IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 12 July 2022, accepted 24 July 2022, date of publication 29 July 2022, date of current version 8 August 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3194989

RESEARCH ARTICLE

Modeling Cascading Failures in Coupled Smart Grid Networks

ALIASGHAR SALEHPOUR[1], (Student Member, IEEE), IRFAN AL-ANBAGI[1], (Senior Member, IEEE), KIN-CHOONG YOW[1], (Senior Member, IEEE), AND XIAOLIN CHENG[2]

[1]Faculty of Engineering and Applied Science, University of Regina, Regina, SK S4S 0A2, Canada
[2]Ericsson Inc., Santa Clara, CA 95054, USA

Corresponding author: Irfan Al-Anbagi (irfan.al-anbagi@uregina.ca)

This work was supported by Ericsson Canada Inc., and Mitacs IT16748 "A Realistic Machine Learning-Based Model for Failure Prediction and Propagation in Smart Grid Networks."

ABSTRACT The smart grid connects components of power systems and communication networks in an interdependent two-way system that delivers electricity to consumers and collects data that enables it to react to usage levels and interference from threats, such as cyber-attacks. In this paper, we propose a novel cyber-attack failure propagation model in smart grids. Our realistic failure propagation model addresses the system's heterogeneity by assigning different roles to its components. We define rules for and interdependencies of failure propagation and propose a new approach to studying cascading failures. In addition, our graph model identifies the most-vulnerable nodes. The model implements power flow analysis to guarantee that all transmission lines work below capacity and remove lines exceeding capacity. The model also considers that control packets could encounter different delays regarding the communication network structure and investigates the impact of communication delay on the failure of power components. Our results establish that by considering both power and communication characteristics and interdependencies, cascading failures can be modeled more accurately. We show that when we run the power flow analysis, there are a negligible number of failed nodes, which means that our model accurately identifies system failures.

INDEX TERMS Cascading failures, communication delay, cyber-attacks, failure propagation, graph theory, interconnection networks, power flow analysis, realistic model, smart grid.

I. INTRODUCTION

A smart grid network is a complex cyber-physical system (CPS) that introduces new capabilities based on exclusive systems features. These features are designed to improve reliability, performance, and security of traditional power grids [1]. A smart grid incorporates complex dependencies between its various elements, which means that communication components depend on power assets for power supply, and power assets and control systems need communication infrastructure to connect with the network and perform their functions.

The associate editor coordinating the review of this manuscript and approving it for publication was Akin Tascikaraoglu.

The heterogeneous nature of the smart grid makes it difficult to standardize procedures and communication paradigms [2]. These system dependencies and heterogeneous communication architectures introduce new challenges related to cyber security and reliability. The smart grid is a complex network that different characteristics of elements like nodes' centrality have more impact on cascading the information [3]. One of the main challenges is in the cascading failures caused by cyber-attacks or in the failure of a component in the power grid [4]. These attacks may occur when nodes or transmission lines in a smart grid fail [5]. When a power grid asset fails, this failure can propagate across the system due to the interdependencies between the power assets and the communication

components. Based on this, a cyber attack on a grid's communication network can lead to the failure of its power elements.

Cyber-attacks and their cascading effects have caused massive blackouts in recent years. For example, in 2015, Ukrainian power companies experienced a cyber attack that affected more than 225,000 customers and resulted in blackouts across the country [6]. In 2020, the central region of Mumbai, India, experienced a blackout for two hours. Malicious software was pre-positioned on Indian power sector organizations' networks and caused the tripping of circuits at two substations [7]. It affected the frequency of the transmission system in Mumbai and caused a cut-off of the power energy. These blackouts occurred because of the cascading effects of an initial attack on the whole system.

Cascading failures start with the failure of one or several power components and spread across the system. The interdependencies between a system's power and cyber elements mean that an initial failure can propagate throughout the system and lead to power outages and blackouts. When a power component fails, the load is automatically redistributed across the system. Consequently, transmission lines and power components can become overloaded and disconnected from the system [8].

Many studies investigated how to mitigate the cascading failure impacts caused by cyber-attacks. For example, [4], [5], [9]–[11] proposed algorithms to identify the most-vulnerable power lines and components in terms of their susceptibility to cascading attacks to strengthen power systems by protecting these vulnerable assets. These efforts show the importance of addressing the problem of cascading failure attacks on smart grids and the consequences of failing to do so.

Many models have been proposed to investigate cascading failures in CPS and smart grids [10], [12]–[18]. Method of probability, statics, and physics are commonly used in modeling different phenomena in networks [17]. However, some studies did not consider the role of cyber-attacks or cascading failures in communication component failures [8]. Others did not consider the interdependencies between power and communication networks or only modeled the power grid [12]. However, some papers modeled both the networks and the interdependencies between their different components, regardless of the role of their power components and the limitations of their power capacity [10], [12], [13]. The problem with these models is that they underestimated the extent to which power components can fail. For example, studies that used these models did not address how power redistribution can cause failures in transmission lines; that is, when a power component fails, the manner in which the power flow is redistributed through existing transmission lines can cause further failures. This factor was not recognized in these studies.

The main goal of this paper is to model a smart grid network and study the impact of the failure of different components on power and communication networks. This paper proposes a novel model to investigate the effects of cascading failures caused by cyber-attacks in a smart grid environment. We define different roles for power and communication components based on IEEE standard systems, and we consider their characteristics when determining the interdependencies between two networks' elements that are different from the small-cluster model [13]. Our proposed realistic failure propagation (RFP) model is based on the conditions for failure propagation, network topologies, and the interdependencies between components. The failure propagation process consists of practical rules with which to study cascading failures. To make the model more realistic, we also address the role of the capacity of its power elements in addressing the failure propagation process.

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

- We propose a novel model based on IEEE standard bus systems to study the evolution of failure propagation in a smart grid.
- We address the heterogeneity of this system's power components and define novel interdependencies so as to percolate a failure in its power and communication components.
- We define new rules and conditions based on IEEE standards to model failure propagation in the system.
- Our model performs power flow analysis to identify transmission lines that exceed their capacity limits so as to consider the electrical transmission characteristics of the system.
- We model delayed control packets in a communication network to study the consequences of different delays on the functionality of a smart grid network.

The rest of the paper is organized as follows: Section II discusses related work. Section III presents modeling the failure propagation and the RFP model for cascading failure. Section IV outlines cyber-attacks and the failure propagation process. Section V shows the experimental results. Section VI presents four case studies, and, section VII concludes.

II. RELATED WORK

Extensive academic and industrial investigations have been carried out on cyber-attacks and their effects on smart grid networks. The research community has developed different methods of detecting these attacks and has studied the failure propagations they have caused [8], [13], [14], [18]–[20].

Cai *et al.* [14] proposed a model to analyze failure propagation in interdependent power and dispatching data networks in China. Their paper only considered transmission line failures and proposed an algorithm to identify overloaded branches and instability in a system. In [18], a control algorithm was proposed to reduce the impact of propagating failures based on a communication network and power grid models. However, the authors did not study the effect of the failure of communication components but only focused on transmission line failures.

Sun *et al.* [19] presented a two-stage cyber intrusion defense solution in a smart meter network. A Support Vector Machine (SVM) is utilized as a detection technique in the

initial step of intrusion detection to uncover suspicious behavior inside a smart meter. The Temporal Failure Propagation Graph (TFPG) approach is utilized in the second stage to build attack pathways for detecting attack events. In [20], the authors proposed an attack detection framework using supervised machine-learning and deep learning algorithms to assess secured and unsecured networks.

Che *et al.* [12] showed that a well-designed false data injection (FDI) attack can overload critical branches of a power network and, consequently, increase the probability of initiating contingencies and causing a cascading failure. However, the authors only focused on critical grid branches and missed the impact of communication networks on cascading failures.

In [21], the authors proposed a model that identifies critical components that perform cascading failures when experiencing cyber-attacks. Peng *et al.* [22] exploited a game theory optimization method to formulate cascading failures that are induced by overloaded branch chains. Although these models considered the interdependencies of the different components of a smart grid, they omitted the role of power components and cyber elements in the propagation of failures and the impact of cyber-attacks on communication networks.

Various studies have focused on interdependent networks to study failure propagation in a smart grid [23]–[25]. All of the above studies focused on modeling these interdependencies and the impact of failure on a system; however, they omitted the system's heterogeneity, the role of its components, and the power system's electrical characteristics. Therefore, these studies underestimated the impact of cascading failures and did not model all of the parameters of failure propagation.

One of the first models that used to study failure in interconnected networks was the one-to-one model [26]. This model assumed that all components in the power and communication networks are homogeneous, and the failure of each node in a network may cause some nodes in the other network to fail. This model defined a one-to-one dependency between each node in a physical graph and one node in a cyber graph and vice versa. This dependency was presented in two graphs, each with the same number of nodes. Each graph consisted of nodes as components and edges as physical connections between nodes. Therefore, the edges that represented the interdependencies were unidirectional.

The failure propagation process consisted of two rules that considered a node as functional after an initial failure. The first rule stated that a functional node u should belong to the largest connected sub-graph in its network, and the second rule noted that there should be a connection between node u and a node in the other network. Propagating a failure with the initially failed nodes was an iterative process, and nodes that did not consist of the mentioned conditions were removed from the system until there were no further failures.

In another study, Huang *et al.* [13] proposed a small-cluster model to study cascading failures in interdependent systems. The authors assumed two roles for the cyber nodes and more interdependencies between the power and communication components. As we will compare the RFP with the small-cluster model, we will elaborate on this model in the next section.

Based on the assumptions and interdependencies in [26] and [13], both papers adopted simplified models and the same roles for the power elements. Thus, these models were unable to identify different components of the system's physical structure. Both models consider the number of nodes and connections between them to determine the functionality of nodes, and the role of nodes is not influential in the failure propagation. For instance, based on these models, a system without a generator can be considered a functional system. Further, neither method can point out the power flow in a power network nor can they identify lines that exceed their capacity.

Unlike the small-cluster model [13], our RFP model assumes different roles for power components and based on this knowledge, it considers more-complicated interdependencies and rules for failure propagation. We also use power flow analysis to identify the transmission line failures due to these lines' thermal limits. The other difference between the small-cluster and RFP models is that we utilize different delays for control packets to make the RFP model more realistic.

III. MODELING FAILURE PROPAGATION

In this section, we describe the small-cluster model [13]. Then we describe our proposed RFP model. We elaborate on the small-cluster model because we compare our results with this model, which helps us understand our proposed model's fundamentals. We also use the concept of small clusters to ensure that the results are achieved in the same way that can be compared with the small-cluster model. As a result, the RFP model is independent of the small-cluster model. We improve the failure propagation process by utilizing novel interdependencies and rules, nodes' roles, and electrical characteristics of power components.

A. SMALL-CLUSTER MODEL

In general, to model power and communication networks, two separate graphs can be used: $G_{\text{pow}} = (V_{\text{pow}}, E_{\text{pow}})$ 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 the interdependencies between the elements presented in the two graphs in Figure 1.

The small-cluster model [13] assumes different roles in a communication network and more-complex dependencies compared to the one-to-one model. Similar to [26], this model uses two graphs to form the system. It defines two roles for the nodes in the communication network, including the control centers that monitor power nodes and the relay nodes that facilitate communication. Furthermore, all of the power components have the same roles in the power network.

The model also defines the interdependencies between the power and communication components. The model uses the $k - n$ dependency proposed in [27]. Each node in the power

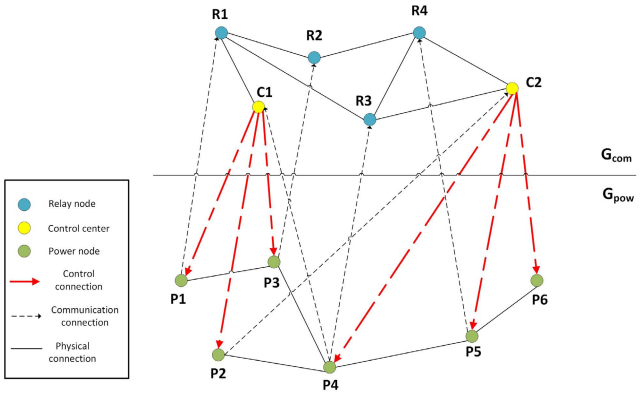

FIGURE 1. An example of small-cluster model where, n=3 and k=1 [13]. Each power node depends on a control center for monitoring and a relay node for communication.

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 the power supply. In the failure propagation process, the algorithm defines a threshold Δ. All clusters with sizes greater than Δ are functional after the failure of the initial nodes. A cluster is a group of connected nodes that are located in one network (either the power or the communication network).

In addition to the nodes that belong to the giant graph component, all of the nodes that belong to clusters of a size larger than Δ are considered functional. These nodes should also connect to at least one node in the other network. The failure propagation process is similar to the one-to-one model [26]. One example of the small-cluster model can be seen in Figure 1, where $n = 3$ and $k = 1$. In Figure 1, the yellow nodes are control centers, and the black nodes present relay nodes.

In the small-cluster model, if a node follows two rules, then it can be considered functional. The first rule is that it should belong to a cluster with a size larger than Δ in its network; the second rule is that there should be at least one inter-link between this node and another node in the other network. The small-cluster model uses synthetic networks to form the power and communication networks. Then the $k - n$ model is used to couple these two networks. The small-cluster model follows percolation theory to show that the system's robustness increases as Δ increases. The model also shows that there is an upper bound for the number of small clusters after the failure propagation, which is also based on percolation theory.

B. REALISTIC FAILURE PROPAGATION SYSTEM MODEL

We use two separate graphs to model the power and communication networks. In Figure 2, we show the power network using 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) ROLES AND DEPENDENCIES OF NODES

The communication network graph (G_{com}) consists of communication and control components. We define two roles

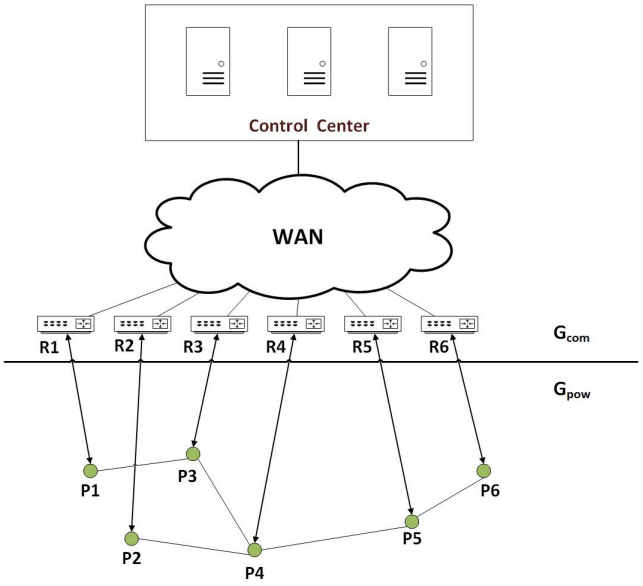

FIGURE 2. Interdependencies between power components and relay nodes in the RFP model. Power nodes are connected to the control center through relay nodes.

for the nodes in G_{com}; namely, the relay nodes that form the communication system and the control center nodes that monitor and control the power nodes [13]. All of the dependencies in the communication network are shown by the edges in the E_{com}. E_{com} is a set of edges representing a physical connection between the communication nodes. The control center nodes are dependent on the relay nodes for communication; that is, for a control node to be able to communicate with other nodes, it needs to be connected to at least one relay node. The power graph, G_{pow}, includes the power components and is used to model the power network.

We use the IEEE 14-, 39-, 118-, and 300-bus systems [28] to define the roles of the power components and to construct the power network. We specify four roles for the power nodes; namely, bus, load, generator, and transformer. We assign these roles according to IEEE standards [29]. These roles identify both the dependencies and the rules for more accurately modeling the power system. These assumptions make our model more realistic because these roles are defined based on actual power systems.

The dependencies between the nodes in the power graph are identified by E_{pow}, which is a set of undirected edges that represents the transmission lines between the power components. For instance, if there is a line between u and v in the power network and $u, v \in G_{\text{pow}}$, then there is an edge like $e_{(u,v)} \in E_{\text{pow}}$ that connects these two nodes in the power graph. Figure 3 (a) shows the IEEE 14-bus reference model [28] that is the standard structure of this test case.

Figure 3 (b) shows the equivalent graph of the IEEE 14-bus test case with nodes and edges. It can be seen that for each power component in the power network, there is an equivalent node in this figure. There are four types of components in the IEEE bus test cases (Figure 3 (a)); namely,

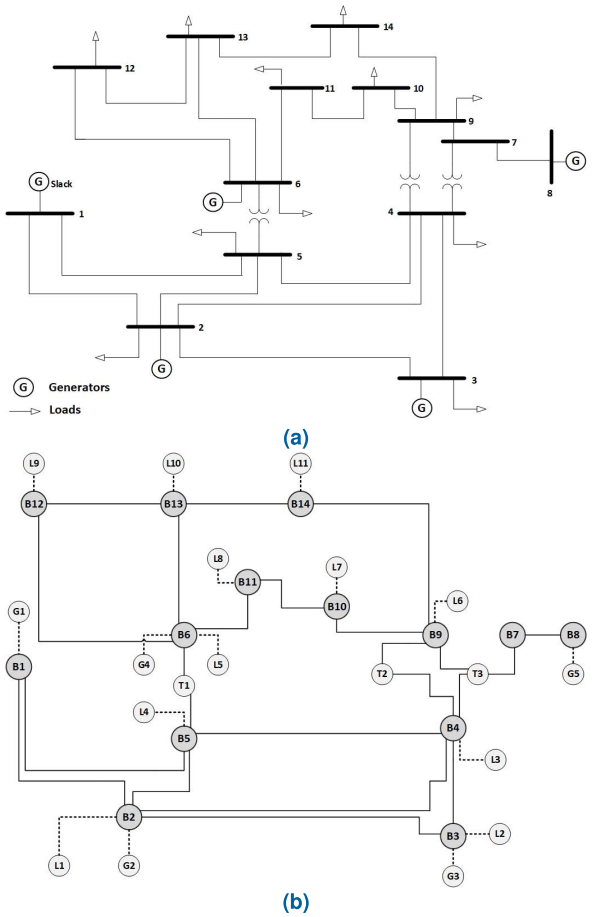

FIGURE 3. The IEEE 14-bus system representation (a) the standard power system, (b) the equivalent graph model. There are four types of power elements, including bus, generator, transformer, and load in the system.

bus, load, generator, and transformer, represented by B, L, G, and T and indicated by the circles in Figure 3 (a). There are 14 buses, 11 loads, five generators, and three transformers in the graph (Figure 3 (b)). Transmission lines carry power from one substation to the other. We use undirected edges in the equivalent graph to present the transmission lines.

2) INTERDEPENDENCIES

An interdependency represents the relationship between the components in power and communication networks. The set of interdependencies is represented by $d_{\text{inter-system}}$. It includes all of the directed edges in the system graph that connects one node from G_{pow} to another in G_{com}, or vice versa. These dependencies are as follows:

a: 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 the control centers are responsible for controlling the power components. The interdependency is represented by a directional arc that shows one-way controllability. The power node cannot be considered functional without this dependency (i.e., when the control center fails). The power node will fail when there is no control center to send commands to this power element and monitor its functions.

In the RFP model, we consider four types of power nodes monitored and controlled by the control center, including bus, generator, transformer, and load. When a control center fails, we consider that these power stations connected to the control center will fail. These power stations are dependent on the control center to operate. Other devices not controlled by the control center will fail based on the failure of these four components. Multiple papers consider this assumption ([13], [30]) because power stations are required to send and receive control packets to/from the control center. Based on the IEC 61850 standards [31], the sampled values from a substation should be measured and sent to the controller with different delays. For example, protection packets are critical and should be sent to the control center with a delay of fewer than three milliseconds [31]. These measured values are used in the control center to calculate values like active and reactive power. Without a control center, there is no central controller to determine the station's operational parameters. As a result, the power station fails.

b: COMMUNICATION

We assume that all power nodes depend on relay nodes to connect to the communication network and to communicate with the control centers. Relay nodes transmit control messages to the power nodes. This is a physical dependency, and if we are to assume that the power node is functional, then there should be a connection between the power node and a relay node. The power node's measured data should be sent to the control center for further decisions. In addition, this power node should receive control commands that specify its next condition. These packets need to be sent through the communication network. Therefore, there should be a physical link between each power component and communication network.

c: 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 its power supply. This assumption is based on two IEEE standards C37.115 [32] and IEEE 1615 [33], which show that each power component should be connected to the utility WAN and the control center through a connecting point (a relay node). The abstract presentation of this dependency can be seen in Figure 2. According to the figure, there is a mutual interdependency between the power components and the relay nodes.

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

C. GENERATING THE SYSTEM

We now describe how we generate test systems and couple power and communication networks. As previously mentioned, these networks are represented by the two different graphs shown in Figure 2. We use Python and the Networkx [34] library to develop our simulator and test our experimental results. We also use Pandapower [35] (an open-source library on Python) to implement a power system and analyze the power flow in our framework. To generate the system, we use Pandapower to implement different IEEE bus models. Then we convert these models to graphs and use Networkx to study the cascade of failures. The communication network consists of both relay and control center nodes. One relay node is responsible for supporting each power node for communication; that is, each power element is connected to the WAN by a relay node. This assumption is based on IEEE standards [32] that are references for the design of power systems. This helps us create a more practical model.

We use the $k - n$ model [13] to connect the control centers to the power nodes. This model is flexible because we can generate different network models and dependencies concerning different values of k and n. For instance, if we choose $k = 1$, and n is selected in a way that there is a certain number of control centers in the system, each power component is controlled by one control center, and each region is monitored by one control center.

The $k-n$ model is an appropriate way to connect the power and communication networks because it can simulate local and distributed control in the power system. Modern power systems facilitate distributed power generation, renewable energy resources, and fast varying demand response management that can be implemented using distributed control mechanisms [36], [37]. Furthermore, local control centers are widely used in current power networks to provide a reliable power supply. For example, New England's power system uses six sub-regional control centers to perform critical functions [38].

Algorithm 1 describes how this happens. With predefined values for k and n, the algorithm chooses the n power nodes that are nearest to each control center with a greedy paradigm and makes a logical connection or interdependency between them (*Control interdependency*). As the location of each power component is identified in the IEEE test cases, this algorithm can be executed to create the control connections in the system.

First, Algorithm 1 chooses one control center; for example, C_x to make logical connections. The algorithm makes a connection between C_x and the nearest power node with a control connection less than k; that is, node P_y. Then the algorithm searches among the neighbors of P_y. If there is a node such as P_z whose control connections are less than k, then the algorithm makes a connection between C_x and P_z. Otherwise, if it cannot find any node, it repeats the search process for P_z's neighbors. The algorithm is repeated for all control centers until there are exactly n logical connections to the power nodes.

Algorithm 1 Connecting Control Centers and Power Nodes

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

All power nodes in the small-cluster model have the same role, and as a result, the model defines general interdependencies based on this. Thus, the model cannot consider the power characteristics of its elements in the failure propagation process. The power network is constructed using synthetic models and is not similar to real networks. Also, the model identifies functional clusters based on the number of nodes, and clusters with no power generation may be considered functional in the small-cluster model. In contrast, we assign different roles to power components that make the RFP more flexible. We define realistic rules which identify functional nodes and clusters. We also analyze power flow to identify and remove transmission lines that exceed heating capacity. Using IEEE standard bus systems, we model the system accurately.

IV. CYBER-ATTACKS AND THE FAILURE PROPAGATION PROCESS

In this section, we discuss the attack model and the types of attacks the RFP model can address. Then we use this model to investigate the failure propagation that is caused by cyber-attacks.

A. THE ROOTS OF CYBER-ATTACKS

A cyber attacker can compromise a smart grid by attacking its power or communication networks. Malicious agents can use a grid's communication system to access its power components and measurement units and change its data or gain information about the system. This paper studies the impact of two types of attacks to build the attack model we use to simulate the failure propagation process that leads to cascading failures. According to [39] and [40], the most common cyber-attacks on smart grid networks are denial of

service (DoS), replay, spoofing, false data injection (FDI), topology, and switching attacks. In this paper, we focus on DoS and FDI attacks because these are common cyber-attacks on smart grid networks and they have the most-devastating impacts on these systems' functionalities [41].

1) FALSE DATA INJECTION

In an FDI attack, sensor or meter data can be used to inject malicious data into a system in order to mislead its operational processes [42]. Attackers can manipulate data through physical attacks or by using a system's communication network to access its measured data. These attacks can cause cascading failures in smart grid networks [43]. One of the impacts of this kind of attack could be load redistribution in a power network [44].

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 power components' measured data and to overload its components. In this paper, we consider an overload attack on a smart grid's power components. In this attack, a malicious agent falsifies the electrical components' loaded power so that it reads as producing more power than than its actual capacity. This overloads these components, which means they should be tripped. The RFP model consists of four types of power components: loads, generators, buses, and transformers. When a load component overloads, load-shedding techniques are used to shed the load from the system. When a generator overloads, it works at overcapacity and this causes circuit breakers to trip, which then causes a generator outage. Buses and transformers are supported by overcurrent protection devices that will trip them when the flow exceeds the line's threshold [43]. We suppose that when a component fails, it is inoperable and should be removed from the simulation.

2) DENIAL OF SERVICE ATTACKS

DoS attacks affect communication networks by rendering their communication nodes dysfunctional. Here, the attacker tries to degrade a network's functionality by sending useless packets through its communication network [45]. As the power grid uses public networks such as IP, an attacker can manipulate a network component to compromise the system.

Sensors send measurement data to the grid's state estimators via its communication network. When the communication network is affected by a DoS attack, the system's measured data can neither be sent nor received. This blocks the communication between the sensors and the state estimators [46]; i.e., its remote transmission measurement data is blocked and lost. We assume that DoS attacks affect measurement channels and that these attacks will be continuous. We also assume that when the measurement is lost, it cannot be generated using a recently received measured signal. The lack of a control signal will lead the control center to consider that the power component has failed. These types of attacks can be detected in the control center [45].

B. FAILURE PROPAGATION PROCESS

After generating the system and initializing the network parameters, the next step is to propagate failures that are caused by an initial attack or failure. Figure 4 shows the failure propagation process used in our RFP model. The first step is to choose which nodes in the communication or power networks will be subjected to the initial attacks. The selection of these nodes depends on the attack strategy and this will be explained in the next section. The nodes that fail, due to these initial attacks, become disabled and therefore cannot participate in the simulation. After removing these 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 we previously defined.

Edges that are directly connected to these nodes should also be removed from the system, including intra- and inter-network edges. As edges represent dependencies between different components in the system, a failing component causes an edge to be removed from the system. By removing these edges, corresponding nodes will lack the interconnections we previously defined.

If a power node is not connected to at least one control center (logical connection) and relay node (physical connection), then it should be considered non-functional. This means that for every power node, such as u, there should be two edges, such as d_{uv} and d_{uw} in the $d_{inter\text{-}system}$, such 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 no power node to support its power supply.

In the next step, an algorithm identifies nodes that belong to a cluster with a size less than Δ. The parameter Δ is a predefined variable that indicates the size of the 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 sizes are each smaller than the giant cluster) are formed. We assume that a cluster with a size greater than Δ and that contains at least one generator is functional in the RFP model. This assumption makes the RFP more realistic because if a cluster lacks a generator, then power cannot be generated, and transmission lines will have no power to transmit. Based on [13], we consider that the nodes that belong to the giant cluster and the small clusters are functional. The non-functional nodes in the power and communication networks have been identified and removed from the system (Figure 4).

Subsequently, the RFP model performs a power flow analysis to identify the transmission lines that exceed their capacity. Removing particular components from the power network causes the system's power flow to be redistributed. This redistribution can cause transmission lines to exceed their power capacity. Using power flow analysis, we identify these transmission lines and remove them from the system because they have become overheated. The process of removing nodes or lines from the system is repeated until there are no more failures (Figure 4). When the failure

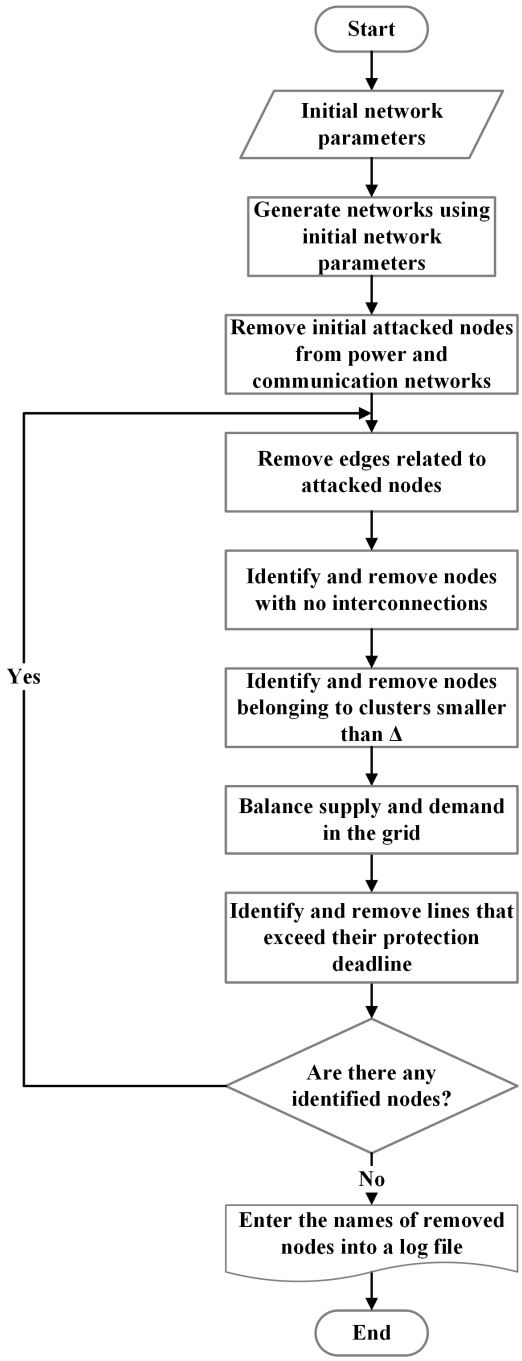

FIGURE 4. Failure propagation process of the RFP model. An iteration is repeated after generating and coupling two networks until the propagation stops.

propagation ends, the names of the failed nodes and edges are stored in a log file. This file will be helpful for further analysis of the steps involved in the failure propagation.

The failure propagation process is based on the interdependencies and rules we defined in the previous section; it provides a realistic model of cascading failures in smart grids. As a result, we find that our RFP model produces more-realistic results, based on our defined assumptions for the failure propagation process.

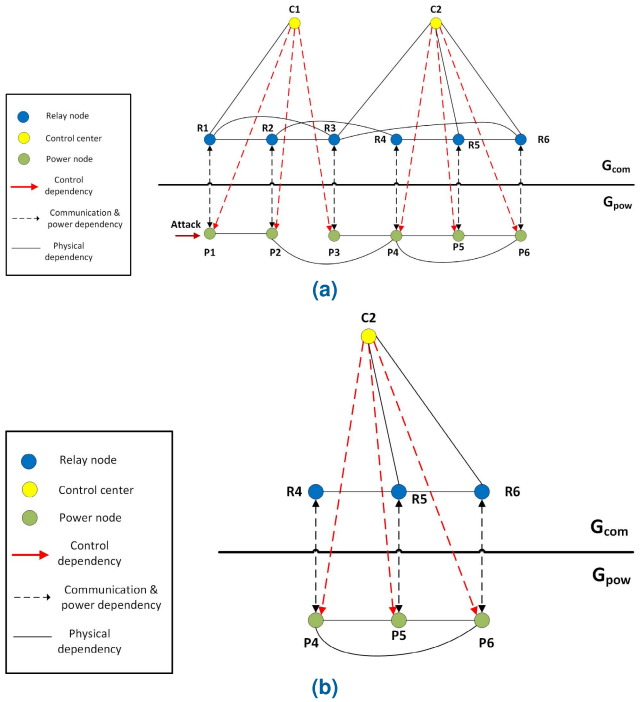

FIGURE 5. An example of failure propagation process. There are 6 power nodes, 2 control centers, and 6 relay nodes in the system. In this example, $k = 1$, $n = 3$, and $\Delta = 3$.

Figure 5a shows an example of a coupled network with six power components, six relay nodes, and two control centers. We explain the failure propagation steps using this figure. Suppose that P_1 is attacked and fails. All edges connected to P_1 are removed from the network. Accordingly, R_1 fails because of the power dependency. In the next step, C_1 fails because it is connected to the communication network through R_1. As a result, P_2 and P_3 fail because of the lack of control connection. Then, R_2 and R_3 fail because they are dependent to P_2 and P_3 for power supply. The failure propagation stops because there is no other failure. The system's final state is shown in Figure 5b.

V. EXPERIMENTAL RESULTS AND ANALYSIS

We evaluate the RFP model under different attack scenarios and compare the results with the small-cluster model [13]. We build the power and communication networks in the small-cluster model using the Barabasi-Albert model [47]. For the power network, we use 14-, 39-, 118-, 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 amount to 34, 80, 283 and 689 nodes for the IEEE 14-, 39-, 118-, and 300-bus systems, respectively.

The RFP is capable of modeling more-complex systems. To generate our communication network, we use the Barabasi-Albert model [47] to connect the communication nodes. The number of nodes in the communication network for the IEEE 14-, 39-, 118-, and 300-bus systems are 55, 133, 469, and 1,148, respectively. We couple the two networks and generate the smart grid system using our approach in

section III. In all of our simulations, the values of the parameters are $n = 3, k = 2$, and $\Delta = 3$. The value of n and k is chosen based on the small-cluster model [13] 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 we average the final functional nodes to achieve more accurate results. Data of the simulation is available on GitHub [48].

The threshold Δ is the minimum number of nodes that, if they are connected, we consider the group of these nodes a functional cluster. The physical meaning is that each cluster is a unit that can generate and transfer power to customers. We choose Δ based on the rules that we define for the functionality of a cluster. There should be at least one generator, bus, and a load at each cluster that considers it functional. Therefore, the minimum value for Δ is three.

We test the RFP model under two different attack scenarios, namely random and targeted attacks. We study these scenarios to identify the most-devastating attacks. First, we inject simultaneous attacks into the system based on the attack scenario. Then we run the failure propagation process and show the components of the power and communication networks that have failed. We repeat this process 100 times for each initial attack size, and we obtain the average of the functional nodes.

A. RANDOM ATTACKS

In the first attack, we randomly select the power and communication nodes and calculate the percentage of functional nodes after the initial failure propagation. Figure 6 shows the percentage of functional nodes versus the number of attacked nodes for different IEEE bus systems. We see that in the IEEE 39-bus system, when approximately 23 percent of the nodes initially fail, the whole system may collapse. More than 30 percent of the nodes fail for other test cases (31 percent for the 14-bus, 39 percent for the 118-bus, and 33 percent for the 300-bus test cases). We observe these results because the number of transmission lines compared to the number of nodes for the IEEE 39-bus system is less than those in the other test cases. Therefore, the IEEE 39-bus test case becomes fragmented faster than the other test systems.

We simulate the small-cluster model [13] with the same number of power and communication nodes and use the Barabasi-Albert model [47] to generate the two networks. The simulation results can be seen in Figure 7. The number of communication and power nodes in the small-cluster model in the figure are similar to those in the IEEE 118- and 300-bus systems, respectively. This means that the number of power nodes for the small-cluster model is 283 and 689, respectively (752 and 1,837, respectively, for all nodes in the system). The RFP 283 and 689 nodes are IEEE 118- and 300-bus systems, respectively.

We can see that the system fails faster in the small-cluster model compared to the RFP model. This is mainly because the small-cluster model assumes general interdependencies, regardless of each node's role, and unnecessary assumptions are made that cause dramatic consequences in some cases.

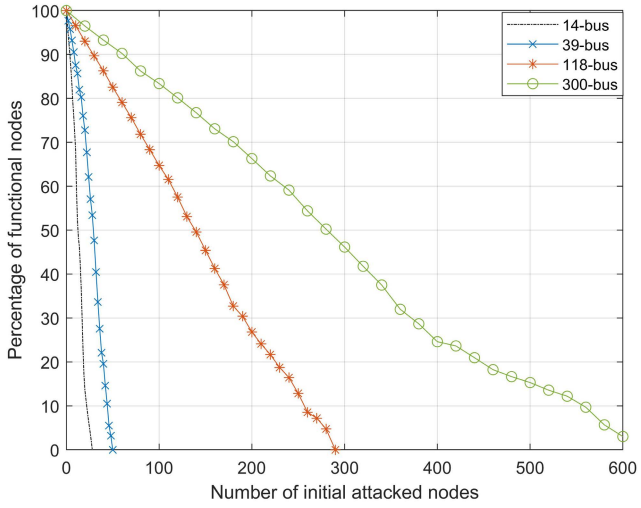

FIGURE 6. Percentage of functional nodes based on the initially attacked nodes in IEEE 14-, 39-, 118, and 300-bus test cases. Initial nodes are chosen randomly, and for each attack size, the number of simulations is 100.

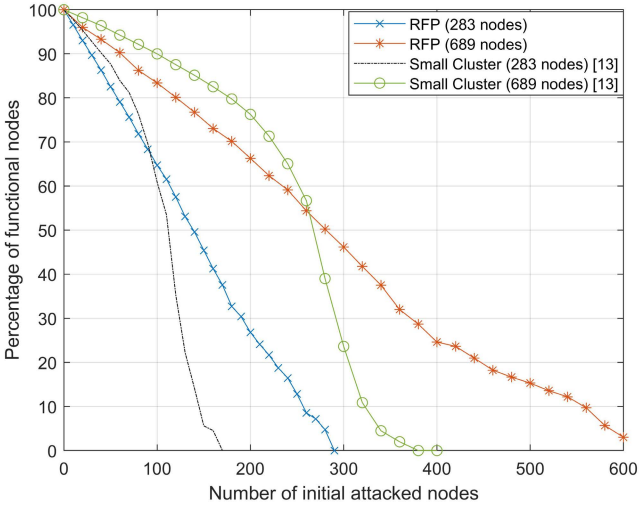

FIGURE 7. Percentage of functional nodes based on the nodes initially attacked in the RFP and Small-Cluster models. The first two cases are the results of the RFP model for 118- and 300-bus test cases. The other two cases are the same network with the same number of nodes for the small-cluster model.

The small-cluster model assumes that all communication nodes are dependent on one power node. As this model does not define any role for its power components, it uses general dependency for this purpose. However, we restrict this dependency to the relay nodes, but this is only based on IEEE standards.

We compare the results for random attacks with [18]. We chose this work because it proposed a model to simulate failure propagation in the power grid based on the dependencies between the power and communication networks and studied the impact of the communication network on the cascading failures. The paper assumed random failures to evaluate the performance of the proposed algorithm. The authors in [18] proposed a model to analyze the dependency of the power system on the control network. The

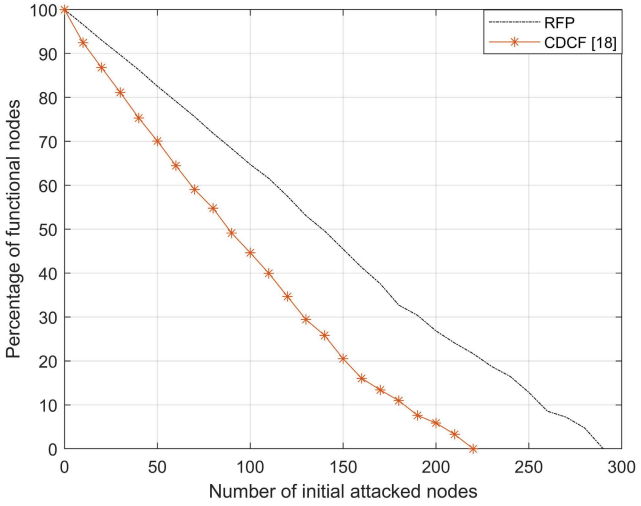

FIGURE 8. Percentage of functional nodes based on the initially attacked nodes in IEEE 118-bus test cases for RFP and CDCF [18] models.

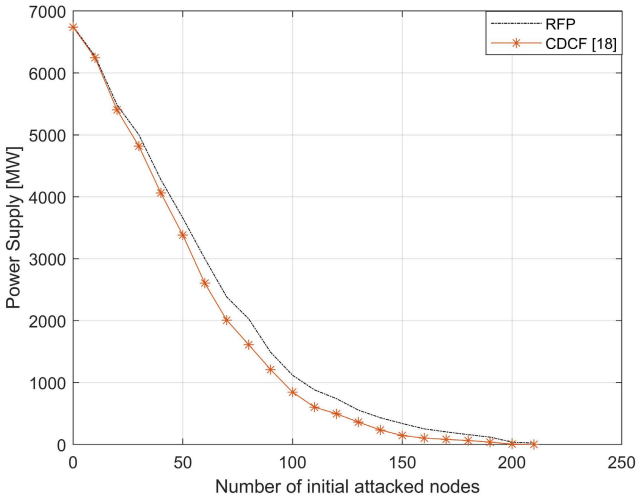

FIGURE 9. The power supplied for customers after failure propagation stops for RFP and CDCF models on an IEEE 118-bus system.

Communications-Dependent Cascading Failures (CDCF) model [18] employed a one-to-one dependency, meaning that each node in the power network depends on one communication node and vice versa. Thus, the number of nodes in the power and communication networks is the same. The CDCF model used IEEE standard bus systems to evaluate the proposed algorithm. The communication network followed the topology of the power network. We use the model presented in [18] to build the system and couple the power and communication networks and do not implement the control mechanism in that paper.

We simulate the RFP and CDCF models on the IEEE 118-bus system with the same number of power nodes. Figure 8 shows the percentage of functional nodes with a random attack strategy for the two models. The system degrades faster in the CDCF model compared to the RFP model because it considers a one-to-one interdependency, and there is no backup node to control and connect the power elements. We also consider the concept of small clusters to increase the robustness of our model with reasonable assumptions that provide better results than other models.

We are interested in comparing the amount of power supplied to customers after the failure propagation stops. Figure 9 shows the power supply for an IEEE 118-bus test case using the RFP and CDCF models. The results are achieved with an average of 100 simulations for each attack size. According to the figure, the power is not a linear function of the number of initially failed nodes. This functionality happens because when we increase the number of failed nodes to more than 30, important generators and load nodes fail, and the demand decreases dramatically. The difference between the two plots in Figure 9 is not big like Figure 8 because the PFA tries to balance generation and demand to provide a higher power supply.

B. TARGETED ATTACKS

We evaluate the RFP model using targeted attacks that can take place in real-world systems. We use the IEEE 300-bus system, as it contains more components and gives a better understanding of the system. The simulation results can be seen in Figure 10. We compare a random attack with inter- and intra-degree attacks. In inter-degree attacks, nodes having more interconnections to other nodes in a second network are more likely to be chosen in the initial attack. However, in an intra-degree attack, it is more probable that nodes with higher intra-degrees are under attack. A node's intra-degree is the number of edges that connect this node to other nodes in its network. From Figure 10, we can see that when the number of initial attacks is high, an intra-degree attack is more devastating compared to other attacks. This is because nodes' intra-degrees vary significantly compared to nodes' inter-degrees. As a result, when a node with a higher intra-degree is attacked, the impact of its failure is more devastating.

In Figure 11, we also compare the RFP with the small-cluster model under inter- and intra-degree attacks. The figure shows that the small-cluster model is also more vulnerable to intra-degree attacks [13].

C. EXAMPLES OF FAILURE PROPAGATION IN THE RFP MODEL

We use Figure 12 to explain the process of failure propagation in the RFP model and show how the outage propagates in two networks. This figure is constructed based on an IEEE 14-bus system. There are 14 buses, 11 loads, 5 generators, and 3 transformers in the figure, which comprises 33 power components. For each power element, there is a relay node that connects the element to the communication network. The values of other parameters are $n = 3$, $k = 1$, and $\Delta = 3$. The power graph (G_{pow}) components are connected based on the IEEE 14-bus standard system based on Figure 3b. Each power node is dependent on a relay node for communication and vice versa. Also, each control center is responsible for monitoring three power nodes ($n = 3$). Because there are too many edges in the figure, we only draw one control

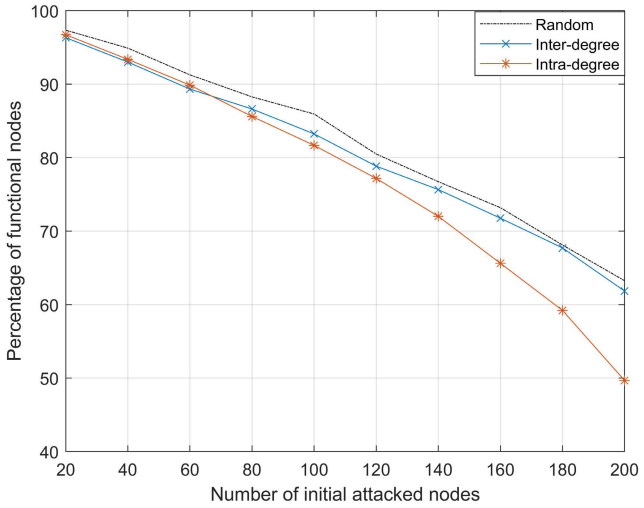

FIGURE 10. Comparison between random, inter-degree and intra-degree attacks on IEEE 300-bus system. For all simulations, the same parameters are applied.

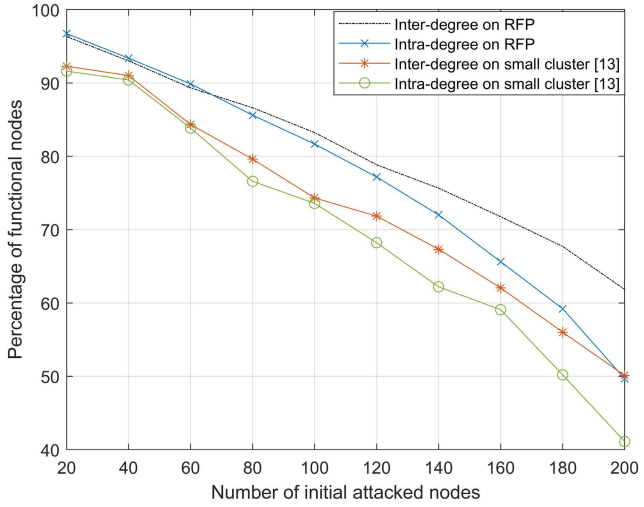

FIGURE 11. Inter- and intra-degree attacks on the RFP and the small-cluster models. All simulations are applied on the IEEE 300-bus system. The first two results are for inter- and intra-degree attacks on the RFP model, and the other two are for the small-cluster model with the same number of nodes and the same initial parameters.

connection between C_1 and B_1 and other control connections are hidden. Each control center monitors three power nodes starting from the left side of the figure, respectively.

We use an attack scenario to explain the RFP steps and show how the failure propagates between two networks. In this case, nodes in Set_1 initially fail as follows: $Set_1 = \{G_1, L_1, T_2, G_3, G_4, B_5, B_7, B_{11}, L_9, B_{13}\}$

After removing nodes in Set_1, connected relay nodes to these power components fail because of the power interdependency. The failed nodes are shown in Table 1. The nodes in the second step of the table are removed because they do not have a power supply from the power network. In step 3, nodes that belong to clusters with a size less than Δ are removed from the system. In the final step, B_1 fails because it is not connected to the communication network because of the failure of R_1.

TABLE 1. Scenario 1: Failed nodes at each step of failure propagation according to Figure 12.

Steps	Failed Nodes
1	$G_1, L_1, T_2, G_3, G_4, B_5, B_7, B_{11}, L_9, B_{13}$
2	$R_{15}, R_{16}, R_{32}, R_{19}, R_{23}, R_5, R_7, R_{11}, R_{28}, R_{13}$
3	$R_1, L_4, B_8, G_5, R_8, R_{24}, L_8, R_{27}, L_{10}, R_{29}, R_{21}$
4	B_1

When the failure propagation stops, a total of 32 nodes fail, which means that 58 percent of nodes are still functional in the example. According to Figure 6, the percentage of functional nodes for the IEEE 14-bus system with 10 initial attacked nodes is 60 percent. This shows that the percentage of functional nodes in the IEEE 14-bus system is similar to this example because we average 100 simulations for each attack size.

However, if nodes with special characteristics are chosen as initially attacked nodes, the result might be different. In the second example, we choose different nodes including: $Set_2 = \{B_4, B_6, G_3, G_5, T_3, L_2, \}$

The number of initially attacked nodes is 6, which is less than the first scenario. Table 2 shows failing nodes at each step. In step one, we remove initial nodes. Then, relay nodes that depend on these nodes fail in step 2 because of power dependency. In step 3, nodes without connection to the communication network fail. In steps 4, 5, and 6, we remove nodes that belong to clusters with a size less than three and nodes with no power supply. Step 7 is important because we remove all nodes in a cluster in the power network with no generator in this cluster. In the final step, nodes in the communication network with no power supply are removed, which causes the system collapses.

The result is unexpected because the system fails with 8 percent of initial failures. Based on Figure 6, the average percentage of attacked nodes for the IEEE 14-bus system to collapse is 31 percent which is entirely different from the results in this example. The difference between this example and the figure occurs because we choose initial nodes intelligently. Two initially failed nodes in the Set_2, including B_4 and B_6 have more intra-connections to other elements in the power system, and removing these nodes makes the system fragmented (Figure 3b). Removing node G_5 causes that there is no generator in the second cluster which fails this cluster. Nodes T_3, L_2, and G_3 play a vital role in the failure propagation because by removing these nodes, relay nodes in the communication network with a high number of intra-connection fail.

According to this example and as seen in Figure 6, we can conclude that the failure of nodes with unique characteristics causes the system to collapse more quickly. These characteristics are nodes with high intra-degree, generators far from other generators, power nodes that support relay nodes with high intra-degree, and interconnecting nodes like B_4 in the example. A similar trend is expected with larger bus systems. For example, as seen in Figures 6 and 7, the system fails when 39 and 33 percent of nodes in the IEEE 118- and

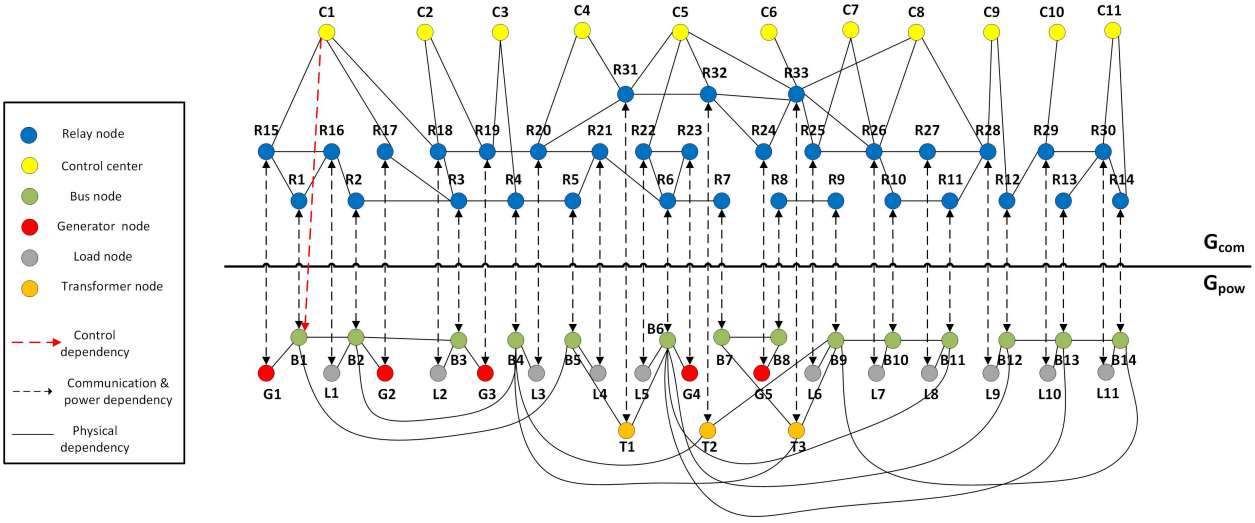

FIGURE 12. An example of the RFP model on an IEEE 14-bus test case. The figure includes 33 power components, 33 relay nodes, and 11 control centers.

TABLE 2. Scenario 2: Failed nodes at each step of failure propagation according to Figure 12.

Steps	Failed Nodes
1	$B_4, B_6, G_3, G_5, T_3, L_2$
2	$R_4, R_6, R_{19}, R_{24}, R_{33}, R_{18}$
3	$C_3, L_3, R_{20}, L_4, L_5, G_4, C_6, C_2$
4	$R_{21}, R_{22}, R_{23}, B_7, T_2, R_5, G_2, B_2$
5	$R_7, R_{32}, B_5, T_1, R_{17}, R_2$
6	$R_{31}, C_4, C_5, B_3, R_3, L_1, R_{16}, B_1, G_1, R_1, C_1, R_{15}$
7	$B_8, L_6, B_9, L_7, B_{10}, B_{11}, L_8, B_{12}, L_9, B_{13}, L_{10}, B_{14}, L_{11}$
8	$C_7, C_8, C_9, C_{10}, C_{11}, R_8, R_9, R_{10}, R_{11}, R_{12}, R_{13}, R_{14}, R_{25}, R_{26}, R_{27}, R_{28}, R_{29}, R_{30}$

300-bus systems initially fail, respectively. However, if we choose initial nodes intelligently with the abovementioned features, the system will collapse faster. This analysis helps us identify more vulnerable nodes that, by strengthening them, the system will be more robust.

VI. CASE STUDIES

In this section, we investigate four different case studies to evaluate the performance of the RFP model and study the failure propagation process. These case studies cover role- and location-based attacks, power flow analysis, and the impact of delay on failure propagation. We compare the results of the location-based case study with the small-cluster model. However, as the small-cluster model does not consider power characteristics and roles for power nodes, it is impossible to compare other case studies' results with this model.

We report the percentage of functional nodes to compare different case studies and the impact of different attack scenarios. Based on these results, we identify power nodes that are more vulnerable to cyber-attacks and the most devastating attack scenario (intra-degree attacks). We also can measure the model's accuracy in identifying failed nodes after failure propagation. Even by considering power-flow analysis (PFA), we prove that there is a negligible difference in the percentage of functional nodes after failure propagation with and without PFA. We also show that some characteristics of power nodes make them vulnerable to cyber-attacks, which are explained in section V.C. These results are achieved by comparing the percentage of functional nodes in different case studies.

A. CASE STUDY 1: ROLE-BASED ATTACKS

In this case study, we investigate the impact of attacking nodes based on the functionality of the system. Figure 13 shows the percentage of functional nodes after an attack on different components in our power network. We consider attacks on buses, loads, generators, and transformers. We cannot compare the results of this attack scenario with the small-cluster model because this model does not define any role for power nodes.

Each initial attack is an FDI attack on specific nodes in the IEEE 300-bus test case. In the case of more than 80 initial attacks, some components are missed in the figure because there are not enough components to run the simulation. For example, since there are only 69 generators in the IEEE 300-bus system, results are missing for the higher number of attacks. The figure clearly shows that attacks on bus nodes are more devastating than attacks on other components. This is because bus nodes are points of connection in the system. Therefore, this kind of attack causes more harm to the system compared to other attacks.

We simulate the same scenario in the communication network and the results can be seen in Figure 14. Attacks on relay nodes are a bit more detrimental compared to random attacks. However, the results of attacks on control centers are interesting. After about 50 percent of the control centers fail (i.e., after 200 initial attacks on the control centers), the

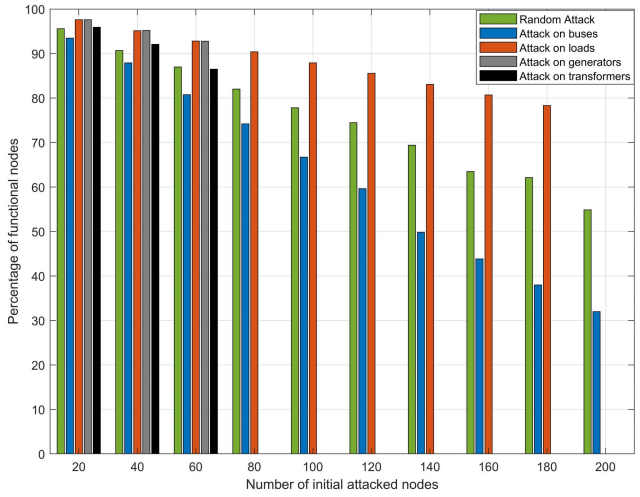

FIGURE 13. The impact of the role of nodes on the severity of an attack on the power network. Random attacks are applied on buses, loads, generators, and transformers in the IEEE 300-bus system.

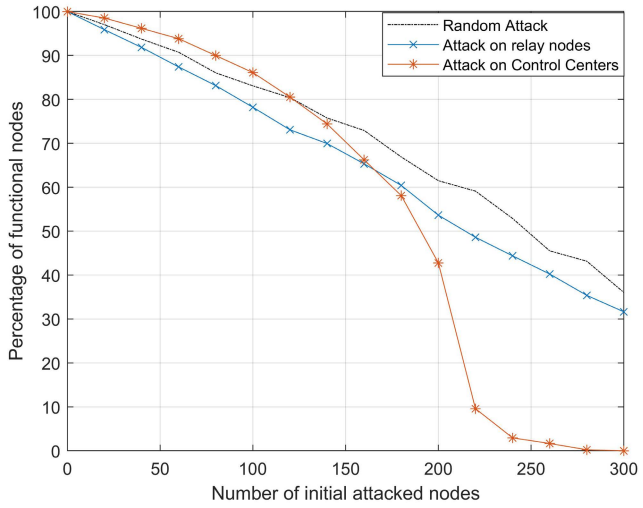

FIGURE 14. The impact of role of nodes on the severity of attack in the communication network. Random attacks are applied on relay and control center nodes and compared with the random attacks on all communication nodes. An IEEE 300-bus system is coupled with a communication network in all simulations.

percentage of functional nodes decreases dramatically. This happens because we use $k = 2$, which means that each power node is monitored by two control centers. When more than half of the control centers fail, the system starts to collapse, and the number of functional nodes declines considerably.

B. CASE STUDY 2: LOCATION OF ATTACKED NODES

In this case study, we investigate the impact of the location of the attacks on the failure propagation. As the IEEE test cases are designed based on actual power systems, the location of the failed nodes may affect the cascading failure.

To investigate how the attack locations affect the system, we can use partitioning methods. Different algorithms are used to partition the power network and study the failure propagation process. Newman's fast algorithm [49] is one of the first algorithms proposed in the literature to partition networks. This algorithm is based on topological community structures and is typically used in unweighted networks.

TABLE 3. Percentage of functional nodes in different partitions. The first two rows are the results of the Newman partitioning algorithm in the RFP model. The last two rows are for the same algorithm in the small-cluster model.

Number of initially attacked nodes	20	40	60	80	100
RFP Partition-1	97.89	96.09	95.61	91.41	87.32
RFP Partition-2	95.55	92.47	90.16	82.71	74.56
Small-Cluster Partition-1	96.84	94.18	90.42	86.28	84.87
Small-Cluster Partition-2	90.21	87.54	81.59	75.5	67.47

One implementation of the Newman algorithm on the IEEE 300-bus system divides the power network into two partitions. Since the sizes of the two partitions are neither equal nor balanced, random attacks on partition 2 are more devastating, as is shown in Table 3. We utilize the same algorithm to partition the small-cluster model. The method divides the small-cluster model into two partitions of different sizes. The percentage of functional nodes based on the number of initially failed nodes is shown in Table 3. Compared to the RFP model, the difference between the functional nodes in two partitions is higher because the small-cluster model uses the Barabasi-Albert method [47] to form the power network. In this method, some nodes have more connections than others and failing these nodes results in more devastating consequences.

We also use a modified version of the Newman algorithm proposed in [50], which we present in Figure 15. This method divides the power network into balanced partitions, using an optimal approach. Based on the results, the number of power nodes in partitions 1 to 3 are 98, 96, and 89, respectively. The simulation results are shown in Figure 16. Based on the results, the number of functional nodes after each partition's initial failure is almost the same. This happens because this method creates partitions of similar size and with the same electrical characteristics.

C. CASE STUDY 3: POWER FLOW ANALYSIS

Here, we investigate the impact of the power capacity of transmission lines in cascading failures, which we show in Figure 17. When a transmission line fails, the power flow is redistributed, and the flow in the remaining lines may increase. As each transmission line has a maximum capacity, the new power flow assigned to this line may exceed its capacity. As a result, these lines may heat up and become inoperable [18]. To identify these lines, we run a power flow analysis (PFA) after each iteration of the failure propagation, and we remove the identified lines from the power network. A PFA uses mathematical analysis to indicate the voltage and current of the power flow in each line and component in a power system. As we previously indicated, the last step of

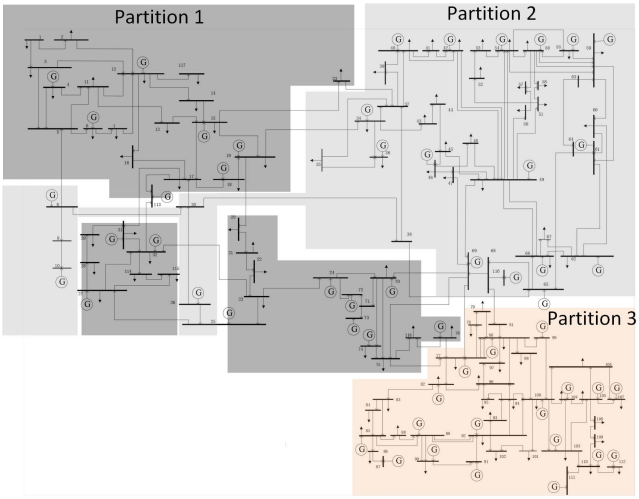

FIGURE 15. The partitioning result of IEEE 118-bus using a modified Newman algorithm [50].

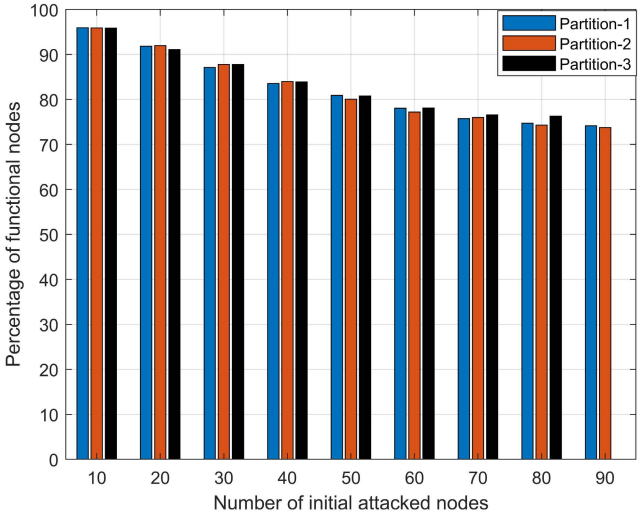

FIGURE 16. Simulation results of modified Newman algorithm in the IEEE 118-bus system. In each plot, the initial attacks are applied on only one partition.

the iteration in the RFP model shown in Figure 4 implements this analysis. In the first step, the graph of the power network is converted to a power system, using Pandapower [35], and then a power flow analysis is run to indicate the flow of each line.

The role of slack buses: Mathematical methods such as Newton-Raphson are used to solve power flow equations and find optimal solutions for the electrical characteristics of power grids, such as active and reactive power. These methods use a reference bus (i.e., a slack bus) to find solutions that can be used to balance active and reactive power. A slack bus is used to solve equations and absorb any uncertainties in the system. However, failure propagation may cause this bus to fail, and as a result, a PFA cannot be completed. To address this problem, a variety of algorithms have been proposed. One of the most commonly used methods is the distributed slack bus [51], which is a heuristic method that assigns system loss to generators. We assume there should be at least one functional generator in each cluster. Therefore, we can implement the distributed slack bus method in our RFP model.

In this paper, we do not implement a dynamic model. We also use a DC model for power analysis because it is commonly used as an approximated version of the AC model in such implementations. The DC and static models are used in multiple papers to identify overheated transmission lines [18], [52]. We use a static model because it can identify transmission lines that exceed their power capacity. We remove these lines from the system to assure that system works appropriately. By removing overheated transmission lines, new failures may occur in the system that propagates in the power and communication networks. The model is acceptably accurate because we study the condition of power nodes in a steady-state and identify failed nodes at each step of failure propagation.

Figure 17 shows the results of implementing PFA in an IEEE 118-bus system. We also implement PFA for an IEEE 300-bus system. We obtain the line capacity data for the IEEE 118-bus test case from [53] and for the 300-bus from [54]. The figure compares the percentages of functional nodes after a failure propagation that is due to initial attacks on the IEEE 118- and 300-bus systems, with and without a power flow analysis. When the number of nodes that fail after an initial attack is low, the system works to full capacity, and when power components fail, the number of failed lines is negligible. When we increase the number of nodes in the initial attack, the two graphs are the same.

According to Figure 17, the percentage of functional nodes is almost the same when the PFA is applied and when it is not. This is mainly because the RFP model accurately identifies the failed nodes and transmission lines even though we do not use the PFA. The model detects the lines that should be removed from the system; each step is shown on the flowchart in Figure 4. The results confirm that the RFP model can accurately model failure propagation.

In some cases, however, power flow analysis does not converge. This is mainly because the mismatches between the generators in the power system and the loads that occur when the generators' failures are higher than the loads. As the IEEE 300-bus system is more sensitive to power loss, this case happens more often than other IEEE test systems. Figure 17 shows that the percentage of functional nodes detected with and without PFA is approximately the same.

D. CASE STUDY 4: EFFECT OF LATENCY ON FAILURE PROPAGATION

In previous simulations, we considered the communication network ideal, where there was no communication delay. This means that all control packets are sent and received simultaneously. A more realistic assumption is that different packets from components are delivered with different latencies. In the real world, this happens because power components have different distances from control centers, and as a result, control messages are delivered with various delays. Here,

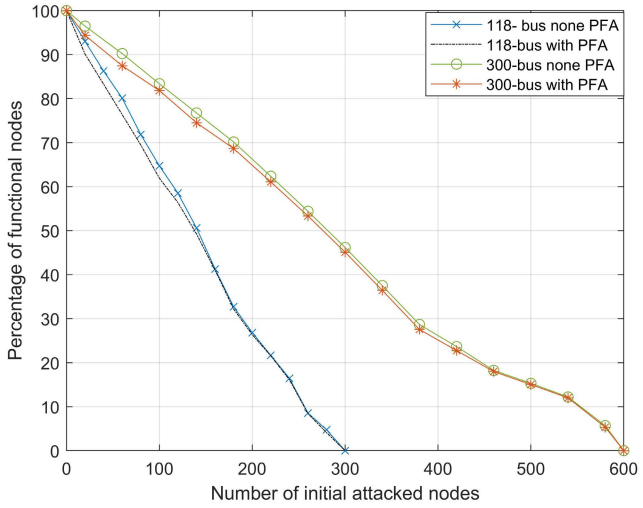

FIGURE 17. The impact of PFA on failure propagation process in the IEEE 118- and 300-bus test cases. The results are compared with and without applying the power flow analysis. As the RFP model identified the failed nodes accurately, there is a negligible difference when the PFA is used.

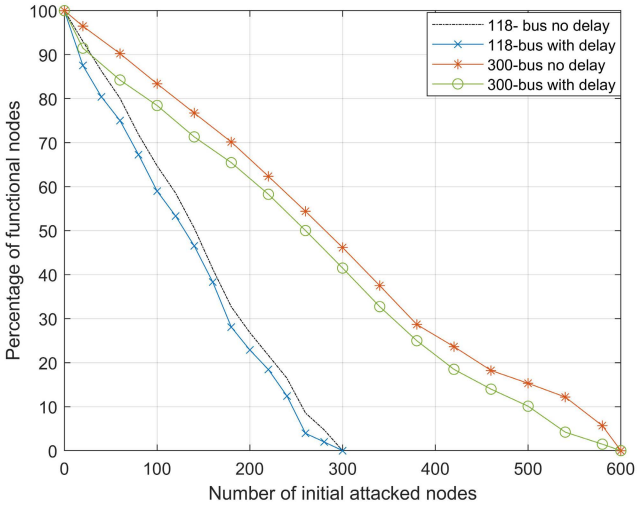

FIGURE 18. The impact of communication delay on failure propagation process in the IEEE 118- and 300-bus test cases. In all simulations the value of threshold $\delta = 100$ ms.

we study the impact of communication delay on the failure propagation process and cascading failures.

Whenever a power component receives a control packet, the related power of the element will change. This change modifies the power flow of transmission lines connected to the power element and other corresponding nodes. These power flow changes make transmission lines heat up and become non-functional [18]. When the power changes more frequently, the probability of heating transmission lines will increase. Consequently, more transmission lines exceed their power capacity. Therefore, a control mechanism is needed to reduce power modifications related to communication delay.

In general, we can model the delay of control packets as a random variable [55]. In our simulations, we define a time threshold δ for the delay of control packets. We employ a simple control algorithm. If the delay of a control message is less than δ, the power modification is applied, and the system is stable. Otherwise (delayed control message), the latest values of electric parameters of the transmission lines are used for evaluation. If the delay of control packets is higher than 2δ, the transmission line is considered a failed line. This delay makes particular transmission lines heat up and become dysfunctional. This delay happens because of cyber-attacks on the power network.

We consider ten percent of the control packets delivered after a defined threshold in our simulations. The delayed packets are chosen randomly. These packets can overload transmission lines and, therefore, cause more power components to be disconnected from the power network. The failure propagates to the communication system and affects the system's functionality. In each iteration of failure propagation shown in Figure 4, we randomly choose control packets with a delay higher than δ and apply the control mechanism we discussed.

Each control packet is sent from the control center to the power component and vice versa through the communication network. The physical meaning of δ is the time taken for control packets to be sent and received using the communication network. We set $\delta = 100$ ms in our simulations, which is a reasonable threshold for delay [18]. This threshold value provides enough time to make all control decisions.

Figure 18 shows the percentage of functional nodes in the IEEE 118- and 300-bus test systems regarding the different communication delays. It is clear that when we consider the delay of control messages, the number of functional nodes decreases. The difference between the ideal system (with no delay) and the system with delayed control packets is higher when the number of initially failed nodes is low. This happens because when more transmission lines participate in power flow analysis the system works to full capacity.

VII. CONCLUSION

In this paper, we proposed a novel realistic failure propagation model (RFP) for smart grid networks. Our model defined novel interdependencies and the role of nodes to study cascading failures. We also defined new rules based on IEEE standards for a smart grid to investigate failure propagation and cascading failures. The proposed RFP model addressed the heterogeneity of the cyber and physical components of the smart grid to model attacks on both power and communication networks. The RFP model considered the electrical parameters of such a system and analyzed power flows to identify overheated transmission lines. We also assumed different communication delays in the system and studied the impact of delayed control packets on the number of functional nodes. These assumptions provide a better understanding of failure propagation and make RFP more realistic. It also proves that without considering PFA, the RFP model works precisely. We compared the RFP model with the small-cluster model and evaluated it under different attack scenarios. We also presented four case studies to investigate our proposed model's performance and study the

effects of cascading failures on different scenarios. Based on the simulation results, we identify the most vulnerable components of the power system to cyber-attacks. This points to the need to strengthen these buses so smart grids' robustness will increase. We also showed that intra-degree attacks are more devastating than other attack scenarios. The results of the RFP model can be used to generate a data set for training an algorithm to predict failure propagation in the smart grid networks. We leave the study of the exact location of these systems' initial failures, using a dynamic model, and comprehensive analysis of different delays of control packets in the failure propagation to a future study that extends the RFP model.

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," *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," *IEEE Access*, vol. 8, pp. 151019–151064, 2020.

[3] M. Jalili and M. Perc, "Information cascades in complex networks," *J. Complex Netw.*, vol. 5, no. 5, pp. 665–693, Oct. 2017.

[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," *IEEE Trans. Power Del.*, vol. 36, no. 4, pp. 2264–2273, Aug. 2021.

[5] O. Boyaci, M. R. Narimani, K. R. Davis, M. Ismail, T. J. Overbye, and E. Serpedin, "Joint detection and localization of stealth false data injection attacks in smart grids using graph neural networks," *IEEE Trans. Smart Grid*, vol. 13, no. 1, pp. 807–819, Jan. 2022.

[6] *Cyber-Attack Against Ukrainian Critical Infrastructure*. Accessed: Dec. 22, 2021. [Online]. Available: https://www.cisa.gov/uscert/ics/alerts/IR-ALERT-H-16-056-01

[7] N. Sharma, A. Acharya, I. Jacob, S. Yamujala, V. Gupta, and R. Bhakar, "Major blackouts of the decade: Underlying causes, recommendations and arising challenges," in *Proc. 9th IEEE Int. Conf. Power Syst., Develop. Towards Inclusive Growth Sustain. Resilient Grid (ICPS)*, Dec. 2021, pp. 1–6.

[8] D. Liu, X. Zhang, and C. K. Tse, "A tutorial on modeling and analysis of cascading failure in future power grids," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 68, no. 1, pp. 49–55, Jan. 2021.

[9] P.-Y. Kong, "Optimal backup power deployment for communication network with interdependent power network," *IEEE Access*, vol. 10, pp. 17287–17299, 2022.

[10] D. Liu and C. K. Tse, "Cascading failure of cyber-coupled power systems considering interactions between attack and defense," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 66, no. 11, pp. 4323–4336, Nov. 2019.

[11] Y. Ji and J. Yuan, "Overhead transmission lines sag and voltage monitoring method based on electrostatic inverse calculation," *IEEE Trans. Instrum. Meas.*, vol. 71, pp. 1–12, 2022.

[12] L. Che, X. Liu, T. Ding, and Z. Li, "Revealing impacts of cyber attacks on power grids vulnerability to cascading failures," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 66, no. 6, pp. 1058–1062, Jun. 2019.

[13] Z. Huang, C. Wang, A. Nayak, and I. Stojmenovic, "Small cluster in cyber physical systems: Network topology, interdependence and cascading failures," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 8, pp. 2340–2351, Aug. 2015.

[14] Y. Cai, Y. Cao, Y. Li, T. Huang, and B. Zhou, "Cascading failure analysis considering interaction between power grids and communication networks," *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 530–538, Jan. 2016.

[15] L. Liu, H. Wu, L. Li, D. Shen, F. Qian, and J. Liu, "Cascading failure pattern identification in power systems based on sequential pattern mining," *IEEE Trans. Power Syst.*, vol. 36, no. 3, pp. 1856–1866, May 2021.

[16] G. Wu, M. Li, and Z. S. Li, "A stochastic modeling approach for cascading failures in cyberphysical power systems," *IEEE Syst. J.*, vol. 16, no. 1, pp. 723–734, Mar. 2022.

[17] M. Jusup, P. Holme, K. Kanazawa, M. Takayasu, I. Romic, Z. Wang, S. Gecek, T. Lipic, B. Podobnik, L. Wang, W. Luo, T. Klanjscek, J. Fan, S. Boccaletti, and M. Perc, "Social physics," *Phys. Rep.*, vol. 948, pp. 1–148, Feb. 2022.

[18] J. Cordova-Garcia, X. Wang, D. Xie, Y. Zhao, and L. Zuo, "Control of communications-dependent cascading failures in power grids," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5021–5031, Sep. 2019.

[19] C.-C. Sun, D. J. S. Cardenas, A. Hahn, and C.-C. Liu, "Intrusion detection for cybersecurity of smart meters," *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 612–622, Jan. 2021.

[20] F. Ünal, A. Almalaq, S. Ekici, and P. Glauner, "Big data-driven detection of false data injection attacks in smart meters," *IEEE Access*, vol. 9, pp. 144313–144326, 2021.

[21] T. N. Nguyen, B.-H. Liu, N. P. Nguyen, and J.-T. Chou, "Cyber security of smart grid: Attacks and defenses," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2020, pp. 1–6.

[22] D.-T. Peng, J. Dong, and Q. Peng, "Overloaded branch chains induced by false data injection attack in smart grid," *IEEE Signal Process. Lett.*, vol. 27, pp. 426–430, 2020.

[23] Q. Long, Z. Ma, F. Liu, S. Mei, and Y. Hou, "Analyzing patterns transference and mitigation of cascading failures with interaction graphs," in *Proc. IEEE PES Innov. Smart Grid Technol. Eur. (ISGT Europe)*, Oct. 2021, pp. 1–5.

[24] 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," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1293–1304, Apr. 2021.

[25] R. J. La, "Influence of clustering on cascading failures in interdependent systems," *IEEE Trans. Netw. Sci. Eng.*, vol. 6, no. 3, pp. 351–363, Jul. 2019.

[26] 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.

[27] Z. Huang, C. Wang, M. Stojmenovic, and A. Nayak, "Balancing system survivability and cost of smart grid via modeling cascading failures," *IEEE Trans. Emerg. Topics Comput.*, vol. 1, no. 1, pp. 45–56, Jun. 2013.

[28] Department of Electrical Engineering and University of Washington. *Power Systems Test Case Archive*. Accessed: Sep. 29, 2021. [Online]. Available: http://www.ee.washington.edu/research/pstca/

[29] *IEEE Guide for the Interoperability of Energy Storage Systems Integrated With the Electric Power Infrastructure*, IEEE Standard 2030.2-2015, 2015, pp. 1–138.

[30] Y. Chen, Y. Li, W. Li, X. Wu, Y. Cai, Y. Cao, and C. Rehtanz, "Cascading failure analysis of cyber physical power system with multiple interdependency and control threshold," *IEEE Access*, vol. 6, pp. 39353–39362, 2018.

[31] C. Brunner, "IEC 61850 for power system communication," in *Proc. IEEE/PES Transmiss. Distrib. Conf. Expo.*, Apr. 2008, pp. 1–6.

[32] *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*, IEEE Standard C37.115-2003, pp. 1–82, 2004.

[33] *IEEE Recommended Practice for Network Communication in Electric Power Substations*, IEEE Standard 1615-2019 (Revision IEEE Standard 1615-2007), 2019, pp. 1–140.

[34] A. A. Hagberg, D. A. Schult, and P. J. Swart, "Exploring network structure, dynamics, and function using networkx," in *Proc. 7th Python Sci. Conf.*, Pasadena, CA, USA, 2008, pp. 11–15.

[35] L. Thurner, A. Scheidler, F. Schäfer, J.-H. Menke, J. Dollichon, F. Meier, S. Meinecke, and M. Braun, "Pandapower—An open-source Python tool for convenient modeling, analysis, and optimization of electric power systems," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 6510–6521, Nov. 2018.

[36] S. Baros, A. Bernstein, and N. D. Hatziargyriou, "Distributed conditions for small-signal stability of power grids and local control design," *IEEE Trans. Power Syst.*, vol. 36, no. 3, pp. 2058–2067, May 2021.

[37] S. Baros and M. D. Ilic, "A consensus approach to real-time distributed control of energy storage systems in wind farms," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 613–625, Jan. 2019.

[38] *Operating the Power System*. Accessed: Jul. 8, 2022. [Online]. Available: https://www.iso-ne.com/about/what-we-do/three-roles/operating-grid

[39] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: A survey," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 1, no. 1, pp. 13–27, Dec. 2016.

[40] R. Deng, P. Zhuang, and H. Liang, "CCPA: Coordinated cyber-physical attacks and countermeasures in smart grid," *IEEE Trans. Smart Grid.*, vol. 8, no. 5, pp. 2420–2430, Sep. 2017.
[41] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using Kalman filter," *IEEE Trans. Control Netw. Syst.*, vol. 1, no. 4, pp. 370–379, Dec. 2014.
[42] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 13, pp. 1–33, May 2011.
[43] L. Che, X. Liu, Z. Shuai, Z. Li, and Y. Wen, "Cyber cascades screening considering the impacts of false data injection attacks," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 6545–6556, Nov. 2018.
[44] Y. Yuan, Z. Li, and K. Ren, "Quantitative analysis of load redistribution attacks in power systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1731–1738, Sep. 2012.
[45] F. Zhang, M. Mahler, and Q. Li, "Flooding attacks against secure time-critical communications in the power grid," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Oct. 2017, pp. 449–454.
[46] C. D. Persis and P. Tesi, "Input-to-state stabilizing control under denial-of-service," *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 2930–2944, Nov. 2015.
[47] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, no. 5439, pp. 509–512, Oct. 1999.
[48] *RFP 2022*. Accessed: Oct. 10, 2021. [Online]. Available: https://github.com/alisalehpour/RFP.git
[49] M. E. J. Newman, "Fast algorithm for detecting community structure in networks," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 69, no. 6, pp. 1–5, Jun. 2004.
[50] C. Zhao, J. Zhao, C. Wu, X. Wang, F. Xue, and S. Lu, "Power grid partitioning based on functional community structure," *IEEE Access*, vol. 7, pp. 152624–152634, 2019.
[51] K. Yamane, "New methods for load flow calculation without any swing bus," M.S. thesis, Massachusetts Inst. Technol., Cambridge, MA, USA, 1971.
[52] Y. Qiu, Q. Zhong, Y. Zhao, G. Wang, and L. Wang, "A method for analyzing the voltage deviation isolation performance with an application in two-stage high-frequency isolated AC-DC converters in LVDC systems," *CPSS Trans. Power Electron. Appl.*, vol. 6, no. 3, pp. 218–226, Sep. 2021.
[53] *IEEE 118-Bus System Data Sheet*. Accessed: Sep. 29, 2021. [Online]. Available: http://motor.ece.iit.edu/data/RSCUC%20/
[54] C. Coffrin, H. L. Hijazi, and P. Van Hentenryck, "The QC relaxation: A theoretical and computational study on optimal power flow," *IEEE Trans. Power Syst.*, vol. 31, no. 4, pp. 3008–3018, Jul. 2016.
[55] M. Wei, Z. Lu, and W. Wang, "Dominoes with communications: On characterizing the progress of cascading failures in smart grid," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2016, pp. 1–6.

ALIASGHAR SALEHPOUR (Student Member, IEEE) received the B.S. degree in computer engineering from Shahed University, in 2006, and the M.Sc. degree in computer engineering from the University of Tehran, Iran, in 2009. He is currently pursuing the Ph.D. degree in electronic systems engineering with the University of Regina, Regina, SK, Canada. His research interests include smart grids, machine learning, low-power design, computer networks, and artificial intelligence algorithms.

IRFAN AL-ANBAGI (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from the University of Ottawa, in October 2013. From 2013 to 2015, he worked as a Postdoctoral Fellow and a Product Development Manager of the "SecCharge" Project, University of Ottawa. He is currently an Associate Professor with the Faculty of Engineering and Applied Science, University of Regina. His research interests include security and reliability in networked systems, including quality of service (QoS), reliability, optimization and cybersecurity—specifically, modeling of failure propagation in networked cyber-physical systems; security and QoS in cloud-edge architectures; implementation of ambient intelligence in the Internet of Things (IoT) systems; and wireless sensor networks and their implementation in critical applications. He is registered as a Professional Engineer with the Association of Professional Engineers and Geoscientists of Saskatchewan (APEGS) and a Professional Engineers Ontario (PEO).

KIN-CHOONG YOW (Senior Member, IEEE) received the B.Eng. (Elect.) degree (Hons.) from the National University of Singapore, in 1993, and the Ph.D. degree from the University of Cambridge, U.K., in 1998. He joined the University of Regina, in September 2018, where he is currently a Professor with the Faculty of Engineering and Applied Science. Prior to joining the University of Regina, he was an Associate Professor with the Gwangju Institute of Science and Technology (GIST), Republic of Korea, from 2013 to 2018; a Professor with the Shenzhen Institutes of Advanced Technology (SIAT), China, from 2012 to 2013; and an Associate Professor with Nanyang Technological University (NTU), Singapore, from 1998 to 2013. From 1999 to 2005, he worked as the Sub-Dean for Computer Engineering with NTU, and worked as the Associate Dean for Admissions with NTU, from 2006 to 2008. He has published over 100 top quality international journals and conference papers. His research interests include artificial general intelligence and smart environments. Artificial general intelligence (AGI) is a higher form of machine intelligence (or artificial intelligence) where the intelligent agent (or machine) is able to successfully perform any intellectual task that a human being can. He is a member of the APEGS and ACM. He has served as a Reviewer for a number of premier journals and conferences, including the IEEE Wireless Communications and the IEEE Transactions on Education. He has been invited to give presentations at various scientific meetings and workshops, such as ACIRS, from 2018 to 2019; ICSPIC, in 2018; and ICATME, in 2021. He is the Editor-in-Chief of the *Journal of Advances in Information Technology* (JAIT).

XIAOLIN CHENG received the M.S. and Ph.D. degrees in computer science from the University of California at Davis, in 2007 and 2012, respectively. He has work experience in network system software development and data science applied in network performance evaluation and optimization. He was a Team Lead with Panasonic Beijing Laboratory developing DTV system software, from 2000 to 2003. He worked as a Software Engineer with Cisco on enterprise WLAN controller, from 2008 to 2011. From 2011 to 2016, he was with AT&T Labs to build up his experience in data science and machine learning. He is currently a Principal Data Scientist with Global AI Accelerator at Ericsson. He was a recipient of the Ericsson Top Performance Competition Award, in 2020.