An Efficient Computational Strategy for Cyber-Physical Contingency Analysis in Smart Grids

Hamid Emadi[1], Joe Clanin[2,4], Burhan Hyder[3], Kush Khanna[3],Manimaran Govindarasu[3], Sourabh Bhattacharya[1,4]
Email: {emadi, jsc, bhyder, kkhanna, gmani, sbhattac}@iastate.edu

***Abstract*—The increasing penetration of cyber systems into smart grids has resulted in these grids being more vulnerable to cyber physical attacks. The central challenge of higher order cyber-physical contingency analysis is the exponential blow-up of the attack surface due to a large number of attack vectors. This gives rise to computational challenges in devising efficient attack mitigation strategies. However, a system operator can leverage private information about the underlying network to maintain a strategic advantage over an adversary equipped with superior computational capability and situational awareness.**

In this work, we examine the following scenario: A malicious entity intrudes the cyber-layer of a power network and trips the transmission lines. The objective of the system operator is to deploy security measures in the cyber-layer to minimize the impact of such attacks. Due to budget constraints, the attacker and the system operator have limits on the maximum number of transmission lines they can attack or defend. We model this adversarial interaction as a resource-constrained attacker-defender game. The computational intractability of solving large security games is well known. However, we exploit the approximately modular behaviour of an impact metric known as the disturbance value to arrive at a linear-time algorithm for computing an optimal defense strategy. We validate the efficacy of the proposed strategy against attackers of various capabilities and provide an algorithm for a real-time implementation.

***Index Terms*—Smart Grids, Cyber-Security, Cyber-Physical Contingency Analysis, Security Games.**

I. Introduction

Analyzing the impact of component failures is critical to successful design, monitoring and control of power grids, communication networks and other cyber-physical systems. Modern power networks are designed to meet the $N-1$ reliability criterion wherein no single line failure critically impacts the functioning of the grid. The problem of identifying and planning for 1-component contingencies has been extensively studied (for example, in [1] [2] [3] [4]). Vulnerability to cyber attacks is an unavoidable consequence of the transition to the smart grid. The possibility of such attacks has made larger-scale component failures more probable and has elucidated the need for consideration of k-component failures to enhance the cyber-security and resiliency of the system [5]. Due to the inherent combinatorial complexity of considering all possible k-component failures, exhaustive and exact $N-k$ cyber-physical contingency analysis in large grids requires exponential time. Indeed, for real-time applications, such analysis in even moderately-sized grids may be computationally infeasible.

In the past, techniques such as heuristic pruning algorithms [6], cutting plane algorithms [7], and probabilistic methods [8] [9] [10] [11] have been proposed to reduce the search space of k-component contingencies. Although each of these methods provides a significant improvement over the enumerative approach, they still suffer from some inherent inefficiencies. For example, the pruning and cutting plane algorithms evaluate a number of non-critical contingencies and some of the probabilistic methods identify only a subset of critical contingencies [10] or require the use of predetermined component failure data [11]. An alternate approach proposed in [12] performs low-order contingency analysis on a reduced grid obtained by comparing the topological and electrical structure of the original grid. However, this reduction can fail to account for the impact of contingencies involving single lines with high power flows. Game-theoretic models have also been proposed in the past to address contingency analysis and investments strategies [13]. They include formulation of contingency analysis as a simultaneous move [14] game as well as a Stackelberg game [15] [11].

Our current work is based on [16] which presents a linear-time algorithm to obtain saddle-point strategies for zero-sum games with additive utility functions. Based on the approximately modular [17] behaviour of of the *disturbance value function* associated with k-line failures [18], we cast the cyber-physical-contingency analysis of a power network as a additive zero-sum game. In Section II, we formulate the problem of k-line contingency analysis as a security game, review the notion of disturbance value introduced in [18], and describe its additive approximation. In Section III, we frame the linear program used to solve the security game as in [14]. We simulate contingency analysis in Section IV on four small networks obtained by augmentation of standard 5,9,14, and 39 bus systems, and compare the results obtained under the additivity assumption by the methods of [16] and [14] with the actual contingency impacts. Finally, in Section V, a heuristic method to implement the defender resource allocation on a

Department of Mechanical Engineering[1], Mathematics[2], Electrical and Computer Engineering[3] and Computer Science[4], Iowa State University, Ames, IA-50011.

grid according to the results of Section IV is proposed and simulated on the augmented 39 bus system.

II. Problem Formulation

Consider a power grid modeled as a graph $G(\nu, \epsilon)$, where the set of vertices $\nu = \{1, \ldots, n\}$ corresponds to the buses, and the set of edges $\epsilon = \{e_1, \ldots, e_m\}$ corresponds to the transmission lines between the buses. We assume that the transmission lines are purely reactive. The weight of edge $e_i \in \epsilon$ is $y_{e_i} = \frac{1}{x_{e_i}}$, where $x_{e_i} > 0$ is the reactance of the transmission line corresponding to e_i. Let $P \in \mathbf{R}^n$ denote the power supply/demand vector whose i^{th} entry is positive when there is generation at bus i, negative when there is load at bus i, and zero when i is a neutral node. We consider an arbitrary direction for the edges and define $D \in \mathbf{R}^{n \times m}$ as the directed incidence matrix of G. Let f denote the vector of power flows in each line in the adopted direction of the edges in G. We consider a lossless and balanced network. In other words, each line is purely reactive and $\sum_{i \in \nu} P_i = 0$. Considering a DC power flow approximation, the power flow equation is given by $f = YD^T PL^\dagger$, where $L \in \mathbf{R}^{n \times n}$ is the Laplacian matrix associated to weighted graph G, $L^\dagger$ denotes the pseudo-inverse of L and $Y = \text{diag}(y_1, \ldots, y_m)$ is a diagonal matrix of the reciprocals of transmission line reactances.

Next, we describe the attack scenario and the attack surface for which the contingency analysis is being performed. We consider a transmission line attack in which an attacker breaches the access points through cyber layer, and trips the relay associated with the individual transmission lines. In order to secure the power network from such attacks, additional security measures need to be deployed at the access points vulnerable to such attacks. However, due to limitations in the attackers resources, we assume that the attacker can trip at most $k_a < m$ transmission lines. Similarly, due to limitations in the cyber-defense budget, the defender can deploy additional security measures on at most $k_d < m$ lines. Therefore, there are $n_a = \binom{m}{k_a}$ and $n_d = \binom{m}{k_d}$ actions for player 1 and player 2 respectively. We assume that neither player has any information about the strategy of the other player. However, information about the network (topology, line reactances) is common information between the players.

In this work, we consider the *disturbance value*, initially introduced in [18], as a metric of the impact of a k-link failure. Let $\mathcal{K}_i = \{e_1, ..., e_k\}$ denote a set of link failures. Let $\phi_{\mathcal{K}_i}$ denote the disturbance value associated with failure of links in $\mathcal{K}_i$. In [18], the authors show that $\phi_{\mathcal{K}_i}$ can be approximated by

$$\phi_{\mathcal{K}_i} \approx \sum_{e_j \in \mathcal{K}_i} \frac{{f_j}^2 r_j}{1 - y_j r_j}, \tag{1}$$

where r_j is the equivalent reactance between the end nodes of line e_j. As a result, high-risk contingencies can be quickly identified by focusing only on lines with high 1-line disturbance values. This approximation is shown to have an approximation error of less than 10% and 0.98 correlation to the actual disturbance value in simulations of 3-line failures that do not cause a disconnection of the grid in the IEEE 118 and 300 bus systems. Considering contingencies with high disturbance values allowed the authors to reduce the space of contingencies in their simulations on these grids by more than 90%.

Given the actions of the 2 players and the impacts associated with any given pair of actions, the contingency analysis problem reduces to find the optimal strategies of the defender.

III. Game-Theoretic Modeling: Optimal defense strategy and maximum impact

In order to find the optimal strategy for the defender, we formulate a strategic security game $(\mathcal{X}, \mathcal{Y}, A)$, where $\mathcal{X}$ and $\mathcal{Y}$ denote the action sets for attacker and defender, respectively, and $\text{card}(\mathcal{X}) = n_a$, $\text{card}(\mathcal{Y}) = n_d$. Every element $x_i \in \mathcal{X}$ represents a set of attacked links. Similarly, $y_i \in \mathcal{Y}$ represents a set of protected links. Each $x_i \in \mathcal{X}$ and $y_i \in \mathcal{Y}$ is a k_a-tuple, and k_d-tuple subset of ϵ, respectively. Let A represent the game matrix or payoff matrix for player 1. Since we consider a zero-sum game, the payoff matrix for player 2 is $-A$. The element in row i and column j, A_{ij}, represents the payoff to the attacker when the defender and attacker choose y_j and x_i, respectively.

In the previous section, we defined $\phi_{\mathcal{K}_i}$ as the impact associated with a k-link failure based on disturbance values and presented an expression for it (1). This can be considered as the payoff/utility for the attacker when it is successful in attacking links in $\mathcal{K}_i$. Since the utility function has the additive property, entries of the cost matrix A are defined as follows:

$$A_{ij} = \sum_{\{l | l \in x_i \cap y_j^c\}} \phi_l. \tag{2}$$

Let p (q) denote the probability vector representing the mixed strategies for player 1 (player 2). The expected utility (impact to the network) when attacker (player 1) and defender (player 2) play mixed strategies p and q, respectively, is $v = p^T A q$. According to the minimax theorem, every finite two-person zero-sum game has a saddle point with the value, v^*, in mixed strategy $p^* = \left[p_1^*, \ldots, p_{n_a}^*\right]^T$ for player 1, and mixed strategy $q^* = \left[q_1^*, \ldots, q_{n_d}^*\right]^T$ for player 2, such that the average gain of player 1 is at least v^* no matter what player 2 does and the average loss of player 2 is at most v^* regardless of the strategy of player 1. That is

$$p^T A q^* \leq {p^*}^T A q^* \leq {p^*}^T A q.$$

Every finite matrix game can be reduced to the following LP problem,

$$\begin{aligned} \underset{p}{\text{maximize}} \quad & v \\ \text{subject to} \quad & v \leq \sum_{i=1}^{n_a} p_i A_{ij}, \quad j = 1, \ldots, n_d \\ & p_1 + \cdots + p_{n_a} = 1, p_i \geq 0 \quad \forall i \end{aligned} \tag{3}$$

However, the dimension of the decision variables in the above formulation is $(n_a + 1)$ which is exponential in terms of m. Based on our previous work in [16] regarding games with

additive utility, (3) can be converted to a new LP in m variables and m constraints as follows:

$$\begin{aligned} \underset{\alpha_1,\ldots,\alpha_m}{\text{maximize}} \quad & \sum_{l=1}^{m-k_d} \alpha_l \phi_l \\ \text{subject to} \quad & \alpha_i \phi_i \geq \alpha_j \phi_j \quad \text{for all} \quad i > j \\ & \sum_{i=1}^{m} \alpha_i = k_a, \quad \alpha_i \leq 1, \quad i = 1, \ldots, m. \end{aligned} \tag{4}$$

where

$$\alpha_j = \sum_{\{i|j \in x_i\}} p_i, \quad \beta_j = \sum_{\{i|j \in y_i{}^c\}} q_i \tag{5}$$

In the above equations, $\alpha = [\alpha_1, \ldots, \alpha_m]^T$ and $\beta = [\beta_1, \ldots, \beta_m]^T$ can be interpreted as the *attack* and *exposure* probability vectors, respectively. For instance, α_j is the summation of all p_i's for which target j lies in action set of x_i. Since we consider additive property, payoff for each player is summation of expected outcome for each target (i.e. attack probability $\times$ impact $\times$ exposure probability). Consequently, we can define the optimality conditions in terms of (α, β). (α^*, β^*) is a NE of a security game $(\mathcal{X}, \mathcal{Y}, A)$ if and only if any feasible deviation from α^* (β^*), does not lead to better payoff for the attacker (defender).

Algorithm 1 presents a technique to compute β^* and v^*. It takes as input the parameters of the problem (ϕ, m, k_a, k_d) and provides the optimal resource allocation strategy for the defender. The overall algorithm runs in $\mathcal{O}(m)$ steps which is a significant improvement from an exponential-time algorithm. Details regarding the complexity and completeness of Algorithm 1 can be obtained in [16].

IV. Simulation Results

In this section, we provide a number of simulations over power networks to show that impacts of k line failures can be approximated by the sum of the individual 1-line failures. That is, we demonstrate that the additivity property is a valid assumption in these networks. Furthermore, we examine the scenario in which players solve the exact game versus the scenario in which the approximated solution obtained via the additive property is taken. We explicitly compare the payoffs to the players in these scenarios.

A. Empirical evaluation of near-modular behaviour of the disturbance value

In this section, we evaluate the validity of approximation in (1) (additivity). We define an approximation error as follows:

$$e = \frac{|\phi_{\mathcal{K}_i} - \sum_{j \in \mathcal{K}_i} \phi_j|}{\phi_{\mathcal{K}_i}} \times 100 \tag{6}$$

We examine four networks with 5,9,14 and 39 busses. In order to obtain networks with edge-connectivity of 3, we augment standard 5,9,14 and 39 bus networks[1] with additional edges. Tables I,II,III and Figure 3 provide details regarding the additional edges. In the new networks, $k_a = 2$ is guaranteed without islanding.

Figure 1 shows the histogram of e for all possibilities of 2-line failure for the four networks. From the figure, we can observe that the gap between the approximation in (1) and reality closes as the size of the network grows. Intuitively, we expect that larger networks have smaller approximation error since the failure of a group of links has less effect on the rest of network as the size of the network grows. Moreover, the structure of the matrices involved in the calculation of the disturbance value [18] further support the aforementioned hypothesis.

[1] 5-bus PJM example from Rui Bo, 9-bus example case from Chow, IEEE 14 -bus case, 39-bus New England case. All cases are examined in MATPOWER 7.1

Algorithm 1 Computation of v^* and β^*

Input: ϕ, m, k_a, k_d
Output: v^* and β^*
for $i = 1 : m$ **do**
  for $j = 1 : m$ **do**
    $s = m - i + 1$, $r = j - i$, $c_i = \sum_{l=s}^{m} \frac{1}{\phi_l}$
    if $(s - 1 \geq r \geq 0) \wedge$
      $(r + m - s \geq k_a \geq r + 1) \wedge$
      $(c_i \phi_{s-r} \geq i - k_d \geq c_i \phi_{s-r-1})$ **then**
      $W_{i,j} = \frac{(k_a - r)(i - k_d)}{c_i} + \sum_{l=s-r}^{s-1} \phi_l$
      case $\leftarrow$ case I
    else if $(s - 1 \geq r \geq 0) \wedge$
      $(r + m - s \geq k_a \geq r + 1) \wedge$
      $(c_i \phi_{s-r-1} + 1 > i - k_d + 1 \geq c_{i+1} \phi_{s-r-1})$ **then**
      $W_{i,j} = (i - k_d + 1 - c_i \phi_{s-r-1}) \phi_{s-1} +$
      $(k_a - r) \phi_{s-r-1} + \sum_{l=s-r}^{s-2} \phi_l$
      case $\leftarrow$ case II
    else
      $W_{i,j} = \infty$
    end if
  end for
end for
$v^* \leftarrow \min W$, $(i^*, r^*, s^*) \leftarrow \text{argmin} W$
if case = case I **then**
  $\beta_1^* = \cdots = \beta_{s^*-1}^* = 1, \quad \beta_j^* = \frac{i - k_d}{c_i \phi_j}, j = s^*, \ldots, m,$
else if case = case II **then**
  $\beta_1^* = \cdots = \beta_{s^*-2}^* = 1$
  $\beta_{s^*-1}^* = i^* - k_d + 1 - c_{i^*} \phi_{s^* - r^* - 1}$
  $\beta_j^* = \frac{\phi_{s^*-r^*-1}}{\phi_j}, j \in \{s^*, ., m\}$
end if

Link Additions to 5-bus Network	
End Busses of e_i	x_{e_i}
1,3	0.02
2,4	0.01
5,3	.02

TABLE I: Links added to the case 5-bus system to ensure 3-edge-connectivity of the grid.

Link Additions to 9-bus Network			
End Busses of e_i	x_{e_i}	End Busses of e_i	x_{e_i}
1,2	0.085	9,7	0.085
1,3	0.161	7,5	0.176
2,3	0.12	9,5	0.176

TABLE II: Links added to the case 9-bus systems to ensure 3-edge-connectivity of the grid.

Link Additions to IEEE 14-bus Network			
End Busses of e_i	x_{e_i}	End Busses of e_i	x_{e_i}
1,3	0.34	10,14	0.085
3,8	0.19	14,11	0.34
8,10	0.27	12,11	0.34

TABLE III: Links added to the IEEE 14-bus systems to ensure 3-edge-connectivity of the grid.

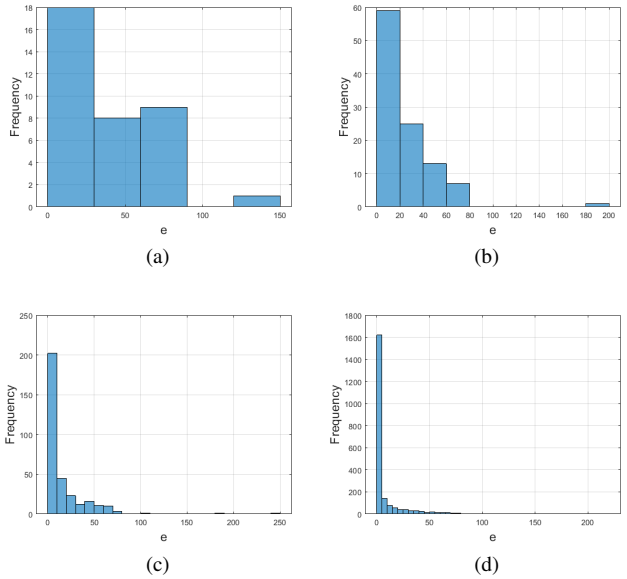

Fig. 1: Figure shows the histogram of e for the (a) 5-bus network (b) 9-bus network (c) 14-bus network.(d) 39-bus network

B. Variations in the attacker models

In this section, we consider the following variations of the attacker model while the defender is assumed to implement β^*:

1) Computationally superior attacker: We consider an attacker who implements a strategy obtained by solving a game without using approximation (1), i.e., one who computes the exact disturbance value of a k-line failure. Figure 2 shows the expected outcome of the play (v_2) for several values of k_d in the 5 and 9 bus networks. Figure 2 shows a close overlap between v_1 and v_2 for both networks. A computationally superior attacker therefore has minimal effect on the expected outcome in the simulations shown in Figure 2. In other words, it is reasonable for the defender to compute their optimal allocation based upon the additivity approximation.

2) Attacker with side information: We consider an attacker that has side information regarding the limited computational capabilities of the defender and implements the output of Algorithm 1. Figure 2 shows the expected outcome of the play (v_3) for several values of k_d for the two different networks. We can observe that v_3 is always smaller than v_2 and v_1. Therefore, an attacker that hedges its play on the side information and thus modifies its play to α^* gets a lower payoff. In light of this result, the defender may wish to hedge its play by allowing the side information to reach the attacker.

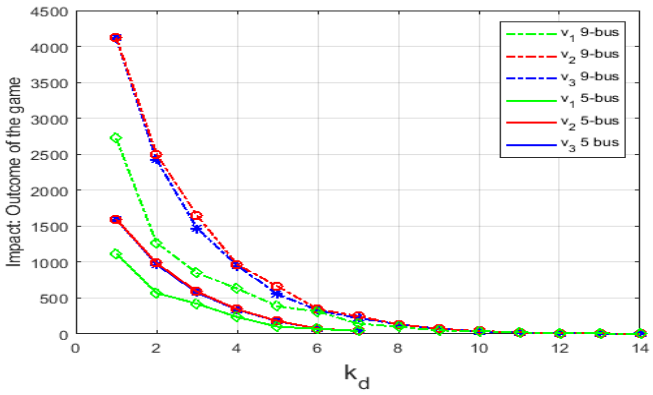

Fig. 2: Figure shows v_1, v_2, v_3 for the 5-bus and 9-bus networks.

V. Implementation of Strategies

In this section, we address the problem of implementing β^* on a real power network. The probability of the defender assigning a resource to a link i when he plays the mixed strategy q^* is $\gamma_i^* = 1 - \beta_i^*$. For a set of indices T, let γ_T^* be the vector of entries of γ^* which occur at the indices in T and denote

$$\bar{\gamma}_T = \frac{\gamma_T^*}{\sum_{i \in T} \gamma_i^*}.$$

Note that selection of target i is deterministic when $\gamma_i^* = 1$ or $\gamma_i^* = 0$. Computing q^* from β^* (from (5)) is computationally challenging, for it requires solving a system of underdetermined equations involving a large (exponential in m) number of unknown variables. Algorithm 2 presents a more efficient strategy for the defender to choose links based on β^*. This approach iteratively chooses links based upon the exposure probabilities obtained using Algorithm 1.

Algorithm 2

Input: γ^*
Output: Selected targets T
$S = \{i | \gamma_i^* = 0\}$ and $T = \{i | \gamma_i^* = 1\}$
$I = \{1, \ldots, m\}$
$count = |T|$
while $count < k_d$ **do**
    j: select 1 target from $I \setminus (T \cup S)$
        with probability $\bar{\gamma}_{I \setminus (T \cup S)}$.
    $T \leftarrow T \cup \{j\}$
    $count \leftarrow count + 1$
end while

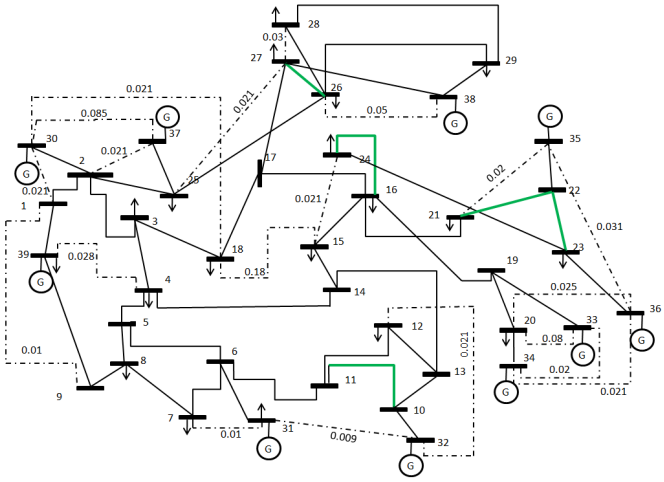

Fig. 3: The augmented 39-bus system used in our simulations. Our link additions to the system are depicted by dashed lines along with the corresponding reactance values. Links shown in green highlight the defender resource allocation for $k_a = 2$,

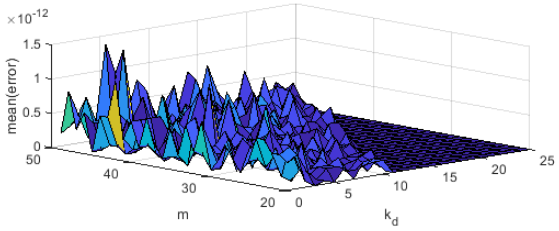

Fig. 4: The difference between v^* and the expected outcome of Algorithm 2 for the defender in 39 bus network. For a specific value of m and k_d, the average error has been computed over 10 different sets of ϕ's over 100 iterations ($i_t = 100$).

Figure 4 shows the difference between v^* and the outcome of the game for 39-bus network when the defender implements Algorithm 2. The difference is computed for several values of m and k_d ($k_a = 2$). For each value of m and k_d, Figure 4 depicts the average difference computed over 10 games with randomly chosen ϕ's after 100 iterations of Algorithm 2. From the figure, we can conclude that difference between the outcome of the game when the defender implements Algorithm 2 and v^* is of the order of 10^{-12} which is negligible. Figure 3 shows the covered links for 39-bus system when $k_a = 2, k_d = 5$.

VI. Conclusion

In this work, we formulate cyber-physical contingency analysis in power networks as an attacker-defender game. Leveraging structural properties of the power network and empirically proven near-modular behaviour of the impact metric, we propose a computationally efficient technique to obtain optimal deployment of cybersecurity measures under budget constraints. We believe that this work is a first-step towards alleviating the "curse of complexity" in N-k cyber-phyiscal contingency analysis. Currently, our examination of this problem does not take into account the possibility of cascading failures, islanding, or variable line capacities. Identification of structural properties of the system that could drastically reduce the computational complexity of cyber-physical contingency analysis involving (a) A wide range of impact metrics that also take into account economics of power generation and distribution; (b) Management of dynamic situations arising from high-impact high-frequency strategic attacks; (c) Attacks that incorporate cascading failures or disconnections of the grid; are aspects of the broader goal to direct future work.

References

[1] Y. Zhao, C. Yuan, G. Liu, and I. Grinberg, "Graph-based preconditioning conjugate gradient algorithm for n-1 contingency analysis," in *2018 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE, 2018, pp. 1–5.

[2] Y. Du, F. Li, J. Li, and T. Zheng, "Achieving 100x acceleration for n-1 contingency screening with uncertain scenarios using deep convolutional neural network," *IEEE Transactions on Power Systems*, vol. 34, no. 4, pp. 3303–3305, 2019.

[3] E. P. R. Coelho, M. H. M. Paiva, M. E. V. Segatto, and G. Caporossi, "A new approach for contingency analysis based on centrality measures," *IEEE Systems Journal*, vol. 13, no. 2, pp. 1915–1923, 2018.

[4] X. Li, P. Balasubramanian, M. Sahraei-Ardakani, M. Abdi-Khorsand, K. W. Hedman, and R. Podmore, "Real-time contingency analysis with corrective transmission switching," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 2604–2617, 2016.

[5] A. Ashok, M. Govindarasu, and J. Wang, "Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid," *Proceedings of the IEEE*, vol. 105, no. 7, pp. 1389–1407, 2017.

[6] S. Hasan, A. Ghafouri, A. Dubey, G. Karsai, and X. Koutsoukos, "Heuristics-based approach for identifying critical n-k contingencies in power systems," in *2017 Resilience Week (RWS)*. IEEE, 2017, pp. 191–197.

[7] R. L.-Y. Chen, A. Cohn, N. Fan, and A. Pinar, "Contingency-risk informed power system design," *IEEE Transactions on Power Systems*, vol. 29, no. 5, pp. 2087–2096, 2014.

[8] L. Che, X. Liu, Y. Wen, and Z. Li, "A mixed integer programming model for evaluating the hidden probabilities of n-k line contingencies in smart grids," *IEEE Transactions on Smart Grid*, vol. 10, no. 1, pp. 1036–1045, 2017.

[9] A. Bagheri and C. Zhao, "Distributionally robust reliability assessment for transmission system hardening plan under $n - k$ security criterion," *IEEE Transactions on Reliability*, vol. 68, no. 2, pp. 653–662, 2019.

[10] Q. Chen and J. D. McCalley, "Identifying high risk n-k contingencies for online security assessment," *IEEE Transactions on Power Systems*, vol. 20, no. 2, pp. 823–834, 2005.

[11] K. Sundar, C. Coffrin, H. Nagarajan, and R. Bent, "Probabilistic n-k failure-identification for power systems," *Networks*, vol. 71, no. 3, pp. 302–321, 2018.

[12] S. Poudel, Z. Ni, and W. Sun, "Electrical distance approach for searching vulnerable branches during contingencies," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 3373–3382, 2016.

[13] B. Hyder and M. Govindarasu, "Optimization of cybersecurity investment strategies in the smart grid using game-theory," in *2020 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. IEEE, 2020, pp. 1–5.

[14] H. Emadi and S. Bhattacharya, "On security games with additive utility," *IFAC-PapersOnLine*, vol. 52, no. 20, pp. 351–356, 2019.

[15] D. Bienstock and A. Verma, "The nk problem in power grids: New models, formulations, and numerical experiments," *SIAM Journal on Optimization*, vol. 20, no. 5, pp. 2352–2380, 2010.

[16] H. Emadi and S. Bhattacharya, "On the characterization of saddle point equilibrium for security games with additive utility," in *International Conference on Decision and Game Theory for Security*. Springer, 2020, pp. 21–32.

[17] S. Fujishige, *Submodular functions and optimization*. Elsevier, 2005.

[18] S. Soltan, A. Loh, and G. Zussman, "Analyzing and quantifying the effect of k-line failures in power grids," *IEEE Transactions on Control of Network Systems*, vol. 5, no. 3, pp. 1424–1433, 2017.