Vulnerability Analysis of Power Systems Based on Cyber-Attack and Defense Models

Saqib Hasan, Amin Ghafouri, Abhishek Dubey, Gabor Karsai, Xenofon Koutsoukos
Institute for Software Integrated Systems, Vanderbilt University, Nashville, TN 37212, USA
Email:{saqib.hasan, amin.ghafouri, abhishek.dubey, gabor.karsai, xenofon.koutsoukos}@vanderbilt.edu

Abstract—**Reliable operation of power systems is a primary challenge for the system operators. With the advancement in technology and grid automation, power systems are becoming more vulnerable to cyber-attacks. The main goal of adversaries is to take advantage of these vulnerabilities and destabilize the system. This paper describes a game-theoretic approach to attacker / defender modeling in power systems. In our models, the attacker can strategically identify the subset of substations that maximize damage when compromised. However, the defender can identify the critical subset of substations to protect in order to minimize the damage when an attacker launches a cyber-attack. The algorithms for these models are applied to the standard IEEE-14, 39, and 57 bus examples to identify the critical set of substations given an attacker and a defender budget.**

Index Terms—**Blackouts, Cascading failures, Cyber-attack, SCADA, Smart grid, RTUs, Resilience.**

I. Introduction

Smart grids are a result of increasing demand for reliable electric energy. The advancement in the grid's technology is responsible for expanding the capabilities of the traditional power grids generation, transmission, and distribution systems. Technologies such as substation automation, phasor measurement units (PMUs), and advanced metering infrastructures (AMIs) are currently deployed to achieve reliable supply for electric power. However, it increases the cyber component in a smart grid, which potentially increases the attack surface. Furthermore, cyber-attacks are documented as one of the major obstacles towards the reliable power system operation [1], [2]. Attackers take advantage of these technological advancements and launch sophisticated attacks causing severe damage to the systems, e.g., recent blackout of Dec 2015 Ukraine [3].

A power network consists of substations, control centers, AMIs etc. The substations have remote terminal units (RTUs) to monitor and control the field devices such as relays, and circuit breakers. These devices can be remotely manipulated to isolate transmission lines from the network during maintenance or faulty conditions [4] that can result in cascading failures. Therefore, RTUs become the primary target for cyber-attacks. The adversary aims to gain complete control of the RTUs and cause severe power system damage by modifying the relay settings, remotely opening circuit breakers, changing measurement data etc. However, the time and effort required in compromising a RTU ensure that an attacker can only access a few RTUs before they are detected [5]. Consequently, strategic attackers try to identify the critical substations to launch a successful attack that maximizes the damage [6].

In order to minimize the damage, defending all the substations simultaneously against cyber-attacks is very difficult given financial budget constraints. Besides, the defense mechanisms become more expensive since dedicated IT professionals are required to continuously monitor the system to identify and patch the vulnerabilities for a stable system operation. Therefore, it becomes necessary to intelligently identify a critical set of substations that can be prioritized and protected to minimize the system damage during a cyber-attack.

Previous works [7]–[15] have explored the frameworks and cyber-attack models that could simulate and analyze specific type of cyber-physical vulnerabilities in the power system. A framework for modeling cyber-physical switching attacks and man-in-the-middle attack is presented in [7], [8]. A class of attacks impacting physical processes excluding anomalies in the cyber-domain is referenced in [9]. Data integrity attacks and load redistribution attacks are discussed in [10], [13]. In [11], the impact of cyber-attacks on the transient stability of the system is described. An approach to identify and protect a subset of measurements from the adversaries considering false data injection attacks is presented in [12]. Node overloading attacks due to increasing load resulting in cascading failures are studied in [14]. The above approaches emphasize on specific vulnerabilities, however, they do not focus on system-wide identification of critical components to attack in a power system. This can provide important insight on prioritizing and protecting the substations and its components for improving the overall system resilience. Moreover, unlike our approach they do not consider a system-wide view on defending against these vulnerabilities especially with limited resource availability.

In this paper, we consider a game-theoretic approach to design an attacker / defender model for power systems. A strategic attacker tries to maximize the damage by identifying the worst-case attack whereas the defender tries to minimize the damage by protecting the critical substations. A worst-case attack refers to an attack on a subset of substations that cause maximum system damage. Here, we consider the cyber-attack on substations to gain access to the RTUs where the adversary can open the circuit breakers by manipulating protection assembly control signals resulting in severe cascading failures. Identifying all the possible attack and defense scenarios is computationally infeasible. Therefore, it is necessary to identify the worst-case attack and defense in an efficient way. The main contributions of the paper are:

- A formal model for an attacker is described, where the cost of attacking any substation is uniform. In this model, the attacker can identify the critical substations and its components that can be manipulated to disconnect transmission lines from the network that maximize system damage based on the attackers budget.
- An efficient polynomial-time algorithm is presented to identify the worst-case attack based on the attacker model.
- A formal model for a defender is described, where the cost of protecting any substation is uniform. In this model, given a defense budget, a defender can identify the critical substations to protect in order to minimize system damage during a cyber-attack.
- An efficient polynomial-time algorithm is presented to identify the critical substations to defend to minimize damage.
- The case study is performed on the standard IEEE-14, 39, and 57 bus systems [16]. Our results show that the approach captures the worst-case attacks on the power network and effectively uses the defense model to minimize the damage.

The remainder of the paper is organized as follows. Section II presents the attacker model followed by the defender model in Section III. Section IV demonstrates the results. The conclusions are provided in Section V.

II. System Model

A power system is a complex network of power generation, delivery, monitoring and control components. The power delivery elements such as transmission lines, buses, and transformers supply power from the generation points to the loads. However, the monitoring and control devices such as protection assemblies and circuit breakers are responsible for isolating faulty elements from the network during abnormal conditions. Due to the advancement in technology, power networks can be remotely controlled using RTUs and SCADA systems. Attackers may compromise these systems and isolate components from the power network causing cascading outages resulting in severe load loss [3].

We consider a power system G_p, where U is a set of buses, G is a set of generators, T is a set of transformers, L is a set of loads, and P is a set of protection assemblies. The power system is divided into substations. Each substation has its own monitoring and control units referred to as RTUs. Let $S = \{S^i\}_{i=1}^m$ be the set of substations. Each substation consists of a set of protection assemblies from P. We define $F(S^i)$ as a function that returns the set of protection assemblies in a substation S^i. Clearly, the union of all the protection assemblies in every substation represents the set of protection assemblies in the power network, that is, $\cup_{i=1}^m F(S^i) = P$.

III. Attacker Model

In this section, we provide the attacker model that could result in maximum load loss in a power network.

A. Worst-Case Attack

The goal of the malicious attacker is to destabilize the power system and maximize the load loss. The attacker achieves this by gaining access to a subset of substations $S^{'} \subseteq S$. The adversary is resource bounded, i.e., it can compromise at most B_S substations. Then, the attacker identifies the protection assemblies $P^{'} \subseteq F(S^{'})$ that will be manipulated to isolate transmission lines from the power network. Here, the attacker manipulates at most B_P protection assemblies. The budget B_P can represent the maximum number of protection assemblies that the attacker can attack due to a stealthiness criterion. Note that a non-strategic attacker may choose a large B_P and potentially attack all the protection assemblies within the compromised substations, however, a more strategic attacker may favor a small B_P as the attack may remain undetected for a longer period of time, which could potentially cause more damage. Also, note that manipulating all the protection assemblies of a substation to isolate power lines may not lead to cascading failures resulting in severe load loss due to the reduction in overall system load. We define the attack on a set of substations $S^{'}$ and protection assemblies $P^{'}$ by A_P.

Let the loads in the power network be defined by L_j and current flowing through each load is given by I_j, where $j = 1$ to $n, n \in \mathbb{N}$. Now, the load loss function is computed as below:

$$J(A_P) = \frac{\sum_{j=1}^{n} L_j}{L_T} \times 100, \ \ \forall I_j = 0 \qquad (1)$$

where L_T is the total system load and A_P is the attack. The problem is formally defined below.

Problem 1 (Worst-Case Attack): Given a power system network G_p, a substation budget B_S, and a protection assembly budget B_P, find a worst-case attack A_P that maximizes the load loss in the power system network. Formally,

$$\begin{aligned} &\underset{S'}{\text{argmax}} \ \max_{P' \subseteq F(S')} \ J(A_P) \\ &s.t. \quad |S^{'}| \leq B_S, \quad |P^{'}| \leq B_P \end{aligned} \qquad (2)$$

B. Algorithm for Finding Worst-Case Attack

Using exhaustive search to identify worst-case attack is computationally infeasible due to the combinatorial nature of search space [17]. Hence, we present an efficient Algorithm 1 to find the worst-case attack. The algorithm starts with an empty set and intelligently selects the critical substations one-by-one that cause maximum system damage. Next, from the selected substations, the algorithm iteratively identifies the protection assemblies to manipulate. It takes as input the power system model G_p, the substation budget B_S, the protection assembly budget B_P, and the substation and its component information S_P^{info}. Here, substation components refer to the protection assemblies of the substation. Then, it finds the worst-case attack by identifying the critical substations S_w to compromise, the transmission lines T_w corresponding to the protection assemblies that are manipulated to be removed from the network, and the resulting load loss L_w. The substation and its components i.e., protection assemblies is denoted by $\hat{S}$, which represents a hash table. At each iteration j, based on S_w, $\hat{S}$ is obtained by using `Substation_comps`(). If S_w is non-empty, the function selects the substations S_w from the power system that cause maximum load loss in the previous iteration

Algorithm 1 Algorithm for Finding Worst-Case Attack

```
Input: $G_p, B_S, B_P, S_P^{info}$
Initialize: $L_w \leftarrow 0, T_w \leftarrow \emptyset, S_w \leftarrow \emptyset, L_g \leftarrow 0$
for $j = 1, \ldots, B_S$ do
    if $S_w = \emptyset$ then
        $\hat{S} \leftarrow \texttt{Substation\_comps}(S_P^{info}, \emptyset)$
    else
        $\hat{S} \leftarrow \texttt{Substation\_comps}(S_P^{info}, S_w)$
    end if
    for all $s \in \hat{S}$ do
        $P_t \leftarrow F(s)$
        $T_P, L_P \leftarrow \texttt{Worst\_Attack}(G_p, P_t, B_P)$
        if $L_P > L_w$ then
            $L_w \leftarrow L_P$, $T_w \leftarrow T_P$, $S_w \leftarrow s$
        end if
    end for
    if $(L_g - L_w) \leq \varepsilon$ then
        break
    else
        $L_g \leftarrow L_w$
    end if
end for
return $S_w, T_w, L_w$
```

and uses it to obtain a new set of substations to select from that may result in maximum damage in the current iteration j. For each $s \in \hat{S}$, $\texttt{Worst\_Attack}(G_p, P_t, B_P)$ computes and returns the transmission line outages corresponding to the selected protection assemblies and load loss denoted by T_P, L_P respectively that cause maximum damage. In each iteration j, if $L_P > L_w$ then the solution is updated. The loop terminates if no further improvement $L_g - L_w$ is observed.

The function Worst_attack() is described as Algorithm 2. The algorithm intelligently selects the critical protection assemblies one-by-one to isolate transmission lines that cause maximum load loss (equation 1). It takes as input the power system model G_p, substation components P_t, and the protection assembly budget B_P. Further, it identifies the maximum load loss $L_w^{'}$ and the outages $T_w^{'}$. The algorithm starts with an empty set and uses $\texttt{Max\_loss}(G_p, P_t, \emptyset)$ to identify the component outages resulting in maximum damage. This function simulates a set of contingencies, i.e., outages of components and returns the one that cause maximum load loss. The components and corresponding load loss is represented by $T_P^{'}$, $L_P^{'}$ respectively. For each iteration i, $\texttt{Updated\_comps}(P_t, T_P^{'})$ uses $T_P^{'}$ and returns a new set of components $\hat{P}_t$ to be removed from G_p depending upon B_P. $\hat{P}_t$ represents a list of contingencies that are needed to be simulated. Next, $\texttt{Max\_loss}(G_p, P_t, \hat{P}_t)$ uses the updated component list $\hat{P}_t$ to identify the maximum load loss causing components in the current iteration i. In each iteration i, if the load loss $L_P^{'}$ is greater than the maximum load loss $L_w^{'}$ then the solution is updated. The worst-case running time of Algorithm 1 is $O(|S| \times |B_S| \times |P| \times |B_P|)$, which is non-exponential.

IV. Defender Model

In this section, we provide the defender model to improve the power system resilience by minimizing the load loss. Here, based on the attack on the substations and its components, a set of critical substations to be protected is identified.

Algorithm 2 Algorithm for Worst_Attack() Function

```
Input: $G_p, P_t, B_P$
Initialize: $L_w^{'} \leftarrow 0, T_w^{'} \leftarrow \emptyset$
$T_P^{'}, L_P^{'} \leftarrow \texttt{Max\_loss}(G_p, P_t, \emptyset)$
$L_w^{'} \leftarrow L_P^{'}$, $T_w^{'} \leftarrow T_P^{'}$
for $i = 1, \ldots, B_P$ do
    $\hat{P}_t \leftarrow \texttt{Updated\_comps}(P_t, T_P^{'})$
    $T_P^{'}, L_P^{'} \leftarrow \texttt{Max\_loss}(G_p, P_t, \hat{P}_t)$
    if $L_P^{'} > L_w^{'}$ then
        $L_w^{'} \leftarrow L_P^{'}$, $T_w^{'} \leftarrow T_P^{'}$
    end if
end for
return $T_w^{'}, L_w^{'}$
```

A. Defender's Problem

The goal of the defender is to improve the system resilience and minimize the load loss possible. A defender achieves this by protecting a subset of substations D_S from the total number of substations S, i.e., $D_S \subseteq S$. The defender is resource bounded, i.e., it can protect at most B_D substations. The substations can be protected using various methods such as better firewall protection against intrusion, application whitelisting, network segmentation [18]. Note that this model can provide important insight upon which substations can be upgraded first considering financial budget constraints and the worst-case attack. The problem is formally defined below.

Problem 2 (Defender's Problem): Given a power system G_p and a defense budget B_D, find a defense strategy D_P that minimizes the load loss in the power network. Formally,

$$\begin{aligned} &\underset{D_S}{\operatorname{argmin}} \; \max_{S^{'} \subseteq S - D_S} \; \max_{P^{'} \subseteq F(S^{'})} \; J(A_P) \\ &s.t. \quad |D_S| \leq B_D, \quad |S^{'}| \leq B_S, \quad |P^{'}| \leq B_P \end{aligned} \tag{3}$$

B. Algorithm for Finding the Critical Substations to Protect

Using exhaustive search to identify the critical substations to protect is computationally infeasible due to the combinatorial nature of search space [17]. Hence, we present an efficient Algorithm 3 to find the set of critical substations to protect. The algorithm starts with an empty set and intelligently selects the critical substations one-by-one to protect that minimizes system damage. It takes the power system model G_p, the substation budget B_S, the protection assembly budget B_P, and the defense budget B_D as inputs. Further, it identifies the critical substations S_D to be protected to minimize the load loss during an attack.

First, the worst-case attack with no defense is obtained using $\texttt{Get\_Attack}(G_p, B_S, B_P, \emptyset, \emptyset)$, which is same as Algorithm 1. It provides the substations $\hat{S}_w$ to compromise that maximizes the damage. From the identified worst-case attack, the substation to be protected is identified using $\texttt{Get\_Attack}(G_p, B_S, B_P, S_D, s)$. This function is similar to Algorithm 1, however, it computes the worst-case attack after removing the substations to be protected S_D and the substation s that belongs to $\hat{S}_w$ from the attackers list of attackable substations. For each iteration i and for each $s \in \hat{S}_w$, the substation to be protected that minimizes the load loss, i.e., if

Algorithm 3 Algorithm to Find Critical Substations to Protect

```
Input: $G_p, B_S, B_P, B_D$
Initialize: $S_d^{'} \leftarrow \emptyset, S_D \leftarrow \emptyset, L_w \leftarrow 100$
$\hat{T}_w, \hat{L}_w, \hat{S}_w \leftarrow$ Get_Attack$(G_p, B_S, B_P, \emptyset, \emptyset)$
for $i = 1, \ldots, B_D$ do
    $L_w \leftarrow 100$
    if $S_D \neq \emptyset$ then
        $\hat{S}_w \leftarrow$ Get_Attack$(G_p, B_S, B_P, S_D, \emptyset)$
    end if
    for all $s \in \hat{S}_w$ do
        $\hat{T}_w, \hat{L}_w, S_{sub} \leftarrow$ Get_Attack$(G_p, B_S, B_P, S_D, s)$
        if $\hat{L}_w < L_w$ then
            $L_w \leftarrow \hat{L}_w$, $S_d^{'} \leftarrow s$
        end if
    end for
    $S_D \leftarrow S_D \cup S_d^{'}$
end for
return $S_D$
```

$\hat{L}_w < L_w$ is identified and the solution is updated, i.e., $S_D \leftarrow S_D \cup S_d^{'}$. Next, depending upon B_D, for each iteration i, the new set of critical substations to compromise $\hat{S}_w$ is obtained using Get_Attack$(G_p, B_S, B_P, S_D, \emptyset)$ based on S_D. This function returns the new worst-case attack by considering only the substations that are not protected. The worst-case running time of Algorithm 3 is $O(|S| \times |B_D| \times |S| \times |B_S| \times |P| \times |B_P|)$, which is non-exponential.

V. Evaluation

To evaluate the developed algorithms, we apply them to the standard IEEE-14, 39, and 57 bus systems. We used a steady state simulator discussed in [17] for our analysis. First, we discuss an attack-defense scenario for the standard IEEE-14 bus system shown in Figure 1. The blue colored dotted lines represent the substations denoted by S1 , . . . , S10. Each transmission line is protected by a pair of protection assembly denoted by PAn, where n ∈ ℕ. These protection assemblies within the substations can be manipulated to open the circuit breakers that can disconnect the transmission lines from the network to initiate the cascading failures causing severe damage to the power network. Table I shows the details of the performed case study. The attack budget for the system is assumed to be 2. However, the defense budget is increased in steps up to a total of 6 substations. From Table I, it is clear that the load loss for the IEEE-14 bus system is significantly minimized by intelligently selecting the substations to be protected. Moreover, with an increase in the defense budget, a total of 57.31% improvement in load loss is observed. The substations that are attacked and defended are mentioned in table I. Similar results for IEEE-39, 57 bus systems can be obtained using the developed models.

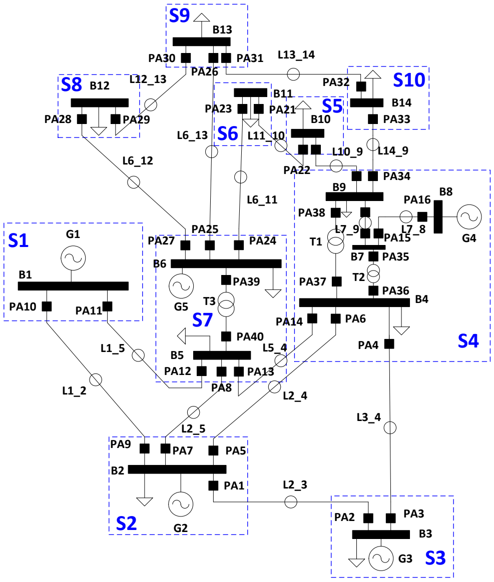


Fig. 1: IEEE-14 Bus System [16]

Now, we identify the worst-case attack and defense for the three standard IEEE systems. Figure 2 represents the load loss as a function of various attack and defense budgets. In each figure the x-axis represents the defense budget and the y-axis represents the overall system load loss. Red, green and blue colored markers represent attack budget 2, 3 and 4 respectively. The respective colored markers at defense budget ‘0’ corresponds to the load loss with no defense. From figure 2, it is clear that by carefully selecting the substations to be protected and with increase in the defense budget the overall system loss is significantly minimized and the adversary is unable to maximize the damage even with increase in the attack budget. In our analysis, we choose a defense budget of 0-50% of the total number of substations for each system.

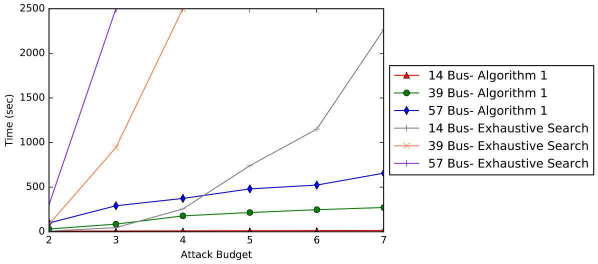


Fig. 3: Attack execution time

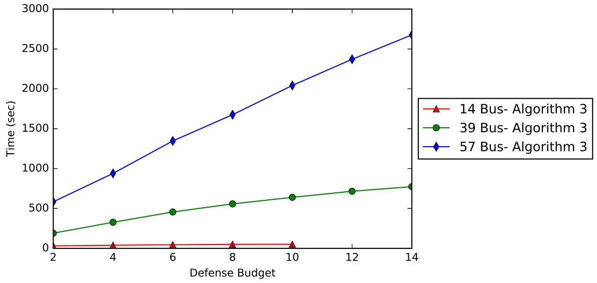
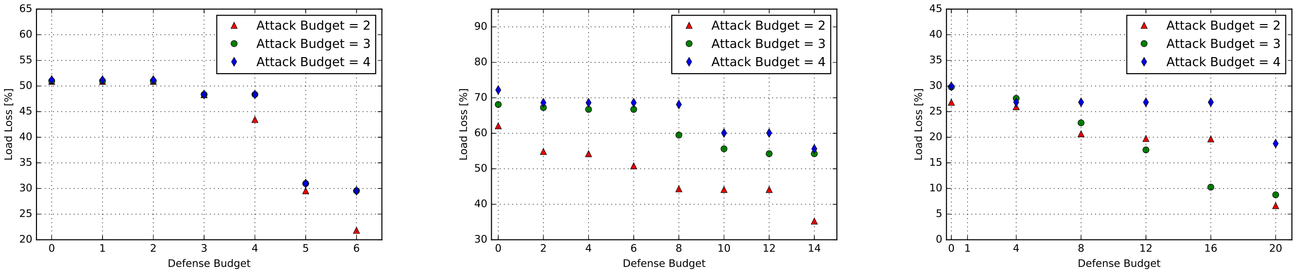


Fig. 4: Defense execution time

Further, we discuss the time taken to identify the worst-case attack and defense shown in figures 3 and 4 respectively. In each figure, the x-axis represents the attack or defense budget whereas the y-axis represents the time. Red, green and blue lines represent the worst-case attack or defense identification time for IEEE-14, 39, and 57 bus systems respectively. From figure 3, it is clear that as the attack budget increases, the time taken to obtain the worst-case attack increases marginally

TABLE I: IEEE-14 Bus System Attack-Defense Scenario

Attack Budget (B_S)	B_P	**Defense Budget** (B_D)	**Pre-Defense Load Loss**	**Post-Defense Load Loss**	**Substations Attacked**	**Substations Defended**	**Improvement** (%)
2	2	3	51.17	48.30	S7	S4, S3, S2	5.61
2	2	4	51.17	43.46	S1, S6	S4, S3, S2, S7	15.07
2	2	5	51.17	29.55	S8, S9	S4, S3, S2, S7, S6	42.25
2	2	6	51.17	21.84	S5, S10	S4, S3, S2, S7, S6, S9	57.31



(a) IEEE-14 bus system

(b) IEEE-39 bus system

(c) IEEE-57 bus system

Fig. 2: Load loss as a function of various attack and defense budgets for different standard IEEE systems.

for the three systems which is insignificant when compared with the time taken by exhaustive search for 14, 39 and 57 bus systems shown by gray, coral, and violet colored lines respectively. The algorithm also provides mostly the same solution for these systems as the exhaustive search. Similar analysis can be performed for defense scenario. Figure 4 shows that as the defense budget increases, the time taken to identify the critical set of substations to be protected increases slightly which is again inconsiderable if compared with the exhaustive search. It clearly shows that our algorithms perform much better than the exhaustive search. This is mainly because of the fact that in each iteration of these algorithms, our search is guided intelligently to significantly reduce the search space in order to obtain an efficient and effective solution.

VI. Conclusions

The attacker and defender models along with the algorithms to obtain the worst-case attack and defense were developed. The main idea of the attacker model is to select the subset of substations causing maximum system damage when compromised by an adversary. However, the defender model operates to protect the subset of substations that minimize the system damage. The case study on IEEE systems showed how the damage to the power network can be significantly reduced by intelligently selecting a subset of substations to protect, given a defense budget. Under financial budget constraints, prioritizing and protecting the critical substations can greatly increase system resilience. Moreover, these algorithms can be easily applied to larger systems with higher attack and defense budgets. As part of the future work, these models can be applied to changing network topologies to provide online solutions for prioritizing defense resources.

Acknowledgment

This work is funded in part by the National Science Foundation under the award number CNS-1329803 and the NSF FORCES project under the award number CNS-1238959.

References

[1] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Computer Networks*, vol. 57, no. 5, pp. 1344–1371, 2013.

[2] D. B. Rawat and C. Bajracharya, "Cyber security for smart grid systems: Status, challenges and perspectives," in *SoutheastCon 2015*.

[3] T. Pultarova, "Cyber security-Ukraine grid hack is wake-up call for network operators [news briefing]," *Engineering & Technology*, 2016.

[4] P. Oman, A. Risley, J. Roberts, and E. Schweitzer, "Attack and defend tools for remotely accessible control and protection equipment in electric power systems," in *55th Conf. for Protective Relay Engineers*, 2002.

[5] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, p. 13, 2011.

[6] "Destructive cyber attacks increase in frequency, sophistication," *AFCEA,[Online] Available at: https://www.afcea.org/content/Article-destructive-cyber-attacks-increase-frequency-sophistication*.

[7] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. Butler-Purry, "A framework for modeling cyber-physical switching attacks in smart grid," *IEEE Transactions on Emerging Topics in Computing*, 2013.

[8] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, E. G. Im, Z. Yao, B. Pranggono, and H. Wang, "Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in smart grid scada systems," 2012.

[9] H. Lin, H. Alemzadeh, D. Chen, Z. Kalbarczyk, and R. K. Iyer, "Safety-critical cyber-physical attacks: Analysis, detection, and mitigation," in *Proceedings of the Symposium and Bootcamp on the Science of Security*. ACM, 2016, pp. 82–89.

[10] S. Sridhar and G. Manimaran, "Data integrity attack and its impacts on voltage control loop in power grid," in *PES General Meeting, 2011*.

[11] B. Chen, S. Mashayekh, K. L. Butler-Purry, and D. Kundur, "Impact of cyber attacks on transient stability of smart grids with voltage support devices," in *Power and Energy Society General Meeting (PES), 2013*.

[12] J. Hao, R. J. Piechocki, D. Kaleshi, W. H. Chin, and Z. Fan, "Sparse malicious false data injection attacks and defense mechanisms in smart grids," *IEEE Transactions on Industrial Informatics*, 2015.

[13] Y. Yuan, Z. Li, and K. Ren, "Quantitative analysis of load redistribution attacks in power systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1731–1738, 2012.

[14] V. Turau and C. Weyer, "Cascading failures caused by node overloading in complex networks," in *Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG), IEEE 2016*, pp. 1–6.

[15] S. Hasan, A. Chhokra, A. Dubey, N. Mahadevan, and G. Karsai, "A simulation testbed for cascade analysis," in *IEEE PES ISGT*, 2017.

[16] http://icseg.iti.illinois.edu/power-cases/, ICSEG.

[17] S. Hasan, A. Ghafouri, A. Dubey, G. Karsai, and X. Koutsoukos, "Heuristics-based approach for identifying critical n- k contingencies in power systems," *Resilience Week*, 2017.

[18] T. R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the cyber attack on the ukranian power grid. defense use case," *SANS ICS*, 2016.