Study of Learning of Power Grid Defense Strategy in Adversarial Stage Game

Shuva Paul, Zhen Ni
School of Electrical Engineering and Computer Science
South Dakota State University
Brookings, SD 57006
Email: {shuva.paul, zhen.ni}@sdstate.edu

***Abstract*—Security of electric power transmission and distribution systems is currently one of the most challenging issues due to rising concerns regarding increased cyber-attacks in the energy sector. In the smart electric power transmission and distribution system, cyber-attackers are capable of causing large-scale damage (including blackout). In response to these attacks in the energy sector, different machine learning based game theory approaches are used to mimic the complex interactions between adversaries (the attacker and defender) in a smart electric power system. Most of the existing works fail to replicate the real-time interactions by verifying the criticality of the identified contingencies or by reflecting the attack impacts on the power system. In this paper, we identify the critical contingencies of an electric power transmission and distribution system adopting an adversarial stage game with value iteration. We adjust the defense strategy from attacker's learned attack action (eventually reduces the generation loss) and provide alternative action choices in case of limited access to the system. Then, we analyze the impact of the learned attack policies in a simulated power system using the PowerWorld simulator in two case studies. All the experiments are conducted on two standard power system test cases (W $\&$ W 6 bus system and IEEE 39 bus system). The effectiveness of the learned policy is verified by adjusting the defender's policy according to the attacker's learned policy. The simulation results successfully prove the efficiency of the proposed research in learning critical contingencies, providing defense strategies, and replicating the attack impacts on power systems.**

***Index Terms*—Reinforcement learning, Markov decision process, defense strategy, adversary, and stage game.**

I. Introduction

Learning methods are becoming popular in different fields of cyber-physical power system. These fields include planning, operation, maintenance, control, and security of the system [1]–[3]. Currently, the vulnerability of the power system has become significantly important due to the increased complexity and inter-connectivity of heterogeneous devices. Several power outage related incidents occurred around the globe recently, such as in Ukraine, Kenya, Nigeria, and New York [4], [5]. In 2017, the number of total power outage events in the United States was $3,526$ and affected almost 36.7 million people. Among the different reasons behind these power outage events, terrorist attack is very crucial. Over 42 international terrorists groups were listed by the United States Department of State around the world as potential threats to the United States in 2006. Attackers conducted approximately $2,500$ attacks against transmission lines and towers in different parts of the globe over the last 10 years [6]. The most frequently attacked element of power transmission and distribution systems is the power stations. Power stations have been attacked more than 500 times in the past decade. According to a recent study conducted by ITIC (information technology industry council), just 60 minutes of downtime causes an organization to lose $\$100,000$. In 2017, power outage events in the United States caused power outages for $284,086$ minutes, which is almost equivalent to 197 days [6]. So, the large amount of financial damage we are bearing due to the power outage events is a major concern for the utility operators and planners. The advancement in cyber-weapons is making the power system more vulnerable. Dragonfly, Dragonfly 2.0, NotPetya, WannaCry, Industroyer, and Stuxnet are among the modern generation cyber weapons [7]. MadIoT (Manipulation of Demand) is one of the recent advances in the attack types which manipulates the demand to cause frequency deviation, cascaded failures, and so on. According to security experts, we are heading towards a *Cyber Pearl Harbor*, and the next $9/11$ will be in the energy sector. Considering the impacts of the cyber-attacks on energy sector, we divide the power system entities into two groups: the terrorists and the authorities or the operators. The terrorists intend to attack the system to cause and maximize damage. On the other hand, the power system operators aim to protect the system elements from loss or to reduce the damages. The interactions between these entities depend on several factors, such as their targets, accessibility to the information, and their rationality. Game theory is a useful analytical tool to analyze these complex interactions between the adversaries. Machine learning can provide a strong foundation to the formulation and solution of these game theoretical models in the adversarial networks. Recently, more research has been attempting to identify the defense strategy of a cyber-physical power system in response to the attack actions using game theory and machine learning [8]–[10].

In [11], the authors implemented a static game theory solution concept, identified as the *Shapley* value, to represent the coalition formation game theory in assessing the component's criticality. The authors in [12], implemented a stochastic game in smart grid security against coordinated

cyber-physical attacks as a two-person zero-sum game. In [13], the authors replicated the cascading failure attacks in the smart power system using a stochastic one-shot game. A two-player game theory-based adversarial framework for a false data injection attack against power system measurements is implemented by the authors in [14]. They implemented a two-player zero-sum game as a one-shot process. In [15], the authors implemented a multi-stage game between the adversaries of the system adopting a sequential attack. They used a reinforcement learning algorithm to solve the game and provide the attacker's optimal action choices. So, the Markov decision processes and game theory have been used recently for solving problems in the smart grid. Some of the aforementioned literature uses collaborative environments for game implementation in the power system. Most of the game related vulnerability analysis in the literature did not verify the severity of the attack by adjusting learned action policies of the attacker. Additionally, they did not consider the limited accessibility over the systems' information and alternative choices of actions. Moreover, the attack impact is rarely analyzed in the aforementioned literature. These limitations obstruct the scope of the existing research in analyzing the vulnerability of the system in the presence of adversaries.

Motivated by the aforementioned literature, our aim is to recreate some high-impact, low-frequency (HILF) events in the grid operation. We implement a stage-game (one-shot game) between the adversaries and propose the solution based on a reinforcement learning algorithm by identifying optimal attack strategies (capable of triggering HILF events). We provide alternative action choices to the attacker in case of limited access to the system. We further validate the severity of the identified contingencies by adjusting the defender's defense strategy following the attacker's learned action. We also illustrate the impact of the learned attack policies in a simulated power system platform (PowerWorld).

The rest of the paper is organized as follows: Section II provides detailed explanation and analysis of the benchmark models, threat and attack model, the attacker-defender two-person stage game. Section III provides details about the design parameters of the game, simulation results and analysis. Finally, we conclude the paper by summarizing the contribution of the paper in Section IV.

II. Problem formulation and solution

In this section, we formulate the gaming framework between the adversaries in the power system. We solve the formulated adversarial stage game using a reinforcement learning algorithm. We discuss the test benches, threat and attack model, and formulation and solution of a two-person stage game between the adversaries.

A. Benchmark model

The majority of simulation studies related to the power system are conducted on standard test cases available online. To conduct the game, W & W 6 bus system, and IEEE 39 bus system are used as the test systems. These models have the following configurations:

Table I: System summary of the test systems used to conduct the adversarial stage game.

	W & W 6 bus system	IEEE 39 bus system
Total loading capacity (MW)	210	6150
Total transmission lines	11	46
Total bus number	6	39
Total generators	3	10

To create the attack scenario the topological information is used by the attacker. The threat and attack model will be explained briefly in the next sub-section.

B. Threat and attack model

We first consider that the cyber-attacker gained access to the control center of electric power system. It has the limited ability to switch transmission lines from active to inactive status (line switching). The threat and attack model is adopted from [15], [16]. The model starts with initializing the pre-contingency power flow. By dispatching the pre-contingency power flow we ensure the $n-1$ contingency security of the system. We apply the contingencies by switching the selected transmission lines from active status to inactive status. Then we apply $n-k$ contingencies, where k is the order of the contingencies. After execution of the attack, the simulation is terminated. Due to the execution of attack, the system may be separated into multiple islands. Then the generator ramp rates are varied to adjust the demand and supply. Once the generators re-dispatch the power flow, the total generation, $\sum_{g\in G} P_g$ is compared to the total demand, $\sum_{d\in D} P_d$ which is defined by Z where, $Z = (\sum_{g\in G} P_g - \sum_{d\in D} P_d > 0)$. Here, G and D are the set of generators and load buses, respectively. If $Z > 0$, generators in the islands are tripped one by one to balance the generation and demand. If $Z < 0$, load shedding occurs as the multiplication of a scalar quantity, λ, where, $\lambda = \frac{\sum_{g\in G} P_g}{\sum_{d\in D} P_d}$. Then, we apply a standard DC power flow to check the overloads in the transmission lines. The overloads are calculated using the formula below:

$$\Delta o_j(t,\Delta t) = \begin{cases} \int_t^{t+\Delta t} (f_j(t) - \bar{f}_j)dt & \text{if} f_j(t) > \bar{f}_j \\ 0 & otherwise \end{cases} \quad (1)$$

Then, we update the relay settings. We use time delayed overcurrent relays to identify the branches to be tripped due to overcurrent. The overcurrent threshold is termed as $\bar{o_j}$. For branch j, if the power flow is f_j and flow limit is $\bar{f}_j$, the outage occurs when concurrent overload o_j exceeds the limit $\bar{o_j}$.

C. Attacker-defender two-person stage game using Q-learning

We formulate the game between the adversaries of the power system as a two-person stage game.

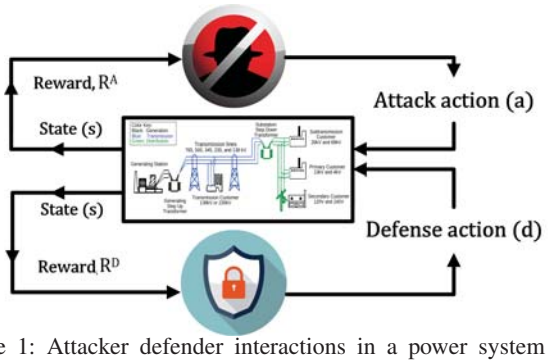

Figure 1: Attacker defender interactions in a power system represented by Q-learning.

Figure 1 shows the attacker-defender interaction in the power system environment represented by a Q-learning framework. Q-learning basically learns the optimal action policies based on the action execution by the agent and its feedback from the environment. The adversaries in the power system act like the agents and the power system itself can be considered as the environment for learning procedures. The rewards are the feedback from the environment as a result of the adversaries' actions. We use typical reinforcement learning to learn the optimal action strategies of the adversaries. The quality of the state of this game is defined by

$$Q(s,a,d) \ = R(s,a,d) + \gamma \sum_{s'} T(s,a,d,s')V_a(s') \quad (2)$$

where, Q is the quality of the state s, associated with actions a, and d. R, represents the reward associated with these actions. γ, represents the discount factor and it ranges from 0 to 1. $T(s,a,d,s')$, represents the transition function to transit from state s to s' due to the execution of action a and d. This state transition is considered equal for all the states. The value of the state for the attacker can be defined by:

$$V_a(s') \ = \max_{\pi \in \Pi} \min_{d} \sum_{a} Q(s',a,d)\pi(a) \quad (3)$$

We assume the defender is a passive player and attacker is the leading player. So, the defender's action will be fixed throughout the game and the attacker will learn via a trial and error process playing against the defender. This problem can be solved using value iteration [17], [18].

$$\begin{aligned} &\max_{\pi} V_a(s') \\ &s.t. \sum_{a \in S_{N_a}} Q(s,a,d)\pi \ \geq V_a(s') \\ &\sum_{a \in S_{N_a}} \pi(a) \ = 1 \\ &\pi(a) \ \geq 0, \forall a \in S_A \end{aligned} \quad (4)$$

The optimal policy can be defined as

$$\pi'(s) = \arg\max_{a} Q_{\pi}(s,a,d) \quad (5)$$

We update the probabilities of the state-action pairs following the formula below

$$Pr(s,a,d) \ \leftarrow \frac{C(s,a,d)}{\sum_{a \in A, d \in D} C(s,a,d)} \quad (6)$$

where, $C(s,a,d)$ represents the number of times state s is visited by the agent (the attacker) while taking action $a \in A$. This probability is calculated based on the frequency of that specific state action pairs visited. The attacker's mixed strategy for a given state s will be:

$$\pi_A(s) \ = [Pr\{a(s) = a_1\}, \ldots, Pr\{a(s) = a_N\}] \quad (7)$$

where

$$\sum_{i=1}^{N} Pr\{a(s) = a_i\} \ = 1 \quad (8)$$

Here $Pr\{a(s) = a_i\}$ is the probability of choosing attack action a_i in state $s \in S_A$. $\pi_A(s)$ is the probability distribution over the attacker's action space associated with state s.

III. Simulation studies

The simulation is conducted using MATLAB R2018a on a standard PC with an Intel(R) i7-6700 CPU running at 3.40GHz and 24.0 GB RAM.

A. Design parameters

In this subsection, we describe the design parameters for the adversarial stage game in cyber-physical power system security.

The collection of targets for the adversaries are termed as attack and defense sets. In this game, the attacker is an active player and the defender is a passive player. We use line switching attack as the attack scheme of this game. So, both the adversaries' target sets will consists of the transmission lines from the test systems. The attacker's target set can be represented by

$$S_a = \{x_1, x_2, \ldots, x_n\} \quad (9)$$

where x_n represents the n^{th} transmission line among the targets of the attacker in the test system. Similarly, the defender's target set can be represented by

$$S_d = \{y_1, y_2, \ldots, y_m\} \quad (10)$$

where y_m represents the m^{th} transmission line among the targets of the defenders in the test system. After each attack-defense action execution, the reward is assigned as the feedback from the environment (the power system). The reward is defined as the generation loss due to the attack-defense actions in the power system. The target of the attacker is to maximize the generation loss of the system while the defender is trying to minimize generation loss with its passive defense policy. The value of γ close to zero ensures that the agent will focus on short term/immediate reward. And the value of γ close to 1 ensures that the agent will focus on long term reward (future reward). In this game, we consider the value of γ as 0.9. So, the agent will focus on long term reward rather than immediate reward. The exploration and exploitation probability is represented by ϵ. It ranges from zero to one. It represents how much of the total iterations the agent (learning) will explore and how much it will follow optimal policy. The value of ϵ initially starts with a relatively large number. Then it gradually reduces to a very small positive value (final ϵ) close to zero. We use generation loss as the immediate reward of an action.

B. Simulation results

In this subsection, we conduct some case studies for stage game between the power system adversaries.

1) Case study 1 (W & W 6 bus system): In this case study, we conduct the stage game between the adversaries in W & W 6 bus system. The system has 6 buses and 11 transmission lines. So, the defender's defense policy will be fixed throughout the game. First, we randomly assume that the defender is defending transmission line 1. We further assume that the defended transmission line cannot be attacked.

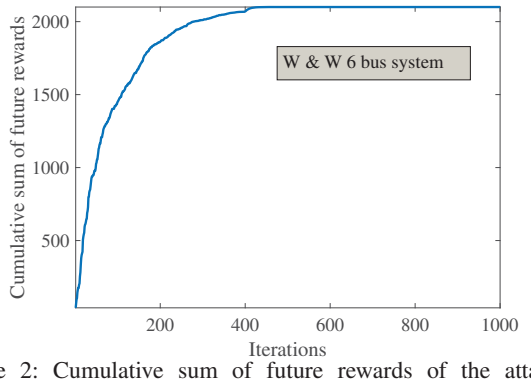

Figure 2: Cumulative sum of future rewards of the attacker in the adversarial stage game. The defender is defending a randomly predefined transmission line (transmission line 1).

Figure 2 shows the cumulative sum of future rewards (Q-values) for the adversarial stage game conducted between the adversaries. The attacker conducts the game for 1000 iterations for learning through a trial and error process. From the figure, we can see that after 400 iterations the learning agent converges to it's optimal policy. The agent follows equation (6) to update the probabilities of these action selections.

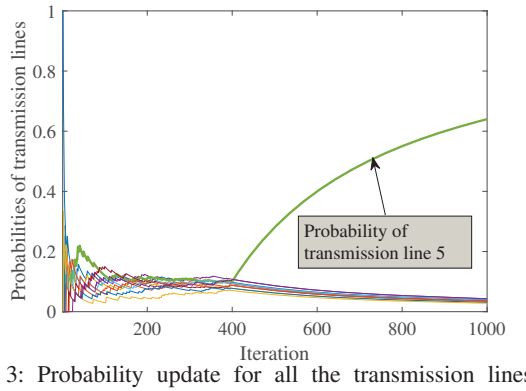

Figure 3: Probability update for all the transmission lines to be selected as an action. The green curve shows the probability update of transmission line 5. The initial oscillation in probability updating of the transmission lines represents the random exploration of the action selection by the attacker.

Figure 3 shows the probability update of the transmission lines of W & W 6 bus system to be selected as an attack action. From this figure, we can see that the probability of transmission line 5 to be selected as an attack action increases after enough exploration (after 400 iterations). The initial oscillations of the probabilities of the transmission lines happens due to the random action selection of the agents during the learning process (exploration). On the other hand, the probabilities of the other transmission lines to be selected as attack actions (optimal actions) drop while following the greedy policy.

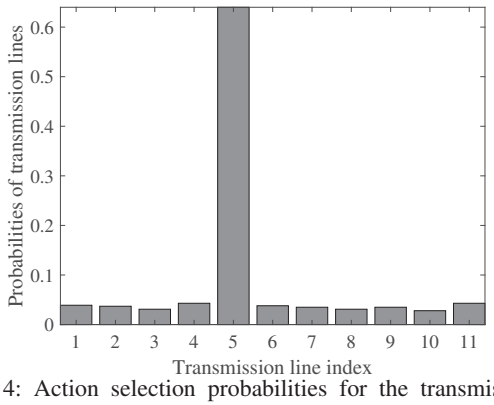

Figure 4: Action selection probabilities for the transmission lines of W & W 6 bus system. Transmission line 5 has the higher probability to be selected as an action while the defender is defending transmission line 1.

Figure 4 shows the probabilities of the transmission lines for action selection. From this figure, we can see that transmission line 5 has the highest probability to be selected as an attack action while the defender is defending transmission line 1. In practical life, it may happen that, after triggering the attack the transmission line is reinforced due to the protection scheme of the system or that specific transmission line or area is connected to distributed energy resources (DER). In that case, attacking on that transmission line will not be successful. In any of these cases, if transmission line 5 is not accessible, connected to DER or reinforced, the attacker will attack the transmission line with the next highest probability. If transmission line 5 is inaccessible, the next highest probability goes with transmission line 4 or 11 which is 0.043. So, the attacker will select these transmission lines as the attack action. Next, we consider that learning the most critical transmission line of W & W 6 bus system, we adjust the defense policy of the defender. Now, the defender will protect transmission line 5. With this new defense policy, we conduct the game again.

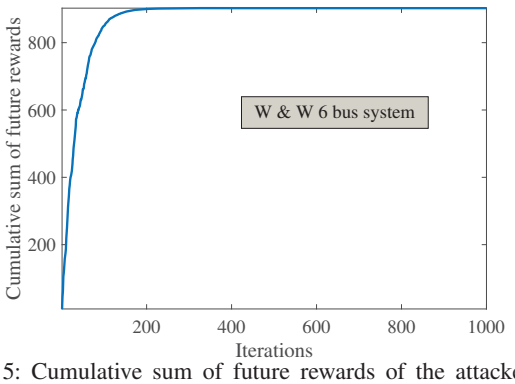

Figure 5: Cumulative sum of future rewards of the attacker in the adversarial stage game with the adjusted defender's policy in W & W 6 bus system. The sum of future rewards reduces as we adjust the defender's policy according to the attacker's learned action policy.

Figure 5 shows the cumulative sum of future rewards for the attacker. Compared to Figure 2, the adjusted policy has lower value of cumulative sum of future rewards (generation loss is reduced).

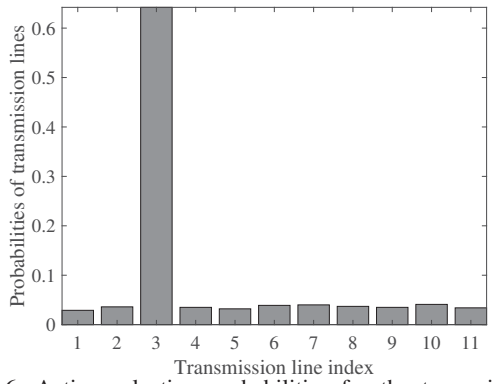

Figure 6: Action selection probabilities for the transmission lines of W & W 6 bus system with the adjusted defender's policy. As the defender is defending transmission line 5 (adjusted), the attacker selects the next most critical transmission line (transmission line 3 to attack.)

Figure 6 shows the action selection probabilities of the transmission lines of W & W 6 bus system with the adjusted defender's policy. So, according to this figure, while the defender is defending transmission line 5, the attacker will attack transmission line 3.

2) Case study 2 (IEEE 39 bus system): In this subsection, we use IEEE 39 bus as the test system to conduct the adversarial stage game and then we analyze the impact of the attack on a simulated power system using the PowerWorld simulator. First, we conduct the stage game on the IEEE 39 bus system to identify the most vulnerable branch/branches from the system.

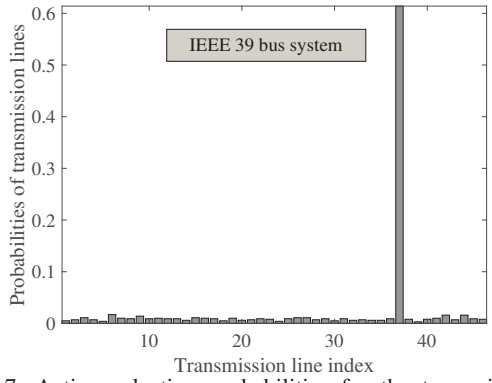

Figure 7: Action selection probabilities for the transmission lines of IEEE 39 bus system. The defender's pre-defined action policy is transmission line 5.

Figure 7 shows the action selection probabilities for an adversarial stage game in the IEEE 39 bus system. From this figure, we can see that transmission line 37 has the highest probability to be selected as an action by the attacker. From several runs, we found that there are actually three transmission lines most vulnerable in the IEEE 39 bus system. They are transmission line 8, 12, and 37. And the selection probability of this transmission lines is 0.614.

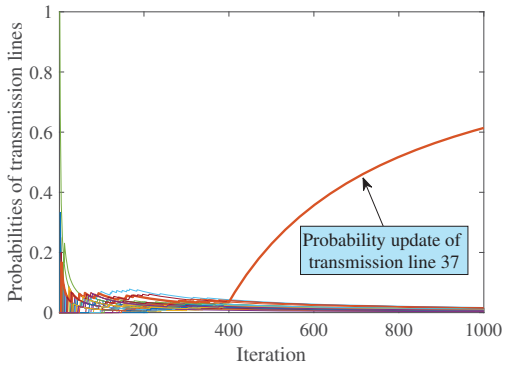

Figure 8: Probability update of the attacker's action selection probabilities for the IEEE 39 bus system. The randomly predefined defense action is transmission line 5. The red curve shows the probability update of transmission line 37 to be selected as the attack action.

Figure 8 shows the updating of the probabilities via trial and error in the learning process. Switching transmission line 37 will cause cascaded failure of several transmission lines (lines 12, 8, 5, 21, 18, 4, and 31). This attack also creates multiple sub-grids from different buses, such as bus 10, 14, 25, and 31 divides into 2, 3, 4, and 5 sub-grids, respectively. There are more buses that divide into multiple sub-grids. Now we move forward to the PowerWorld simulator to observe the impact of the transmission line attack in the simulated power system. We conduct the simulation for 3 seconds and assume the attack happens at 1.5 seconds. We attack transmission line 37 as the target. Transmission line 37 is connecting bus 6 and bus 31. Due to the attack, transmission line 6 opens from both ends. For evaluation of the impact, we consider voltage violation as the index. Several references reported different voltage limits [19], [20]. We assume the voltage limit for bus voltages in per unit is 0.9 to 1.1.

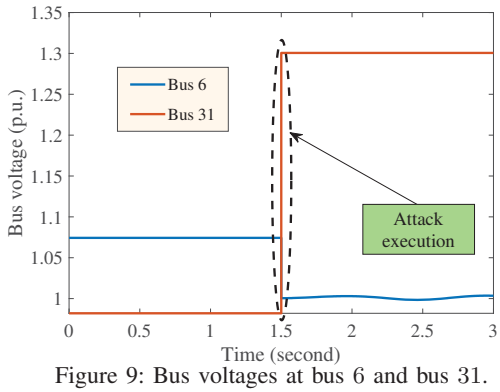

Figure 9: Bus voltages at bus 6 and bus 31.

Figure 9 shows the bus voltages at bus 6 and bus 31. Voltage at bus 6 drops from 1.074 to 1.003, which is within the range. But, voltage at bus 31 rises from 0.982 to 1.301, which is above the upper limit of the voltages (p.u.). So, bus 31 violates the voltage limit. Figure 10 shows the generation and load change before and after switching transmission line 37 in IEEE 39 bus system. The attack over transmission line 37 reduces the generation and load of the system by creating disturbances in the system.

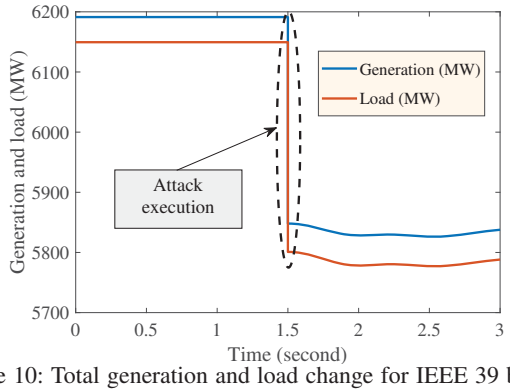

Figure 10: Total generation and load change for IEEE 39 bus system before and after the attack. Both units are in MW.

Figure 11 shows the line current flow (p.u.) in transmission line 37. The figure shows that the current drops to zero at 1.5 seconds due to the initiation of the attack.

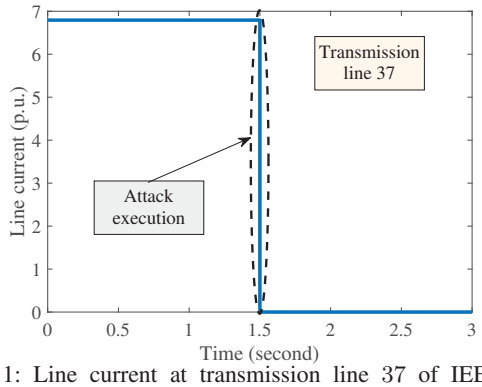

Figure 11: Line current at transmission line 37 of IEEE 39 bus system.

Apart from the impacts on the bus voltages and generations, the frequency of the system also becomes unstable due to the attacks. According to the European Network of Transmission System Operators for Electricity (ENTSOE) standards, if the frequency of the European grid goes beyond the range $[47.5Hz$ - $51.5Hz]$, the system can hardly avoid a blackout.

IV. Conclusion and Discussion

Learning based vulnerability identification and defense strategy formulation is becoming very crucial. In this paper, we implement a stage game between the adversaries of the power system and identify the critical elements of that power system. In case study I, we identify the critical transmission line of the W & W 6 bus system, provide alternative action choices for the attacker and further prove that timely adjustment of the defense strategy from the learned attack actions reduces the system loss. In case study II, we identify the critical elements of the IEEE 39 bus system and further analyze the impact of the attack in the power system using the PowerWorld simulator. These outcomes of the case studies will provide clear insight for learning the defense strategy in the adversarial grid environment.

Acknowledgment

This work is supported in part by National Science Foundation under grant $\#OIA-1833005$ and $\#ECCS-1726964$.

References

[1] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Systems Journal*, vol. 11, pp. 1644–1652, Sep. 2017.

[2] D. S. Terzi, B. Arslan, and S. Sagiroglu, "Smart grid security evaluation with a big data use case," in *2018 IEEE 12th International Conference on Compatibility, Power Electronics and Power Engineering (CPE-POWERENG 2018)*, pp. 1–6, April 2018.

[3] Z. Zheng, Y. Yang, X. Niu, H. Dai, and Y. Zhou, "Wide and deep convolutional neural networks for electricity-theft detection to secure smart grids," *IEEE Transactions on Industrial Informatics*, vol. 14, pp. 1606–1615, April 2018.

[4] V. Africa, *NIGERIA: TOTAL BLACKOUT AS POWER GRID COLLAPSES*, June 2018 (accessed November 28, 2018). Available at: https://alternativeafrica.com/2018/06/16/nigeria-total-blackout-as-power-grid-collapses.

[5] P. Fairley, *Averting the Blackout of the Century*, March 2016 (accessed November 28, 2018). Available at: http://discovermagazine.com/2016/march/15-blackout-of-the-century/.

[6] EATON, *Blackout Tracker*, 2017 (accessed November 2, 2018). Available at: http://electricalsector.eaton.com/forms/BlackoutTrackerAnnualReport.

[7] S. Rolley, *A foreign entity has breached the US power grid*, September 2017 (accessed November 28, 2018). Available at: http://willcountynews.com/2017/09/09/a-foreign-entity-has-breached-the-us-power-grid/.

[8] S. Paul and Z. Ni, "A study of linear programming and reinforcement learning for one-shot game in smart grid security," in *2018 International Joint Conference on Neural Networks (IJCNN)*, pp. 1–8, July 2018.

[9] M. Touhiduzzaman, A. Hahn, and A. Srivastava, "A diversity-based substation cyber defense strategy utilizing coloring games," *IEEE Transactions on Smart Grid*, pp. 1–1, 2018.

[10] Z. Ni, S. Paul, X. Zhong, and Q. Wei, "A reinforcement learning approach for sequential decision-making process of attacks in smart grid," in *2017 IEEE Symposium Series on Computational Intelligence (SSCI)*, pp. 1–8, Nov 2017.

[11] F. Pourahmadi, M. Fotuhi-Firuzabad, and P. Dehghanian, "Application of game theory in reliability-centered maintenance of electric power systems," *IEEE Transactions on Industry Applications*, vol. 53, pp. 936–946, March 2017.

[12] L. Wei, A. I. Sarwat, W. Saad, and S. Biswas, "Stochastic games for power grid protection against coordinated cyber-physical attacks," *IEEE Transactions on Smart Grid*, vol. 9, pp. 684–694, March 2018.

[13] W. Liao, S. Salinas, M. Li, P. Li, and K. A. Loparo, "Cascading failure attacks in the power system: A stochastic game perspective," *IEEE Internet of Things Journal*, vol. 4, pp. 2247–2259, Dec 2017.

[14] Q. Wang, W. Tai, Y. Tang, M. Ni, and S. You, "A two-layer game theoretical attack-defense model for a false data injection attack against power systems," *International Journal of Electrical Power & Energy Systems*, vol. 104, pp. 169 – 177, 2019.

[15] Z. Ni and S. Paul, "A multistage game in smart grid security: A reinforcement learning solution," *IEEE Transactions on Neural Networks and Learning Systems*, pp. 1–12, 2019.

[16] M. J. Eppstein and P. D. H. Hines, "A random chemistry algorithm for identifying collections of multiple contingencies that initiate cascading failure," *IEEE Transactions on Power Systems*, vol. 27, pp. 1698–1705, Aug 2012.

[17] C. Y. T. Ma, D. K. Y. Yau, X. Lou, and N. S. V. Rao, "Markov game analysis for attack-defense of power networks under possible misinformation," *IEEE Transactions on Power Systems*, vol. 28, pp. 1676–1686, May 2013.

[18] Y. Xiang and L. Wang, "A game-theoretic study of load redistribution attack and defense in power systems," *Electric Power Systems Research*, vol. 151, pp. 12 – 25, 2017.

[19] S. R. Islam, D. Sutanto, and K. M. Muttaqi, "A decentralized multi-agent based voltage control for catastrophic disturbances in a power system," in *2013 IEEE Industry Applications Society Annual Meeting*, pp. 1–8, Oct 2013.

[20] S. Satsangi, A. Saini, and A. Saraswat, "Clustering based voltage control areas for localized reactive power management in deregulated power system," 2012.