Risk-aware Attacks and Catastrophic Cascading Failures in U.S. Power Grid

Wenkai Wang†, Qiao Cai*, Yan (Lindsay) Sun†, and Haibo He†
† ECE Department, Stevens Institute of Technology, Hoboken, NJ 07030
* ECE Department, University of Rhode Island, Kingston, RI 02881

Abstract—The power grid network is a complex network which is subjected to attacks and cascading failures. In this paper, we study the vulnerabilities of power grid in terms of cascading failures caused by node failures. Specifically, we define three metrics, the percentage-of-failure, Required Redundancy (RED), and Risk if Failure (RIF), to represent the critical level for each node. Based on these metrics, we can easily find the optimal victim nodes which attackers should choose to attack in order to cause cascading failure. From the defense point of view, these nodes are the weakest components of the power grid system and need more protection. With the results in this paper, we can be more aware of the risk level faced by the system if some nodes are taken down. Simulation results demonstrate the effectiveness of the proposed optimal victim nodes selection strategy.

Keywords: Power grid; Attack; Cascading failure; Risk Analysis

I. INTRODUCTION

Power grid has been widely recognized as one of the most complicated complex systems. With more than 9,200 electric generating units and 300,000 miles of transmission lines, the U.S. power grid can be considered as one of the largest interconnected machines on earth [1]. From the network security research point of view, we are facing an extremely large-scale of highly interconnected structure with different types of heterogeneous energy resources, which could suffer from either physical or cyber failures and intentional attacks.

Recently many important research findings and discussions regarding cascading failures have been presented in the community [2]–[7]. For instance, cascade-based attack and vulnerability analysis was presented in [2]. Two different attacks, either removal of the network nodes in descending or ascending order of the loads, were discussed and analyzed. The paper concluded a counter-intuitive finding: under certain system parameters, attacking the nodes with lowest loads can be more harmful than attacking the nodes with highest loads. In another cascading failure analysis [3] which is based on single-node attack, simulation results suggested that the loss of a single substation can result in up to 25% loss of transmission efficiency by an overload cascading failure. In [6], multi-node attack in complex networks was presented. It concluded that network topology has important impacts on the network behavior in response to failure and attacks. While most of the existing work on power grid attack assumes the attack happens on nodes, investigations were conducted in [7] concerning the attack on grid links. Specifically, two types of problems, the attack-induced cascading breakdown and range-based attacks on links, were presented in detail in that paper.

In studying cascading failures of power grid, it has been widely recognized that topological structure has a key impact [8]–[11]. For instance, structural vulnerability of the North American power grid was investigated in [8]. The connectivity loss resulting from the failure of generators and the removal of transmission substations were presented. To provide in-depth understanding of the topological impact on power grids, P. Hines et al presented a comparative study of different topological structure including random, preferential-attachment, and small-world structure [9]. It was reported that the power grid responds substantially differently under these abstract models.

While the aforementioned works mainly focus on attack, people also looked at the defense side to improve the network capability to resist cascading failures. For instance, in [12], it derived a theoretical upper bound of the network capacity that are safe against cascading failure. In [13], evolutionary algorithm was used to evolve complex networks to be resilient to cascading failure. It was suggested that clustering, modularity, and long path lengths are important factors to improve the complex networks’ capability in defending against attacks.

While the existing research results have provided many useful suggestions and insights about the cascading failure of power grid, the fully understanding of its behaviors under different types of attacks still remains a grand challenge. In this paper, we aim to investigate the vulnerabilities of power grid network under different attack strategies. Our proposed research suggested that although load of node has important impacts on the cascading failure, it is not always the best strategy from both attack and defense point of view. Instead, we propose three new metrics, the percentage-of-failure, Required Redundancy (RED), and Risk if Failure (RIF), to analyze the network cascading failure characteristics. Our simulation results suggest that unlike the existing load-based attacks, these new metrics can provide much more in-depth understanding of the system behavior under cascading failures. These results are important for identifying the most vulnerable nodes of the power grid, which can surely assist to improve the network capability in response to attacks.

The rest of the paper is organized as follows. Section II introduces the network model and attack model in power grid. Section III describes the proposed work including traditional load based attack strategy and our proposed attack strategies. Simulation results are shown in Section IV. Finally discussion and conclusion are made in Section V.
II. System Model

In this section, we introduce the network model and attack model of the power grid. The proposed work and simulation results are all based on the model discussed in this section.

A. Network Model

The power grid network can be modeled as a graph with substations as its nodes and transmission lines as its edges. In this paper, we study the Western North American power grid network [14]. When electrical power is transferred from power plants to end consumers, it may flow through several substations. The load of each substation is defined as the transmitting capabilities that it allows electrical power to pass through. The load, which is also referred to as betweenness, is usually calculated as the number of shortest paths that traverse the node in complex networks [3], [8]. In this paper, we adopt a model using the degree of each node and the degrees of its neighboring nodes to calculate load [2].

Denote $k_i$, the degree of node $i$, in the model proposed in [2], the initial load $L_i$ of node $i$ is defined as

$$L_i = \left\{ k_i \left( \sum_{m \in \Gamma_i} k_m \right) \right\}^\alpha,$$

where $\Gamma_i$ is the node set that contains all the neighbors of node $i$ and $\alpha$ is a tunable parameter that can control the distribution of initial load.

When a node fails because of self malfunction or attacks, the load carried by this node is supposed to be redistributed. In this paper, we adopt the redistribution model proposed in [2], i.e., the load is redistributed to the neighbor nodes of the failed node. The load redistributed to neighbors is proportional to the initial load of the neighbors. Specifically, when node $i$ is down, the additional load $\Delta_{ij}$ assigned to its neighbor $j$ is,

$$\Delta_{ij} = L_i \frac{L_j}{\sum_{m \in \Gamma_i} L_m}$$

Each node has a capacity which is the maximum load that it can carry. In previous works on complex networks [3], [6], [8], it is generally assumed that the capacity $C_i$ of node $i$ is proportional to its initial load $L_i$, i.e.,

$$C_i = T \ast L_i,$$

where $T$ is system tolerance. Higher $T$ value means higher capacity of each node.

When a node fails, the load of its neighboring nodes is increased due to the load redistribution. For the neighboring nodes, if their load after redistribution exceeds their capacity, they will fail too and their load will be redistributed in the same way. We can anticipate that this may cause further breaking down of other nodes. In complex networks literatures this phenomenon is called Cascading Failure.

B. Attack Model

The power grid networks are subjected to various types of attacks, including cyber attacks and physical attacks. In this paper, we mainly study the physical attack. Specifically, we study the case that a substation is physically taken down by attackers. When a node fails, we assume it is out of service and cannot share load from its failed neighbors anymore.

III. Proposed Work

Our primary goal of this research is to understand the vulnerabilities of power grid by investigating various attack strategies. This investigation will provide essential knowledge for protecting the power grid in future research.

In this section, we first discuss the traditional attack strategy (Section III-A), then propose new metrics for describing power grid vulnerability (Section III-B), and finally design new attack strategies for attacking a single substation (Section III-C).

A. Traditional Attack Strategy: Largest-Load

In this work, we refer the nodes that are taken down by attackers as victim nodes. The optimal attack strategy is to pick the victim nodes whose failure will cause the most severe cascading failure in the power grid. The severity of a cascading failure can be described by the total number of failed nodes (due to overloading) after the victim nodes are taken down.

To simplify the discussion, we start from the single-node attack, in which the attackers have the capability to take down one victim node. The problem is the strategy of the single-node attack, i.e., when the attackers have the capability to take down one node, which node should they choose as the victim node? In the current literature [2], [3], [8], the attackers always choose the victim nodes according to load.

**Traditional attack strategy:** choosing the victim node as the node with the largest load

This strategy is based on the fact that the failure of a node with large load leads to a large redistributed load to its neighbors. Then it is highly possible that some neighboring nodes are broken down because of the redistributed load. This attack strategy has been widely used when studying vulnerabilities of the power grid and defense solutions. However, can it represent the strongest attack?

From the attacker’s point of view, the traditional attack strategy has a severe limitation. That is, it hardly considers about power grid topology while the topology plays a critical role in cascading failures. In power grid networks, the nodes with higher load usually have higher degrees and they have a lot of neighbors to redistribute their load. On the contrary, for a node with lower load, it is possible that it is only connected to one or two neighbor nodes. The initial load of the neighbors can also be very different in different scenarios. The number of neighbors and the neighbors’ initial load, which all play important roles in cascading failures, are not considered in the traditional load-based attack strategy.

In Fig. 1, we pick two representative nodes from the Western North America power grid networks to illustrate the above discussion. Node A, shown in the left plot, carries high load 1414. When node A is down, its load is redistributed to its 14 neighbors. For example, according to equation (2), node B, which has initial load 846, needs to carry 176.7 additional load after node A is knocked down. Although the total amount
Given the network topology and the initial load, for a fixed network size, the damage of cascading failures depends on system tolerance and attack strategy. Specifically, let $\lambda(T, i)$ denote the percentage-of-failure when the system tolerance is $T$ and node $i$ is chosen as the victim node. Therefore, the load-based traditional attack strategies may not be effective to find the victim nodes that cause severe cascading failures.

![Load redistribution example. “X: y + z” means node X has initial load y, and receives additional load z after the victim node is taken down.](image)

To evaluate the damage of cascading failures, one metric we can use is the percentage-of-failure defined as,

$$\lambda = 1 - \frac{N'}{N},$$

where $N$ is the number of nodes before the attack and $N'$ is the number of survived nodes after the attack.

Obviously, $\lambda$ is a direct measure of severity of attacks, and depends on system tolerance and attack strategy.

Let $\lambda(T, i)$ denote the percentage-of-failure when the system tolerance is $T$ and node $i$ is chosen as the victim node. Given the network topology and the initial load, for a fixed system tolerance value ($T$), we can run the simulation and obtain $\lambda(T, i)$ for each node in the network. Obviously, $\lambda(T, i)$ can be used as a metric by the attacker to choose the victim nodes. That is, strategy $\lambda$: choosing the victim node as the node with the highest $\lambda(T, i)$ value.

However, this strategy has several limitations. Fig. 2 shows the sorted percentage-of-failure for all nodes under three fixed system tolerance value ($T = 1.2, 1.4$ and $1.6$). We made the following observations.

- First, $\lambda$ is very sensitive to $T$. If the system tolerance value is different for different regions of the network, or can dynamically change, the $\lambda$ value for each node cannot be accurately estimated.

- Second, even if $T$ is fixed for all nodes, we see two “extreme” cases. Some nodes have $\lambda = 0.002$, meaning that no other nodes are taken down except the victim node itself, i.e., the breaking down of these nodes will not cause cascading failure. The other nodes have $\lambda$ close to 1, meaning that they will break down almost the entire network. In Fig. 3 a), the histogram of $\lambda$ for $T = 1.4$ is shown. It is clear seen that the nodes can be divided into two categories based on $\lambda$ values, but their subtle differences cannot be well captured by $\lambda$.

- Third, to obtain $\lambda$ for a particular node, we need to conduct simulation, which can be complicated when the network size is large.

Due to all above limitations, percentage-of-failure (i.e. $\lambda$) is not a good metric for the attackers to choose victim nodes and for the system administrator to find system vulnerabilities.

**Required Redundancy (RED)**

To overcome the first and second limitations of the percentage-of-failure metric, we develop a new metric called Required Redundancy (RED). The RED value of node $i$ is defined as the minimal required system tolerance value such that cascading failure does not occur when node $i$ is taken down.

![Histogram for a) percentage-of-failure when $T = 1.4$ b) Required Redundancy (RED) c) Risk if Failure (RIF)](image)
1.1 the RIF values for all nodes in the Western North American network. Compared with the calculation of RED, the calculation of RIF is computed based on local network information: the initial loads of node \( i \) is the victim node. We define RIF of node \( i \) as

\[
RIF_i = \frac{L_i}{\sum_{m \in \Gamma_i} L_m}.
\]

Recall that \( L_i \) is the load of node \( i \) and \( L_m, \forall m \in \Gamma_i \) are the loads of \( i \)'s neighbors. \( RIF_i \) is the ratio between the initial load of node \( i \) and the total initial load of \( i \)'s neighbors. Roughly speaking, the higher the RIF value is, the more likely the cascading failure occurs if node \( i \) is taken down. In other words, RIF roughly describes the risk of the network if node \( i \) is the victim node.

From equation (5), we see that \( RIF_i \) only depends on local information: the initial loads of node \( i \) and its neighbors. Compared with the calculation of RED, the calculation of RIF is extremely simple and does not need to simulate the entire network.

Next, we answer the question that whether RIF can be used to replace RED in the search for the victim node. We compute the RIF values for all nodes in the Western North American power grid network and plot the histogram in Fig. 3 c). We can see that Fig. 3 c) is very similar to Fig. 3 b), which indicates that there may be a strong correlation between RED and RIF.

Fig. 5 demonstrates such correlation. The x-axis is RIF and the y-axis is RED. Each node, which has a RIF and RED value pair, is represented by a blue dot in Fig. 5. In other words, the dots represent the original data set of the RED values of all nodes versus their corresponding RIF values. Besides the original data set, we also construct the worst-case and best-case data set. For the nodes with the same RIF values, find the node with the largest (or smallest) RED value, and put this node in the worst-case (or best-case) data set. There are three lines in Fig. 5. The lower curve is the least square fitting for the best-case data set. The middle line is the least square fitting for the original data set. The top line is the least square fitting for the worst-case data set. We have made two important observations.

- There is a strong linear relationship between RED and RIF in the original and the worse-case data sets.
- From the worst-case least square fitting curve in Fig. 5, we can see that if we know the RIF of a node, we can use a linear equation to estimate the upper bound of its RED value. With a very high probability, the estimated upper bound is very close to its true RED value. The true RED can be smaller than the upper bound, with a very small probability.

In conclusion, we can use RIF, which is very easy to calculate, to describe whether a node is critical in terms of causing cascading failures. A node with low RIF value is not critical for sure. A node with high RIF is highly likely to be critical. The RIF metric can be very useful for attackers to design attack strategies or for the system administrator to analyze system vulnerabilities.

1.2 Initial Load as a Metric Recall that the traditional attack strategies pick victim nodes based on load. We examine whether the load metric can really describe whether a node is critical in terms of causing the cascading failure.

Fig. 6 a) shows the distribution of initial load for all nodes. It is observed that most nodes have very low initial load, whereas a few nodes have very high initial load. The initial load follows power law distribution, which is a feature of many complex networks [4], [7], [10], [13].
We define a RIF-based attack strategy as searching the victim node in a subset of network nodes. To find the victim node, one needs to simulate the case that node \( i \) fails. When there are \( N \) nodes in the power grid, \( N \) such simulations need to be performed in order to search the victim node. In the Western North America power grid networks, \( N = 4941 \). If we need to find \( \text{AS}_{\text{opt}} \), for dynamically changing load distributions, the computation involved can be too expensive.

Instead, a more practical strategy is to reduce the searching space by finding the victim node in a subset of network nodes. We define a RIF-based attack strategy as

- \( \text{AS}_{\text{rif;K}} \): Among the top \( K \) nodes with the highest RIF value, select one victim node that yields the largest RED value.

That is, one needs to compute the RIF values for all network nodes, select \( K \) nodes with the largest RIF values, obtain the RED values of these \( K \) nodes, and finally pick the victim nodes with the highest RED value. Since computing RIF is extremely simple, the computation complexity of \( \text{AS}_{\text{rif;K}} \) is about \( \frac{K}{N} \) of the computation complexity of \( \text{AS}_{\text{opt}} \).

Furthermore, we will compare \( \text{AS}_{\text{rif;K}} \) with two other schemes

- \( \text{AS}_{\text{rand;K}} \): From \( K \) randomly picked nodes, select the node that yields largest RED value as the victim node.
- \( \text{AS}_{\text{load;K}} \): Among the top \( K \) nodes with the highest load, select one victim node that yields the largest RED value.

The comparison results will be shown in Section IV.

### C. Attack Strategy

If attackers have the capability to break down one node, they have to choose which victim node to attack. This is referred to as the single node attack strategy, denoted by \( \text{AS}^s \).

The optimal attack strategy, denoted by \( \text{AS}_{\text{opt}} \), is to find the victim node that has the largest RED value among all nodes. However, RED cannot be computed by any close form equations. Instead, to obtain the RED value for node \( i \), one needs to simulate the case that node \( i \) fails. When there are \( N \) nodes in the power grid, \( N \) such simulations need to be performed in order to search the victim node. In the Western North America power grid networks, \( N = 4941 \). If we need to find \( \text{AS}_{\text{opt}} \) for dynamically changing load distributions, the computation involved can be too expensive.

Instead, a more practical strategy is to reduce the searching space by finding the victim node in a subset of network nodes. We define a RIF-based attack strategy as

- \( \text{AS}_{\text{rif;K}} \): Among the top \( K \) nodes with the highest RIF value, select one victim node that yields the largest RED value.

As a summary, we have discussed four metrics to predict whether a node is critical in terms of causing cascading failures.

- **Initial load**: used in the traditional attack strategy and is not effective;
- **Percentage-of-failure (\( \lambda \))**: a direct measure but has three limitations;
- **Required redundancy (RED)**: a good metric but requires complicated computation;
- **Risk if failure (RIF)**: a good metric and only needs simple computation.

### IV. Simulation Results

As described in Section II-A, in this paper we study the Western North American power grid network, which is composed of \( N (= 4941) \) substations and \( M (= 6594) \) transmission lines, to demonstrate and test the proposed approaches. We built a simulator using Matlab to simulate the load redistribution process and the consequence of different attacks. The parameter \( \alpha \) in equation (1), which determines the range of initial load, is set to be 1.

We first evaluate the three single-node attack strategies described in Section III-C. They are the load-based attack strategy (\( \text{AS}_{\text{load;K}}^s \)) representing the traditional scheme in the current literature, the RIF-based attack strategy (\( \text{AS}_{\text{rif;K}}^s \)) proposed in this paper, and the random selection strategy (\( \text{AS}_{\text{rand;K}}^s \)) representing a naive attack scheme. For \( \text{AS}_{\text{rand;K}}^s \), we run the simulation for 1000 times for each parameter setting. Then we get the average RED value or percentage-of-failure value.

Fig. 7 shows the strength of three attack strategies measured by RED for different \( K \) values. The y-axis is the RED value of the selected victim node. Recall RED is the minimal required system redundancy to avoid cascading failures. The higher this RED value is, the stronger the attack is. The x-axis is the \( K \) value, changing from 1 to 60. The higher the \( K \) value is, the more computation is needed to find the victim node. We have made the following observations,

- **When \( K = 1 \)**, the attacker can choose the node with the largest load in \( \text{AS}_{\text{load;1}}^s \), randomly choose a node in \( \text{AS}_{\text{rand;1}}^s \), or choose the node with the largest RIF in \( \text{AS}_{\text{rif;1}}^s \). The corresponding RED values for \( \text{AS}_{\text{load;1}}^s \), \( \text{AS}_{\text{rand;1}}^s \) and \( \text{AS}_{\text{rif;1}}^s \) are 1.225, 1.225 and 1.8, respectively. We see that the load-based attack is not stronger than the random attack, when \( K = 1 \). On the other hand, the RIF-based scheme already achieves the maximum RED value. Although this result is for a specific network setup, it shows the obvious strength of the RIF-based attack strategy.
- **As \( K \) increases**, the search for the victim node is conducted among a larger set of nodes. Obviously, the strength of \( \text{AS}_{\text{rand;K}}^s \) increases gradually with \( K \).
K causes a severe cascading failure in which 96% of nodes are.

AS is always lower than that of cascading failures for K.

are three major observations. First, when different attack strategies are used, in Fig. 8. There are three major observations. First, when K = 1, AS increases a severe cascading failure in which 96% of nodes are taken down. Second, when K = 1, AS and AS do not cause cascading failure because their percentage-of-failure values are almost 0. Third, as K increases, AS can cause cascading failures for K ≥ 5, while its percentage-of-failure is always lower than that of AS.

As a summary, the RIF-based strategy has two major advantages.

- It has extremely good performance when K = 1. That is, without running any simulations, RIF yields a strong attack strategy: picking the node with the highest RIF value as the victim node.

- To achieve the same attack strength, it requires significantly less computation complexity. With the same computation complexity, it yields stronger attacks.

V. DISCUSSION AND CONCLUSION

In this paper, we investigated the vulnerabilities of the US power grid networks by studying various attack strategies that cause cascading failures. In particular, we analyzed the traditional load-based attack strategy and found that it often is not the most effective way to cause cascading failures. Then we proposed several metrics to describe the critical level of nodes. These metrics, including percentage-of-failure, Required Redundancy (RED) and Risk if Failure (RIF), built foundation for finding effective attack strategies. Simulation results showed that the RIF-based scheme is extremely effective in finding the optimal victim node, the load-based scheme is less efficient, and the random scheme is the worst.

While the attack strategies discussed in this paper is designed for single-node attack, we can extend the strategies to multi-node attack case by attacking two or more nodes within a neighborhood. In the future, we will also generalize the proposed attack strategies. For example, it would be interesting to demonstrate that the attack strategies are still effective under different load redistribution models and different power grid topologies. Another important factor that we want to take into account is the physical property of power flows, which may provide substantial insights for cascading failures in this particular complex network. As a summary, The new metrics and the single-node attack strategies proposed in this paper are expected to be an important part of the foundation for investigations on more complicated attacks in power grid.

REFERENCES