Albarakati and Bikdash
Applied Network Science (2022) 7:13
https://doi.org/10.1007/s41109-022-00451-5

Applied Network Science

RESEARCH Open Access

Empirical framework for identification of the most harmful malicious attacks on a smart grid

Aiman J. Albarakati[1*] and Marwan Bikdash[2]

*Correspondence:
a.albarakati@mu.edu.sa
[1] College of Computer and Information Science, Majmaah University, Majmaah, Saudi Arabia
Full list of author information is available at the end of the article

Abstract

The aim of this paper is the identification of the most harmful malicious attacks in a smart grid with basis on the removal of buses in a particular sequence. For that, we define the Electrical Most Damaging Element (EMDE) and the Iterated Centrality Measure (ICM). The EMDE is the element that leads to the largest unsatisfied load increase after removed, in the current state of the smart grid. The ICM is a meaningful scaled centrality for iterated attacks. Attack strategies such as the IEMDE (Iterated Electrical Most Damaging Element) and the Iterated Most Central Element (IMCE) are proposed as references for evaluating the impact of failure sequences by comparison. For each fault strategy approach, the vulnerability curves as well as a scalability analysis are presented. It is demonstrated that the IEMDE approximated the $N-k-\varepsilon$ algorithm, but with reduced computational expense. Furthermore, the IMCE approach provided an efficient fault profile close to the performance of the IEMDE. Although this framework is applied in this paper to failures in buses, it can similarly be applied to other elements. Future research will be focused in applying these concepts to transmission lines.

Keywords: Vulnerability assessment, Graph theory, Powergrid, Centrality measures, Matpower

Introduction

Electric energy supply systems are critical infrastructures interdependent with other essential systems such as water supply, telecommunications and the Internet. The lack of electricity for a prolonged time can lead to severe risks. Therefore, the event of a malicious attack aiming to damage the integrity of the electric power system represents a major concern for authorities in charge of security (Seger 2004; Parfomak 2004; Office of Technology Assessment 1979; Mijuskovic 2000). This has motivated the study of power systems' vulnerability, and in recent years many research works have been carried out in this field (Abedi et al. 2019; Mehrdad et al. 2018; Cuadra et al. 2015; He and Yan 2016).

In this context, researchers have developed vulnerability measures to bring new knowledge and tools for protecting the integrity of power systems. With the aim of identifying critical elements in the power grid, different centrality measures based on degree, closeness and betweenness have been proposed (Nasiruzzaman et al. 2011; Sun

et al. 2018; Bompard et al. 2010; Nasiruzzaman et al. 2012, 2012; Nasiruzzaman and Pota 2011); such measures can take into account the structure of the power grid, its power flow and impedance electrical properties. The impact of top buses removal from a power system with basis on centrality was studied in Nasiruzzaman et al. (2012), comparing topological centralities with electrical centralities. It was demonstrated that the impact of removing buses according to topological centralities is lower than the impact of doing it with basis on electrical centralities. In addition, when comparing electrical betweenness and closeness, the removal of nodes according to closeness caused a higher impact on the path length, while the removal according to betweenness produced a significant impact on the load supply capacity and the connectivity. The topological structure and the robustness of power grids were studied in Arianos et al. (2009), where the authors introduced the concept of net-ability and generalized the geodesic distance concept for power grids. It was evidenced that the influence of failures in lines according to net-ability corresponds with the DC power flow calculation of overload.

Additionally, research evaluating the impact of intentional attacks on power systems and how to mitigate it has been motivated by the threat of terrorism. Possible malicious attacks can be made through electromagnetic (Dehbaoui et al. 2009), informatics-based (Hawrylak et al. 2012), and physical means (Liu et al. 2013; David 2014); the targets of such attacks may also include different equipment of the power system in the areas of transmission, generation, control, monitoring and communications (National Research Council 2002). The location of the most of transmission and generation equipment represents a risk since they must be outdoors, accessible to malicious attacks (Agarwal et al. 2010; Bilis et al. 2013).

Although the current progress in the operation and design of power grids allows the improvement of their efficiency and profitability, it also increases their complexity and stress due to the incorporation of modern technologies and energy sources (National Research Council 2002; Kinney et al. 2005). Hence, it is important that the design of modern power systems includes considerations for reducing vulnerability, correctly addressing all the security concerns. Furthermore, the power grid must comply with requisites of adaptability, intelligence and robustness in front of ill-intentioned attacks (NIST 2010). That scenario, will not be achievable without the creation and improvement of tools to model and analyze the strategies for prevention and recovery from possible threats to the power grid (National Research Council 2002).

It has been evidenced that electric power systems are robust under traditional failures, but they may be vulnerable in front of targeted attacks (Salmeron et al. 2004; Duman et al. 2017). A systematic attack on susceptible areas of the electric power system may produce a cascade failure and a possible long-term blackout, if the traditional structure of the power grid is considered (National Research Council 2002). Researchers have addressed the impact of malicious attacks in the power system with different methods. For instance, using optimization to maximize the load shedding in a power grid (Salmeron et al. 2004; Arroyo and Galiana 2005), to identify the groups of elements that can cause a blackout (Chen et al. 2014, 2012), or to determine the expansion planning under deliberate attacks (Arroyo et al. 2010; Davarikia et al. 2020).

There are diverse approaches applied to determine the effects of ill-intentioned attacks over the power systems, some of them are: examination of historical records (Farrell

et al. 2004), fault tree analysis (Volkanovski et al. 2009), applications of game-theory to simulate possible attacks (Holmgren et al. 2007; Bompard et al. 2009, 2008; Jian et al. 2013; Piccinelli et al. 2017, Yuan and Zeng 2020), and identification of vulnerable elements and areas using complex network theory (Panigrahi 2017; Adebayo et al. 2018). Interdependent structures, such as the cyber network that monitors and controls the power system has been considered for vulnerability analysis as well (Guo et al. 2017; Vellaithurai et al. 2015; Zhang et al. 2019; Meyur 2020). Moreover, simulations that evaluate different defense strategies have been proposed (Rose 2007; Wang 2017; Ouyang et al. 2017).

Nevertheless, there is research field is still open for the development of a framework to analyze the impact of attacks and consequent failures in the power system. The research presented in this paper focuses on identifying deliberate attack sequences consisting of buses or transmission lines removals that produce the largest electrical damage measured as the extent of brownout damage. Identifying such sequences will be crucial for suggesting strategies to increase the robustness of the smart grid in front of such attacks.

Particular attention is paid to solutions that are computational efficient for a given state, because an accurate estimation of vulnerability is not independent of the current power flow and generation state of the grid. Efficiency is important because the number of possible and relevant grid states is very large. The contributions are the following:

1 Development of a framework based on the concept of relation between electrical damage and physical damage. This is an important tool for settling some key matters such as: (a) the most harmful attacks; (b) the most predictive centrality measure; (c) the most reliable physical damage measure; and (d) the vulnerability level of a grid compared to other.
2 Introduction and application of various malicious attack algorithms, namely the Iterated Electrical Most Damage Elements (IEMDE) and the Iterated Most Central Elements (IMCE).
3 Efficient identification of the most malicious attacks according to the framework of electrical damage versus physical damage.
4 Identification of the fastest methods for quantification of the most harmful attacks in terms of computational complexity.

Background

In this research, the estimation of unsatisfied load after each fault has been carried out using the simulation tool Matpower (Zimmerman et al. 2015). This is a high credibility package oriented to research and education based on MATLAB (http://www.mathworks.com/) for the solution of power flow and optimal power flow problems (with flexible options and different algorithms) among other functions.

The normalized ULTotal Unsatisfied LoadUnsatisfied Load (UL) represents the proportion of power demand not met by the available generation. This is similar to energy not-supplied (Hashemi-Dezaki et al. 2015) or load shedding measures (Correa and Yusta 2013). The UL for a particular fault profile, assuming the removal of the first k buses as part of the fault evolution, is calculated as

$$\mathrm{UL}(\beta(1:k)) = 1 - \sum_{n_i} \frac{\mathrm{PS}(n_i)}{\mathrm{PD}}, \tag{1}$$

where β denotes the vector of ordered buses of particular fault profile, in MATLAB notation $1:k$ is the vector of bus indices from 1 to k, PSSatisfied Power LoadPS(n_i) denotes the satisfied power load of island n_i formed after the removal of buses, and PDTotal Power DemandPD is the power demand of the whole system. A total blackout corresponds to an maximum level of unsatisfied load $\mathrm{UL}(N;\beta) = 1$, and may result after removing a limited set of elements, for instance removing all generators.

The fault profiles can be classified into two types: natural faults, due for instance to hurricanes, and malicious attacks. There is a variety of such attacks depending on the means (cyber vs. physical), extent geographically (local vs. global), and random versus targets. For random attacks, the elements are removed according to a typically uniform probability distribution. For targeted malicious attacks, it is assumed that the attackers might have information about the power grid such as the topological or electrical structure, electric features and system limitations. It is logical to assume that if the attackers have sufficient information about the power grid, the attacks could have a larger impact, as they could determine critical points of the network.

Attackers might access the information of topological structure through particular companies [e.g., Platts (Platts 2014)], and might estimate electric characteristics of components such as impedance using standard values and typical calculations. However, the tolerances of the system are hardly available and are difficult to be clearly known by attackers (Kinney et al. 2005; Wang and Rong 2009; Wang et al. 2011; Zhu et al. 2014). Therefore, attack strategies can be classified into those having access to the tolerance of the system and not having access to such tolerance. While the unknown system tolerance strategies are based on degree, load, risk of failure and load distribution vector, the known system tolerance strategies are based on percentage of failures and exhaustive search approach (Kinney et al. 2005; Wang and Rong 2009; Wang et al. 2011).

A popular centrality-based attack is the Remove Most Central Element First (RMCEFRemove Most Central Element FirstRMCEF) fault profile, where the attacker is assumed to have knowledge about a centrality score of the power grid's elements. In the RMCEF attack, centrality scores are computed using one of the standard techniques such as those in Eqs. (2)–(4) based on a a weighted or unweighted adjacency matrix that represents the structure of the grid. The buses are sorted according to their centrality scores from high to low and afterward they are removed according to such order.

There are 3 popular definitions of centrality:

$$\text{(Degree) } c_{Di} = \frac{\sum_j a_{ij}}{\sum_i \sum_j a_{ij}}, \tag{2}$$

$$\text{(Eigenvector) } c_{Ei} = \frac{1}{\lambda_{max}} \sum_{j=1}^{N} a_{ij} u_j, \tag{3}$$

$$\text{(Betweenness) } c_{Bi} = \sum_{j \neq k \neq i} \frac{\sigma_{jk}(i)}{\sigma_{jk}}, \tag{4}$$

where $\sum_j a_{ij}$ represents the sum of the weights from the links connected to node i, $\sum_i \sum_j a_{ij}$ is the sum all the elements of the adjacency matrix A, u_j is the jth element of the eigenvector of A corresponding to the largest eigenvalue λ_{max}, σ_{jk} is the number of shortest paths between nodes j and k, and $\sigma_{jk}(i)$ is the number of these shortest paths between j and k, passing through node i.

For a selected centrality, we denote with $c(i)$ the centrality calculated for node i, normalized to obtain $\sum_i c(i) = 1$. In this paper centralities are based in Power Traffic Matrix (PTM) which is the weighted adjacency matrix with weights that represent the active power flow on each link of the power grid. Other measures have been proposed in Cuadra et al. (2015).

Framework

The discussion about the methods to assess the vulnerability of power systems has been extensive in the last decade. Important part of the research has been dedicated to study the physical damage on power grids, by accounting it through different metrics related to their physical structure such as degree clustering coefficient (Albert et al. 2004), average path length (Albert et al. 2004), degree centrality (Bilis et al. 2013) and size of attack (Brummitt et al. 2012). On the other hand, several research works have studied the electrical damage, using metrics such as loss of power (Martinez-Anido et al. 2012), load shedding (Correa and Yusta 2013) and energy not supplied (Martinez-Anido et al. 2012). Nevertheless, few have taken into consideration both physical and electrical damages on the power grid (Correa and Yusta 2013; Bilis et al. 2013; Mei et al. 2011).

The distinction between physical damage measures and electrical damage measures is essential to settle criteria for vulnerability assessment in power systems. The measures of physical damage intend to characterize the size of the attacks by accounting the elements or the structural connections affected, while the electrical damage measures are related to the effect over the electrical performance of the power grid. The concept of vulnerability in essence attempts to measure the degradation of the performance depending on the size of the attack. For instance, an exceptionally robust grid can withstand severe physical damage presenting very low degradation in electrical performance.

In this sense, the proposed framework integrates physical damage and electrical damage measures with the aim of clearly and unambiguously defining: (a) the most harmful attack; (b) the most predictive centrality measure; (c) the most reliable measure of physical damage; and (d) the vulnerability level of a grid compared to other.

Figure 1 is presented as an illustration of this approach. To define the curve $\mathcal{C}_0$ for a particular power system, the procedure consists in designing an attack sequence by selecting a measure of physical damage, a fault profile, and a measure of electrical damage. Once the attack sequence is designed, the electrical damage is measured using an simulation. For example, we can select NOE as physical damage measure, UL as electrical damage measure and an attack profile based in RMCEF, then use an empirical simulation of DC power flow or cascading failures to determine the electrical damage measures for the attack profile.

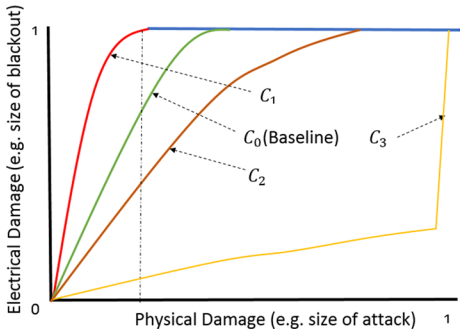


Fig. 1 Illustration of the framework

In this manner, different power grids, damage measures and fault profiles according to centrality measures can be compared using a vulnerability curve. In Fig. 1, the vulnerability curve $\mathcal{C}_1$ is higher than the baseline curve $\mathcal{C}_0$, depending on the whole attack design, we can obtain relevant information from these curves:

(a) Assuming that $\mathcal{C}_1$is the a vulnerability curve for grid A, and $\mathcal{C}_0$ is determined for grid B with the same attack design, it can be concluded that the grid B is less vulnerable than the grid A, because a similar physical damage produces a lower electrical damage in the grid of B.

(b) If we consider that $\mathcal{C}_1$ was obtained with a different fault profile than $\mathcal{C}_0$, it implies that this attack profile is more harmful.

(c) Considering that $\mathcal{C}_2$ or C_3 was obtained like $\mathcal{C}_0$, but with a different measure of physical damage implies that such measure is potentially more unreliable, because it appears that more intense attacks (according to physical damage) are required to obtain an equivalent electrical damage.

(d) And, if we assume that $\mathcal{C}_1$ in the same way that $\mathcal{C}_0$, but the electrical damage is measured through a different empirical simulation, then it is evident that such simulation exposes more vulnerabilities in the power grid than the one applied for calculating $\mathcal{C}_0$.

In general, the increment on the VPM is a quantitative measure of the degradation of robustness of the grid.

Proposed attack profile

Two different types of malicious attack profiles are introduced and described in this section.

Iterated attack based on the most central element (IMCE)

The IMCE is introduced as an attack in which the element with the highest centrality in the current grid is attacked and removed. The main feature is that the centrality score is recalculated after the removal of an element. The idea under this attack profile is that the centrality measures change after the removal of the most central element (MCE), thus the second most central element in the initial ranking may not be the most central once the MCE is removed. Then the vector of centralities must be recomputed to obtain the new ranking of elements according to centrality.

For this matter, we define a sequence of grids as $\Gamma^0, \Gamma^1, \Gamma^2, \ldots, \Gamma^N$ where Γ^i is the resulting grid from the removal of the MCE in the grids Γ^{i-1}. Also, $\zeta_j(\Gamma^i)$ is the centrality score of the element j in the grid Γ^i, and e_i represents the index of the MCE of such grid, as follows

$$e_i = \text{MCE}(\Gamma^i) = \text{argmax}_j(\zeta_j(\Gamma^i)). \tag{5}$$

Furthermore, the value of centrality is denoted as z_i, as follows

$$z_i = \zeta_{e_i}(\Gamma^i) \tag{6}$$

And the subsequent grid, in the corresponding sequence, is defined as

$$\Gamma^{i+1} = \Gamma^i - \{e_i\}. \tag{7}$$

It is noted that $\zeta_j(\Gamma^i)$ is not normalized, thus it is necessary to determine a normalized centrality vector, given by

$$Z_i = \left(1 - \sum_{j<i} z_j\right) z_i \tag{8}$$

This is called the Iterated Centrality Measure (ICM), considered the most meaningful scaled centrality generated by the IMCE,

$$\boldsymbol{Z} = [Z_1, Z_2, \ldots]. \tag{9}$$

In the case that a collapse happens at an iteration $i = \ell$, or in case that the attack ends at $i = \ell$, the centrality of the remaining elements is equal to the so far unassigned centrality. That is,

$$Z_{\ell+1} = Z_{\ell+2} = \cdots = \frac{1}{N - \ell + 1} \sum_{i=1}^{\ell} Z_i. \tag{10}$$

For a better physical interpretation of the proposed centrality Z_i, it is wanted that it is a monotonically decreasing sequence. In this sense, it can be demonstrated that the 1-norm of the sequence is equal to one by construction, i.e., $\|\boldsymbol{Z}\|_1 = \sum_j Z_j = 1$. This means that the sum of centralities is equal to one, and they are almost monotonically decreasing without the need of applying any sorting. Algorithm 1 presents a pseudo-code that describes the proposed approach to find the removed elements, the unsatisfied load, and the corresponding ICM.

Algorithm 1: Algorithm for IMCE attacks

- Initialize Grid to IEEE baseline
  - while Grid is not collapsed. z@
    - calculate the centrality and find the MCE
    - find the damage done by removing MCE using Matpower
    - update the Grid
- return MCEs and the corresponding ULs

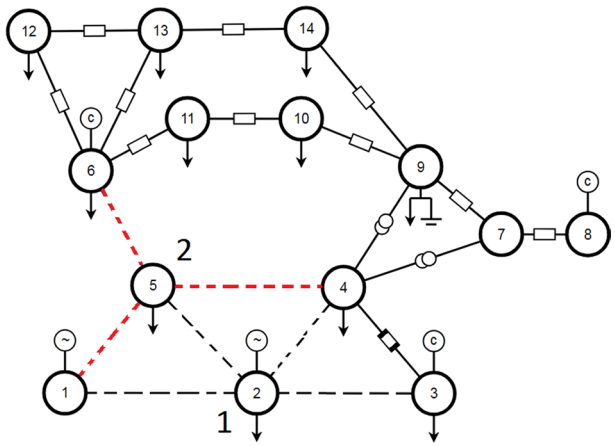


Fig. 2 IEEE 14-bus power system representation of the IMCE fault profile The transmission lines disconnected after the removal of buses are identified (dashed lines)

Table 1 Buses removed under the ICME according to different centrality measures

IEEE 300 Bus			IEEE 118 Bus		
Deg.	**Eig.**	**Bet.**	**Deg.**	**Eig.**	**Bet.**
109	3	78	9	9	77
3	167	81	49	5	68
116	109	31	5	38	19
98	98	86	89	49	12
210	112	38	69	89	15
36	170	54	38	30	49
167	36	36	30	69	30
170	210	109	30	64	37
20	144	190	25	25	100
2	160	198	59	59	23
160	20	194	64	68	96
...	...	...	...	...	...

In order to exemplify the IMCE previously described, the IEEE 14-bus test power system is employed. In terms of the degree centrality, the bus 2 is the most central, with a normalized degree score equal to 0.25. That bus is removed, and the modified grid Γ^1 that is shown in Fig. 2 is obtained (the black dashed lined represents the links that are removed as consequence of removing bus 2). Then, the degree centrality score is recalculated for such grid, resulting that the most central bus is the bus 5, with a normalized degree score equal to 0.20. Therefore, it corresponds to remove such bus, leading to the new grid Γ^2, as shown in Fig. 2 (the red dashed lines represent the links that are removed when bus 5 is attacked). In Table 1 the initial sequences of buses removed under IMCE using different centrality measures are presented for the IEEE 118-bus system and the IEEE 300-bus system, and it is noted that the sequences are different for different centrality measures.

Furthermore, we suppose for instance, that collapse occurs after removing two buses. Then,

$$\begin{aligned} Z_1 &= z_1 \\ Z_2 &= (1 - z_1)z_2 \end{aligned} \tag{11}$$

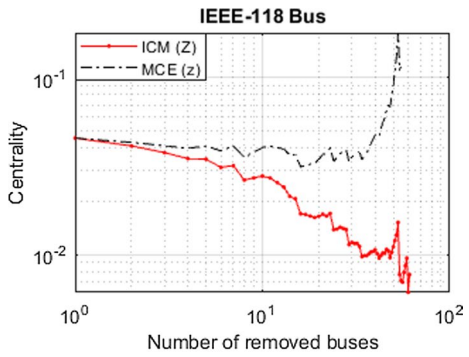
and the next Z scores are determined as

$$Z_3 = Z_4 = \cdots = \frac{1}{14-2}\left(1 - \sum_{i=1}^{2} Z_i\right). \tag{12}$$

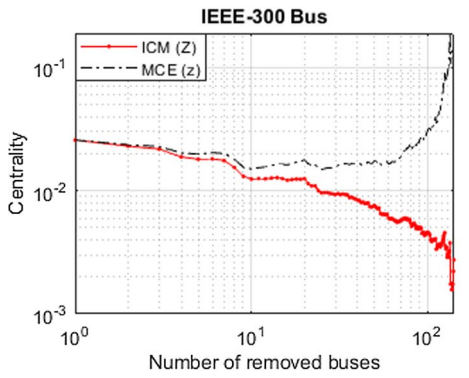
Therefore, we obtain

$$\sum_{i=1}^{14} Z_i = Z_1 + Z_2 + 12\left[\frac{1-(Z_1+Z_2)}{12}\right] = 1. \tag{13}$$

where it is noted that Z_i are not sorted in this equation. Figure 3 shows the logarithm of the ICM for the IEEE test power grids of 118 and 300 buses, where it is observed to be monotonically decreasing.



(a) IEEE 118-bus system



(b) IEEE 300-bus system

Fig. 3 Logarithm of degree centrality with basis on ICM (red) and MCE (black)

Iterated attack based on the electrical most damaging element (IEMDE)

The IEMDE is defined in this work as an attack that is based in the removal of the element that generates the largest raise in the UL of the power grid in the current state. The iterated attack generates a sequence of grids in which the electrical most damaging element (EMDE) is removed, such sequence is $\tilde{\Gamma}^0, \tilde{\Gamma}^1, \tilde{\Gamma}^2, \ldots, \tilde{\Gamma}^N$, where $\tilde{\Gamma}^i$ is the resulting grid after the removal of the EMDE of $\tilde{\Gamma}^i$. That means,

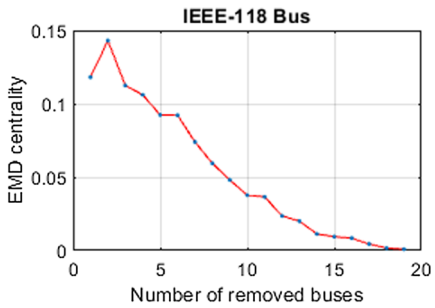
$$\tilde{\Gamma}^i = \tilde{\Gamma}^{i-1} - \text{EMDE}(\tilde{\Gamma}^{i-1}) \tag{14}$$

and the iterated EMD centrality is

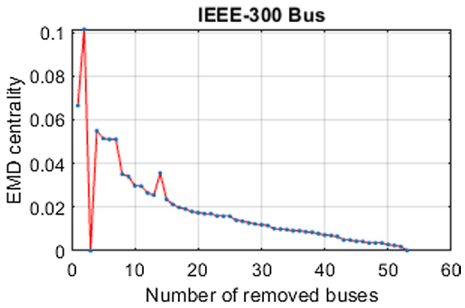
$$\tilde{z}_i = \text{UL}(\tilde{\Gamma}^i) - \text{UL}(\tilde{\Gamma}^{i-1}). \tag{15}$$

In the same way that for the IMCE, we observe that $\|\boldsymbol{z}\|_1 = \sum_j z_j = 1$. Figure 4 shows how these centrality scores are almost monotonically decreasing for the IEEE 118-bus and 300-bus test power systems.

Algorithm 2 illustrates the proposed approach for computing the IEMDE using pseudo-code. Also, as an example of the application of this approach, we employed the IEEE 14-bus test grid. When the Algorithm 2 is applied, we obtain the sequence of EMDE's [3, 4, 5, 1], which are the buses to remove until the grid collapses. The grid is shown in Fig. 5, and the links removed for the IEMDE are denoted with dashed lines.



(a) IEEE 118-bus system



(b) IEEE 300-bus system

Fig. 4 Proposed iterated EMD centrality

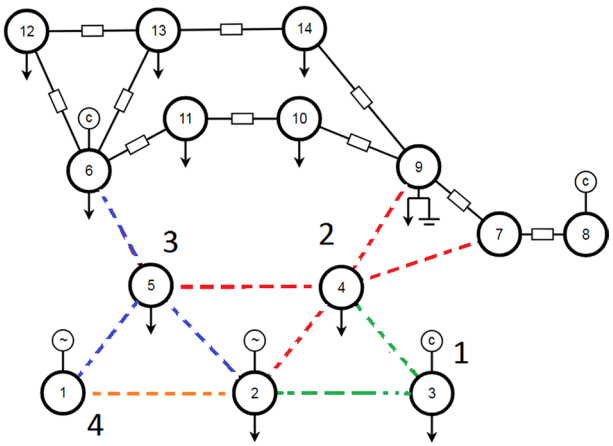


Fig. 5 IEEE 14-bus test grid applying the EMDE failure sequence [3, 4, 5, 1]. The dashed lines are the links (transmission lines) disconnected after the removal of the EMDEs

Table 2 Initial buses removed corresponding to the EMDE for IEEE 118-bus and IEEE 300-bus test systems

IEEE 118			IEEE 300		
EMDE	**UL**	$\tilde{z}$	**EMDE**	**UL**	$\tilde{z}$
69	0.118	0.118	170	0.066	0.066
89	0.261	0.143	98	0.174	0.108
80	0.374	0.113	109	0.230	0.056
8	0.480	0.106	3	0.281	0.051
66	0.572	0.092	166	0.332	0.051
65	0.664	0.092	165	0.375	0.043
26	0.738	0.074	216	0.410	0.035
100	0.798	0.060	217	0.444	0.034
49	0.846	0.048	118	0.474	0.030
61	0.883	0.037	122	0.503	0.029
59	0.920	0.037	2	0.530	0.027
25	0.944	0.024	213	0.555	0.025
12	0.964	0.020	210	0.591	0.036
54	0.975	0.011	141	0.615	0.024
...	...		...	...	

Algorithm 2: The Algorithm for IEMDE attack

- while Grid is not collapsed
  - iterate over remaining buses in Grid z@
    - determine the damage done by removing bus using MatPower
  - identify the MDE for this Grid
  - remove MDE and update the Grid
- return MDE's and the corresponding UL's for each stage

In addition, the IEMDE malicious fault profile was applied to the IEEE 118-bus and the IEEE 300-bus systems, and the initial sequence of EMDE's are shown in Table 2. It is

noted that the removal of each of these elements leads to an important increment in the UL, and the EMDE ($\tilde{\Gamma}^0$) produces the highest $\tilde{z}$.

The framework proposed here has been though for attacks on buses, lines, or combination of both. To illustrate this, Table 3 shows the transmission lines that generate the highest damage for the IMDE applied to the IEEE 300-bus system. It is noted that the first EMDE does not present the largest value of $\tilde{z}$, in fact $\tilde{z}_1 = 0.0375 < \tilde{z}_7 = 0.0585$, which matches with our intuition. In this sense, it is expected that the grid is initially strong and able to tolerate the failure of one element, but as the grid losses elements it becomes more vulnerable. That explains why, in the sixth stage of the IMDE with the removal of the corresponding EMDE a higher impact is obtained.

The attack profiles IMCE and IEMDE proposed here are somewhat similar to the one considered in Zhu et al. (2014) with an approach on sequential cascading failures. In that work, all possible attack sequences are considered and the Sequential Attack Graph is constructed from them. Nevertheless, one limitation of such proposal is the huge amount of cascading failures to consider, for example, the analysis of the IEEE 30-bus system requires the simulation of about 24,000 cascading failures.

Comparing various attack profiles

In the following, the Vulnerability Prediction Measure (VPM) is revised for the fault profiles with the algorithms described in Section Propsed Attack Profiles. Furthermore, several attack strategies are compared using this approach.

Analyzing the vulnerability curve and VPM of the fault strategies

The vulnerability curves resulting of the IMCE attack applied to the different test power grids and for every centrality measure selected are presented in Fig. 6. It is noted that the curves for eigenvector centrality and degree centrality are very close to each other and both present higher values of unsatisfied load than the betweenness centrality. This agrees with VPM scores shown in Table 4, which are very similar for the eigenvector and

Table 3 Transmission lines from low to high MDE, and their UL determined with Matpower

EMDE	(From, to)	UL	$\tilde{z}$
400	(263,109)	0.0375	0.0375
404	(264,118)	0.0569	0.0194
405	(251,12)	0.0866	0.0297
406	(252,17)	0.1024	0.0158
407	(255,33)	0.1165	0.0141
408	(259,49)	0.1377	0.0212
394	(249,3)	0.1962	0.0585
410	(258,48)	0.1962	0
411	(262,59)	0.1981	0.0019
395	(260,53)	0.2295	0.1971
396	(261,54)	0.2465	0.017
397	(265,145)	0.2635	0.017
398	(254,23)	0.2870	0.0235
...	...	...	...

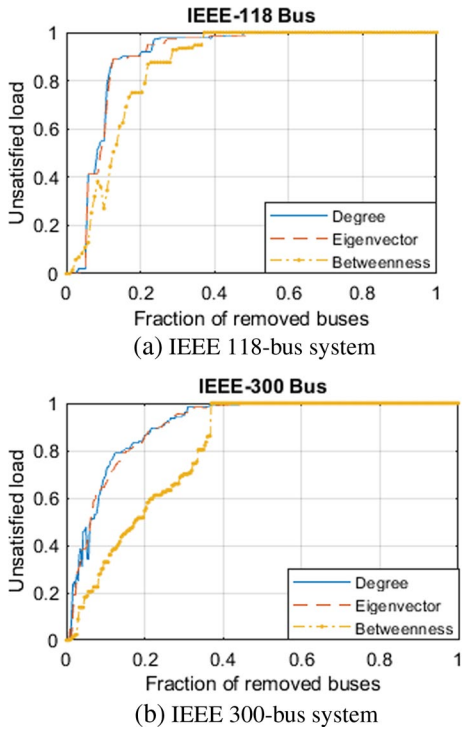


Fig. 6 Vulnerability curves for the IMCE fault profile based on PTM centralities and fraction of removed elements (FOE)

Table 4 Comparison of VPM scores using PTM centralities under IMCE malicious attack

IEEE system	Centrality	VPM score
	Deg	0.900
118	Eig	0.897
	Bet	0.849
	Deg	0.905
300	Eig	0.905
	Bet	0.807

degree centrality. This also implies that the IMCE attack under such centralities is more damaging than under the betweenness, in fact the removal of approximately a third of the elements leads to a complete blackout.

For the IEMDE attack profile, the vulnerability curves corresponding to the test systems is shown in Fig. 7. These curves are steeper compared to the ones from IMCE attack, indicating the severity of the IEMDE, and this is confirmed with the VPM scores in Table 5, which are higher than the ones in Table 5. The IEMDE profile in the studied power grids leads to a blackout after the removal of less than the 20% of the buses.

The IEMDE, compared to other attacks in this research, is the most severe, except for fault sequences identified by the $N-k-\epsilon$ algorithm. Therefore, this attack profile (IEMDE) can be employed as a reference for comparison in order to test the harm intesity of different attack profiles.

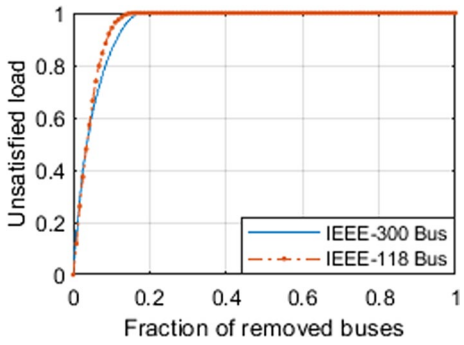


Fig. 7 Vulnerability curves produced by the IEMDE fault profile for IEEE 118-bus and IEEE 300-bus systems

Table 5 Results of VPM for the EMDE attack

IEEE system	VPM
30	0.942
57	0.927
118	0.958
300	0.954

Comparison of attack profiles based on the vulnerability curve and the VPM

This section presents a comparison between the attack profiles proposed in this work (IMCE and IEMDE), the Remove Most Central Element First (RMCEF) attack and the worst case random (WCR) attack. Here, the random attacks strategy is implemented through a Monte Carlo simulation consisting in the removal of a permutation of buses on each realization and the measurement of the corresponding unsatisfied load. The VPM is calculated for each random sequence (permutation) after the removal of every bus, and the WCR denotes the scenario with the highest VPM of all the realizations (400 realizations were performed).

Several observations are made from the vulnerability curves corresponding to the aforementioned attack strategies (Fig. 8): (a) IEMDE attack produces the steepest vulnerability curve in comparison with RMCEF, WCR and IMCE, (b) IEMDE attack vulnerability curve is smoother than the rest, (c) IMCE curve is close to the IEMDE curve, and (d) for larger grids (IEEE 300-bus), the vulnerability curves are more predictable and have less abrupt variations.

In Table 6 the VPM scores for the different attack strategies simulated are presented. The attack profiles that consider centrality measures are based in PTM centralities and may not hold for other centralities. The results show that the VPM for the IMCE attack with basis on PTM degree centrality is similar to this score with basis on PTM eigenvector centrality for both IEEE systems studied. Therefore, given such similarity, it is preferable to use the degree centrality as it is less complex to calculate.

The results for the PTM degree centrality RMCEF show VPM scores of 0.891 and 0.854 for IEEE-118 and IEEE-300 respectively. These are not far from the VPM scores obtained for the IMCE (0.900 and 0.905 respectively) and for the IEMDE (0.958 and 0.954 respectively). Then, the RMCEF fault profile with degree centrality provides good

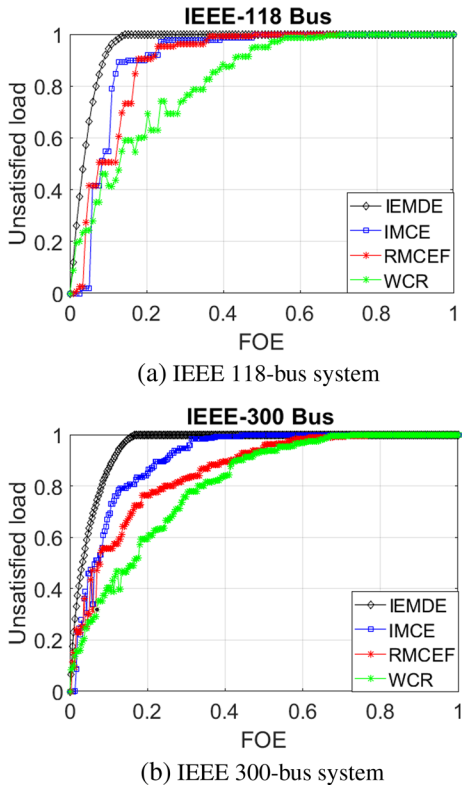


Fig. 8 Vulnerability curves for different attack strategies: IEMDE, WRC, IMCE (for PTM degree) and RMCEF (for PTM degree) performed

Table 6 Comparison of the VPM for the different attack profiles under consideration

IEEE system	Centrality	WCR	RMCEF	IMCE	IEMDE
118	Deg	0.769	0.891	0.900	
	Eig	0.744	0.582	0.897	0.958
	Bet	0.756	0.738	0.849	
300	Deg	0.771	0.854	0.905	
	Eig	0.761	0.632	0.905	0.954
	Bet	0.773	0.660	0.807	

understanding about the most damaging elements on the system. Nevertheless, the scores obtained with RMCEF under PTM betweenness and eigenvector are considerably lower and do not bring such information.

In addition, the VPM scores corresponding to the IEMDE attack profile for the IEEE-118 bus and the IEEE-300 systems are comparable. This happens also in the scores for the IMCE attack with PTM degree and the fraction of removed elements (FOE).

Alignment with the IEMDE sequence

It is important to introduce a procedure to compare two attack profiles to determine the most damaging sequence. In this section, we propose the Attack Sequence Misalignment (ASM) measure computation as a method to find the similarity between two

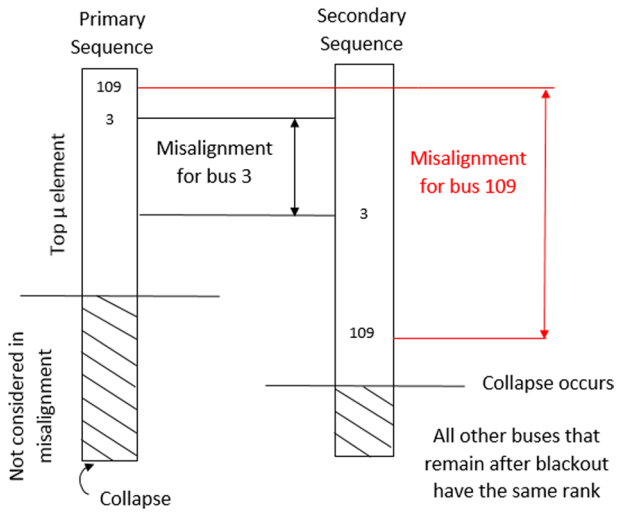


Fig. 9 Explanation of the ASM application between two fault sequences

Table 7 Calculated ASM for IEEE test systems considered with primary sequence IEMDE

	IEEE-118 IEMDE	**IEEE-300 IEMDE**
IMCE$_D$	6.03	15.15
IMCE$_E$	6.08	16.25
IMCE$_B$	7.68	23.04
RMCEFF$_D$	6.29	18.56
RMCEFF$_E$	7.42	21.65
RMCEFF$_B$	7.73	23.44

different attack profiles. Considering two sequences of elements removed, the difference in the location of an element in both sequences is determined. Such difference is averaged over the top elements in what is defined here as the primary sequence. The IEMDE sequence is the primary sequence of the most elements. This is needed because of the electrical collapse after the most damaging elements are removed. Figure 9 exemplifies this concept.

Note that for IEEE-118 Bus the ASM shows 5.90 for the IEMDE as a primary sequence , and IMCE$_D$ as a secondary sequence. The calculation of ASM was performed for attack profiles IMCE and RMCEF with different centralities leading to Table 7. Results show that the most similar sequence compared with the IEMDE is the IMCE with degree centrality followed by the IMCE with eigenvector centrality. While the IMCE and RMCEF fault profiles according to betweenness centrality presented the worst ASM.

Computational cost of attacks

In the subsequent, the time complexity of the proposed attack strategies is discussed. The least complex algorithm from the ones studied in this research is the RMCEF as it is not iterative to determine the elements to remove. The proposed algorithms and

the $N-k-\epsilon$ approach are shown in Fig. 10 in order of time complexity, from the lower to the highest.

Newton–Raphson power flow calculation is one of the most costly operations performed. Regarding the time complexity of the Newton–Raphson solution for the power flow, it has been demonstrated that for a sufficiently close initial point, it converges with a quadratic rate. The execution time and the convergence of the AC power flow with Newton–Raphson depends on different aspects such as the number of buses of the grid, its structure and the initial values selected for the unknown variables. For a fully connected system with N buses it converges approximately in $O(N^3 \log N)$. Nevertheless, the solution of AC power flow with Matpower uses the sparsity of power systems to improve such complexity to $O(N)$.

If the time complexity of the proposed fault strategies is evaluated in function of the power flow calculation as an elemental operation, then RMCEF entails only one power flow computation and one centrality computation, thus its complexity is $O(N)$. It is noted also, that IMCE requires the calculation of N times the power flows, and N times the centralities of the system. Furthermore, the IEMDE complexity is $O(N^2/2)$ as it requires the calculation of power flows N^2 times. And the Monte-Carlo simulation of random failure sequences for n realizations will require the computation of n power flows.

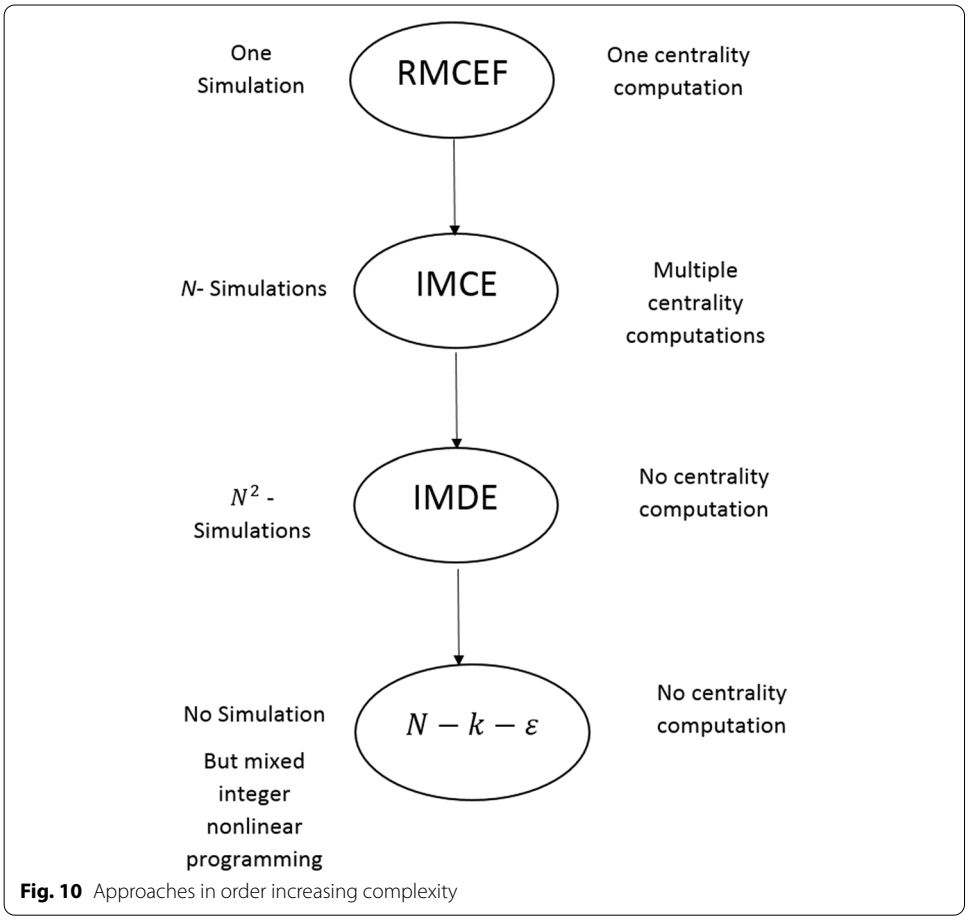


Fig. 10 Approaches in order increasing complexity

Comparing the results of execution time from the proposed attack strategies with the results replicated from Chen et al. (2014) with the application of the $N-k-\varepsilon$ strategy, it is noted that the proposed algorithms present lower execution times in terms of scaling. This is shown in Fig. 11, where the $N-k-\varepsilon$ algorithm executes in $O(N^3)$ approximately, which is more time expensive than the proposed algorithms.

Conclusions

This research presents an empirical framework for identifying and analyzing malicious attacks according to the impact in the power system. Concepts such as the ICM(z), the EMDE, and the ASM, which help to define and compare the most harmful attacks, are introduced. Moreover, the attack strategies IMCE and IEMDE are proposed for evaluating the impact of failure sequences by comparison.

The main contribution of this research was the identification of the malicious attack strategies that are more harmful for a smart grid by the removal of a sequence of its buses. As a result of the comparison of different attack profiles using the IEEE 118 bus and 300 bus test systems and the proposed framework, it is demonstrated that the IEMDE attack is the most harmful attack strategy, in terms of the VPM. This attack strategy presented a higher VPM than the WCR, the RMCEF attack and the IMCE attack sequences, and represents an approximation to the the $N-k-\varepsilon$ attack strategy with a lower computational effort.

In addition, it is shown that the IMCE attack strategy with degree and eigenvector PTM centralities are the most similar to the IEMDE fault profile. This means that such attack strategies can be useful for predicting harmful attacks with a reduced computational complexity.

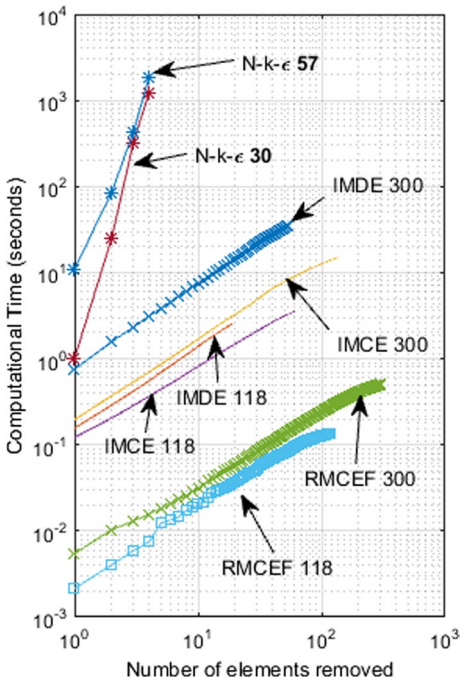


Fig. 11 Comparing the running time versus number of elements removed

Although this approach is applied here to failures in buses, it can be also implemented to failures in different elements of the power grid. Future research will be focused in applying these concepts to transmission lines.

Abbreviations

EMDE: Electrical most damaging element; ICM: Iterated centrality; MCE: most central element Measure; PD: Total power demand; PS: Satisfied power load; RMCEF: Remove most central element first; UL: Total unsatisfied load.

Authors' contributions

AA and MB conceived, designed and carried out the research, AA carried out the simulations, AA wrote the manuscript MB supervised the research. Both authors read and approved the final manuscript.

Availability of data and materials

The data set used in this article is available in the cited references.

Author details

[1]College of Computer and Information Science, Majmaah University, Majmaah, Saudi Arabia. [2]Computational Data Science and Engineering, North Carolina A&T state University, Greensboro, NC, USA.

Received: 23 July 2020 Accepted: 1 March 2022
Published online: 14 March 2022

References

Abedi A, Gaudard L, Romerio F (2019) Review of major approaches to analyze vulnerability in power system. Reliab Eng Syst Saf 183:153–172

Adebayo I, Jimoh A, Yusuff A (2018) Techniques for the identification of critical nodes leading to voltage collapse in a power system. Int J Emerg Electr Power Syst 19(2):1–14

Agarwal PK, Efrat A, Ganjugunte SK, Hay D, Sankararaman S, Zussman G (2010) Network vulnerability to single, multiple, and probabilistic physical attacks. In: Proceedings of the military communication conference, San Jose, CA, USA, pp 1824–1829

Albert R, Albert I, Nakarado GL (2004) Structural vulnerability of the North American power grid. Phys Rev E 69:4

Arianos S, Bompard E, Carbone A, Xue F (2009) Power grids vulnerability: a complex network approach. Chaos 19:013119

Arroyo JM, Galiana FD (2005) On the solution of the bilevel programming formulation of the terrorist threat problem. IEEE Trans Power Syst 20(2):789–797

Arroyo JM, Alguacil N, Carrion M (2010) A risk-based approach for transmission network expansion planning under deliberate outages. IEEE Trans Power Syst 25(3):1759–1766

Bilis EI, Kroger W, Nan C (2013) Performance of electric power systems under physical malicious attacks. IEEE Syst J 7(4):854–865

Bilis EI, Kroger W, Nan C (2013) Performance of electric power systems under physical malicious attacks. IEEE Syst J 7(4):854–865

Bompard E et al (2009) Risk assessment of malicious attacks against power systems. IEEE Trans Syst Man Cybern A Syst Hum 39(5):1074–1085

Bompard E, Napoli R, Xue F (2008) Vulnerability of interconnected power systems to malicious attacks under limited information. Eur Trans Electr Power 18(8):820–834

Bompard E, Wu D, Xue F (2010) The concept of betweenness in the analysis of power grid vulnerability. In: Proceedings of the complexity engineering, Rome, Italy, pp 52–54

Brancucci Martinez-Anido C, Boladoa R, De Vriesb L, Fulli G, Vandenbergh M, Masera M (2012) European power grid reliability indicators, what do they really tell? Electr Power Syst Res 90:79–84

Brummitt CD, DaSouza RM, Leicht EA (2012) Suppressing cascades of load in interdependent networks. Proc Natl Acad Sci 109(12):E680–E689

Chen RL, Cohn A, Fan N, Pinar A (2012) "$N - k - \varepsilon$" survivable power system design. In: Proceedings of the international conference on probability methods applied to power systems, pp 459–464

Chen R, Cohn A, Fan N, Pinar A (2014) Contingency-risk informed power system design. IEEE Trans Power Syst 29(5):2087–2096

Correa GJ, Yusta JM (2013) Grid vulnerability analysis based on scale-free graphs versus power flow models. Electr Power Syst Res 101:71–79

Cuadra L, Salcedo-Sanz S, Del Ser J, Jimenez-Fernandez S, Geem ZW (2015) A critical review of robustness in power grids using complex networks concepts. Energies 8(9):9211–9265

Davarikia H, Barati M, Al-Assad M, Chan Y (2020) A novel approach in strategic planning of power networks against physical attacks. Electr Power Syst Res 180:106140

David JE (2014) Double threat: *US grid vulnerable on two fronts*. http://www.cnbc.com/

Dehbaoui A, Lomne V, Maurine P, Torres L, Robert M (2009) Enhancing electromagnetic attacks using spectral coherence based cartography. In: Presented at the international conferenec, VLSI (VLSI-SoC), Florianopolis, Brazil

Duman O, Zhang M, Wang L, Debbabi M (2017) Measuring the security posture of IEC 61850 substations with redundancy against zero day attacks. In: IEEE international conference on smart grid communications (SmartGridComm), pp 108–114

Farrell AE, Zerriffi H, Dowlatabadi H (2004) Energy infrastructure and security. Annu Rev Environ Resour 29:421–469

Guo J, Han Y, Guo C, Lou F, Wang Y (2017) Modeling and vulnerability analysis of cyber-physical power systems considering network topology and power flow properties. Energies 10(1):87
Hashemi-Dezaki H, Askarian-Abyaneh H, Haeri-Khiavi H (2015) Reliability optimization of electrical distribution systems using internal loops to minimize energy not-supplied (ENS). J Appl Res Technol 13(3):416–424
Hawrylak PJ, Haney M, Papa M, Hale J (2012) Using hybrid attack graphs to model cyber-physical attacks in the smart grid. In: Proceedings of the 5th international symposium on resilient control systems, Salt Lake City, UT, USA, pp 161–164
He H, Yan J (2016) Cyber-physical attacks and defences in the smart grid: a survey. IET Cyber-Phys Syst Theory Appl 1(1):13–27
Holmgren AJ, Jenelius E, Westin J (2007) Evaluating strategies for defending electric power networks against antagonistic attacks. IEEE Trans Power Syst 22(1):76–84
Jian Z, Shi L, Yao L, Masoud B (2013) Electric grid vulnerability assessment under attack-defense scenario based on game theory. In: IEEE PES Asia–Pacific power and energy engineering conference (APPEEC), pp 1–5
Kinney R, Crucitti P, Albert R, Latora V (2005) Modeling cascading failures in the North American power grid. Eur Phys J B 46:101–107
Liu X, Ren K, Yuan Y, Li Z, Wang Q (2013) Optimal budget deployment strategy against power grid interdiction. In: Proceedings of the IEEE INFOCOM, Turin, Italy, pp 1160–1168
MATLAB. http://www.mathworks.com/
Mehrdad S, Mousavian S, Madraki G, Dvorkin Y (2018) Cyber-physical resilience of electrical power systems against malicious attacks: a review. Curr Sustain Energy Rep 5(1):14–22
Mei S, Zhang X, Cao M (2011) Power grid complexity. Springer
Meyur R (2020) A Bayesian attack tree based approach to assess cyber-physical security of power system. In: 2020 IEEE Texas power energy conference, TPEC 2020, pp 1–6
Mijuskovic N (2000) Serbia restoration after war damages May-99. Presented at the CIGRE Session, SC 39 workshop on large disturbances
Nasiruzzaman ABM, Pota HR, Anwar A (2012) Comparative study of power grid centrality measures using complex network framework. In: IEEE international power engineering and optimization conference Melaka, Malaysia, pp 176–181
Nasiruzzaman ABM, Pota HR, Mahmud MA (2011) Application of centrality measures of complex network framework in power grid. In: IECON 2011—37th annual conjerence on IEEE industrial electronics society, pp 4660–4665
Nasiruzzaman ABM, Pota HR, Mahmud MA, Islam F (2012) Modified centrality measure based on bidirectional power flow for smart and bulk power transmission grid. In: Proceedings of the 2012 IEEE international power engineering and optimization conference (PEDCO), Melaka, Malaysia, 6–7 June 2012, pp 159–164
Nasiruzzaman ABM, Pota HR (2011) Transient stability assessment of smart power system using complex networks framework. In: IEEE power and energy society general meeting, San Diego, CA, pp 1–7
Nasiruzzaman ABM, Pota HR, Barik MA (2012) Implementation of bidirectional power flow based centrality measure in bulk and smart power transmission systems. IEEE PES Innovative Smart Grid Technologies, pp 1–6
National Research Council (2002) Making the nation safer: the role of science and technology in countering terrorism. National Academies Press
NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0. NIST Special Publication 1108, January 2010. http://www.nist.gov/public_affairs/releases/smartgrid_interoperability_final.pdf
Office of Technology Assessment (1979) The effects of nuclear war. U.S. Congress
Ouyang M, Xu M, Zhang C, Huang S (2017) Mitigating electric power system vulnerability to worst-case spatially localized attacks. Reliab Eng Syst Saf 165(February):144–154
Panigrahi P (2017) Vulnerability analysis of weighted Indian power grid network based on complex network theory. In: 2017 14th IEEE India council international conference (INDICON), pp 1–6
Parfomak PW (2004) Pipeline security: an overview of federal activites and current policy issues. Congressional Research Service, Rep. RL31990
Piccinelli R, Sansavini G, Lucchetti R, Zio E (2017) A general framework for the assessment of power system vulnerability to malicious attacks. Risk Anal 37(11):2182–2190
Platts (2014) GIS data. www.platts.com
Rose A (2007) Economic resilience to natural and man-made disasters: multidisciplinary origins and contextual dimensions. Environ Hazards 7(4):383–398
Salmeron J, Wood K, Baldick R (2004) Analysis of electric grid security under terrorist threat. IEEE Trans Power Syst 19(2):905–912
Seger KA (2004) Utility security: a new paradigm. PennWell, p 238
Sun Y, Yang D, Meng L, Gao X, Hu B (2018) Universal framework for vulnerability assessment of power grid based on complex networks. In: The 30th Chinese control an decision conference (2018 CCDC), pp 136–141
Vellaithurai C, Srivastava A, Zonouz S, Berthier R (2015) CPIndex: cyber-physical vulnerability assessment for power-grid infrastructures. IEEE Trans Smart Grid 6(2):566–575
Volkanovski A, Eepin M, Mavko B (2009) Application of the fault tree analysis for the power system reliability. Reliab Eng Syst Saf 94(6):1116-1127J
Wang C et al (2017) Robust defense strategy for gas-electric systems against malicious attacks. IEEE Trans Power Syst 32(4):2953–2965
Wang J, Rong L (2009) Cascade-based attack vulnerability on the US power grid. Saf Sci 47:1332–1336
Wang W, Cai Q, Sun Y, He H (2011) Risk-aware attacks and catastrophic cascading failures in U.S. power grid. In: Proceedings of the IEEE GLOBECOM
Yuan W, Zeng B (2020) Cost-effective power grid protection through defender–attacker–defender model with corrective network topology control. Energy Syst 11(4):811–837
Zhang H, Peng M, Guerrero JM, Gao X, Liu Y (2019) Modelling and vulnerability analysis of cyber-physical power systems based on interdependent networks. Energies 12(18):3439

Zhu Y, Yan J, Sun Y, He H (2014) Revealing cascading failure vulnerability in power grids using risk-graph. IEEE Trans Parallel Distrib Syst 25(12):3274–3284. https://doi.org/10.1109/TPDS.2013.2295814
Zimmerman RD, Murillo-Sanchez CE, Thomas RJ (2015) Matpower v5.1 user's manual

Publisher's Note