes more of a part in all attack sequences.

5. Conclusions

In this paper, we propose the interdependent Cyber-Physical model, and the definitions of target set, attack unit, attack set, attack sequence are given to describe the model more clearly. The attack model is also proposed to present the attack process, and we divide the attack sequence into three kinds: simultaneous attack, sequential attack and composite attack. Through numerical simulations, we find: (1) with some target sets, sequential attack can cause more damage than simultaneous attack in a single load-induced physical network; (2) in an interdependent Cyber-Physical network, sequential attack can also lead to a better attack effect with some target sets, and half of them are the correspondence of the target sets in single load-induced physical networks; (3) composite attack may cause much more damage than both sequential attack and simultaneous attack. Thus, we suggest that the defenders should take simultaneous attack, sequential attack and composite attack into account when they try to select the critical nodes.

There are manifold Cyber-Physical systems, and different models can be built to simulate their robustness under different attacks. In future work, we would build more models with different types of systems.

Author Contributions: P.C. and P.Z. proposed the model and attack strategies. P.C. designed the experiment. P.C., P.X. and S.C. completed the experiments and analysis together. All the authors contributed to the writing and reviewing of this paper.

Funding: This research was funded by the National Natural Science Foundation of China (Grant No.61572514 and Grant No.61402508) and Changsha Science and Technology Project (Grant No.K1705007).

Conflicts of Interest: The authors declare no conflict of interest

References

1. Paul, S.; Ni, Z. Vulnerability analysis for simultaneous attack in smart grid security. In Proceedings of the Power & Energy Society Innovative Smart Grid Technologies Conference, Washington, DC, USA, 23–26 April 2017; pp. 1–5.
2. Zhu, Y.; Yan, J.; Tang, Y.; Sun, Y.; He, H. The sequential attack against power grid networks. In Proceedings of the IEEE International Conference on Communications, Sydney, Australia, 10–14 June 2014; pp. 616–621.
3. Yan, J.; Tang, Y.; Zhu, Y.; He, H. Smart Grid Vulnerability under Cascade-Based Sequential Line-Switching Attacks. In Proceedings of the IEEE Global Communications Conference, San Diego, CA, USA, 6–10 December 2015; pp. 1–7.
4. Zhu, Y.; Yan, J.; Tang, Y.; Sun, Y.L.; He, H. Coordinated attacks against substations and transmission lines in power grids. In Proceedings of the Global Communications Conference, Austin, TX, USA, 8–12 December 2016; pp. 655–661.
5. Zhu, Y.; Yan, J.; Tang, Y.; Sun, Y.L.; He, H. Joint substation-transmission line vulnerability assessment against the smart grid. *IEEE Trans. Inf. Forensics Secur.* **2017**, *10*, 1010–1024. [CrossRef]
6. Cuadra, L.; Salcedo-Sanz, S.; Ser, J.D.; Jimenez-Fernandez, S.; Zong, W.G. A Critical Review of Robustness in Power Grids Using Complex Networks Concepts. *Energies* **2015**, *8*, 9211–9265. [CrossRef]
7. Fan, W.; Liu, Z.; Hu, P.; Mei, S. Cascading failure model in power grids using the complex network theory. *IET Gen. Transm. Distrib.* **2016**, *10*, 3940–3949.
8. Xiang, Y.; Ding, Z.; Zhang, Y.; Wang, L. Power System Reliability Evaluation Considering Load Redistribution Attacks. *IEEE Trans. Smart Grid.* **2016**, *8*, 889–901. [CrossRef]
9. Mo, H.; Wagle, N.S.; Zuba, M. Cyber-physical systems. *Computer* **2009**, *42*, 88–89. [CrossRef]

10. Wen, G.; Wenwu, Y.U.; Xinghuo, Y.U.; Jinhu, L. Complex Cyber-Physical Networks: From Cybersecurity to Security Control. *J. Syst. Sci. Complex.* **2017**, *30*, 46–67. [CrossRef]
11. Karnouskos, S. Stuxnet worm impact on industrial cyber-physical system security. In Proceedings of the Conference on IEEE Industrial Electronics Society (IECON 2011), Melbourne, Australia, 7–10 November 2011; pp. 4490–4494.
12. Chen, T.M.; Abu-Nimeh, S. Lessons from Stuxnet. *Computer* **2011**, *44*, 91–93. [CrossRef]
13. Li, W.; Xie, L.; Deng, Z.; Wang, Z. False sequential logic attack on SCADA system and its physical impact analysis. *Comput. Secur.* **2016**, *58*, 149–159. [CrossRef]
14. Liu, X.; Li, Z.; Liu, X.; Li, Z. Masking Transmission Line Outages via False Data Injection Attacks. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 1592–1602. [CrossRef]
15. Wang, J.; Hui, L.C.K.; Yiu, S.M.; Cui, X.; Wang, E.K.; Fang, J. A Survey on the Cyber Attacks Against Non-linear State Estimation in Smart Grids. In Proceedings of the Australasian Conference on Information Security and Privacy, Melbourne, Australia, 4–6 July 2016; pp. 40–56.
16. Pan, K.; Teixeira, A.M.H.; Cvetkovic, M.; Palensky, P. Combined data integrity and availability attacks on state estimation in cyber-physical power grids. In Proceedings of the IEEE International Conference on Smart Grid Communications, Sydney, Australia, 6–9 November 2016; pp. 271–277.
17. Liu, X.; Shahidehpour, M.; Li, Z.; Liu, X.; Cao, Y.; Li, Z. Power System Risk Assessment in Cyber Attacks Considering the Role of Protection Systems. *IEEE Trans. Smart Grid.* **2017**, *8*, 572–580. [CrossRef]
18. Mansfield-Devine, S. A process of defence—Securing industrial control systems. *Netw. Secur.* **2017**, *2017*, 14–19. [CrossRef]
19. Weaver, G.A.; Davis, K.; Davis, C.M.; Rogers, E.J.; Bobba, R.B.; Zonouz, S.; Berthier, R.; Sauer, P.W.; Nicol, D.M. Cyber-Physical models for power grid security analysis: 8-substation case. In Proceedings of the IEEE International Conference on Smart Grid Communications, Sydney, Australia, 6–9 November 2016; pp. 140–146.
20. Wang, Y.N.; Lin, Z.Y.; Liang, X.; Xu, W.Y.; Yang, Q.; Yan, G.F. On modeling of electrical cyber-physical systems considering cyber security. *Front. Inf. Technol. Electr. Electron. Eng.* **2016**, *17*, 465–478. [CrossRef]
21. Orojloo, H.; Azgomi, M.A. A game-theoretic approach to model and quantify the security of cyber-physical systems. *Comput. Ind.* **2017**, *88*, 44–57. [CrossRef]
22. Havlin, S. Julius Edgar Lilienfeld Prize Talk: Catastrophic cascade of failures in interdependent networks. *Nature* **2010**, *464*, 1025–1028.
23. Wang, J.; Wu, Y.; Li, Y. Attack robustness of cascading load model in interdependent networks. *Int. J. Mod. Phys. C* **2015**, *26*, 1550030 [CrossRef]
24. Peng, X.; Yao, H.; Du, J.; Wang, Z.; Ding, C. Load-induced cascading failures in interconnected networks. *Nonlinear Dyn.* **2015**, *82*, 97–105. [CrossRef]
25. Athay, T.; Podmore, R.; Virmani, S. A Practical Method for the Direct Analysis of Transient Stability. *IEEE Trans. Power Appl. Syst.* **1979**, *98*, 573–584. [CrossRef]
26. Barabasi, A.L.; Albert, R. Emergence of Scaling in Random Networks. *Science* **1999**, *286*, 509–512. [PubMed]
27. Pengshuai, C.; Peidong, Z.; Peng, X.; Shao, C. Simulations-of-Cyber-Physical-Systems. Available online: https://github.com/EvenCui/Simulations-of-Cyber-Physical-systems (accessed on 7 September 2018).