The Sequential Attack against Power Grid Networks

Yihai Zhu, Jun Yan, Yufei Tang, Yan (Lindsay) Sun, and Haibo He
Department of Electrical, Computer, and Biomedical Engineering, University of Rhode Island, Kingston, RI 02881
Email: {yhzhu,jyan,ytang,yansun,he}@ele.uri.edu

***Abstract*—The vulnerability analysis is vital for safely running power grids. The simultaneous attack, which applies multiple failures simultaneously, does not consider the time domain in applying failures, and is limited to find unknown vulnerabilities of power grid networks. In this paper, we discover a new attack scenario, called the sequential attack, in which the failures of multiple network components (i.e., links/nodes) occur at different time. The sequence of such failures can be carefully arranged by attackers in order to maximize attack performances. This attack scenario leads to a new angle to analyze and discover vulnerabilities of grid networks. The IEEE 39 bus system is adopted as test benchmark to compare the proposed attack scenario with the existing simultaneous attack scenario. New vulnerabilities are found. For example, the sequential failure of two links, e.g., links 26 and 39 in the test benchmark, can cause 80% power loss, whereas the simultaneous failure of them causes less than 10% power loss. In addition, the sequential attack is demonstrated to be statistically stronger than the simultaneous attack. Finally, several metrics are compared and discussed in terms of whether they can be used to sharply reduce the search space for identifying strong sequential attacks.**

***Index Terms*—Sequential Attack, Cascading Failure, Vulnerability Analysis, Power Grid Network**

I. Introduction

Electric grid networks have been developed over decades and become increasingly interconnected and complex. Although mechanisms and regulations have been applied to maintain the stability and security of power transmissions, large-scale blackouts are still not inevitable. Examples of recent cases include 2003 Northeast American [1] and 2012 India [2], which brought catastrophic consequences. In these cases, failures of one or a few components can trigger the successive failures of other components, which is referred to as the *cascading failure*.

To understand the inherent characteristics of blackouts, researchers have investigated the consequence of multiple failures of links/nodes in grid networks by revealing the mechanism involving in cascades [3], [4], identifying vulnerable collections (i.e., combinations of links/nodes) [5]–[7], and designing powerful malicious attack strategies [8]–[14]. In the current literature, the investigation of multiple failures often assumes that all failures occur simultaneously. This assumption, however, omits the fact that multiple failures can occur sequentially. The attackers, who can launch simultaneous attacks, can also attack links/nodes sequentially according to a carefully designed time sequence. In other words, the assumption of simultaneous failures has apparent limitations to comprehensively exploit the characteristics of cascading failures in reality.

The cascading failures in real life involved the sequences of various events, e.g., voltage collapse, generators shunt down, and transmission lines tripping. The cascade process lasts probably minutes, hours or even days [1], [2]. Thus, time domain is an essential dimension to analyze cascading failures. It is without exception for the well-established cascade models, including complex network models [10], [12], [15], [16] and power-flow models [4], [17], to capture the stages of cascading failures. Therefore, sequentially failing links/nodes is highly possible in reality. The **contribution** of this work is to study sequential failures from the attacker's perspective, and answer the following questions. If the attacker can knock down several links sequentially, when and which links should they knock down (i.e., attack)? Will this sequential attack cause more damage, measured by *blackout size*, than the simultaneous attack? Will the understanding on the sequential attack reveal new vulnerability (i.e., vulnerable collections of links) in the power grid?

In this paper, we investigate sequential attacks on links to demonstrate the sequential attack, and address the above questions. The sequential attack is defined as follows.

- In a multiple-link sequential attack, the attacker uses either physical- or cyber-attacks to fail multiple links in sequence, aiming to cause damage, measured by the blackout size here, to the power grid.

We study the link sequential attack on IEEE 39 bus system from two aspects. First, comparisons between the sequential attack and the simultaneous attack is performed, demonstrating that the sequential attack can reveal new vulnerabilities of power grids. For example, the sequential failure of two links (links 26 and 39) can cause 80% power loss, whereas the simultaneous failure of them causes less than 10% power loss. Second, we find that the sequential attack is statistically stronger than the simultaneous attack. Finally, several metrics have been investigated in terms of whether they are useful in reducing the search space of finding strong sequential attacks.

The remainder of this paper is organized as follows. Section II describes the system model, the sequential attack, and cascading failure simulator (CFS). Section III demonstrates the new vulnerabilities discovered by the sequential attack. Section IV discusses experiments and results. Finally, the conclusion is drawn in Section V.

II. Network Model

Generally speaking, a power grid consists of *substations* and *transmission lines*. Substations are categorized into generators

978-1-4799-2003-7/14/$31.00 ©2014 IEEE

(producing and supplying power), demand substations (delivering power to customers), and neutral substations according to different functionalities. Transmission lines are in charge of transmitting electricity among substations in the entire grid network. In this paper, we view a power grid as a network, with substations as *nodes* and transmission lines as *links*. In addition, generators, demand substations and neutral substations are relatively viewed as generation nodes, demand nodes and neutral nodes. Due to its simplicity, we adopt the DC power-flow model instead of the AC power-flow model. The DC power-flow models are widely used in the study of cascading failures [5], [16], [17], and are also suitable for understanding the sequential attack. In the future work, we can surely extend this study by adopting other power-flow models. To study the sequential attack in IEEE 39 bus system [18], we plan to find all possible sequential attacks and understand their impact through simulations. Therefore, as the first step, we build a sequential CFS based on the simultaneous CFS in [5]. Fig. 1 illustrates the flow diagram of the sequential CFS, the detailed description of which is given as follows.

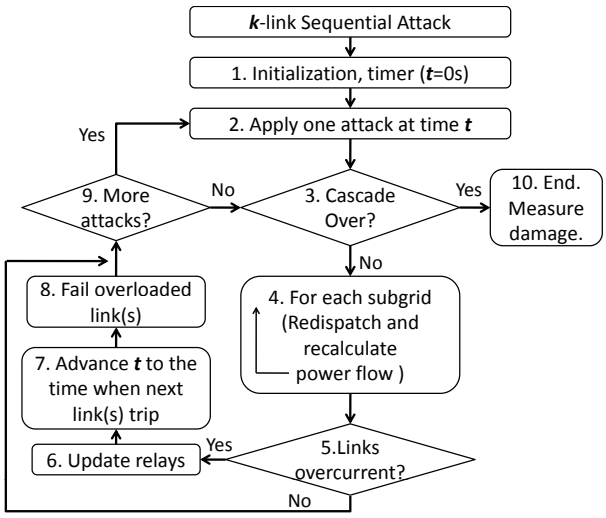

Fig. 1. Flow chart of the sequential CFS adopted in this paper.

Step 1: Assume an attacker has chosen k links to attack and determined the attack sequence. The choice of these k links as well as the attack sequence is referred to as the *attack strategy*. These k attacks will be performed in k stages. In each stage, one link will be failed by the attacker (see Step 2), whereas additional links may be failed due to overloading (see Step 5-8).

Step 2: Fail one link according to the attack strategy at time ***t***, and update the topology and electrical features of the grid network.

Step 3: Check whether cascades are over, based on user-definition criterion. If yes, quit CFS and measure damage. The criterion and the damage measurement will be explained at the end of this section.

Step 4: When the topology of the grid network changes due to applying attacks or failures of links, the whole grid might be split into several subgrids, which means the balance of power supply/demand might be broken. In each subgrid, the re-dispatch of generation and shedding of demand are conducted to meet the new balance as follows. First, ramp the generation up or down to meet the demand as closely as possible. Second, if after ramping the new balance is not achieved, adjust the generation and demand to meet the balance [5]. When reaching the new balance, DC power-flow is recalculated to obtain new current on links in each subgrid.

Step 5: Check link overloading. If there is (are) overloaded link(s), go through Steps 6 to 8 to deal with the overloading; otherwise go directly to Step 9 to check next possible attack.

Step 6: For a link with overloading, the time-delayed overcurrent relay are used to monitor and determine whether and when the link fails [5]. For instance, if a link is overloaded at time ***t***, its thermal begin to accumulate. Until $t+\Delta(t)$, when the accumulated thermal exceeds its thermal limitation, this link fails. For each link, its thermal limitation is considered to be the level such that it can tolerate 5s of carrying 50% above its capacity. Obviously, different overloaded links have different $\Delta(t)$, unless there are some links with identical initial power flow and thermal accumulation. Among all overloaded links, we choose the link with the smallest $\Delta(t)$ value. This chosen link will be removed in Step 8. The corresponding $\Delta(t)$ value is referred to as $\Delta_{min}(t)$.

Step 7: Advance the timer to when next failure happens, i.e., $t = t + \Delta_{min}(t)$.

Step 8: Remove the chosen link(s) and update the topology and electrical features of the grid network.

Step 9: Check whether all attacks are finished. If not, the current time ***t*** is the "stage" for next attack.

Step 10: When the simulator quits, the damage is evaluated according to user-defined measures.

Here are some explanations about the above steps. In Step 2, the attacker fails the links according to the attack strategy. If the attacker aims to fail k links, the attack will have k stages. In each stage, one link is failed. The attack enters stage n, $(2 \leq n \leq k)$ from stage $n-1$ when either of the following conditions is satisfied. In stage $n-1$, there are no overloaded links. Or, in stage $n-1$, there exists overloaded link(s) and one such link is failed in Step 8.

In Step 3, the simulator stops when both of the following conditions satisfy. First, the attacker has already failed k links. Second, there are no overloaded links. The rationale behind the two conditions is to make sure that all attacks are fully conducted and the cascades are completed.

In Step 10, the damage measure is chosen as the *blackout size*, defined as,

$$\lambda = 1 - \frac{P^{'}}{P} \tag{1}$$

where P and $P^{'}$ represent the total power demand before and after applying attacks, respectively. The definition, similar to that in [19], is the normalized power loss of a power grid. Note that different measures, such as *connectivity loss* [9] and

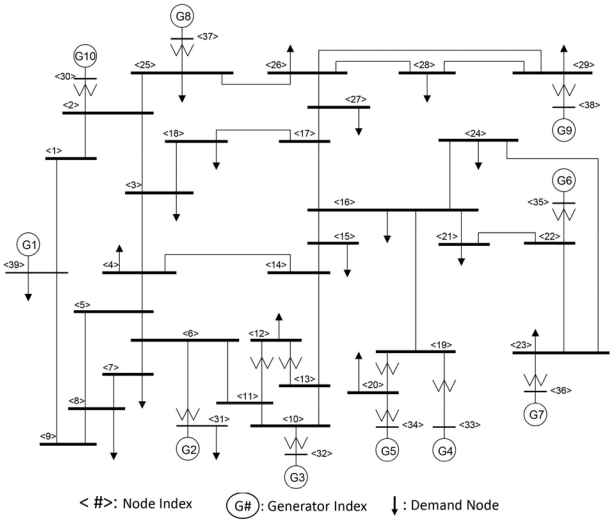

Fig. 2. The topology of IEEE 39 bus system [20].

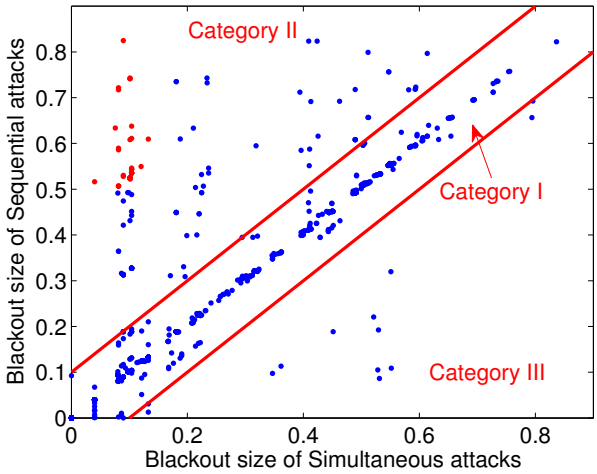

Fig. 3. The strength of the sequential attack and the simultaneous attack on all two-link combinations of IEEE 39 bus system.

average inverse geodesic length [11], can also be exploited to evaluate the final damage. Blackout size, in our opinion, is more straightforward than other measures in revealing how much a power grid network loses its functionality in supplying power to customers.

III. New Vulnerability Revealed by the Sequential Attack

Due to complex operating surroundings, tripping of transmission lines is highly possible in reality. This contributes to most of existing major blackouts [1], [2]. In this section, we will demonstrate new vulnerabilities of power grid networks by investigating the sequential attack on links. In Section III-A, the testing setup is briefly introduced, and new vulnerabilities are demonstrated in III-B.

A. Introduction of Testing

We adopt IEEE 39 bus system, the well known 10-generator New-England power grid, as the test benchmark. The topology is shown in Fig. 2, which consists of 39 nodes and 46 links. Within these 39 nodes, there are 10 generation nodes and 21 demand nodes. Among these 46 links, 11 and 37 of them are connecting with generation nodes and demand nodes, respectively. In addition, for simplification these 46 links are labeled as l_1 to l_{46}.

B. New Vulnerability Demonstration

In existing works [5], [9], [11], [15], [19], strong attacks on power grids are often defined based on the simultaneous attack. For example, a k-link *simultaneous attack strategy* defines a set of k links as victim links. Simultaneous CFSs [5], [15] are used to simulate the failures of k links at the same time and measure the attack strength with certain measures, such as blackout size and connectivity loss. The attack strategy that causes the largest damage is referred to as the *strongest attack(s)*. For the attack strategies that cause large damage, the links and combination of links in these strategies represent the *vulnerability of the grid*.

In what follows in this section, we will demonstrate two features of the sequential attack.

- There are more strong sequential attacks than strong simultaneous attacks.
- The non-vulnerable combination of links that corresponds to a weak simultaneous attack can become highly vulnerable when the sequential attack is considered, because such combination leads to large damage when attacked sequentially.

In other words, vulnerability analysis based on the simultaneous attack has limitations, and the sequential attack reveals new vulnerabilities.

Next, we describe how to demonstrate new vulnerabilities. On IEEE 39 bus system with 46 links, there are in total $\binom{46}{k}$ k-link combinations. For each combination, we measure the strength of the simultaneous attack, denoted by λ_{sim}, and the strength of the sequential attack, denoted by λ_{seq}. The simultaneous CFS adopted in this paper is similar to the sequential CFS, described in Section II. The only modification is to fail all victim links in Step 2 at the first stage, and the simultaneous CFS only has one stage. λ_{sim} is the normalized blackout size, as defined in Equ. 1.

For each k-link combination, there are $k!$ possible orders to conduct the sequential attack. For example, for each two-link combination (l_i, l_j), the attacker can either attack l_i first or attack l_j first. Therefore, for each k-link combination, we perform $k!$ simulations to obtain the strengths of all possible sequential attacks, and pick the attack that yield the largest damage. This largest damage is denoted by λ_{seq} for this particular k-link combination sequential attack.

For demonstration, we examine all two-link combinations. There are in total $\binom{46}{2}$ = 1,035 two-link combinations. Each two-link combination has two values: λ_{sim} representing the strength of the simultaneous attack and λ_{seq} representing the strength of the sequential attack. We plot λ_{seq} versus λ_{sim} in Fig. 3. There are 1,035 dots, each of which represents one two-link combination.

For systematically comparing the sequential attack and the

TABLE I
CASE STUDIES OF THE SEQUENTIAL ATTACK.

Two-link combination	Ranking by $\lambda_{seq} - \lambda_{sim}$	The Sequential Attack			The Simultaneous Attack		
		λ_{seq}	Sequences of Failed Branches	# of Subgrids	λ_{sim}	Sequences of Failed Branches	# of Subgrids
l_{26},l_{39}	1	0.83	$l_{26} \rightarrow l_{39} \rightarrow l_3 \rightarrow l_{42} \rightarrow l_1 \rightarrow l_6 \rightarrow l_{13} \rightarrow l_9 \rightarrow l_{23}$	6	0.09	l_{26},l_{39}	2
l_{10},l_{33}	2	0.74	$l_{10} \rightarrow l_{33} \rightarrow l_3 \rightarrow l_{42} \rightarrow l_{23} \rightarrow l_1 \rightarrow l_8 \rightarrow l_{28} \rightarrow l_{38} \rightarrow l_9$	5	0.1	l_{10},l_{33}	2
l_8,l_{34}	3	0.72	$l_8 \rightarrow l_{34} \rightarrow l_3 \rightarrow l_{23} \rightarrow l_{42} \rightarrow l_{13}, l_{28} \rightarrow l_4, l_{29}$	6	0.08	l_8,l_{34}	2
l_{24},l_{33}	4	0.74	$l_{24} \rightarrow l_{33} \rightarrow l_3 \rightarrow l_{42} \rightarrow l_6 \rightarrow l_4, l_{28} \rightarrow l_{13}, l_{38} \rightarrow l_9$	6	0.1	l_{24},l_{33}	2
l_6,l_{33}	5	0.74	$l_6 \rightarrow l_{33} \rightarrow l_3 \rightarrow l_{42} \rightarrow l_{24} \rightarrow l_4, l_{28} \rightarrow l_{13}, l_{38} \rightarrow l_9$	6	0.1	l_6,l_{33}	2
l_8,l_{27}	6	0.71	$l_8 \rightarrow l_{27} \rightarrow l_3 \rightarrow l_{23} \rightarrow l_{42} \rightarrow l_{13}, l_{28} \rightarrow l_4, l_{29}, l_{38}$	7	0.08	l_8,l_{27}	2
l_8,l_{13}	7	0.63	$l_{13} \rightarrow l_9 \rightarrow l_8 \rightarrow l_{26} \rightarrow l_3, l_{23} \rightarrow l_{42} \rightarrow l_4$	5	0.08	$l_8, l_{13} \rightarrow l_{23}$	2
l_9,l_{28}	8	0.73	$28 \rightarrow 38 \rightarrow 9 \rightarrow 3 \rightarrow 42 \rightarrow 1 \rightarrow 13 \rightarrow 7 \rightarrow 24$	5	0.18	$l_9, l_{28} \rightarrow l_{38}$	2
l_9,l_{38}	9	0.73	$l_{38} \rightarrow l_{28} \rightarrow l_9 \rightarrow l_3 \rightarrow l_{42} \rightarrow l_1 \rightarrow l_{13} \rightarrow l_7 \rightarrow l_{24}$	5	0.18	$l_9, l_{38} \rightarrow l_{28}$	2
l_8,l_{20}	10	0.64	$l_8 \rightarrow l_{20} \rightarrow l_3 \rightarrow l_{42} \rightarrow l_{13} \rightarrow l_4, l_{28} \rightarrow l_{38}$	5	0.1	l_8, l_{20}	2

simultaneous attack, we divide all dots into three categories.

- *Category I*: The sequential attack and the simultaneous attack have similar strengths. If the difference between λ_{seq} and λ_{sim} is smaller than θ (i.e., $\mid \lambda_{seq} - \lambda_{sim} \mid \leq \theta$), this dot belongs to this category, where θ is the numerical threshold to quantify the closeness between λ_{seq} and λ_{sim}. In Fig. 3, $\theta = 0.1$.
- *Category II*: The sequential attack is stronger than the simultaneous attack. If $\lambda_{seq} - \lambda_{sim} > \theta$, the dot is classified into this category.
- *Category III*: The sequential attack is weaker than the simultaneous attack. If $\lambda_{seq} - \lambda_{sim} < -\theta$, the dot is put in this category.

As shown in Fig. 3, most of dots are classified into Category I, while there are a considerable amount of dots that are classified into Category II and only a few dots belong to Category III. The illustration supports the observations we listed at the beginning of this subsection. The dots marked with red color, whose $\lambda_{sim} < 0.15$ and $\lambda_{seq} \geq 0.5$ in Fig. 3, are particularly interesting to investigate. These dots represent the vulnerability that is revealed through the sequential attack study, but not recognized by the simultaneous attack.

IV. SIMULATIONS AND RESULTS

Simulations in this paper are conducted in Matlab environment, including the implementation of simulators and calculating DC power flows using MATPOWER toolbox [18]. IEEE 39 bus system, which has been described in Section III-A, is chosen as the test benchmark to conduct all experiments and demonstrate our observations.

A. Demonstration of the Sequential Attack: A Case Study

In Section III-B, we have demonstrated that the sequential attack reveals vulnerabilities that are previously unknown. This discovery is very interesting and meaningful. For the same set of victim links, attacking them simultaneously or sequentially can lead to dramatically different blackout sizes. In this subsection, we take a closer look at such the difference through specific examples.

Recall that λ_{sim} and λ_{seq} represent the normalized blackout sizes of the simultaneous attack and the sequential attack, respectively. We are interested in the two-link combinations,

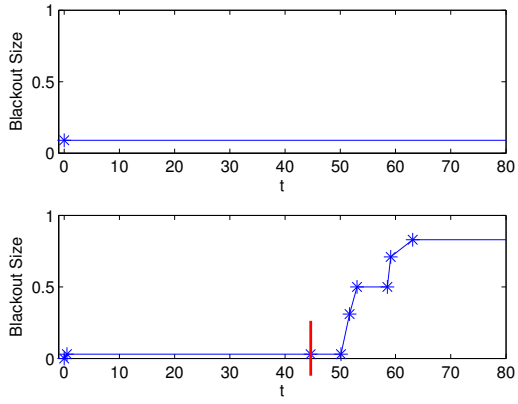

Fig. 4. The case study on the link combination (l_{26},l_{39}). The upper and lower subplots represent the simultaneous attack and the sequential attack, respectively. The blue-star points stand for when links are attacked/failed. The red line in the lower subplot represents when l_3 fails during cascades.

whose $\lambda_{seq} - \lambda_{sim}$ value is the largest ones. These combinations correspond to the red colored dots at the top-left corner in Fig. 3. In Table I, we list 10 two-link combinations with the largest differences between their λ_{sim} and λ_{seq} and the corresponding sequences of link failures. Take the link combination (l_{26},l_{39}) as an example. If l_{26} and l_{39} fail simultaneously, the main grid network is still almost connected with only one generator loss and the blackout size is 9%. In the sequential attack, l_{26} fails first, which leads to the redistribution of power. The power redistribution makes the load on certain links increase and almost reaches their capacities. Then, l_{39} fails. The loss of the generator connecting to l_{39} causes power redistribution again. As a result, the load of l_3 begins to exceed its capacity. After some delay [5], l_3 fails due to overloading. The failure of l_3 further leads to the serials of failures on l_{42}, l_1, l_6, l_{13}, l_9 and l_{23} within a short period of time. Eventually, the whole grid network is separated into six subgrids, and 83% power supply is lost.

In Fig. 4, we show how the blackout size changes versus time. The x-axis and y-axis denote the time and the blackout size, respectively. The upper subplot is for the simultaneous attack, and the lower subplot is for the sequential attack. In both cases, l_{26} and l_{39} are the victim links. Each star represents a link failure, due to either attack or overloading. The detailed method to determine failure time based on overheating can be found in [5]. It is clearly seen that the failure of l_3 triggers

cascades in the grid network, whereas l_3 is overloaded only in the sequential attack case.

There are many other link combinations similar to the combination (l_{26},l_{39}). Nine such cases are also shown in Table I. All these link combinations have not been recognized as vulnerable combinations, if the investigation only consider the simultaneous attack. In other words, due to the study on sequential attacks, we now recognize the danger of the sequential failure of such link combinations. The discovery of this new vulnerability provides not only a new angle to understand strong attacks, but important information for proper protection of the power grid network.

B. The Sequential Attack versus the Simultaneous Attack

Another observation from Fig. 3 is that the sequential attack can improve the strength of many two-link attacks. Does this observation still hold in k-link attacks, where $k > 2$? For general comparison, we classify the dots in Fig. 3 into three categories, as discussed in Section III-B.

In this substation, we make the comparison among Categories I, II and III. In other words, we count the number of dots belonging to each category and compare the percentages of three categories. For instance, in Fig. 3 there are in total 1,035 dots, 85.6% in Category I, 13.14% in Category II and 1.26% in Category III. We conducted experiments for three-link and four-link attacks. When $k = 3$ (i.e., three-link attack), there are 15,180 link combinations. When $k = 4$, there are 163,185 link combinations. The statistic results are shown in Table II, and we make the following observations.

First of all, the sequential attack is statistically stronger than the simultaneous attack. Comparing Category II and Category III in Table II, it is clearly seen that Category II takes a remarkable percentages, while the percentages of Category III are pretty small, less than 2%. In order words, except Category I (i.e., two attack scenarios have similar performances.), the number of link combinations in Category II is much larger than that of Category III.

Next, as k increases, Category II becomes increasingly dominant. In Table II, while k increases, the percentages of Category I sharply decrease, the percentages of Category II increase, while the percentages of Category III nearly stay the same. This result is easy to understand. When k increases, the attacker has more flexibility to arrange when to attack which link. This flexibility is highly likely to lead stronger attacks. Thus, the percentage of Category II increases dramatically.

Finally, it is notable that there exist a small percentage of k-link combinations, whose simultaneous failures are stronger than sequential failures. Although the percentages of Category III are small, this does show a few k-link combinations should be failed simultaneously in order to reach strong performances. Therefore, in the future study, we plan to study a hybrid attack strategy in which the simultaneous and sequential attacks can be combined.

C. Metrics for Finding Strong Sequential Attacks

In this subsection, we will introduce the ways to reduce the search space for finding strong sequential attacks. Roughly speaking, the search space for the sequential attack comes from two parts. The first part is from the number of candidate links. That is to determine a set of victim links. The second part is to determine the order of the sequential attack, given a set of k victim links. For instance, suppose there are N links of a grid network, and we study k-link sequential attacks. Currently, the search space for the exhaustive search is $\binom{N}{k}*k!$, where $\binom{N}{k}$ and $k!$ contribute to the spaces of the first part and the second part, respectively. As discussed in Section III, there are few existing works discussing which order of the sequential attack is the best. Therefore, it is not easy to reduce the search space in the second part. Luckily, k is usually not a large number, because the attacker's capability is often limited. Therefore, it is highly desirable to reduce the search space in the first part.

TABLE II
THE STATISTIC COMPARISON AMONG CATEGORIES I, II AND III.

k-link	Category I	Category II	Category III
$k = 2$	85.6%	**13.14**$\%$	1.26%
$k = 3$	69.57%	**28.83**$\%$	1.6%
$k = 4$	52.45%	**46.24**$\%$	1.32%

In the current literature [10], [11], [13], [19], many attack metrics have been proposed to help determine a small set of links, referred to as the *candidate links*, which are more likely to yield strong simultaneous attacks. A nature extension is to see whether these metrics are helpful to limit the size of candidate links for finding strong sequential attacks. Four metrics will be studied in this paper.

- *Metric 1*: Random selection, determining candidate links by randomly choosing among all links.
- *Metric 2*: Generator-connection, selecting the links that are connected with generators as candidate links.
- *Metric 3*: Degree, choosing candidate links by ranking degree values of links from high to low.
- *Metric 4*: Load, choosing candidate links by ranking load values of links from high to low.

Metric 1, without using any information of grid networks, is adopted as the metric for comparison purpose. Metric 2 considers that links connecting to generators are of importance to power grids. Metric 3 exploits the information of the topology to determine candidate links. The degree of a link here is defined as the summation of the degrees of its two endpoints [11]. Metric 4 uses the initial load on links to elect the candidate link set. The load of links is defined as the power flows on links [19], similar to the load definitions in [10], [11], [13].

There are 46 links in IEEE 39 bus system, and 11 links are connecting with generators. The candidate links of Metric 2 are these 11 links. The same number of candidate links are selected for Metric 3 and Metric 4 according to the degree and load values of links, respectively. The experiments are done as follows. First, we investigate k-link sequential attacks, where k is set be 2, 3, 4, 5 and 6, respectively. Second, for a given k, the k links are randomly chosen from the 11 candidate links when Metrics 2, 3, 4 are used. While the k links for Metric

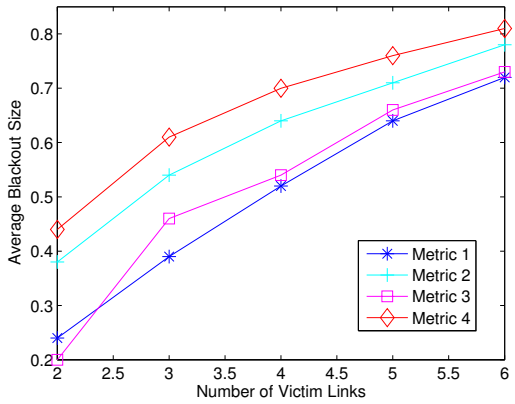

Fig. 5. Performance comparison among Metric 1: random selection, Metric 2: generator-connection, Metric 3: degree, and Metric 4: load.

1 is randomly chosen from 46 links. Finally, for each k value and each metric, simulations are conducted 1,000 times, and results are averaged.

Performance comparison among four metrics is demonstrated in Fig. 5, where x-axis and y-axis represent the number of victim links (i.e., k) and the averaged blackout size. It is clearly seen from Fig. 5 that Metrics 2, 3 and 4 are all more useful than Metric 1 in finding strong multiple-link sequential attacks. Especially, Metric 4 works much better than Metric 1 in terms of averaged blackout size.

Next, the reduction of the search space for Metric 4 is discussed by being compared with Metric 1. As discussed above, the sizes of candidate link sets for Metric 1 and Metric 4 are 46 and 11, respectively. The search spaces of Metrics 1 and 4 are shown in Table III. A explicit observation is that the search space of Metric 4 is significantly smaller than that of Metric 1.

As a summary, we can reduce the search space for strong sequential attacks by only examining the links with high load.

V. Conclusion

In this paper, we proposed a new attack scenario, the sequential attack, on power grid networks. Different from the traditional attack scenario, while fails multiple links simultaneously, the proposed attack scenario supposes multiple attacks occur sequentially during cascades. The new attack scenario is tested on IEEE 39 bus system. Some new vulnerabilities of grid networks are found. Many weak attacks from the perspective of the simultaneous attack are redefined as strong attacks by employing the sequential attack. These discoveries are insightful to evaluate structural vulnerability of grid networks. In addition, topological and electrical features are demonstrated to be useful for attackers to effectively and efficiently obtain strong sequential attacks.

Concerning possible directions for future investigation on the sequential attack, one promising extension would be to further discuss the relation between the sequences and the final performance. It will be very meaningful to discover the possible patterns of strong sequential attacks. Another useful direction is to completely study the behaviors of cascades along with time domain. The third angle is highly recommended to study malicious sequential attack strategies.

TABLE III
Comparison of the search spaces of Metric 1 and Metric 4.

	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$
Metric 1 $\binom{46}{k}$	1,035	15,180	163,185	1,370,754	9,366,819
Metric 4 $\binom{11}{k}$	55	165	330	462	462

Acknowledgment

This work was supported by National Science Foundation (NSF) under grant CNS 1117314 and CNS 0643532.

References

[1] U.S.-Canada Power System Outage Task Force, "Final report on the august 14, 2003 blackout in the united states and canada: Causes and recommendations," April 2004.
[2] India blackouts leave 700 million without power. The Guardian. [Online]. Available: http://www.guardian.co.uk/
[3] M. V. (Lead), K. Bell, Y. Chen, B. Chowdhury, I. Dobson, P. Hines, M. Papic, S. Miller, and P. Zhang, "Risk assessment of cascading outages: Methodologies and challenges," *IEEE Transactions on Power Systems*, vol. 27, no. 2, 2012.
[4] S. Mei, F. He, X. Zhang, S. Wu, and G. Wang, "An improved OPA model and blackout risk assessment," *IEEE Transactions on Power Systems*, vol. 24, no. 2, pp. 814–823, 2009.
[5] M. J. Eppstein and P. Hines, "A "random chemistry" algorithm for identifying collections of multiple contingencies that initiate cascading failure," *IEEE Transactions on Power Systems*, vol. 27, no. 3, pp. 1698–1705, 2012.
[6] J. Yan, H. He, and Y. Sun, "Integrated security analysis on cascading failure in complex networks," *IEEE Transactions on Information Forensics and Security*, in press.
[7] C. M. Davis and T. J. Overbye, "Multiple element contingency screening," *IEEE Transactions on Power Systems*, vol. 26, no. 3, pp. 1294–1301, 2011.
[8] J. Yan, Y. Zhu, H. He, and Y. Sun, "Multi-contingency cascading analysis of smart grid based on self-organizing map," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 4, pp. 646–656, 2013.
[9] R. Albert, I. Albert, and G. L. Nakarado, "Structural vulnerability of the North American power grid," *Physical Review E*, vol. 69, no. 2, 2004.
[10] W. Wang, Q. Cai, Y. Sun, and H. He, "Risk-aware attacks and catastrophic cascading failures in u.s. power grid," in *IEEE Global Telecommunications Conference*, 2011, pp. 1–6.
[11] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han, "Attack vulnerability of complex networks," *Physical Review E*, vol. 65, no. 5, 2002.
[12] Y. Zhu, Y. Sun, and H. He, "Load distribution vector based attack strategies against power grid systems," in *IEEE Global Telecommunications Conference*, Anaheim, CA, USA, Dec.3-7 2012.
[13] P. Crucitti, V. Latora, and M. Marchiori, "Model for cascading failures in complex networks," *Phys. Rev. E*, vol. 69, 045104(R), 2004.
[14] Y. Zhu, J. Yan, H. He, and Y. Sun, "Revealing cascading failure vulnerability in power grids using risk-graph," *IEEE Transactions on Parallel and Distributed Systems*, in press.
[15] R. Kinney, P. Crucitti, R. Albert, and V. Latora, "Modeling cascading failures in the north american power grid," *Eur. Phys. J. B*, vol. 46, pp. 101–107, 2005.
[16] Y. Zhu, J. Yan, Y. Sun, and H. He, "Risk-aware vulnerability analysis of electric grids from attacker's perspective," in *IEEE Innovative Smart Grid Technologies Conference*, Washington, USA, Feb.24-27 2013.
[17] S. Mei, X. Zhang, and M. Cao, *Power Grid Complexity*. Beijing: Tsinghua University Press, 2011.
[18] R. Zimmerman, C. Murillo-Sanchez, and R. Thomas, "MATPOWER: Steady-state operations,planning, and analysis tools for power systems research and education," *Power Systems, IEEE Transactions on*, vol. 26, no. 1, pp. 12–19, 2011.
[19] P. Hines, E. Cotilla-Sanchez, and S. Blumsack, "Do topological models provide good information about electricity infrastructure vulnerability?" *Chaos*, vol. 20, no. 3, 2010.
[20] [Online]. Available: http://www.sel.eesc.usp.br/ieee/IEEE39/main.htm