Critical components identification for cyber-physical power systems considering time-varying operational states

Liu, Yigu; Semertzis, Ioannis; Stefanov, Alexandria; Palensky, Peter

DOI
10.1145/3470481.3472702

Publication date
2021

Document Version
Final published version

Published in
9th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems, MSCPES 2021, Held as part of the Cyber-Physical Systems and Internet-of-Things Week, Proceedings

Critical Components Identification for Cyber-Physical Power Systems Considering Time-Varying Operational States

Yigu Liu, Ioannis Semertzis, Alexandru Stefanov, Peter Palensky
Department of Electrical Sustainable Energy
Delft University of Technology
Delft, the Netherlands
y.liu-18@tudelft.nl

ABSTRACT

The security issues of Cyber-Physical power Systems (CPS) have attracted widespread attention from scholars. Vulnerability assessment emerges as an effective method to identify the critical components and thus increase the system resilience. While efforts have been made to study the vulnerability features of power systems under the occurrence of a single, discrete disturbance or failure at a specific time instant, this paper focuses on identifying the critical components of the cyber-physical system considering time-varying operational states. To investigate the potentially ever-changing CPS vulnerability features, in this paper we construct a database of cascading failure chains using quasi-dynamic simulations to capture the vulnerability relationships among components under time-varying operational states. Then, by adopting sequential mining algorithms, we mine the most frequent cascading failure patterns and identify the critical components based on the data mining results. Simulation studies are conducted on IEEE 39-bus and IEEE RTS-96 systems to evaluate the effectiveness of the proposed method for the identification of critical components at both cyber and physical layers.

KEYWORDS

cyber-physical systems, vulnerability assessment, data mining algorithms.

ACM Reference Format:

Yigu Liu, Ioannis Semertzis, Alexandru Stefanov, Peter Palensky. 2021. Critical Components Identification for Cyber-Physical Power Systems Considering Time-Varying Operational States. In *MCPES'21: 9th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems, May 18, 2021, Virtual Event*, 7 pages. https://doi.org/10.1145/3470481.3472702

1 Introduction

With the rapid development of Information and Communication Technologies (ICTs) and Operational Technologies (OTs), the power grids are now tightly coupled with communication infrastructures in an unprecedented way, which forms a complex, interdependent Cyber-Physical System (CPS). Digitalization is expected to increase power grid sustainability, affordability, and resiliency. However, cyber-related vulnerabilities are inevitably introduced in the cyber-physical system, which can be exploited by adversaries and thus weaken power grid robustness and security of supply. Furthermore, they also exacerbate the breadth and depth of cascade propagation when CPS experiences disturbances, which increase the overall system vulnerability with catastrophic potential consequences.

Vulnerability assessment is typically used to enhance cyber-physical system security by identifying the weak points in the system. The current vulnerability assessment methods for CPS can be broadly grouped into two categories: (i) topology-based methods [1][2], which abstract the CPS into an interdependent network and evaluate the systematic vulnerabilities from a structural perspective, and (ii) operation-based methods [3][4], which consider the CPS operational aspects, e.g., power flow and information communication, in either or both cyber-physical domains. For topology-based methods, Buldyrev et al. [1] adopt percolation theory to prove that a broader degree distribution increases the vulnerability of the interdependent networks to random failures. Complex network theory [2] is also a popular method to construct indices and evaluate the vulnerability of system components, e.g., degree, closeness, and betweenness. However, topology-based methods naturally neglect the heterogeneity of nodes in both cyber and physical layers and focus on the structure of the interdependent network. Consequently, the inherent physical mechanisms, e.g., power flows and routing protocols, at both CPS layers are ignored, which may result in unrealistic conclusions. To this end, Falahati et al. [3] use a linear programming model to maximize the data connection at the cyber layer and adopt a DC optimal power flow model to minimize the load curtailment. Furthermore, Ye et al. [4] define an interaction model to simulate the cascading failures in CPS.

Although efforts have been made on modeling and systematic evaluation of CPS vulnerability, the current literature has an obvious drawback. The existing work only evaluates the CPS at a single time instant. However, we argue that this may not always be the case. Instead of considering CPS disturbances or failures as single-occurrence events, in this research we treat them as a set of sequential discrete events. Disturbances and failures can occur at any time instant during CPS operation over a certain time period. Meanwhile, the operational states, e.g., loads and power flows, are constantly varying in time. Under such assumption, the vulnerability features generated by the existing static methods,

*Both authors contributed equally to this research.

MCPES'21, May 19–21, 2021, Nashville, TN, USA

ACM ISBN 978-1-4503-8608-1/21/05.
https://doi.org/10.1145/3470481.3472702

which aim at a particular time instant may not be applicable to time-varying CPS operational states. To this end, a fundamentally new approach is needed to systematically capture the vulnerability characteristics and identify the most critical CPS components to develop effective and economic mitigation strategies.

To address these issues, in this paper, we propose a novel cascading failure model considering the interaction between cyber and physical layers for every single time instant. Based on quasi-dynamic simulations, we generate a database of cascading failure chains. This contains various operating conditions. We adopt the PrefixSpan sequential mining algorithm [5] to identify the frequent sequential cascading patterns. Vulnerability indices are constructed based on complex network theory to evaluate the importance of components in the cascading failure process and identify the critical components in CPS. The contributions of this paper are summarized as follows:

1) This paper proposes a novel vulnerability assessment method for the identification of critical components in CPS considering the time-varying operational states.

2) This paper investigates CPS modeling from both topological and operational perspectives. From a topological perspective, the cyber topology and structural interdependency between cyber and physical layers are thoroughly investigated. From an operational perspective, we present a detailed modeling process considering the interaction between cyber and physical layers.

3) Based on the constructed CPS model, a database of cascading failure chains is constructed containing systematic vulnerability features. Moreover, we introduce sequential data mining algorithms to identify the frequent cascading failure patterns and design vulnerability metrics to identify the critical cyber-physical system components.

The remainder of this paper is organized as follows. Section II discusses the system vulnerability under time-varying operational states. Section III provides the modeling and simulation process of cascading failures. Section IV presents the identification of critical components. The case study and conclusion are presented in Section V and Section VI, respectively.

2 System Vulnerability Considering Time-varying Operational States

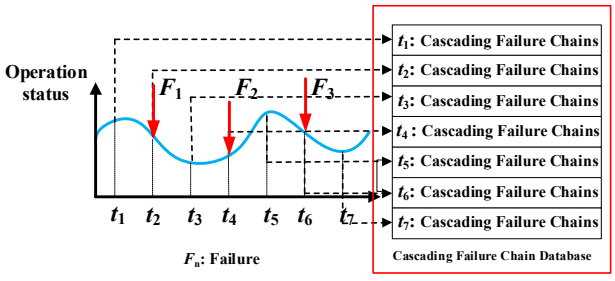


Figure 1: The time-varying operational states of CPS.

In previous discussion, we argue that the current vulnerability assessment methods may not be applicable or even feasible when considering the change of CPS operational status. As shown in Fig. 1, in a real-world scenario, the operational states of CPS are constantly changing, which means the system will react to failures or disturbances differently at various time instants. More concretely, the cyber-physical system may show different cascading failure patterns under time-varying operational states, which will directly change the vulnerability features. In this context, we first model a failure, e.g., line tripping, in CPS to trigger the cascading failures at a specific time instant, e.g., t_2, t_4 or t_6 as represented in Fig. 1. To thoroughly investigate the vulnerability characteristics of CPS at a specific time instant, we consider that any component in the cyber-physical system may fail, and we generate possible cascading failure chains for all components. These cascading failure chains contain the detailed vulnerability features of CPS at the time instant. By combining cascading failure chains of all-time instants, a cascading failure chain database is generated, which captures the intricate relationships among components and reveals the fault propagation mechanism of CPS under different operating conditions. For instance, for a certain time interval $[t_1, t_u]$, suppose the cascading failure chain set includes $\boldsymbol{X}_{CF}(t_1)$ at t_1, $\boldsymbol{X}_{CF}(t_2)$ at t_2 ,..., $\boldsymbol{X}_{CF}(t_u)$ at t_u, then the cascading failure chain database $\boldsymbol{X}_D$ can be presented as:

$$\boldsymbol{X}_D = \left\{ \boldsymbol{X}_{CF}(t_u) \middle| 1 \le u \le U \right\} \tag{1}$$

The definition of $\boldsymbol{X}_{CF}(t_u)$ can be found in Section III, Part C. At last, we intend to employ sequential data mining algorithms to mine the cascading failure database and identify the critical components of CPS. Generally, the sequential data mining algorithms return the patterns that are frequently shown in the database. For cyber-physical systems, if a cascading failure pattern frequently appears in $\boldsymbol{X}_D$, it means that the corresponding components play a critical role in the cascading process. If such critical components are reinforced and cyber secure, the system resilience will be greatly improved.

3 Modeling of CPS and Cascading Failures

In this Section, we investigate CPS modeling from both topological and operational perspective. We model the cascading failures at each time instant to show how CPS will react to disturbances under different operating conditions. Then, by collecting the cascading failure chains at each time instant, a database is generated to further reveal the systematic vulnerability features of the cyber-physical system.

3.1 Topological Modeling of CPS

In this paper, we abstract the CPS into an interdependent network, in which nodes and edges are used to represent the cyber-physical system components and interconnections among them, respectively.

Physical Layer: the generators, substations and loads are considered as physical nodes, while the transmission lines and transformers are considered as physical edges. Consequently, we can directly map a power grid into an undirected and unweighted graph based on its own topology.

Cyber Layer: the Supervisory Control and Data Acquisition (SCADA) system in the control center and station control systems in substations are abstracted into cyber nodes, while their communication links are considered as cyber edges. It is worth mentioning that for the cyber layer we only consider the influence of the cyber layer topology on the physical layer operation. In this research, we do not consider the detailed communication mechanisms, e.g., routing protocols. Typically, the communication networks for power grids are implemented as double-star or mesh networks [6][7] From the perspective of complex network theory, double-star networks are scale-free networks [8]. The control centers are considered hub nodes with higher degrees in the system. If one of these nodes fail, the cyber-physical system will suffer severe consequence. The double star networks are sensitive to intentional cyber-physical attacks, but resilient to random failures. On the other hand, mesh networks, as opposite to double-star networks, show the feature of small-world [9], which indicates that mesh networks have a broader degree distribution and are more vulnerable to random failures. Generally, a broader degree distribution increases the robustness of complex networks. However, when cyber and physical layers are coupled to form an interdependent network, a broader degree distribution increases the vulnerability of the interdependent networks to random failures [1]. Meanwhile, the research of Ye et al. [4] also shows that power grids coupled with double-star communication network have a lower probability of catastrophic failures than with mesh networks. Therefore, in this paper, we adopt the double-star network to model the topology of the cyber system.

Structural Interdependency: in this paper, we consider the interdependence between cyber and physical layers as a "one-to-one" correspondence [1]. The number of nodes in the cyber layer is the same as in the physical layer, and a cyber node is exclusively interconnected with a physical node. Parshani et al. [10] defines the interdependency of networks as intersimilarity from a topology perspective and investigates the robustness of interdependent networks under different intersimilarities. The results show that for scale-free networks, the interdependency should be "degree-to-degree", which means that the node with the highest degree in the cyber layer should be interconnected with the node with the highest degree in the physical layer.

3.2 Operational Modeling of CPS

Failures such as protection maloperation or loss of communications may trigger cascading effects in the cyber-physical system. Furthermore, when power grids are tightly coupled with communication infrastructures, the extent of fault propagation in CPS may be significantly increased considering the complex interdependencies between the cyber and physical layers. For example, one disturbance in one network may simultaneously have an influence within the network and on its interdependent networks. In this subsection, we present the simulation process of generating the cascading failure chains for every time instant used to generate the cascading failure chain database.

When the power system is congested, system operators redispatch generation or even shed load to ensure that the power grid is securely and economically operated. Therefore, an optimal DC power flow model represented by equations (2) – (7) is used to minimize the load shedding when disturbances occur in the cyber-physical system.

$$\min \sum_{y \in D} W_y \left| p_y - P_{dy} \right| \tag{2}$$

$$s.t. \quad \boldsymbol{F} = \boldsymbol{AP} \tag{3}$$

$$\sum_{x=1}^{n} p_x = 0 \tag{4}$$

$$P_{dy} \le p_y \le 0, y \in D \tag{5}$$

$$P_{gx}^{\min} \le p_x \le P_{gx}^{\max}, x \in G \tag{6}$$

$$-F_l^{\max} \le F_l \le F_l^{\max}, L_l \in \boldsymbol{L} \tag{7}$$

where G and D are the set of generators and loads, respectively, W_y is the cost of load shedding, $\boldsymbol{L} = \{L_l | l = 1,2,...,N_l\}$ is the set of branches in the power grid and $\boldsymbol{P} = [p_1, p_2, ..., p_k, ...]^{\mathrm{T}}$ is the vector of power node injections. Equation (3) represents the DC power flow equation. $\boldsymbol{A}$ is the nodal admittance matrix and $\boldsymbol{F} = [F_1, F_2, ..., F_l, ...]$ is the vector of branch power flows. p_y represents the load of node y. P_{dy} represents the rated load at node y. p_x represents the output power of generator x. $P_{gx}^{\max}$ and $P_{gx}^{\min}$ are the upper and lower limits of the output power of generator x, respectively. $F_l^{\max}$ is the transmission capacity of the l-th branch.

Ye et al. [4] propose an interaction model and analyses the system performance under both intentional attacks and random failures. Dong et al. [11] propose a probabilistic failure model to simulate the cascading process between cyber and physical layers. Based on these works, an interactive model is used to capture the main features of both cyber and physical layers and give a rough approximation to describe the interdependency between the two layers, which is presented as follows.

Cascading failures in the same layer: we consider that cascading failures in power grids are mainly caused by load redistribution when branches are disconnected and by hidden failures. Due to a hidden failure [12], the outage of branch L_l

may cause the failure of its neighbors with a low probability P_1. When a branch is overloaded due to system load redistribution, we assume that the branch will be disconnected with a probability P_2. We do not consider the mutual influence among cyber nodes, i.e., the failure of a cyber node will only influence the data communication and will not cause a failure of other cyber nodes.

The impact of disturbances in the cyber layer to the physical layer: we consider that the cyber nodes are directly coupled with the physical nodes of power grids. When a cyber node is out of service, the control center loses the remote monitoring and control capabilities of the physical node and all corresponding branches in the substation. Consequently, when these branches are overloaded, they will operate in an insecure state and will be eventually disconnected by system protection after a period of time. On the other hand, a failed cyber node may be on the communication path between the control center and another cyber node. Under such circumstances, we consider that the control center also loses the monitoring and control capabilities of the associated physical nodes.

3.3 Construction of Cascading Failure Chain Database

In this paper, we investigate systematic cyber-physical system vulnerabilities. Therefore, we include various cascading failure scenarios by assuming that each component is possible to fail at every time instant. More specifically, we trip all the branches one by one to collect all possible cascading failure chains at every time instant. Then, by repeating the same process, the cascading failure chains are combined to generate the cascading failure chain database as shown in Fig. 1. The detailed simulation process of one single time instant is presented in Fig. 2. A disconnected branch is removed from the power grid topology. The updated topology is represented by N_{real}. Furthermore, we consider $N_{control}$ to be a subset of N_{real} for which the system operator still has monitoring and control capabilities. The branches connected to the physical nodes affected by the failure of their corresponding cyber nodes are removed from $N_{control}$. We consider that the cyber nodes are vulnerable to cyber attacks and some will fail due to malicious attacks or other contingencies in each iteration. The cyber nodes will be removed with a small probability P_3.

The cascading failure process at time instant t_U starts by disconnecting branch L_l and scanning for cyber and hidden failures. The N_{real} and $N_{control}$ CPS topologies are updated. The DC power flow is first calculated based on the updated N_{real}. If there are overloaded branches, we calculate the optimal DC power flow based on the updated $N_{control}$. The results of the optimal DC power flow give the power injections for the physical nodes in $N_{control}$. The redispatch of generation with minimum load shedding costs is implemented using N_{real}. We calculate load redistribution based on the new power injections and previously available measurements for the physical nodes affected by the failure of their cyber nodes. The overloaded branches are disconnected with their corresponding probabilities. It is worth mentioning that a branch may be disconnected based on local measurements by protection relays and control commands from the control center. When a branch is overloaded, system operators will adjust the generation or initiate load shedding. If the overload is not mitigated, the branch will be tripped by overload protection. Therefore, in our paper, we assume that when a branch is overloaded, it is tripped by local protection with a probability P_2. The process is repeated until there are no further overloaded branches. The cascading failure chain is exported to the database.

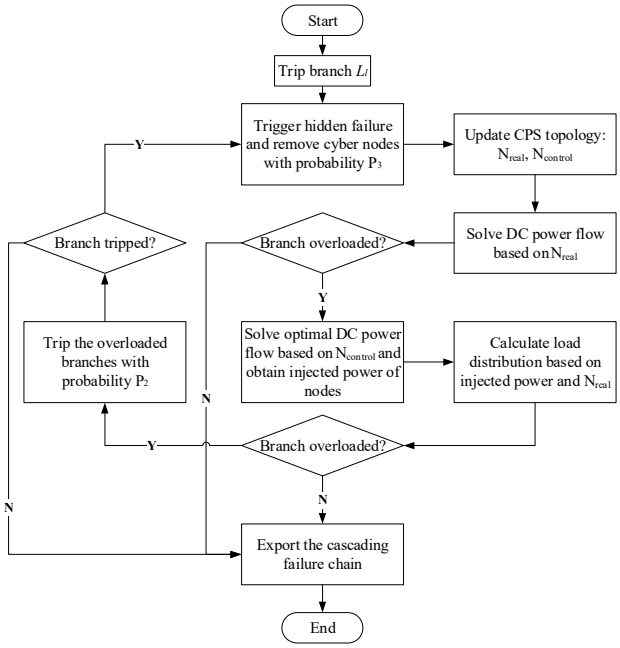


Figure 2: Simulation process of cascading failures.

It is worth mentioning that the simulation process illustrated in Fig. 2 is used to generate the cascading failure chain $\boldsymbol{X}_{CF}^{L_l}(t_u)$ initiated by the disconnection of branch L_l at t_u. To thoroughly capture the vulnerability features of CPS and generate the cascading failure chain $\boldsymbol{X}_{CF}(t_u)$ at t_u, this simulation should be conducted for every branch in $\boldsymbol{L}$. This can be represented by equations (8) and (9).

$$\boldsymbol{X}_{CF}^{L_l}(t_u) = \rho(C_1, C_2, \ldots, C_n), C_k \in \boldsymbol{C} = \boldsymbol{V}_C \cup \boldsymbol{L} \tag{8}$$

$$\boldsymbol{X}_{CF}(t_u) = \left\{ \boldsymbol{X}_{CF}^{L_l}(t_u) \middle| L_l \in \boldsymbol{L} \right\} \tag{9}$$

where $\rho(C_1, C_2, \ldots, C_n) = C_1 \rightarrow C_2 \rightarrow, \ldots, \rightarrow C_n$.

$\boldsymbol{V}_C = \left\{ v_g \middle| g = 0,1,2,..., N_g \right\}$ represents the set of cyber nodes at the cyber layer. The cascading failure chain database $\boldsymbol{X}_D$ can be generated based on equations (1) and (9).

4 Critical Components Identification from a Data Mining Perspective

In this section, we take advantage of the fact that $\boldsymbol{X}_{CF}^{L_l}(t_u)$ can be viewed as a *sequence* for data mining and employ the PrefixSpan sequential data mining algorithm to capture the most frequent cascading failure sequence, i.e., CPS vulnerable sequence. Based on the identified patterns, we propose a vulnerability metric to further quantify the vulnerability of each component in the cyber-physical system.

4.1 Identification of Vulnerable Cascading Failure Sequence

For a cyber-physical system, the cascading failure chain database can be very large, in which some cascading failure patterns may show up repeatedly. We use the frequency of these patterns to quantify the vulnerability of each CPS component. The cascading failure patterns are defined as candidate sequences waiting to be evaluated whether they are vulnerable sequences or not.

Definition 1 (candidate sequence): Based on the definition of $\boldsymbol{X}_{CF}^{L_l}(t_u)$, if there exists $\{C_{j1}, C_{j2}, \ldots, C_{js}\} \subseteq \{C_1, C_2, \ldots, C_n\}$, a sequence $\alpha = \rho(C_{j1}, C_{j2}, \ldots, C_{js})$ is called a *subsequence* of a cascading failure chain $\boldsymbol{X}_{CF}^{L_l}(t_u)$, which can be denoted as $\alpha \triangleright \boldsymbol{X}_{CF}^{L_l}(t_u)$.

Normally, the frequency of a candidate sequence indicates the vulnerability of its associated components. To quantify such frequency, the definition of vulnerability degree is defined as follows:

Definition 2 (vulnerability degree): for a candidate sequence $\alpha = \rho(C_{j1}, C_{j2}, \ldots, C_{js})$, the vulnerability degree is defined as:

$$V_D(\alpha) = \left| \left\{ \rho \middle| (\rho \in \boldsymbol{X}_D) \wedge (\alpha \triangleright \rho) \right\} \right| \tag{10}$$

Based on the definitions above, PrefixSpan can be adopted to identify the vulnerable sequence with higher vulnerability degrees. The details of PrefixSpan are reported in [5].

4.2 Vulnerability Metric for Critical Components Identification

Based on the vulnerable sequences identified above, in this part, we propose a vulnerability metric to further quantify the vulnerability of each CPS component. As discussed in Section III, for each cascading failure chain $\boldsymbol{X}_{CF}^{L_l}(t_u)$, the components highly positioned in the chain result in high vulnerabilities. Therefore, we propose a metric named *total sequential vulnerability* to identify the critical components in the cyber-physical system.

Definition 3 (total sequential vulnerability): for a vulnerable sequence $\beta_m = \rho(\ldots, C_i, \ldots)$, the sequential vulnerability $S_{\beta_m}(C_i)$ of component C_i in β_m is defined as

$$S_{\beta_m}(C_i) = N_{\beta_m} - \delta_{\beta_m}(C_i) + 1 \tag{11}$$

where N_{β_m} is the number of components in β_m and $\delta_{\beta_m}(C_i)$ is the order of C_i in β_m. Based on equation (11), by combining the sequential vulnerability of component C_i in all M vulnerable sequences containing C_i, the total sequential vulnerability of C_i can be represented as

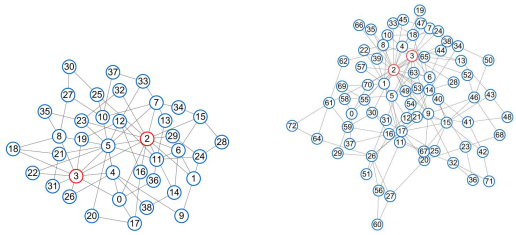
$$S(C_i) = \sum_{m=1}^{M} S_{\beta_m}(C_i) \tag{12}$$

5 Case Study

In this section, we conduct experiments on IEEE 39-bus and IEEE RTS-96 models to evaluate the effectiveness of the proposed method. Their cyber-physical systems and the proposed method are implemented in Python. The probabilities for the simulation of cascading failure chains are set as follows: $P_1 = 0.05$, $P_2 = 0.95$, $P_3 = 0.01$.

5.1 Generation of Cyber Layer

As discussed in Section III, we use a scale-free network to simulate the cyber layer. Based on the Barabási–Albert (BA) model [8], Fig. 3 shows the generated cyber topologies of IEEE 39-bus and IEEE RTS-96 system, respectively.



(a) (b)

Fig. 3: Cyber layer topology: (a) IEEE 39-bus system, (b) IEEE RTS-96 bus system.

5.2 Critical Components Identification

The method proposed in Section III is used to generate the vulnerable sequences of IEEE 39-bus and IEEE RTS-96 system. For IEEE RTS-96 system, we use the peak loads of each week for a 52-week load profile to simulate the time-varying operational states of CPS. For IEEE 39-bus system, we change the load proportionally in each simulation over 52 weeks. In the final

database, there are 1901 cascading failure chains for IEEE 39-bus system and 6479 cascading failure chains for IEEE RTS-96 system. Fig. 4 shows all the vulnerable sequences identified for the two test systems. Furthermore, based on equations (11)-(12), the total sequential vulnerabilities are calculated to quantify the vulnerabilities of CPS components in the test systems. Table I and II show the top 5 components in both cyber and physical layers with the highest total sequential vulnerabilities.

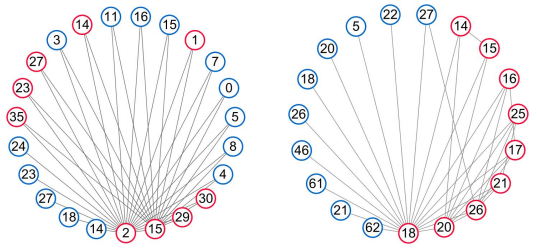


Fig. 4: Vulnerable Sequence Identification: (a) IEEE 39-bus system, (b) IEEE RTS-96 bus system. The cyber nodes are represented with blue, while the power system branches are represented with red.

From the perspective of degree distribution, in Fig. 4(a), the components with the highest degree are branches 2, 15 and 29. This ranking is different from the ranking of total sequential vulnerability. This is because the total sequential vulnerability also considers the position of components in a vulnerable sequence. When a component frequently appears at the start position of a sequence, it means this component has a more significant impact on other components in the system. If the cyber-physical security of such components can be strengthened, then the scale of cascading failures will be reduced and thus the system will be more resilient. It is worth mentioning that although the degree distribution and total sequential vulnerability of power nodes are much higher than the ones of the cyber nodes, they are equally important for cyber-physical systems.

TABLE I. VULNERABLE COMPONENTS OF IEEE39-BUS SYSTEM SORTED BY TOTAL SEQUENTIAL VULNERABILITY

Branches in Physical Layer			**Nodes in Cyber Layer**		
Ranking	***ID of Branches***	$S(C_i)$	***Ranking***	***ID of Nodes***	$S(C_i)$
1	2	50	1	3	5
2	15	24	2	16	4
3	1	5	3	11	3
4	35	4	4	15	3
5	23	4	5	8	3

TABLE II. VULNERABLE COMPONENTS OF IEEE RTS-96 SYSTEM SORTED BY TOTAL SEQUENTIAL VULNERABILITY

Branches in Physical Layer			**Nodes in Cyber Layer**		
Ranking	***ID of Branches***	$S(C_i)$	***Ranking***	***ID of Nodes***	$S(C_i)$
1	18	93	1	27	3
2	20	64	2	5	2
3	16	25	3	18	1
4	26	23	4	21	1
5	17	17	5	20	1

On the other hand, as shown in Table I and II, we can observe that the span of $S(C_i)$ is quite large, which means, taking IEEE 39-bus system as an example, branch 2 is more vulnerable than branch 23, and by extension, other branches ranked behind branch 23 in the system. Such results indicate that for cyber-physical systems, there is a limited number of critical components, which must be reinforced and cyber secure. In our case, Table I and II give the top 5 critical components in both cyber and physical layers of the IEEE 39-bus and IEEE RTS-96 systems.

6 Conclusion and Future Work

This paper focuses on revealing the vulnerability features of cyber-physical systems considering the time-varying operational states. First, we model the cascading failures considering the interaction of cyber and physical layers. By combining cascading failure chains of all-time instants, a cascading failure chain database is generated. This captures the intricate relationships among components and reveals the fault propagation mechanism of CPS under different operating conditions. The PrefixSpan sequential data mining algorithm is adopted to identify the vulnerable sequences. The total sequential vulnerability metric is proposed to quantify the vulnerabilities of CPS components. The simulation results show that there is only a limited number of critical CPS components. The resilience of the cyber-physical system can be greatly improved if these critical components are reinforced and cyber secured. This paper provides a new perspective on CPS vulnerability assessment. As an extension to this paper, one can perform an in-depth study of considering the cyber-related operational mechanisms, e.g., routing protocols and information flows, when modeling the cascading failures between the cyber-physical layers.

REFERENCES

[1] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, “Catastrophic cascade of failures in interdependent networks,” in Nature, vol. 464, pp. 1025–1028, Apr. 2010. DOI: https://doi.org/10.1038/nature08932

[2] Amin Abedi, Ludovic Gaudard, Franco Romerio, “Review of major approaches to analyze vulnerability in power system”, in Reliability Engineering & System Safety, vol. 183, pp. 153-172, 2019. DOI: https://doi.org/10.1016/j.ress.2018.11.019

[3] B. Falahati, Y. Fu and L. Wu, "Reliability Assessment of Smart Grid Considering Direct Cyber-Power Interdependencies," in IEEE Transactions on Smart Grid, vol. 3, no. 3, pp. 1515-1524, Sept. 2012. DOI: 10.1109/TSG.2012.2194520

[4] Y. Cai, Y. Cao, Y. Li, T. Huang and B. Zhou, "Cascading Failure Analysis Considering Interaction Between Power Grids and Communication Networks," in IEEE Trans. Smart Grid, vol. 7, no. 1, pp. 530-538, Jan. 2016. DOI: 10.1109/TSG.2015.2478888.

[5] J. Pei et al., "Mining sequential patterns by pattern-growth: the PrefixSpan approach," in IEEE Transactions on Knowledge and

Data Engineering, vol. 16, no. 11, pp. 1424-1440, Nov. 2004. DOI: 10.1109/TKDE.2004.77.

[6] G. W. Li, W. Y. Ju, X. Z. Duan, and D. Y. Shi, “Transmission characteristics analysis of the electric power dispatching data network,” in Proc. CSEE, vol. 32, no. 22, pp. 141–148, 2012. DOI: 10.13334/j.0258-8013.pcsee.2012.22.020

[7] J. Hu, Z.-H. Li, and X. Z. Duan, “Structural feature analysis of the electric power dispatching data network,” in Proc. CSEE, vol. 29, no. 4, pp. 53–59, 2009. DOI: CNKI:SUN:ZGDC.0.2009-04-010

[8] Albert-László Barabási*, Réka Albert, “Emergence of Scaling in Random Networks,” in Science, vol. 286, no. 5439, pp. 509-512, Oct 1999. DOI: 10.1126/science.286.5439.509

[9] Watts, D., Strogatz, S. “Collective dynamics of ‘small-world’ networks.” in Nature, vol. 393, pp. 440–442, June 1998. DOI: https://doi.org/10.1038/30918

[10] R. Parshani, C. Rozenblat, D. Ietri, C. Ducruet, and S. Havlin, “Intersimilarity between coupled networks,” in Europhy. Lett., vol. 92, no. 6, 2010. DOI: 10.1209/0295-5075/92/68002

[11] D. Zhengcheng, F. Yanjun, T. Meng, “Influences of Various Coupled Patterns and Coupling Strength on Power-communication Coupled Networks,” in High Voltage Engineering, vol. 41, no. 10, pp. 3464-3469, Oct. 2015. DOI: 10.13336/j.1003-6520.hve.2015.10.038

[12] F. Yang, A. P. S. Meliopoulos, G. J. Cokkinides and Q. B. Dam, "Effects of Protection System Hidden Failures on Bulk Power System Reliability," in 2006 38th North American Power Symposium, Carbondale, IL, USA, 2006, pp. 517-523. DOI: 10.1109/NAPS.2006.359621