1-2023

Data-Integrity Aware Stochastic Model for Cascading Failures in Power Grids

Rezoan Ahmed Shuvro
Marquette University

Pankaz Das
Marquette University

Jamir Shariar Jyoti
Marquette University

Joana Abreu
Eversource Energy

Majeed M. Hayat
Marquette University, majeed.hayat@marquette.edu

IEEE Transactions on Power Systems, Vol. 38, No. 1 (January 2023): 142-154. DOI.

Data-Integrity Aware Stochastic Model for Cascading Failures in Power Grids

Rezoan Ahmed Shuvro
Department of Electrical and Computer Engineering, Marquette University, Milwaukee, WI
Pankaz Das
Department of Electrical and Computer Engineering, Marquette University, Milwaukee, WI
Jamir Shariar Jyoti
Department of Electrical and Computer Engineering, Marquette University, Milwaukee, WI
Joana M. Abreu
Eversource Energy, Hartford, CT
Majeed M. Hayat
Department of Electrical and Computer Engineering, Marquette University, Milwaukee, WI

Abstract:

The reliable operation of power grids during cascading failures is heavily dependent on the interdependencies between the power grid components and the supporting communications and

control networks. Moreover, the system operators' expertise in dealing with cascading failures can play a pivotal role during contingencies. In this paper, a dynamical probabilistic model is developed based on Markov-chains, which captures the dynamics of cascading failures in the power grid. Specifically, a previously developed Markov-chain based model is extended to capture the trade-off between the benefits of having a robust communication infrastructure and its vulnerability from data integrity (e.g., cyber-attacks). State-space reduction of the complex interactions between power grids, communication networks and system operators is achieved by judiciously specifying the state variables of the Markov chain. The impact of system operators' probability of error during a cascade-mitigation action is incorporated into the model as a function of the state variables of the Markov chain. A point of diminishing returns is observed beyond which the effect of information infidelity outweighs the benefits of having more information. For a given level of cyber threat, an optimal size of a communication network is observed that minimizes the expected number of transmission-line failures before the cascade stops.

SECTION I. Introduction

The North-American power grid is one of the biggest connected physical networks consisting of three sub-units: the generating units, the transmission network, and the distribution units. Moreover, modern power grids are prime examples of complex interdependencies between the grid components and the associated communication and control networks. Synchronized operation between the grid layers (power grid and the communication network) and system operators is pivotal for the day-to-day operation of the grid. Due to the complex nature of the operation, power grids are prone to cascading failures, which may be initiated by small scale disturbances such as a limited number of failed lines and often lead to a partial or complete blackout of the grid [1], and [2]. Cascading failures start from failures of a small set of critical grid components such as transmission lines and generators [3]. This necessitates a load redistribution, upon which overloading of components may occur, which may result in additional failures, and so on. It is not a coincidence that all the top five blackouts in the world (in terms of customer sufferings) occurred in the last decade [4]. A wide range of triggers can initiate cascading failures. For example, historical triggers of cascading failures include but not limited to natural disasters, equipment failures, system operator error in decision making, and cyber-attacks [5], [6]. Due to the rapid advancement as well as enhancement of communication capability, and the distributed, information-centric nature of the grid, concerns over data integrity are increasing at an alarming rate [7], [8], [9].

Power grids are interdependent heterogeneous systems that leverage the advent of communication technologies to deliver energy to end customers reliably [10]. Power grids are prone to cyber-attacks leading to breach in confidentiality, integrity, availability, and accountability. Cyber attackers use malware to gain partial or full control of the target (e.g., grid operator, SCADA system, communication protocols such as Modbus, DNP3) and can initiate a wide range of attacks such as scanning attacks, denial of service (DOS), man-in-the-middle attacks, replay attacks, jamming channels, false overloading, altering the grid parameters (e.g., line tripping thresholds), manipulation of demand via IoT, time-delay-switching (TDS) attacks to name a few [7]. High wattage IoT devices that are connected to the power grid, such as air conditioners and refrigerators, can also lead to blackouts [11].

Fig. 1 sketches the various interdependencies among three layers (e.g., power grid, communication network and system operator) that exist in a power grid. The communication assets and increasing the system operators' effectiveness are pivotal to increasing the reliability of the grid. Clearly, there is a trade-off between increased dependence on informed decision making to enhance the grids reliability on the one hand, and exposure to cyber attacks on the other hand. Efforts in these fronts require balancing the trade-off between the grid's reliability enhancement and its resilience to data integrity, which is a vital scope of this paper.

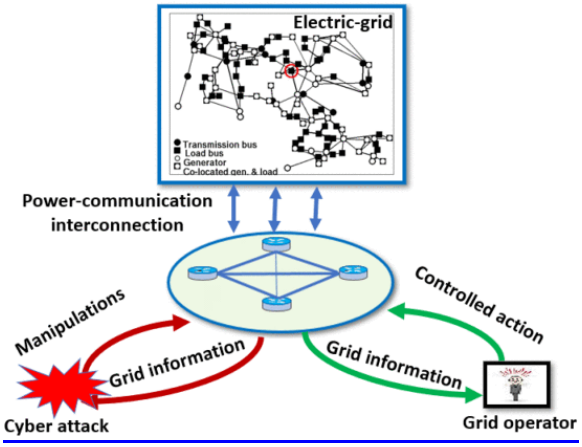


Fig. 1. Interdependencies among the power grid (e.g., IEEE 118 bus system), the communication network, cyber attackers and system operators.

In this paper, we generalize a previously developed cascading failure model [12] to an interdependent setting, which captures the benefits and risks of information through the communication network. Compared to existing Markov-chain based works [12]–[14], the original contributions of the new model, termed Interdependent-Stochastic Abstract State-space Evolution (ISASE), are as follows. First, the model explicitly includes a state variable that represents the dynamical state of cyberthreat in the grid and it extends the transition probability matrix to capture the new state transitions. Second, the model presents, for the first time to the best of our knowledge a novel mathematical representation of the interdependencies and dynamic interactions among data-integrity level, failures in transmission lines, and the performance of human operators. In particular, the load-shedding actions, which were assumed static in prior works, are extended to become dynamically dependent upon the level of data-integrity level, the interconnectivity between the power grid and the supporting communication network, and the human-operator performance. This new dynamic load-shedding formulation allows us to not only capture the benefits of having interconnectivity between the power grid, and the communication network but also capture the harm of having faulty information due to cyberthreat and system operator error. Third, the human-error probability is, too, dependent on the level of cyberthreat, which accounts for the possibility that the decisions of grid operators are adversely influenced by a security breach. One of the key benefits of the model beyond prior works is that it is capable of producing the probability distribution of the size of a blackout considering the potential harm from lack of data integrity and operator error. This, in turn, enables the formulation and solution of an optimization problem for finding the optimal level of interconnectivity that maximizes the benefits of information and minimizes the risk of a cascading failure induced by the interdependency.

The paper is organized as follows. We provide a review of the germane current literature in Section II. The analytical framework of the model is presented in Section III. We discuss the results in Section IV and conclude the paper in Section V.

SECTION II. Related Works

Modeling cascading failures in complex systems with special attention to cascades in power grids has gained significant attention in the research community in the last two decades. Efforts can be categorized mainly in three approaches: (i) network/graph-theoretic approaches (including complex-system theory) [15]–[19], (ii) power-system simulations [3], [20]–[24], and (iii) analytical probabilistic models [12], [25]–[29]. Since the behavior of cascading failures is stochastic, we are particularly interested in dynamical probabilistic approaches which use concepts such as Markov chains, branching processes, regeneration theory, and percolation theory to model cascading-failure dynamics. Models in this domain include detailed-grid focused [2], [12], [20], as well as interdependent models that include interdependencies between the power grid and the communication network [18], [21], [25], [26]. Various modeling efforts dealing with cascading-failure dynamics have been effectively summarized in [1], [5].

Since our work is focused on understanding the interdependency between the power-grid layers, we mainly review interdependent stochastic efforts here. A first kind of a model to investigate the interdependencies and interactions among two complex systems can be found in [22]. Buldyrev *et al.* used graph-based approaches to show the catastrophic effects of cascading failures where failures in one network can eventually create a ripple effect to collapse the entire interconnected network [18]. A two-phase control policy to mitigate the cascading failure in the power grid was proposed in [21]. Of particular relevance to this work is the work by Rahnamay *et al.*, who developed a Markov-chain based model using an equivalence-class approach that reduces the complex grid state-space into a reduced order and effectively predicts the probability distribution of blackout sizes [12]. In a subsequent work, the interdependence between two coupled network was modeled using individual Markov chains for each network and associated rules for coupling [26]. In contrast to the work reported in [18] and [26], which captures the negative impacts of interdependence, Hines *et al.* showed that interconnecting networks could enhance the reliability of the grid [25]. They analyzed the interdependency between the power grid and the associated communication network and reported that the optimal interdependence exists when the inter-connectivity is maximum [25]. This conclusion is plausible if the risk of faulty information is ignored. Brummit *et al.* reported that there exists an optimal interdependency in complex networks [17].

Developing cyber-physical systems security frameworks is an emerging field of study gaining a lot of traction. There have been a few preliminary works on modeling the effect of data integrity on smart grids and cyber-threat's interaction on the dynamics of cascading failures in the smart grid [7], [30]–[32]. A Markov decision process based model for intrusion and defense in competition for control of the substations is proposed in [33]. A security-oriented cyber-physical state estimation (SCPSE) system is presented in [34], which, at each time instant, identifies the compromised set of hosts in the cyber network and the maliciously modified set of measurements obtained from power system sensors. Authors in [35] developed a Dirichlet-based probabilistic model to detect opportunistic attackers. In [36], authors analyzed various network architectures and showed that implementing certain

architectures enhances substation network security. In [37], an intrusion detection system has been developed, by fusing Non-Nested Generalized Exemplars (NNGE) and State Extraction Method (STEM) to better understand cyber intrusions. Yamashita *et al.* analyzed the cyber related contingencies initiated from substations in [38]. Ding *et al.* surveyed the secure state estimation techniques under various performance indicators and defense strategies [39]. Impact of data attacks on state estimation were discussed in [40]–[42]. However, none of these works focus on the interdependence between the effect of cyber security on the other components on power grids and cascading failures.

The literature mentioned above analyzed the interdependence between the power grid and communication network, but all of them ignored to capture the benefits and harms of system operators' performance into the model. Also, they do not capture the benefit and harm of communication at the same time. For example, if the grid operators are inexperienced, stressed, or do not have the mitigation plans available to them, protecting the grid from cascading failures cannot be guaranteed due to the rapid escalating nature of cascading failures. In a recent article, human operators' role in the reliability of the power grid was embedded in a Markov-chain model for the grid [13]. The model uses human error probability calculation techniques from [43], which used the standardized plant analysis risk-human (SPAR-H) method [44]–[46] to calculate the human error probabilities based on grid operator interviews. However, to the best of our knowledge, no stochastic model has been developed that captures both the benefits and harms of interdependencies from power-grid, communication networks and system operators. In addition, no previous work optimizes the interdependency that maximizes the reliability of the grid by minimizing the probability of a cascade. The formulation of this optimization problem is the area of concentration of this paper.

SECTION III. I-SASE Model Framework

In this section, we will discuss the three layers of the power grid and our approach to integrate them in a Markov chain.

A. Preliminaries

Various physical attributes of the power grid collectively contribute to cascading failures. Such attributes include but not limited to power generation and load, power-flow distribution using transmission network, voltage and phases of transmission lines, system protection schemes, load dispatch capabilities, and cyber-security protection schemes. To develop a scalable and analytically tractable model for the grid with such a detailed state-space requires enormous computational resources, which may not be feasible. Dimensionality reduction techniques based on machine learning such as principal component analysis can be effective here with the cost of losing the detailed state-space information. To solve this problem analytically, Rahnamay *et al.* introduced an equivalence-class concept for state-space reduction and developed the Markov-chain based SASE model [12]. The detailed flow diagram of the cascading failure simulation using Matpower is presented in Fig. 2. The model was developed using DC power flow approximation. The detailed spate-space of the power grid is partitioned into equivalence classes using a selected set of state variables. The state variables, which are significantly correlated to cascading failures, are chosen through extensive analysis using simulation of cascading failures. Such a coarse partitioning of the state-space renders a reduced state-space with a handful of aggregate state variables (termed as abstract state, S). Members of each equivalence class are detailed states that are deemed indistinguishable as far as the cascading

behaviour is concerned. To model the cascading behavior in a Markov-chain model, Rahnamay *et al.* used the number of transmission-line failures, F, the maximum capacity of the failed lines, C^{max}, and a binary variable, I, indicating a cascading or an absorbing mode during the cascade evolution. Specifically, the variable, I, depends on the dynamics of the grid. Namely, $I = 0$ represents a cascade-continue mode, and $I = 1$ represents a cascade-stop mode. Hence, the reduced state of the power grid [12] is represented by $S = (F, C^{max}, I)$ and the dynamics of the cascading failures using the state variables were modeled using a Markov chain over the reduced state space. The state transitions of the Markov chain were extracted using full state-variable Monte-Carlo simulations of the power grid. The authors considered one failure transitions in the Markov chain, i.e., the overall duration of the cascading failures is divided in such a short time ΔT such that only one failure is allowed. Since the transition probabilities were estimated from full-scale simulations of the power grid, they implicitly capture the role of the omitted variables of the Markov chain. In addition, the state-dependent transition probabilities were fitted to a parametric equation that involved the three operating parameters of the grid, which are (1) the ratio between the load and the maximum generation in the grid, r; (2) the uncertainty in the flow of information, e.g., the error in estimating the power flow in transmission lines (capacity-estimation error), e; and (3) the constraint over implementing load shedding in the grid, θ. More specifically, for an equivalence class with $I = 1$, formulation for a parametric cascade-stop probability, P_{stop}, was introduced. In particular, $P_{stop}(S_i)$, was formulated using a linear combination of the state variables F_i and C_i^{max} [12]:

$$P_{stop}(S_i) = wP_{stop}^{(1)}(F_i) + (1 - w)P_{stop}^{(2)}(C_i^{max}). \quad (1)$$

Here $P_{stop}^{(1)}(F_i)$ is the probability that the cascade stops when the number of failures is F_i. From [12] we know that $P_{stop}^{(1)}(F_i)$ has a bowl-shape pattern and $P_{stop}^{(2)}(C_i^{max})$, which is the probability that the cascade stops when the maximum capacity of the failed lines is C_i^{max}, has an exponentially decreasing pattern that is high (low) when the maximum capacity of the failed transmission line is low (high). Parametric formulation of $P_{stop}^{(1)}(F_i)$ and $P_{stop}^{(2)}(C_i^{max})$ has been done in [12] based on extensive simulations of the power grid. In particular, three power-grid operating parameters were fitted using the same simulations described above to characterize the transition probabilities of the Markov chain [12].

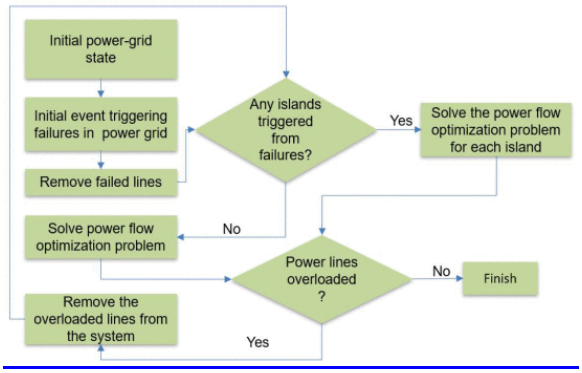


Fig. 2. Flow chart of the simulation framework

Later, Wang *et al.* extended the SASE model to include the effect of system operators' error on the reliability of the power grid [13] called h-SASE (human- SASE). This was done by introducing operators' response level as a state variable in the Markov chain. Specifically, the h-SASE model [13] used four distinct operators' response levels and quantified human-error probability for every grid state during cascading failures.

In the next subsection, we extend the capability of the h-SASE model to include the effect of data integrity, which is one of the most challenging fronts in recent times to protect critical infrastructures like the power grid and introduce the I-SASE model. The I-SASE model captures the interdependencies between the three elements of grid, i.e., the power grid, the communication network and the human operators. The model further reduces the state space of the Markov chain (through mapping of the human error probability as a function of the state variables) and introduces data integrity as a new state variable. This extension of the Markov chain is critical to answering the following fundamental question: how can we balance the trade-off between grid's performance enhancement and robustness to information infidelity?

B. Development of the I-SASE Model

The ith state of the I-SASE model is defined using $S_i = (F_i, C_i^{max}, L_i, I_i)$, $i = 1,2, \dots, M$, where the size of the state-space becomes $M = |\mathcal{F}||\mathcal{C}||\mathcal{I}||\mathcal{L}|$, where $|\mathcal{F}|$, $|\mathcal{C}|$, and $|\mathcal{L}|$ is the number of the transmission lines, capacities, and data integrity levels, and $|\mathcal{I}| = 2$. Note that the level of human operator error will be mapped as a function of the state variables of the Markov chain. The ith index of a state S_i is equal to $2|\mathcal{C}||\mathcal{L}|(F_i - 1) + 2|\mathcal{L}|C_i^{index} + 2(L_i - 1) + I_i + 1$, where $F_i \in \{1,2, \cdots |\mathcal{F}|\}$, $C_i^{index} \in \{1,2, \cdots |\mathcal{C}|\}$, $L_i \in \{1,2, \cdots |\mathcal{L}|\}$ and $I_i \in \{0,1\}$. For example, in the IEEE 118-bus network, the total number of transmission lines, $|\mathcal{F}| = 186$, considering $|\mathcal{C}| = 5$ and $|\mathcal{L}| = 3$, there are 5,580 distinct states of the Markov chain and $S_1 = (1,1,1,0)$ is the first state of the Markov chain.

At this stage, we summarize the difference between our model with the previous model in [12]. First, in this model, we consider the dynamics of the system operator error and cyber threat for modeling the state transitions, which are not considered in [12]. Second, we consider a dynamic load-shedding parameter, θ_i in our model (discussed in the following subsection) as opposed to the fixed parameter introduced in [12]. In particular, the load-shedding constraint parameter is dependent on the state. Hence, our model can be considered as a generalization of the model in [12].

C. Influence of Data Integrity on the Reliability of the Power Grid

Clearly, increasing the power-communication inter-connectivity would increase communication capability to achieve better control of the grid. At the same time, such change will increase the risk of data integrity issues to the grid because of wider exposure. To capture this critical attribute of the grid associated with the cyber threats, we introduce a new state variable, L, which can represent the various levels of data integrity. Specifically, we consider three distinct data integrity levels, $\{\ell_1, \ell_2, \ell_3\}$, to capture the scenarios from low, medium and high risks of cyber threats. In real-world low cyber risk can be interpreted as a robustly secure network (e.g., military network) under normal operation and a high risk can be interpreted as a network exposed to significant cyber threat (e.g., internet) under normal operating conditions. For example, demand manipulation through IoT devices can be

considered as low cyber risk and malware attacks to gain control over SCADA systems can be considered as high cyber risk.

D. Effect of Interdependencies Among the Various Layers of the Power Grid

Interdependence between power grid and the associated communication network can lead to three scenarios contributing cascading failures: (1) effective handing of information can minimize cascading failures through taking appropriate actions, (2) increased communication capability also adds vulnerability to the grid in the form of data integrity and (3) the incorrect actions of the system operators dealing with cascading events can lead to further escalation of the event. In the following subsections, we describe the interactions among various layers of the power grid and model their influence on cascading failures.

1) Influence of Communication Networks on the Propagation of Cascading Failures

The grid information is conveyed to the control center through the communication network infrastructure. The topology of the grid and the communication network are not necessarily identical. However, power-grid nodes (i.e., substations) are equipped with communication facilities to send (receive) information (instructions). It is important to note that not all the grid nodes are connected to the communication networks. The SCADA, which is a computer system network that connects power and communication nodes using different communication mediums (e.g., fiber, microwave) use this interconnection to collect information of all the nodes of the grid [25].

Fig. 3 shows two examples of inter-connectivity between the power grid and communication network. From the control center, all the power grid nodes are accessible but through different interconnections. Hence, it is intuitive that during a cascading failure, the propagation of failures in the networks, depicted in Fig. 3, would be different. Power-grid system operators use the interconnections, which we denote by number of interconnections, N_{pc}, to send appropriate control actions for sensing, monitoring, and maintaining the stable health of the grid [25]. With this setting, we define maximum inter-connectivity when all the power-grid nodes (buses) have an associated interconnection, i.e., if the grid has N nodes, then there can be a maximum of N power-communication interconnections, denoted by N_{pc}^{max}. Intuitively, the maximum number of interconnections should maximize the availability of all the information to the system operators. However, in practice, due to constraints on communication infrastructure cost, $N_{pc} < N_{pc}^{max}$.

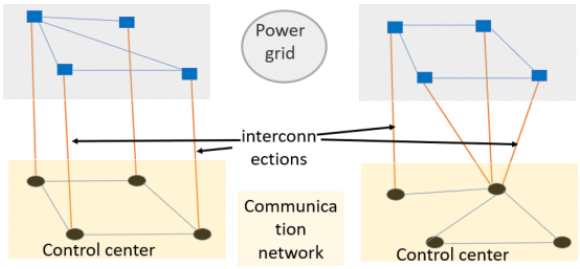


Fig. 3. Inter-connectivity between the power grid and the communication network in power grids.

We define the *level of power-communication inter-connectivity*, k, as the ratio between power-communication interconnections to the maximum number of interconnections, i.e., $k = \frac{N_{pc}}{N_{pc}^{max}}$, where a

higher value of k indicates a stronger inter-connectivity while a lower value of k indicates weaker inter-connectivity. Failure of interconnection is considered as loss of information. Later, we will show that k controls the dynamics of the Markov chain through its influence on the load-shedding constraint, θ_i, which, in turn, influences the probability-transition matrix of the Markov chain. In particular, we will show that there exists a power-communication interconnection level, k for which the effect of cascading failures is at a minimum. Most reported works consider a direct effect of failures in the communication network on the power grid during cascading events [25], [26]. In this paper, we assume that loss of information during cascading failures is initiated from power-node failures. Failures can be triggered for various reasons but can be categorized broadly in the following three categories: network equipment failures, natural disasters, and the human error [6]. Since cascading failures happen in a short duration in time, a communication-node failure due to a transmission-line (power-node) failure is highly unlikely, i.e., although the power-communication interconnection may go down, the intra-connectivity within the communication network is likely to remain unaffected by any incidents in the power grid. In contrast, note that transmission-line failures increase the probability of a power node (bus) failure, which, in turn, increases the likelihood of failures of power-communication interconnections, N_{pc}. For example, when all the transmission lines associated with a power grid node fail, we consider failure of the associated power-communication interconnection.

2) Influence of System Operators on the Reliability of Power Grids

From preventive maintenance to protective actions, system operators are actively involved in managing the health of the grid and mitigating any risk that can lead to an outage scenario. However, errors in the decision during contingencies by the system operators can lead to a larger blackout than usual. System operators have to deal with contingencies under time constraints, stress, and the complexity of the problem. Moreover, factors such as experience, work process, procedures, ergonomics, fitness can affect the capability of making an appropriate decision during contingencies. Following the work in [13], [43], we extend the Markov chain model in [47] to include a mapping between the operators' error probability and the grid states. The model obtained the human-error probability (HEP) as a function of operators' performance shaping factors (PSFs), and the grid operating conditions, such as available time, complexity, and human performance attributes, e.g., stress, training, and working environment, which are based on the SPAR-H method. Moreover, a mapping between grid states and operator response levels was established utilizing the empirical (calculated from real operator data) probability distribution of the PSFs [43]. Specifically, the mapping was established based on a histogram-equalization principle, assuming a monotone relationship between the HEP values and the number of line failures [47].

In this paper, we extend the mapping reported in [47] between the HEP values and grid states considering the newly added cyber threat level variable, L. For example, for the 118 bus network, without considering L, the cardinality of grid state-space were 1,860, which is now increased to 5,580 with the three levels of L. Three realizations (representing nominal, medium, and extreme PSF values from [43]) of the system operators' error probability against the indexes of the state are plotted in Fig. 4. Note that for nominal PSFs, the HEP is mostly zero as opposed to one for extreme along with the index of the state. For the medium PSFs, the HEP monotonically increases to unity with the state index. Note that a separate state variable was used for human factors in [13], which was a deterministic

function of the state variables. Further, [47] includes more PSFs (eight compared to two in [13]) and includes a histogram equalization process to eventually map HEP as a function of the state variables of the Markov chain. Hence, the human factor state variable is absorbed using the other variables, which ensures a significant reduction in the state-space of the Markov chain. In this paper, we assume that operators do have enough time to make decisions between state transitions during the cascading failure propagation. Ideally, operators will be able to trigger control actions (e.g., load shedding) between states to mitigate the risk of cascading failures. In practice, however, cascading failures happen extremely fast, and there would be cases when the operators' decisions cannot be implemented in between each state transition. This is one limitation of our model. However, our approach is an approximation to the real-world scenario when decisions are not implemented at every step. This delay in implementing action by operators can be addressed through taking actions after multiple state transitions, depending on the communication and processing delay of the SCADA system. Note that the HEP affects the transition probabilities of the Markov chain through the load shedding constraint, θ, as described in the next subsection.

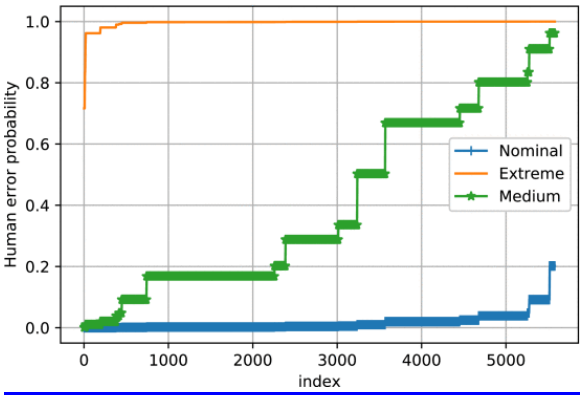


Fig. 4. Human error probability (HEP) mapped with state indexes of the Markov chain for various operators' PSFs.

3) Influence of Load Shedding Constraint on the Propagation of Cascading Failures

In [12] and [13], a fixed load-shedding constraint parameter, $\theta \in [0,1]$ was considered, which is the ratio of loads where load shedding is restricted and the total load of the grid. Intuitively, the constraint of load shedding is negatively correlated with the level of inter-connectivity, i.e., increasing the level of interconnectivity, k, increases the availability of information, which, in turn, reduces the constrain on load-shedding and hence lower θ. With power node failures, the corresponding interconnection is also broken, which increases θ. To capture this dynamical behavior, we generalize the fixed θ in [12] as described below.

We consider load-shedding constraint, θ, a dynamic parameter that depends on three components: the level of inter-connectivity (k), system operators' error probability (HEP(S_i)), and the number of line failures (F_i). Specifically, we define the *dynamic load shedding constraint*, θ_i for any state, S_i, as

$$\theta_i = \min\left(1, \mathrm{HEP}(S_i) + \left(1 - k + \frac{kqF_i}{N_{pc}^{max}}\right)\right),$$

(2)

where HEP(S_i) is the HEP for the state S_i, $q = \frac{V}{|\mathcal{F}|}$, where V is the number of nodes (buses). Note that under normal operation (no transmission-line failures and no human error probability), θ_i is inversely proportional to k, i.e., increasing the level of inter-connectivity decreases the constraint on load shedding. For example, for a scenario when $F_i = 0$ and HEP(S_i) $= 0$, if $k = 1$, then, from (2), $\theta_i = 0$, i.e., if the information is fully available then there is no constraint on load-shedding. During the propagation of cascading failures, θ_i increases as transmission line failure (through F_i) increase as well as due to increase in the level of human error probability (through HEP(S_i)) captured in (2). For example, when $F_i = |\mathcal{F}|$, then load-shedding constraint is at maximum irrespective of human operator error and interconnectivity. A simplified block diagram showing the interdependency among the power grid-layers as well as the proposed framework to model the cascading failures is shown in Fig. 5.

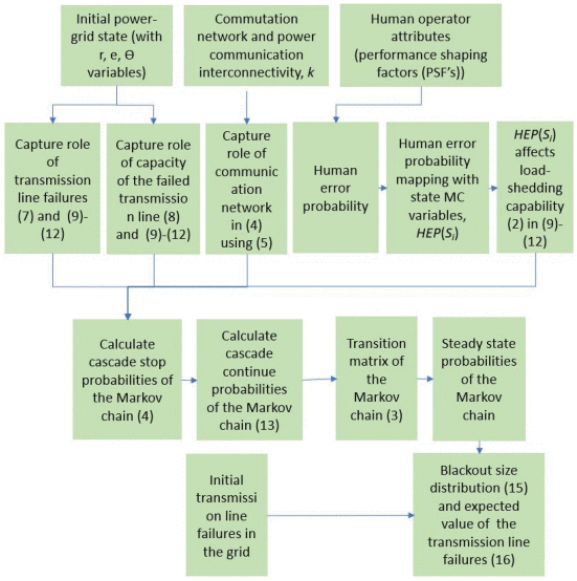


Fig. 5. Block diagram of the I-SASE model. Numbers in parentheses represent the relevant equations.

SECTION IV. Transition Probabilities of the I-SASE Markov Chain Model

The transition matrix of the I-SASE was developed following the approach in [12], [13]. The state-space of the Markov chain is a $2|\mathcal{F}||\mathcal{C}||\mathcal{L}| \times 2|\mathcal{F}||\mathcal{C}||\mathcal{L}|$ matrix. In the subsequent calculations we consider $|\mathcal{C}| = 5$ and $|\mathcal{L}| = 3$, i.e., five types of transmission line capacities and three levels of cyber threat (low, medium and high). In our model, we did not consider any restoration of the failed lines during the propagation of cascading failures, i.e., the number of failed lines is monotone until it reaches to an absorbing state. There are three types of transitions allowed in the Markov chain: from a transitory state to another transitory state with the same capacity, higher capacity, or an absorbing state. We show the various types of transitions of the Markov chain in Fig. 6. Here $P_{hc}(S_i)$ is the transition probability to a state with higher capacity, which will be formulated later. Recall that an absorbing state is a state of the Markov chain where the cascading failures end. For transitioning within the transitory states, we allow one additional line failure at the subsequent time-step, i.e., from F_i to $F_i + 1$, there are $|\mathcal{C}||\mathcal{L}|$ possible transitions within the Markov chain. Due to the monotone

assumption of the line failures, the transition matrix $\mathbb{P}$ is an upper diagonal matrix. The transition probability, $f(S_j|S_i)$ from state $S_i = (F_i, C_i^{max}, L_i, I_i)$ to state $S_i = (F_i, C_i^{max}, L_i, I_i)$, is given below:

$$f(S_j|S_i) = \begin{cases} 1 \text{if } F_j = F_i, C_j^{max} = C_i^{max}, L_j = L_i, \\ I_j = I_i = 1, \\ P_{stop}(S_i) \\ \text{if } F_j = F_i, C_j^{max} = C_i^{max}, L_j = L_i, \\ I_j = 1, I_i = 0, \\ P(S_j|S_i) \text{if } F_j = F_i + 1, C_j^{max} \in \mathcal{C}, \\ L_j \in \mathcal{L}, I_j = 0, \\ 0. \end{cases}$$

(3)

As described in III-A, $P_{stop}(S_i)$ and $P(S_j|S_i)$ represent the cascade-stop probability at state S_i and cascade continue probability to state S_j from S_i, respectively. In this paper these have an extended formulation that includes the effect of state variable L as described in the following section.

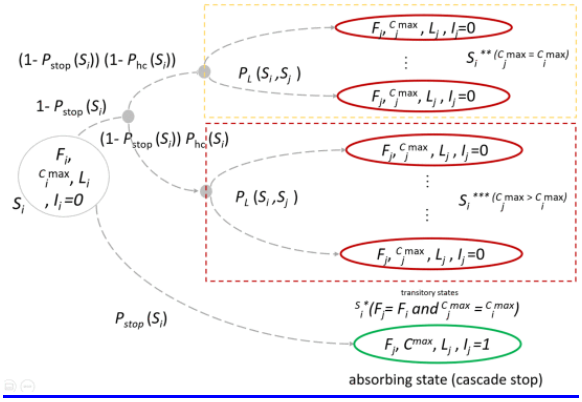


Fig. 6. Schematic diagram of the state transitions of the Markov chain.

A. Cascade-Stop Probability, $P_{stop}(S_i)$

We refine the formulation of $P_{stop}(S_i)$ (as described in Section III) from [12] as follows to include the effects of cyber threat:

$$P_{stop}(S_i) = (1 - k\phi_{L_i}(F_i))(wP_{stop}^{(1)}(F_i) + (1-w)P_{stop}^{(2)}(C_i^{max}))$$

(4)

The first term $1 - k\phi_{L_i}(F_i)$ in (4) controls the cascade stop probability considering the effect of cyber threat as described in the previous subsection. Here $\phi_{L_i}(F_i) \in [0,1]$ represents cyber threat probability

for any given state. Note that for a fixed $\phi_{L_i}(F_i)$, when k is low, the term $1 - k\phi_{L_i}(F_i)$ is high indicating cyber threat has low effect on cascade stop probability and cascading failures. On the contrary, when k is high, $1 - k\phi_{L_i}(F_i)$ is low, which indicates that higher inter-connectivity reduces the probability of cascade stop.

Note that $\phi_{L_i}(F_i)$ can be any arbitrary monotonically increasing function of F_i. In this paper, we have used the following expression:

$$\phi_{L_i}(F_i) = \lambda(L_i)\left(1 - \frac{e^{(\gamma q F_i)} - 1}{e^{(\gamma N_{pc}^{max})} - 1}\right),$$

(5)

where $\lambda \in [0,1]$ controls the probability of cyber threat due to added interdependence between power and communication network, $\gamma \in [0,1]$ is a constant that shapes the exponential function and $q = \frac{V}{|\mathcal{F}|}$, where V is the number of nodes (buses). We consider three ranges of λ for the three levels of cyber threat.

$$\lambda(L_i) \in \begin{cases} [0,0.25], \text{if} L_i = 1 \\ (0.25,0.75], \text{if} L_i = 2 \\ (0.75,1], \text{if} L_i = 3 \end{cases}$$

(6)

Under normal operation, the ranges and the value of $\lambda(L_i)$ represent the grid's protection measure against possible cyber threats. For example, low probability of cyber threat indicates that the grid is protected against a variety of cyber threats like demand manipulation through IoT devices, DoS, and malware attacks. Note that when there are no line failures in the power grid, $\phi_{L_i}(F_i) = \lambda$, indicating the level of cyber threat prevailing due to the nature of protection used to resist cyber attacks. When the failures propagate in the power grid during cascading failures, the probability of a cyber threat decreases as the size of the power grid decreases due to failures in the transmission lines and power nodes. This, in turn, increases the cascade-stop probability in (4). Again, when all the transmissivvvon lines have failed ($qF_i = N_{pc}^{max}$), the cyber threat probability is zero, i.e., $\phi_{L_i}(F_i) = 0$, which is intuitive. Thus, depending on the level of cyber threat during cascade propagation, cascading failures escalate at different rates, which is captured in equation (4). In this way, through $\phi_{L_i}(F_i)$, we model the impact of cyber threats in the power systems on the cascade-stop probability.

The second term in $P_{stop}(S_i)$ has already been discussed in (1) and it has not been changed in the I-SASE model. The formulations of $P_{stop}^{(1)}(F_i)$ and $P_{stop}^{(2)}(C_i^{max})$ were developed based on extensive cascading failure simulations over the IEEE 118 bus grid and as given below [12]:

$$P_{stop}^{(1)}(F_i) = \begin{cases} a_1\left(\frac{a_2|\mathcal{F}| - F_i}{a_2|\mathcal{F}|}\right) + \epsilon \text{if} 1 \leq F_i \leq a_2|\mathcal{F}|, \\ \epsilon \text{if} a_2|\mathcal{F}| < F_i \leq 0.6|\mathcal{F}|, \\ Q(F_i) \text{if} 0.6|\mathcal{F}| < F_i \leq |\mathcal{F}|, \end{cases}$$

(7)

and

$$P_{stop}^{(2)}(C_i^{max}) = \max\left\{a_3\left(\frac{\max\{\mathcal{C}\} - C_i^{max}}{\max\{\mathcal{C}\}}\right)^4, a_4\right\}.$$

(8)

The parameters a_1, a_2, a_3, a_4, and ϵ govern the shape of the cascade-stop probability and they are obtained through curve fitting to data from simulations. Here, ϵ is a small value in [0, 0.1] [12].

Parametric relationships between the above parameters and the operating parameters (r, e, θ) of the grid were also established in [13]. The parametric formulation of a_1, a_2, a_3, a_4 are obtained from the simulation based parametric fitting approaches described in [12], [13], [48]:

$$\begin{aligned} a_1 &= \quad max(0.02, 0.4 - 0.25r - e(0.2 - e) - 0.25\theta_i), \\ a_2 &= \quad max(0.01, 0.6 - 0.4r - 0.5e - 0.3\theta_i), \\ a_3 &= \quad max(0.02, 0.4 - 0.25r - e(0.2 - e) - 0.25\theta_i), \end{aligned}$$

(9)(10)(11)

and

$$a_4 = max(0.01, 0.1 - 0.05r - 0.1e(0.2 - e) - 0.07\theta_i).$$

(12)

Here we adopted (9) and (10) from [13], replaced θ with θ_i, and (11) and (12) were formulated using the same parametric fitting technique used for (9) and (10).

B. Cascade-Continue Probability, $P(S_j|S_i)$

We extend the calculation of the cascade-continue probabilities, $P(S_j|S_i)$ of the Markov chain from [12] to include the impact of cyber threat variable as

$$P(S_j|S_i) = \begin{cases} P_{cont}(S_i)(1 - P_{hc}(S_i)) \dfrac{u(L_j)}{\sum_{l:L_l \geq L_i} u(L_l)} \\ \text{if} C_j^{max} = C_i^{max}, \\ P_{cont}(S_i) P_{hc}(S_i) \dfrac{w(C_j^{max})}{\sum_{m:C_m > C_i^{max}} w(C_m)} \\ \dfrac{u(L_j)}{\sum_{l:L_l \geq L_i} u(L_l)} \\ \text{if} C_j^{max} > C_i^{max}, \end{cases}$$

(13)

where $P_{cont}(S_i) = 1 - P_{stop}(S_i)$ and

$$P_{hc}(S_i) = \min(1, \alpha(F_i + \beta)^3).$$

(14)

In (13), $P_{hc}(S_i)$ is the transition probability to a state with higher capacity and the $w(C_j^{max})$'s are capacity weight parameters calculated from power grid simulations in [12]. In this paper, we include the quantity $u(L_j)$, which are the transition weight parameters for the cyber threat variable. Here in (13), we expanded the state transitions for the newly added state variables of the Markov chain. Note that in [12], we had two state variables which resulted in a maximum of five possible cascade-continue state-transition in the Markov chain (transition with one transmission line failures with different capacity levels). In this paper we further add three levels for the new state variable, L, which leads to a maximum of fifteen cascade-continue possible state-transition in the Markov chain. With $u(L_j)$'s in (13), we model the additional state-transition probabilities. These weight parameters govern the transition probabilities due to cyber threat in the Markov-chain. For example, if the $u(L_j)$'s has the same weights then from (13), the probability of transition from S_i to all possible S_j states are equally likely. For our three-level cyber threat state variable, when the cyber threat probability is low, then $u(\ell_1)$ will have higher weight value than the other two. As a result, $P(S_j|S_i)$ would be higher for states with $(L_j = 1)$ compared to the remaining two cases. This ensures the reflection of cyber threat levels in the state transition dynamics. Transition probabilities between different levels of cyber threat variables would result in different blackout sizes. In a physical system, to extract $u(L_j)$'s, first we need to categorize the various types of cyber attacks into L_j's. This can be done by studying the impact of those attacks in the grid. Intuitively, the effect of a malware or ransomware attack will be different compared to demand manipulation attack. Since failing transmission lines in real word networks for modeling purposes is not feasible, determining the $u(L_j)$'s from live power grid would be challenging. However, it is possible to create a digital twin (virtual representation that acts as the real-time digital counterpart of the real-world power grid) with various levels of cyber protection and then simulate cascading failures to determine the $u(L_j)$'s as well as the ranges of λ. Here we assume different

functions of $u(L_j)$'s in the analytic simulation to observe the pattern of blackout size distributions. In (14), α and β are constants obtained from [12].

Note that in this model we have considered a simple abstraction of cyber threat, an arbitrary monotone function for cyber threat probability, and modeled its impact on cascading failures in power grids. The model captures the robustness of the communication network from cyber attack through the variable λ, which is a mechanism introduced in (5) to control the probability of cyber threat due to added interdependency between the power and communication networks. However, for completeness of the model, it is required to have a model for λ as a function of the communication network. For example, if the communication network is robust and highly secured (e.g., military network), compared to public networks (e.g., the internet), the effect of the cyber threat on the reliability of the power grid would be different and it must be modeled for completeness. Detailed mapping of various types of cyber attacks with data integrity levels are the scope for future work. Specific values of $u(L_j) \in \{u(\ell_1), u(\ell_2), u(\ell_3)\}$ were selected in an arbitrary fashion rather than being extracted from an empirical study.

As defined in Section III, the total number of states of the Markov chain is $2|\mathcal{F}||\mathcal{C}|\mathcal{L}|$. Since $|\mathcal{C}|$ and $|\mathcal{L}|$ are fixed numbers in the I-SASE model, the size of the state space of the Markov chain scales linearly as a function of the number of transmission lines. From the definition of an index of a state [13] addressed in Section III $2|\mathcal{C}||\mathcal{L}|(F_i - 1) + 2|\mathcal{L}|C_i^{index} + 2(L_i - 1) + I_i + 1$, it is evident that the indices of transitory states and absorbing states are odd and even, respectively. Now for any given initial condition, we can calculate the limiting distribution of the failed transmission lines for a given initial state. Note that the Markov chain is not ergodic due to the presence of absorbing states. Hence, the limiting distribution will be dependent on the initial condition. Let $\boldsymbol{\pi}_0$ be a vector that denotes the probability mass function of the initial state, S_0 of the Markov chain. Next, let the vector $\boldsymbol{\pi}^{(S_0)} = (\pi_i^{(S_0)}, i = 1, \dots, 2|F||\mathcal{C}||L|$ represent the limiting distribution of the Markov chain starting from the state S_0, where $\pi_i^{(S_0)}$ is the steady-state probability of the state S_i. Hence, $\boldsymbol{\pi}^{(S_0)} = \boldsymbol{\pi}_0 \lim_{k\to\infty} \mathbb{P}^k$. The conditional probability that a power grid eventually reaches a steady-state with F_i failures from an initial state S_0 is

$$p(F_i|S_0) = \sum_{n=1}^{|\mathcal{C}||L|} \pi_{2(F_i-1)|\mathcal{C}||L|+2n}^{(S_0)},$$

(15)

which is the blackout-size distribution given an initial condition of the grid. In (15), we add all the probabilities having the final number of transmission line failure (when cascading ends) in the steady state for each capacity and data integrity combination to find the total probability of a transmission line failure (the subscript of π represent the index of the steady-state probabilities). Using the distribution of blackout sizes, we can calculate the expected number of transmission-line failures, $\mathrm{E}[F_i|S_0]$, given the initial condition, S_0, as follows,

$$\mathrm{E}[F_i|S_0] = \sum_{f_i=1}^{|F|} f_i p(f_i|S_0)\,.$$

(16)

This completes the complete formulation of the model.

To summarize, the inputs to the model are the initial state variables, $S_0 \in (F_0, C_0^{max}, L_0, I_0)$ and the operating parameters such as r, e, θ_0, k, and the initial system operator PSFs. The input parameters are used to evaluate the transition matrix using the formulation developed in Section IV, which, in turn, is used to find the various metrics i.e., the steady-state distribution of the blackout size, and the expected value of the number of transmission-line failures.

SECTION V. Results

In this section, we illustrate the capabilities of the I-SASE model using the IEEE 118-bus topology. In Fig. 7, we plot the steady-state distribution of the transmission-line failures under various initial conditions of the grid. Observe that, the orange-arrowed line (for nominal loading level, capacity estimation error and low initial failures) follows an exponential distribution. However, for high loading level, capacity estimation error and low/high initial failures we observe a power law distribution (which indicates cascading failures) represented by blue-circled and green lines respectively. Note that the capabilities of the model have been tested with the IEEE 118-bus and the IEEE 300-bus topology. However, the model has not been tested with a bigger system due to computational limitations, for example with the 80,000-bus synthetic grid developed for the Power Systems Engineering Research Center (PSERC) S-92 G project, which is a scope for future work.

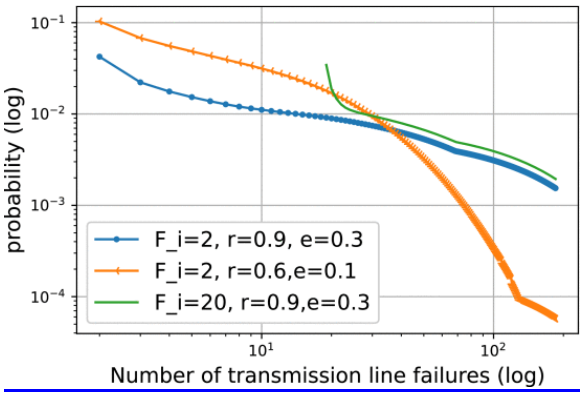
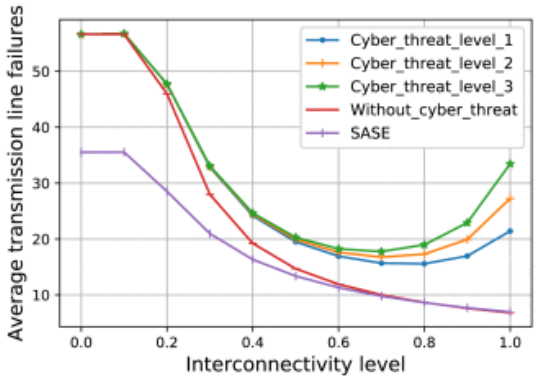


Fig. 7. Steady-state distribution of transmission-line failures (log-log) for various initial conditions.

A. Optimal Power-Communication Inter-Connectivity

We use the expected value of the transmission-line failures as a measure of grid reliability, which can be calculated using (16). Increasing inter-connectivity (represented by the parameter k, which was introduced in Section III) reduces constraint on load shedding but increases the cyber threat probability. Thus, we anticipate the existence of an optimal inter-connectivity that minimizes $\mathrm{E}[F_i|S_0]$ subject to k for a given grid condition. Again, increasing the number of

transmission-line failures reduces inter-connectivity, which, in turn, increases load-shedding constraint and system operators' error probability but reduces cyber threat. In Fig. 8(a), we plot $\mathrm{E}[F_i|S_0]$ for different levels of data integrity. Notice that when cyber threat is not considered, increasing inter-connectivity decreases $\mathrm{E}[F_i|S_0]$, and the optimal value of inter-connectivity is unity, which matches the observed behavior in [25]. However, when data integrity and nominal system operator error probability is considered, and for a chosen initial condition, S_0 ($F_i = 2,\ C_i^{max} = 20,\ r\ = 0.7,\ e = 0.1$), we observed an optimal inter-connectivity at 80%. As we increase inter-connectivity, cyber threat starts to play its role, and there exists a point of diminishing returns (at nearly 80% in Fig. 8(a)) beyond which the cyber threat dominates over the capability to implement load-shedding and thus the expected number of transmission-line failures increase. In Fig. 8(b), we plot the average transmission line failures for different levels of data integrity for the IEEE 300-bus system (411 transmission lines, which leads to 12,330 distinct states of the Markov chain). We observe an optimal inter-connectivity at 70%. Similarly to IEEE 118-bus system, as we increase the inter-connectivity from this optimal level, the expected number of transmission-line failures increase due to the impact of cyber threat, as cyber threat dominates over the capability to implement load-shedding.



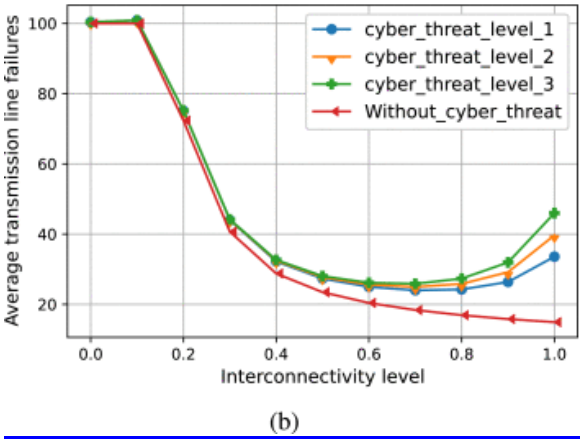


Fig. 8. Expected transmission-line failures for IEEE 118-bus and 300-bus systems with various inter-connectivity, and cyber threat level. (a) For IEEE 118-bus system, we considered $F_i = 2$, $C_i^{max} = 20$, $r\ = 0.7$, $e = 0.1$ and nominal human error level. (b) For IEEE 300-bus system, we considered $F_i = 10$, $C_i^{max} = 20$, $r\ = 0.7$, $e = 0.1$ and nominal human error level. We can observe a point of diminishing returns when cyber threat is considered.

Recall that our proposed model is a generalization of the SASE model in [12]. Thus, if we exclude the effect of data integrity and system operator errors, the model collapses to the SASE model. In that case, θ is a fixed parameter and does not change with the dynamics of the cascading failure. We have plotted $\mathrm{E}[F_i|S_0]$ using the SASE model against various levels of inter-connectivity in Fig. 8(a) for the IEEE 118-bus system. Note that when the SASE model is considered (i.e., without cyber threat and operators' error), inter-connectivity level and load shedding constraint parameters are fully correlated, i.e., as k increases, the constraint on load shedding is relaxed, which, in turn, reduces the expected number of transmission-line failures. In Fig. 8(a), we observe that when inter-connectivity level is high, average transmission line failures for the SASE (purple-bar) and without cyber threat (red-dash) shows similar trend, but not when inter-connectivity level is low. This is because without cyber threat (red-dash) case, system operators' error is considered, which created the difference between the two plots. However, when inter-connectivity level is high, load-shedding capability increases significantly, superseding the effect of operator error, i.e., for higher level of inter-connectivity, the effect of human operator error is negated as the operators' have more options (due to having more information) to find solution to mitigate the risk of a cascading failures.

B. Role of System Operators in Cascading Failure

Recall from Fig. 4 that the relationship between the operator error and the state is monotone. Error in operators' decision-making adds a constraint on load-shedding capability, which reduces the probability of cascade stopping and hence increases $\mathrm{E}[F_i|S_0]$. The effect of various operator performance scenarios can be visualized in Fig. 9. We observe an exponential distribution for the nominal HEP, whereas a power-law distribution for the extreme HEP (approximately represented by the probabilities is observed in log-log scale). Note that the exponential (power-law) distribution results in low (high) expected number of transmission-line failures. Although the other parameters of the Markov chain are fixed, changing the initial PSF levels from nominal to extreme (which exists due to the different level of experience of the operator, ergonomics, work process, and operating procedure availability) can influence the outcome significantly.

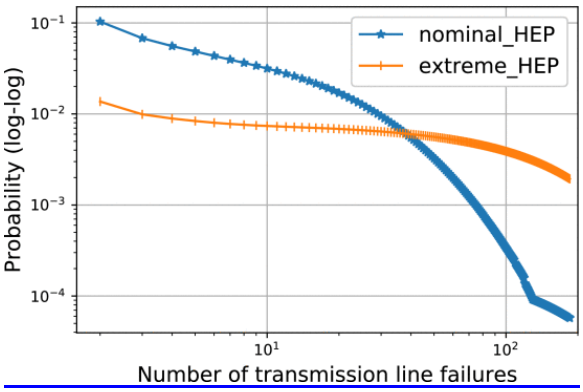
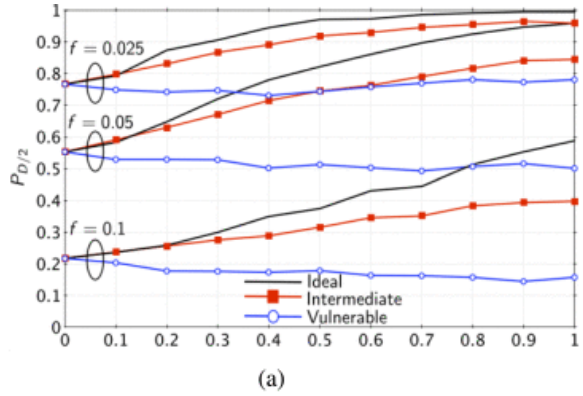


Fig. 9. Probability distribution of the blackout size for nominal and extreme system operator error scenario. As an initial condition, we considered $F_i = 2$, $C_i^{max} = 20$, $L = 1$, $r = 0.7$, $e = 0.1$.

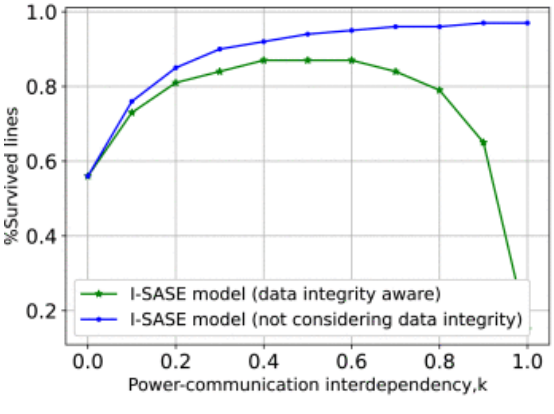
C. Comparison With Other Models

A comparison between the approaches reported in [18], [25] and the current I-SASE model is shown in Fig. 10. Fig. 10(a) is adopted from [25] and Fig. 10(b) is obtained using the I-SASE model. The vertical

axis in Fig. 10(a) represents the percentage of loads served after the cascade ends. Moreover, f represents various percentage of initial line failures. The ideal case (represented by the black line) represents a scenario when communication failures do not effect power failures. The vulnerable case (represented by the blue-circled line) represents the work in [18], where failure in power has deterministic impact on communication. The intermediate case (represented by the red-squared line) represents the work by Korkali *et al.*, where failures in communication results in failure in power nodes probabilistically. If we follow the solid red circled line in Fig. 10(a), we can see that as the interdependency is increased, the percentage of loads served after the cascade ends increases and the maximum is found when the interdependency level reaches its maximum value of unity. In Fig. 10(b) we show the results obtained using the I-SASE model (we assume a linear correlation between the percentage of average survived lines with percentage of load served). If we do not consider data integrity (represented by the blue-circled line), we also obtain the similar result as reported in [25]. When the data integrity is considered, then we see that the percentage of average survived lines increases initially (represented by the green-stared line) with increase in interdependence. It is interesting to note that there exists a point of diminishing returns beyond which the harm of communication outweighs the benefits of communication. Thus, beyond a certain level of power-communication interdependency, k, we add more risk to the grid compared to the benefits of information.



(a)



(b)

Fig. 10. Comparison of the effect of various levels of power-communication interdependency reported in [25] and the I-SASE model: (a) % of served loads after cascade ends for various interdependency levels (adopted from [25]) and (b) % of survived lines for various interdependency levels using the I-SASE model.

SECTION VI. Conclusion

A Markov chain has been proposed for predicting the dynamics of cascading failures while considering the effect of data integrity and system operator-error. The state variables include the number of failed transmission lines, the maximum capacity of the failed lines, the level of cyberthreat, as well as a binary state variable describing whether or not cascading failures are continuing. Included in the transition probability matrix of the Markov chain is a novel mathematical representation of the interdependencies and dynamic interactions among data integrity, failures in transmission lines, and the performance of human operators. For example, the load-shedding actions implemented by human operators are dynamically dependent upon the level of data integrity, the interconnectivity between the power grid and the supporting communication network, and the human-operator performance. The human-error probability is, too, included in the transition probability matrix while being dependent on the level of data integrity. The model is used to generate the steady-state probability distribution of the size of a blackout resulting from cascading failures that are triggered by initial transmission-line failures. Notably, the calculated blackout-sized probability distribution considers the potential harm from lack of data integrity and operator error. The mean of the steady-state number of failed lines was used as a metric to find the optimal level of interconnectivity that maximizes the benefits of information and minimizes the risk of a cascading failure induced by the interdependency.

The model predicts that the presence of risks in data integrity leads to the existence of a point of diminishing returns when the harm from lack of data integrity outweighs the benefits of having maximal information about the grid as load-shedding decisions are made. Specifically, there is an optimum level of interconnectivity between the grid and the supporting communication network that yields the minimum number of failed transmission lines in the steady state. This work provides a scalable analytical approach for determining the reliability for information-centric grids by taking into account data integrity and operator-error issues. Future extensions include developing a Markov decision process based strategy to mitigate the risk of cascading failures, which would ensure information protection, a key component to North America Electric Reliability Corporation - Critical Infrastructure Protection (NERC-CIP) standards.

References

1. K. Sun, Y. Hou, W. Sun and J. Qi, Power System Control Under Cascading Failures: Understanding Mitigation and System Restoration, Hoboken, New Jersey, USA, Wiley-IEEE Press, 2019.

2. R. Baldick et al., "Initial review of methods for cascading failure analysis in electric power transmission systems IEEE PES CAMS task force on understanding prediction mitigation and restoration of cascading failures", *Proc. IEEE Power Energy Soc. Gen. Meeting- Convers. Del. Elect. Energy 21st Century*, pp. 1-8, 2008.

3. Y. Yang, T. Nishikawa and A. E. Motter, "Small vulnerable sets determine large network cascades in power grids", *Science*, vol. 358, no. 6365, 2017.

4. "List of major power outages", Jul. 2019, [online] Available: https://en.wikipedia.org/wiki/Listofmajorpoweroutages.

5. H. Guo et al., "A critical review of cascading failure analysis and modeling of power system", *Renewable Sustain. Energy Rev.*, vol. 80, pp. 9-22, 2017.

6. P. Hines, J. Apt and S. Talukdar, "Trends in the history of large blackouts in the United States", *Proc. IEEE Power Energy Soc. Gen. Meeting- Convers. Del. Elect. Energy 21st Century*, pp. 1-8, 2008.
7. Z. El Mrabet, N. Kaabouch, H. El Ghazi and H. El Ghazi, "Cyber-security in smart grid: Survey and challenges", *Comput. Elect. Eng.*, vol. 67, pp. 469-482, 2018.
8. "Electricity grid cybersecurity: DOE needs to ensure its plans fully address risks to distribution systems", 2021, [online] Available: https://www.gao.gov/products/gao-21-81.
9. The White House, "Act sheet: Biden administration announces further actions to protect U.S. critical infrastructure", 2021, [online] Available: https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/fact-sheet-biden-administration-announces-further-actions-to-protect-u-s-critical-infrastructure/.
10. X. Fang, S. Misra, G. Xue and D. Yang, "Smart grid-the new and improved power grid: A survey", *IEEE Commun. Surv. Tut.*, vol. 14, no. 4, pp. 944-980, Oct.–Dec. 2012.
11. S. Soltan, P. Mittal and H. V. Poor, "BlackIoT: IoT botnet of high wattage devices can disrupt the power grid", *Proc. 27th USENIX*, pp. 15-32, 2018.
12. Rahnamay-Naeini et al., "Stochastic analysis of cascading-failure dynamics in power grids", *IEEE Trans. Power Syst.*, vol. 29, no. 4, pp. 1767-1779, Jul. 2014.
13. Z. Wang et al., "Impacts of operators' behavior on reliability of power grids during cascading failures", *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 6013-6024, Nov. 2018.
14. R. A. Shuvro et al., "Correlating grid-operators' performance with cascading failures in smart-grids", *Proc. IEEE PES Innov. Smart Grid Technol. Europe*, pp. 1-5, 2019.
15. P. Crucitti, V. Latora and M. Marchiori, "Model for cascading failures in complex networks", *Phys. Rev. E*, vol. 69, no. 4, 2004.
16. A. E. Motter, "Cascade control and defense in complex networks", *Phys. Rev. Lett.*, vol. 93, no. 9, 2004.
17. C. D. Brummitt, R. M. D'Souza and E. A. Leicht, "Suppressing cascades of load in interdependent networks", *Proc. Nat. Acad. Sci.*, vol. 109, no. 12, pp. E680-E689, 2012.
18. S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley and S. Havlin, "Catastrophic cascade of failures in interdependent networks", *Nature*, vol. 464, no. 7291, pp. 1025-1028, 2010.
19. A. Smolyak, O. Levy, I. Vodenska, S. Buldyrev and S. Havlin, "Mitigation of cascading failures in complex networks", *Sci. Rep.*, vol. 10, no. 1, pp. 1-12, 2020.
20. I. Dobson et al., "Complex systems analysis of series of blackouts: Cascading failure critical points and self-organization", *Chaos: An Interdiscipl. J. Nonlinear Sci.*, vol. 17, no. 2, 2007.
21. M. Parandehgheibi et al., "Mitigating cascading failures in interdependent power grids and communication networks" in Smart Grid Commun., IEEE, pp. 242-247, 2014.
22. B. A. Carreras, D. E. Newman, P. Gradney, V. E. Lynch and I. Dobson, "Interdependent risk in interacting infrastructure systems", *Proc. 40th Annu. Hawaii Int. Conf. System Sci.*, pp. 112-112, 2007.
23. B. Schäfer, D. Witthaut, M. Timme and V. Latora, "Dynamically induced cascading failures in power grids", *Nature Commun.*, vol. 9, no. 1, pp. 1-13, 2018.
24. M. Noebels, I. Dobson and M. Panteli, "Observed acceleration of cascading outages", *IEEE Trans. Power Syst.*, vol. 36, no. 4, pp. 3821-3824, Jul. 2021.
25. M. Korkali, J. G. Veneman, B. F. Tivnan, J. P. Bagrow and P. D. Hines, "Reducing cascading failure risk by increasing infrastructure network interdependence", *Sci. Rep.*, vol. 7, 2017.

26. M. Rahnamay-Naeini and M. M. Hayat, "Cascading failures in interdependent infrastructures: An interdependent Markov-chain approach", *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 1997-2006, Jul. 2016.

27. Z. Wang et al., "A Markov-transition model for cascading failures in power grids", *Proc. 45th Hawaii Int. Conf. Syst. Sci*, pp. 2115-2124, 2012.

28. U. Nakarmi, M. Rahnamay-Naeini and H. Khamfroush, "Critical component analysis in cascading failures for power grids using community structures in interaction graphs", *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 3, pp. 1079-1093, Jul.–Sep. 2020.

29. X. Wu, D. Wu and E. Modiano, "An influence model approach to failure cascade prediction in large scale power systems", *Proc. Amer. Control Conf.*, pp. 4981-4988, 2020.

30. B. Huang, A. A. Cardenas and R. Baldick, "Not everything is dark and gloomy: Power grid protections against IoT demand attacks", *Proc. 28th USENIX Secur. Symp.*, pp. 1115-1132, 2019.

31. S. Soltan, M. Yannakakis and G. Zussman, "Power grid state estimation following a joint cyber and physical attack", *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 1, pp. 499-512, Mar. 2018.

32. X. Zhang, D. Liu, C. Zhan and K. T. Chi, "Effects of cyber coupling on cascading failures in power systems", *IEEE Trans. Emerg. Sel. Topics Circuits Syst.*, vol. 7, no. 2, pp. 228-238, Jun. 2017.

33. Y. Chen, J. Hong and C.-C. Liu, "Modeling of intrusion and defense for assessment of cyber security at power substations", *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2541-2552, Jul. 2018.

34. S. Zonouz, K. M. Rogers, R. Berthier, R. B. Bobba, W. H. Sanders and T. J. Overbye, "SCPSE: Security-oriented cyber-physical state estimation for power grid critical infrastructures", *IEEE Trans. Smart Grid*, vol. 3, no. 4, pp. 1790-1799, Dec. 2012.

35. B. Li, R. Lu, W. Wang and K.-K. R. Choo, "DDOA: A dirichlet-based detection scheme for opportunistic attacks in smart grid cyber-physical system", *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 11, pp. 2415-2425, Nov. 2016.

36. R. Bulbul, P. Sapkota, C.-W. Ten, L. Wang and A. Ginter, "Intrusion evaluation of communication network architectures for power substations", *IEEE Trans. Power Del.*, vol. 30, no. 3, pp. 1372-1382, Jun. 2015.

37. U. Adhikari, T. H. Morris and S. Pan, "Applying non-nested generalized exemplars classification for cyber-power event and intrusion detection", *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 3928-3941, Sep. 2018.

38. K. Yamashita, C.-W. Ten and L. Wang, "Dynamical analysis of cyber-related contingencies initiated from substations", *Proc. Secur. Cyber-Physical Syst.*, pp. 223-246, 2020.

39. D. Ding, Q.-L. Han, X. Ge and J. Wang, "Secure state estimation and control of cyber-physical systems: A survey", *IEEE Trans. Syst. Man Cybern. Syst.*, vol. 51, no. 1, pp. 176-190, Jan. 2021.

40. O. Kosut, L. Jia, R. J. Thomas and L. Tong, "Limiting false data attacks on power system state estimation", *Proc. 44th Annu. Conf. Inf. Sci. Syst.*, pp. 1-6, 2010.

41. O. Kosut, L. Jia, R. J. Thomas and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures", *Proc. First IEEE Int. Conf. Smart Grid Commun.*, pp. 220-225, 2010.

42. X. Liu and Z. Li, "False data attacks against AC state estimation with incomplete network information", *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2239-2248, Sep. 2017.

43. J. M. Abreu et al., "Modeling human reliability in the power grid environment: An application of the spar-h methodology", *Proc. Hum. Factors Ergonom. Soc. Annu. Meeting*, vol. 59, no. 1, pp. 662-666, 2015.

44. D. Gertman et al., "The SPAR-H human reliability analysis method", *US Nucl. Regulatory Commission*, vol. 230, pp. 35, 2005.

45. R. L. Boring and H. S. Blackman, "The origins of the spar-h method's performance shaping factor multipliers", *Proc. IEEE 8th Hum. Factors Power Plants HPRCT 13th Annu. Meeting*, pp. 177-184, 2007.

46. H. S. Blackman, D. I. Gertman and R. L. Boring, "Human error quantification using performance shaping factors in the spar-h method", *Proc. Hum. Factors Ergonom. Soc. Annu. Meeting*, vol. 52, no. 21, pp. 1733-1737, 2008.

47. R. A. Shuvro, P. Das, J. M. Abreu and M. M. Hayat, "Correlating grid-operators' performance with cascading failures in smart-grids", *Proc. IEEE PES Innov. Smart Grid Technol. Europe*, pp. 1-5, 2019.

48. Rahnamay-Naeini et al., "Impacts of operating characteristics on sensitivity of power grids to cascading failures", *Proc. Power Energy Soc. Gen. Meeting*, pp. 1-5, 2016.