A Realistic Failure Propagation Model for Smart Grid Networks

Aliasghar Salehpour[1], Irfan Al-Anbagi[1], Kin Choong Yow[1], and Xiaolin Cheng[2]

[1]*Faculty of Engineering and Applied Science*, *University of Regina*, Regina, Canada ,
[2]*Ericsson Inc.*, Santa Clara, CA, USA

***Abstract*—A smart grid connects components of power systems and communication networks through complex and interdependent relationships. The heterogeneous nature of these systems and interdependencies between their elements make them vulnerable to cyber attacks. Hence, reliable approaches should be used to secure the smart grid. In this paper, we propose a novel cyber-attack failure propagation model in a smart grid environment. Our Realistic Failure Propagation (RFP) model addresses the system's heterogeneity by assigning different roles to its components. We define rules and interdependencies for failure propagation and propose a new process to study the behavior of cascading failures. The RFP model implements power flow analysis to ensure that all transmission lines work under their capacity and remove lines that exceed the capacity.**

***Index Terms*—Smart grid, failure propagation, cyber attacks, cascading failures, graph theory, interconnection networks, realistic model, power flow analysis.**

I. Introduction

A smart grid network is a complex cyber-physical system (CPS) that introduces new capabilities based on its exclusive features [1]. The smart grid incorporates complex dependencies between its elements, which means communication components depend on power assets for power supply, and power assets and control systems need communication infrastructure to connect and perform their functions [2]. These dependencies and the heterogeneous communication architectures introduce new challenges related to cyber-security and reliability. One of the main challenges is the cascading failures caused by a cyber attack or failing a component in the power grid. Failure of an element can propagate in the system due to the interdependencies between power assets and communication components. Based on this, a cyber attack on the communication network can lead to the failure of power elements.

Massive blackouts have been caused by cyber attacks and cascading effects in recent years, e.g., in 2015, Ukrainian power companies experienced a cyber attack that affected many customers and resulted in a blackout in some regions of Ukraine [3]. This blackout happened because of cascading effects of the initial attack on the whole system. Many studies have been carried out to mitigate cascading failure impacts caused by cyber attacks [4]–[6]. These efforts show the importance and consequences of cascading failure attacks in the smart grid.

Many models have been proposed to investigate cascading failures in CPS and the smart grid [5], [7]–[10]. Some studies did not consider the failure of communication components caused by cyber attacks or cascading failures [11]. Others did not consider interdependencies between the power and communication networks or only model the power grid [7]. On the other hand, a few papers attempted to model both networks and interdependencies between different components regardless of the role of power components and their power limitations [5], [7], [10]. The problem with these models is that they underestimate the failure of power components. For example, they cannot model the failure of transmission lines caused by the redistribution of power.

The main goal of this paper is to model the smart grid network and study the impact of the failure of different components on the power and communication networks. This paper proposes a novel model to investigate the effect of cascading failures caused by a cyber attack in a smart grid environment. Our proposed Realistic Failure Propagation (RFP) model is based on failure propagation conditions, network topologies, and interdependencies between components.

The main contributions of this paper can be summarized as follows:

- We propose a novel model based on the IEEE standard bus systems to characterize the failure propagation in smart grids with more realistic settings.
- We define novel interdependencies to percolate the failure regarding the different roles for power and communication components and new rules for failure propagation.
- We perform power flow analysis to identify transmission lines that exceed their capacity limit to consider electric characteristics of the system.

The rest of the paper is organized as follows: Section II discusses the related work. Section III presents the RFP model. Section IV outlines the failure propagation process. Section V presents the experimental results, and finally, section VI presents the conclusions.

II. Related Work

Extensive academic and industrial investigations have been carried out on cyber attacks and their effects on smart grid networks. This research has resulted in different methods to detect attacks and study the failure propagation caused by these attacks [8]–[11]. Cai *et al.* [8] proposed a model to analyze the failure propagation in interdependent power and dispatching data networks in China. In [9], a control algorithm was proposed to reduce the impact of propagating failures

based on a communication network and the power grid models. However, the paper did not study the attack model and the impact of failure on the communication components.

Che *et al.* [7] showed that a well-designed false data injection (FDI) attack could overload critical branches and, as a result, increase the initiating contingencies probabilities and cause a cascading failure. However, the authors only focused on critical grid branches and missed the impact of the communication network on cascading failures.

Various studies have focused on interdependent networks to study failure propagation in the smart grid [12]–[14]. However, all of the above studies focused on modeling interdependencies and the impact of failure on the system and omitted the system's heterogeneity, the role of components, and the power system's electrical characteristics. Therefore, they underestimated the impact of cascading failures and did not model all parameters in failure propagation.

One of the first models that studied failure in interconnected networks is the one-one model [15]. The model assumed that all components in the two networks are homogeneous, and the failure of each node in a network may cause some nodes in the other network to fail. The paper utilized two graphs with the same number of nodes to model the system. It defined a one-one dependency between each node in the physical graph and one node in the cyber graph and vice versa. In another study, Huang *et al.* [10] proposed a model named small cluster to investigate cascading failures in interdependent systems. As we compare the RFP with the small cluster, we will elaborate on this model in the next section.

Based on the assumptions and interdependencies in [10] and [15], both methods adopted simplified models and the same roles for the power elements. As a result, these models could not identify different components of the physical aspect of the system. In addition, both methods did not know the power flow in the power network and could not identify lines that exceeded their capacity.

Unlike the above work, our RFP model assumes different roles for power components, and based on that; it considers more complicated interdependencies and rules for failure propagation. We also use power flow analysis to identify the failure of transmission lines in the power network because of the thermal limits.

III. Realistic Failure Propagation (RFP) Model for Cascading Failures

In this section, we first briefly describe the small cluster model. Then, we describe our proposed RFP model.

A. Overview of Small Cluster Model

In general, to model the power and communication networks, we can use two separate graphs; $G_{\text{pow}} = (V_{\text{pow}}, E_{\text{pow}})$ for the power network and $G_{\text{com}} = (V_{\text{com}}, E_{\text{com}})$ for the communication network. Another term is E_{dep} which represents interdependencies between elements of the two presented graphs. The small-cluster model [10] assumes different roles in the communication network and more complex dependencies compared to the one-one model. It defines two roles for nodes in the communication network, including the control center to monitor power nodes and relay nodes for communication. Furthermore, all power components have the same role in the power network.

The model also defines interdependencies between power and communication components. The model uses the $k-n$ dependency proposed in [16]. In the $k-n$ dependency, each node in the power network is controlled by k control center nodes, and each control node supports n power nodes. In addition, each cyber component depends on a power node for power supply. In addition to nodes belonging to the giant graph component, all nodes belonging to clusters larger than Δ are considered functional. A cluster is a group of alive nodes in the same network (power or communication networks) after the failure of initial nodes. These nodes also should connect to at least one node in the other network.

B. RFP System Model

We use two separate graphs to model the power and the communication networks. We represent the power network with the graph $G_{\text{pow}} = (V_{\text{pow}}, E_{\text{pow}})$ and the communication network with $G_{\text{com}} = (V_{\text{com}}, E_{\text{com}})$.

1) Nodes' Roles and Dependencies: The G_{com} consists of communication and control components. We define two roles for nodes in G_{com}, namely, relay nodes that connect the communication system and control center nodes that monitor and control power nodes [10]. All dependencies in the communication network are represented by edges in the E_{com}. E_{com} is a set of edges representing a physical connection between communication and control nodes. The power graph, G_{pow}, includes the power components and is used to model the power network.

We use the IEEE 118- and 300-bus systems [17] to define the roles of power components and construct the power network. We specify four roles for power nodes, namely, bus, load, generator, and transformer. We assign these roles according to the IEEE standards [18]. These roles identify dependencies and rules to model the power system more accurately. These considerations make our model more realistic because these roles are defined based on power systems.

The dependencies between nodes in the power graph are identified by E_{pow}, which is a set of undirected edges that represent transmission lines between power components. For instance, if there is a line between u and v in the power network and $u, v \in G_{\text{pow}}$, there is an edge like $e_{(\text{u,v})} \in E_{\text{pow}}$ that connects these two nodes in the power graph.

2) Interdependencies: An interdependency represents the relationship between components in the power and communication networks. The set of interdependencies is represented by $d_{\text{inter-system}}$. It includes all directed edges in the system graph that make the physical or logical connections between one node from G_{pow} to another in G_{com} or vice versa. Interdependencies in real-world systems are unidirectional according to [19]. Thus, all interdependencies in our model are

unidirectional based on real-world networks. This assumption makes our model more realistic. These interdependencies are:

Control: We assume that all power nodes depend on control center nodes for controlling and monitoring. This assumption is a logical interdependency and means that control centers are responsible for controlling the power components. The power node cannot be considered functional without this dependency (i.e., when the control center fails).

Communication: We assume that all power nodes depend on relay nodes to connect to the communication network and communicate with control centers. Relay nodes transmit control messages to the power nodes. This connection is a physical dependency, and there should be a connection between the power node and a relay node to assume that the power node is functional. The power node's measured data should be sent to the control center for further decisions.

Power supply: We assume that a power node connects to the communication network via a relay node. Also, this relay node depends on the power node for the power supply. This assumption is based on two IEEE standards including, C37.115 [20], and IEEE 1615 [21] to show that each power component should be connected to the utility WAN and control center through a connecting point (a relay node).

Apart from the above interdependencies, we consider two rules related to the system's functionality. The first rule, there should be at least one operational generator in each cluster. The second rule, there should be at least one bus and one control center in the system, and without them, the system will collapse.

C. RFP System Implementation

We now describe the generation of test environment and power and communication networks coupling. We use Python and NetworkX [22] library to develop our simulator and achieve experimental results. We also use Pandapower [23] (an open-source library on Python) to implement a power system and analyze power flow in our framework. To generate the system, we implement different IEEE bus models using Pandapower. Then, we convert the models into graphs and use NetworkX to study the cascade of failures. One relay node is responsible for supporting each power node for communication, i.e., each power element is connected to the WAN by a relay node. This assumption is based on IEEE standards [20] that are references to the design of the power systems. As a result, this helps the model to be more practical.

We use the $k-n$ model [10] to connect control centers to power nodes. Algorithm 1 describes how control centers connect to power nodes. With predefined k and n values, the algorithm chooses n nearest power nodes to each control center with a greedy paradigm. It makes a logical connection or interdependency between them (*Control interdependency*).

First, Algorithm 1 chooses one control center, like C_{x}, to make logical connections. It connects between C_{x} and the nearest power node whose control connections are less than k, i.e. node P_{y}. Then, it searches in the neighbors of P_{y}. If there is a node like P_{z} that its control connections are less than k, the algorithm makes a connection between C_{x} and P_{z}. Otherwise, if it cannot find any node, it repeats the search process for neighbors of P_{z}. The algorithm is repeated for all control centers until all control centers have exactly n logical connections to the power nodes.

Algorithm 1 Connecting the control center and power nodes

1: **Input:** G_{pow}, The set of control nodes.
2: **for** (All control nodes $\mathrm{C_x}$) **do**
3: **if** ($|\mathrm{ControlConnections(C_x)}| < n$) **then**
4: choose the nearest power node ($\mathrm{P_y}$) to $\mathrm{C_x}$ that its
5: control connections is less than k
6: Connect($\mathrm{C_x}$ to $\mathrm{P_y}$)
7: $\mathrm{Set_a} \leftarrow$ neighbors($\mathrm{P_y}$)
8: Flag $\leftarrow 0$
9: **for** (each $\mathrm{P_z}$ in $\mathrm{Set_a}$) **do**
10: **if** ($|\mathrm{ControlConnections(P_z)}| < k$) **then**
11: Connect($\mathrm{C_x}$ to $\mathrm{P_z}$)
12: Flag $\leftarrow 1$
13: break()
14: **end if**
15: **end for**
16: **if** (Flag == 0) **then**
17: Repeat from line 7 for $\mathrm{P_z}$
18: **end if**
19: **end if**
20: **end for**

IV. Failure Propagation Process

This section investigates the attack model and failure propagation process caused by an initial failures or cyber attacks.

A. Attack Model

A cyber attacker can compromise a smart grid by attacking its power or communication networks. Malicious agents can use the communication system to access its power components and measurement units and change the data or gain information about the system. Denial of Service (DoS) and False Data Injection (FDI) are common cyber attacks on the smart grid networks that cause the most devastating impact on the system's functionality [24].

1) FDI attacks: In FDI attacks, the attacker compromises sensor or meter data by injecting malicious data into the system to mislead the grid operation. The attacker can manipulate data through physical attacks or by using a system's communication network to access its measured data. These attacks can cause a cascading failure in the smart grid network [25]. One of the impacts of this kind of attack could be load redistribution in the power network [26].

To plan an FDI attack, we assume that the attacker knows the system and its architecture. Another assumption is that the attacker has enough resources to alter the measured data of the power components and the overload power components. In this paper, we consider the overload attack on power components. In this attack, the loaded power of electrical components is falsified by a malicious agent to a value higher

than its capacity. Therefore, this component is overloaded and should be tripped [25]. When a power element is overloaded, the attacker can trip the breakers of the component [25]. Therefore, the component will fail and should be removed from the system. We assume that the failed component is nonfunctional and is removed from the simulation until the end of failure propagation.

2) DoS attacks: These attacks can make communication nodes dysfunctional and can be detected in the control center [27]. An attacker attempts to degrade the functionality of the network by sending useless packets through the communication network. As the power grid uses public networks like IP, an attacker can manipulate a network component to compromise the system.

Sensors send the measurement data to the state estimators via the communication network. When the communication network is affected by a DoS attack, the measured data cannot be sent or received. As a result, the communication between sensors and state estimators is blocked [28], i.e., remote transmission measurement data is blocked and lost. We assume that the DoS attack affects the measurement channel and will be continuous. We also assume that when the measurement is lost, it cannot be generated using a recently received measured signal. Therefore, the control center considers that the power component has failed because of the lack of its control signal. Finally, we assume that when a power component is considered disconnected by the control center, it is failed and will be eliminated from the simulation.

B. The Failure Propagation Process in the RFP Model

After generating the system and initializing the network parameters, the next step is propagating failures caused by an initial attack or failure. Figure 1 shows the failure propagation process used in the RFP model. The first step is choosing initially attacked nodes in the communication or power networks. The selection of initial nodes depends on the attack strategy and will be explained in the next section. The initially failed nodes are disabled and cannot participate in the simulation. After removing the initially attacked/failed nodes, an iterative process is executed until the propagation stops. In this process, we identify nodes and edges that should be removed from the power and communication networks based on the rules and interdependencies that we previously defined.

Edges that are directly connected to attacked nodes are removed from the system, including intra- and inter-network edges. As edges represent dependencies between different components in the system, failing a component causes the removal of the edge from the system. Some nodes will not have a previously defined interconnection by removing these edges. If a power node is not connected to at least one control center (logical connection) and a relay node (physical connection), then it is considered non-functional. It means that for every power node like u there should be two edges like d_{uv} and d_{uw} in the $d_{\text{inter-system}}$ that v is a control center and w is a relay node. On the other hand, a communication node will not be functional if there is not a power node that supports it for power supply.

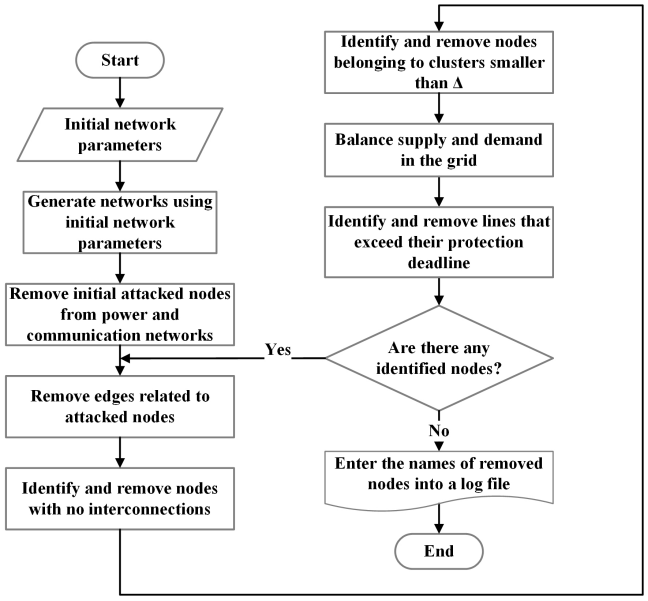

Fig. 1: Failure propagation process in the RFP model.

In the next step, the algorithm identifies nodes that belong to a cluster with a size less than Δ. The parameter Δ is a predefined variable and indicates the size of functional clusters. After removing nodes and edges from the system, a giant cluster (defined as the largest connected group of nodes in each network) and small clusters (whose size is smaller than the giant cluster) are formed. We assume that a cluster with a size of more than Δ and containing at least one generator is functional in the RFP model. This consideration makes the RFP model more realistic because the power cannot be generated without a generator in a cluster.

Subsequently, the RFP model performs power flow analysis to identify transmission lines that exceed their capacity. By removing failed components in the power network, the power flow is redistributed. The redistribution causes certain lines to exceed their power capacity. With the power flow analysis, we identify these transmission lines and remove them from the system because they are overheated. If nodes or lines are removed from the system, the process is repeated until there are no more failures (see Figure 1). When the failure propagation stops, the identity of failed nodes and edges are stored in a log file. This file is helpful for further analysis and steps of failure propagation.

The failure propagation process is based on interdependencies and rules we defined in the previous section, and it provides a realistic model of cascading failures in the smart grid. As a result, the RFP model produces more realistic results based on the defined relations in the failure propagation process.

V. Experimental Results and Analysis

We evaluate the RFP model under different attack scenarios and compare the results with the small cluster model [10]. We

build the power and communication networks in the small cluster model using the Barabasi-Albert model [29]. For the power network, we use the 118-bus and 300-bus systems. After adding all of the buses, loads, generators, and transformers to the power graph, the number of nodes in the power network is 283 and 689 nodes for the 118-bus and 300-bus systems, respectively.

To generate the communication network, we use the Barabasi-Albert model [29] to connect communication nodes. The number of nodes in the communication network for the 118-bus and 300-bus systems is 469 and 1,148, respectively. We couple the two networks and generate the smart grid system using our approach in section III. In all simulations, the value of parameters is $n = 3$, $k = 2$, and $\Delta = 4$. The value of n and k is chosen based on the small-cluster model [10] to achieve the same results. Δ is large enough to ensure a generator exists in each cluster and at least one bus in the system. We simulate the system 100 times for each initial number of attacks and average the final functional nodes to achieve more accurate results. We test the RFP model under random and targeted attacks (explained later). First, we inject simultaneous attacks into the system based on the attack scenario. Then, we run the failure propagation process and show components of the power and communication networks that have failed. We consider the impact of the power capacity of transmission lines in cascading failures.

A. Random Attacks

In the first attack, we select nodes randomly and calculate the percentage of functional nodes after the initial failure propagation. We simulate the small cluster model [10] with the same number of power and communication nodes. The simulation results can be seen in Figure 2. The number of power nodes in the Small Cluster model is 283 and 689 nodes, respectively, similar to the IEEE 118-bus and 300-bus systems. Therefore, the number of all nodes in the system is 752 and 1,837. We can see that the system fails faster in the small cluster model than the RFP model. This happens because the small cluster model assumes general interdependencies regardless of the role of each node and makes unnecessary assumptions that cause dramatic consequences in some cases.

B. Targeted Attacks

We evaluate the RFP model under targeted attacks that can take place in real-world systems. We use the IEEE 300-bus system as it contains more components and can show a better behavior of the system. The simulation results can be seen in Figure 3. We compare the random attack with inter- and intra-degree attacks on the RFP model in this figure. In inter-degree attacks, nodes with more interconnections to other nodes in the second network are more likely to be chosen in the initial attack. In intra-degree attacks, nodes with higher intra-degrees are more likely to be attacked. The intra-degree of a node is the number of connections to other nodes within its network.

From Figure 3, we can see that when the number of initial attacks is high, an intra-degree attack is more devastating

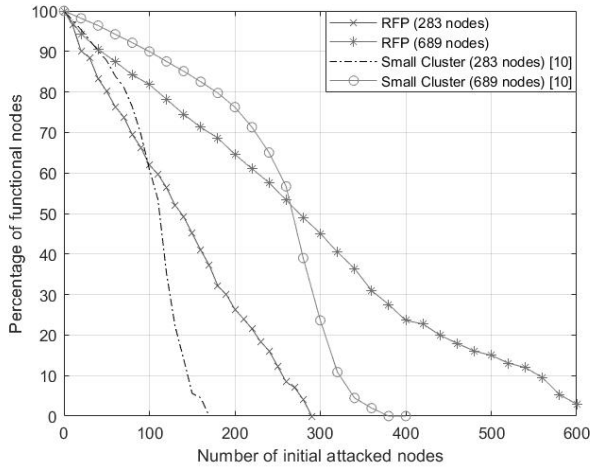

Fig. 2: Percentage of functional nodes based on the initial attacked nodes in the RFP and Small Cluster models.

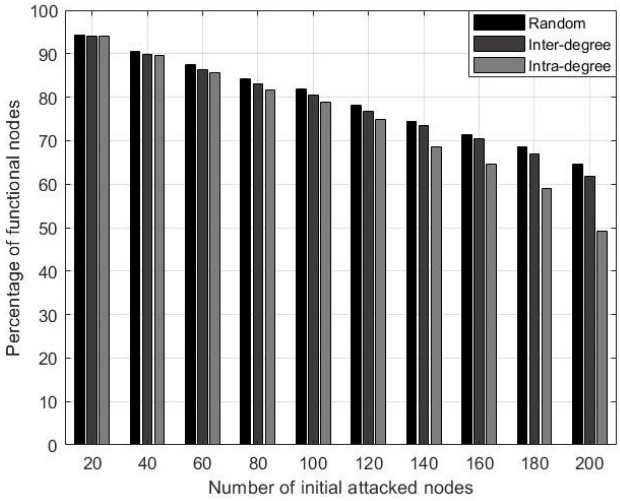

Fig. 3: Random, inter-degree and intra-degree attacks on the RFP model.

compared to other attacks. The reason is that the intra-degree of nodes varies significantly compared to the inter-degree of nodes. We also compare the RFP with the small cluster model under inter- and intra-degree attacks. Figure 4 shows that the small cluster model is also more vulnerable to intra-degree attacks compared to inter-degree attacks. This result is similar to what the authors achieved in [10], i.e., the intra-degree attacks make the system more vulnerable in the small cluster model. The second observation is that the RFP model degrades less than the small cluster model in targeted attacks.

VI. Conclusions

In this paper, we proposed a Realistic Failure Propagation (RFP) model for smart grid networks. Our model considers novel interdependencies and the role of nodes to analyze cascading failures. We also defined new rules based on IEEE standards for the smart grid to investigate the failure propagation and cascading failures. The RFP model considers

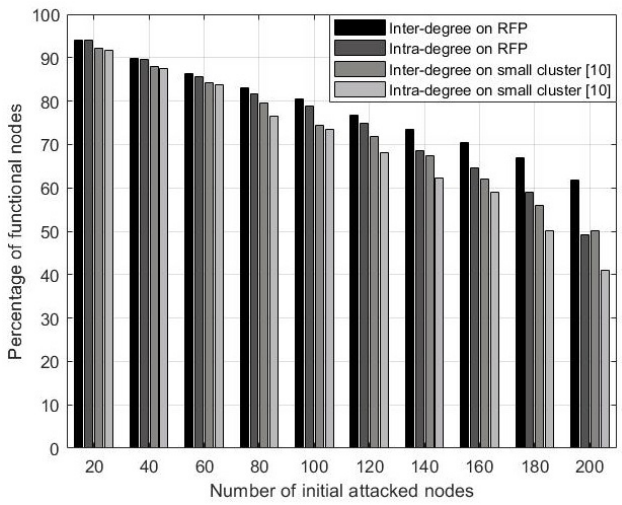

Fig. 4: Inter-degree and intra-degree attacks on the RFP and the small cluster models.

electrical parameters of the system and analyzes power flow to identify overheated transmission lines. This assumption provides a better perspective of the failure propagation and makes the RFP more realistic. We compared the RFP model with the small-cluster model and evaluated it under different attacks scenarios. As future work, we plan to study the exact location of initial failures and the impact of generator failures on the system. To demonstrate the accuracy of the experimental results, we plan to verify the results using the percolation theory and compare them with actual data.

ACKNOWLEDGMENT

This work was funded by the Ericsson Canada Inc. and Mitacs IT16748 “A Realistic Machine Learning-based Model for Failure Prediction and Propagation in Smart Grid Networks”.

REFERENCES

[1] S. Aggarwal, N. Kumar, S. Tanwar and M. Alazab, ”A Survey on Energy Trading in the Smart Grid: Taxonomy, Research Challenges and Solutions,” in IEEE Access, vol. 9, pp. 116231-116253, 2021.

[2] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan and L. Mihet-Popa, ”Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications,” in IEEE Access, vol. 8, pp. 151019-151064, 2020.

[3] Cyber-Attack Against Ukrainian Critical Infrastructure. Accessed: Feb. 12, 2022. [Online]. Available: https://ics-certus-cert.gov/alerts/IRALERT- H-16-056-01.

[4] T. N. Nguyen, B. -H. Liu, N. P. Nguyen, B. Dumba and J. -T. Chou, ”Smart Grid Vulnerability and Defense Analysis Under Cascading Failure Attacks,” in IEEE Trans. on Power Delivery, vol. 36, no. 4, pp. 2264-2273, Aug. 2021.

[5] D. Liu and C. K. Tse, ”Cascading Failure of Cyber-Coupled Power Systems Considering Interactions Between Attack and Defense,” in IEEE Trans. on Circuits and Systems I, vol. 66, no. 11, pp. 4323-4336, Nov. 2019.

[6] H. Shayan and T. Amraee, ”Network Constrained Unit Commitment Under Cyber Attacks Driven Overloads,” in IEEE Trans. on Smart Grid, vol. 10, no. 6, pp. 6449-6460, Nov. 2019.

[7] L. Che, X. Liu, T. Ding and Z. Li, ”Revealing Impacts of Cyber Attacks on Power Grids Vulnerability to Cascading Failures,” in IEEE Trans. on Circuits and Systems II: Express Briefs, vol. 66, no. 6, pp. 1058-1062, June 2019.

[8] 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. on Smart Grid, vol. 7, no. 1, pp. 530-538, Jan. 2016.

[9] J. Cordova-Garcia, X. Wang, D. Xie, Y. Zhao and L. Zuo, ”Control of Communications-Dependent Cascading Failures in Power Grids,” in IEEE Trans. on Smart Grid, vol. 10, no. 5, pp. 5021-5031, Sept. 2019.

[10] Z. Huang, C. Wang, A. Nayak and I. Stojmenovic, ”Small Cluster in Cyber Physical Systems: Network Topology, Interdependence and Cascading Failures,” in IEEE Trans. on Parallel and Distributed Systems, vol. 26, no. 8, pp. 2340-2351, 1 Aug. 2015.

[11] D. Liu, X. Zhang and C. K. Tse, ”A Tutorial on Modeling and Analysis of Cascading Failure in Future Power Grids,” in IEEE Trans. on Circuits and Systems II: Express Briefs, vol. 68, no. 1, pp. 49-55, Jan. 2021.

[12] M. Rahnamay-Naeini and M. M. Hayat, ”Cascading Failures in Interdependent Infrastructures: An Interdependent Markov-Chain Approach,” in IEEE Trans. on Smart Grid, vol. 7, no. 4, pp. 1997-2006, July 2016.

[13] C. -L. Chen, Q. P. Zheng, A. Veremyev, E. L. Pasiliao and V. Boginski, ”Failure Mitigation and Restoration in Interdependent Networks via Mixed-Integer Optimization,” in IEEE Trans. on Network Science and Engineering, vol. 8, no. 2, pp. 1293-1304, 1 April-June 2021.

[14] R. J. La, ”Influence of Clustering on Cascading Failures in Interdependent Systems,” in IEEE Trans. on Network Science and Engineering, vol. 6, no. 3, pp. 351-363, 1 July-Sept. 2019.

[15] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, “Catastrophic cascade of failures in interdependent networks,” Nature, vol. 464, pp. 1025–1028, Apr. 2010.

[16] Z. Huang, C. Wang, M. Stojmenovic and A. Nayak, ”Balancing System Survivability and Cost of Smart Grid Via Modeling Cascading Failures,” in IEEE Trans. on Emerging Topics in Computing, vol. 1, no. 1, pp. 45-56, June 2013.

[17] University of Washington, Dept. of Electrical Engineering. Power systems test case archive, Accessed: Mar. 30, 2021, Published online at: http://www.ee.washington.edu/research/pstca/, 1999.

[18] ”IEEE Guide for the Interoperability of Energy Storage Systems Integrated with the Electric Power Infrastructure,” in IEEE Std 2030.2-2015 , vol., no., pp.1-138, 30 June 2015.

[19] J. Shao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, ”Cascade of failures in coupled network systems with multiple support-dependent relations,” Phys. Rev. E, vol. 83, pp. 1-9, Mar. 2011.

[20] ”IEEE Standard Test Method for Use in the Evaluation of Message Communications Between Intelligent Electronic Devices in an Integrated Substation Protection, Control and Data Acquisition System,” in IEEE Std C37.115-2003 , vol., no., pp.1-82, 30 June 2004.

[21] ”IEEE Recommended Practice for Network Communication in Electric Power Substations,” in IEEE Std 1615-2019 (Revision of IEEE Std 1615-2007) , vol., no., pp.1-140, 8 Nov. 2019.

[22] A. A. Hagberg, D. A. Schult, and P. J. Swart, “Exploring network structure, dynamics, and function using networkX,” in Proc. 7th Python Sci. Conf., Aug. 2008, pp. 11–16.

[23] L. Thurner *et al.*, ”Pandapower—An Open-Source Python Tool for Convenient Modeling, Analysis, and Optimization of Electric Power Systems,” in IEEE Trans. on Power Systems, vol. 33, no. 6, pp. 6510-6521, Nov. 2018.

[24] R. Deng, P. Zhuang and H. Liang, ”CCPA: Coordinated Cyber-Physical Attacks and Countermeasures in Smart Grid,” in IEEE Trans. on Smart Grid, vol. 8, no. 5, pp. 2420-2430, Sept. 2017.

[25] L. Che, X. Liu, Z. Shuai, Z. Li and Y. Wen, ”Cyber Cascades Screening Considering the Impacts of False Data Injection Attacks,” in IEEE Trans. on Power Systems, vol. 33, no. 6, pp. 6545-6556, Nov. 2018.

[26] Y. Yuan, Z. Li and K. Ren, ”Quantitative Analysis of Load Redistribution Attacks in Power Systems,” in IEEE Trans. on Parallel and Distributed Systems, vol. 23, no. 9, pp. 1731-1738, Sept. 2012.

[27] F. Zhang, M. Mahler and Q. Li, ”Flooding attacks against secure time-critical communications in the power grid,” 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm), 2017, pp. 449-454.

[28] C. De Persis and P. Tesi, ”Input-to-State Stabilizing Control Under Denial-of-Service,” in IEEE Trans. on Automatic Control, vol. 60, no. 11, pp. 2930-2944, Nov. 2015.

[29] A. L. Barabsi and R. Albert, ”Emergence of scaling in random networks,” Sci., vol. 286, no. 5439, pp. 509–512, Oct. 1999.