Adaptive Protection of Power Grids against Stealthy Load Alterations

Anjana Balabhaskara*, Sunandan Adhikary*, Ipsita Koley*, Soumyajit Dey*, Ashish R. Hota†
*Department of Computer Science, †Department of Electrical Engineering, Indian Institute of Technology Kharagpur
Email: { anjanab@kgpian, mesunandan@kgpian, ipsitakoley@, soumya@cse, ahota@ee }.iitkgp.ac.in

***Abstract*—High-energy IoT-controlled loads like large-scale Heating, Ventilation, and Air Conditioning (HVAC) are vulnerable to load alteration attacks. Attackers can compromise HVAC sensor readings and increase the load demand to cause cascading voltage failures and, eventually, blackouts. This work proposes an adaptive protection mechanism that updates the operating threshold for a voltage protection system to detect such attacks before they cause blackouts.**

I. Introduction

Power grids are designed to generate and supply electricity as consumers demand through their grid network, spanning a wide area. Frequent data acquisition and control with smarter control software maintain the operational efficiency of power grids. However, the increased connectivity of the high-voltage loads exposes the grid to malicious attacks, like *load alteration attacks (LAA)* that aim to destabilize and disconnect the grid by altering loads [1].

When the power demand is at its peak (*peak time*), or during equipment failures or extreme weather conditions, a sudden increase in load demand (i.e., load changes close to the grid's supply-power capacity) can cause a voltage drop. Such voltage failures can trigger a cascading effect, where one part of the power system's instability can spread to other areas. An attacker can easily sense such vulnerable situations and launch LAAs, causing additional components to fail and potentially resulting in a widespread blackout as a domino effect. Manipulation of Demand via IoT (MaDIoT) attack is a notorious variant of LAA that targets high energy loads with internet connectivity [2]. Instead of attacking random targets, manipulating the loads connected to the most vulnerable buses has better success rates in causing blackouts even in the presence of protection systems [3].

State-of-the-art grid protection systems operate with constant voltage thresholds that are pre-decided based on nominal line voltage. Further, the activation delay of such systems is inversely proportional to deviation of line voltage from the threshold. Such protection systems are easily bypassed by attacks mentioned in [3]. As a countermeasure, the authors of [3] propose to shed loads based on voltage dropping rate, instead of shedding fixed set of loads. However, works like [3] do not model the activation delay of protection units. Hence, it is entirely possible that voltage failure can occur before the protection units are activated. This questions the adaptiveness of state-of-the-art voltage protection systems.

In this work, we 1) establish scenarios where protection units are faithfully modeled with variable activation delays, and 2) demonstrate attacks leading to voltage failure and eventual blackouts actually happening before the protection units get enough time to activate. To address this, we propose a *learning-enabled adaptive protection system (APS)* that can adaptively update its voltage protection threshold based on the rate of the change in voltage characteristics of the most vulnerable bus. The APS is formulated using a competitive multi-agent reinforcement learning (MARL) environment with one RL agent learning to tune the protection threshold in the presence of another adversarial RL agent trying to perform a successful LAA.

The authors acknowledge the generous grants received from SERB (DST), project reference No SPR/2020/000200 for supporting this work.

II. Protection System & Attack Models

System Model: Fig. 1 presents schematic of a standard IEEE-14bus power system. In this grid network, there are 3 power generation units (marked with G), The transmission lines are connected to loads via buses as shown in the schematic diagram of the grid in Fig. 1. To cater to the load demands, the power grids are equipped with automatic control units that maintain desired voltage and frequency levels ($120V$ and $60Hz$ in USA). These automatic control units are implemented as part of a Supervisory Control and Data Acquisition (SCADA) unit, which is also used for the implementation of the protection schemes.

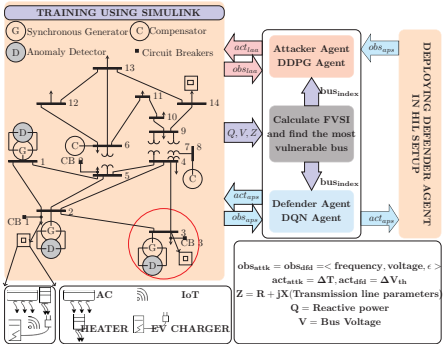


Fig. 1: Overview of our methodology

State-of-the-art Protection Systems: In a grid, there exist voltage, frequency and current protection systems in each area/bus for isolating faulty areas/buses to avoid widespread blackouts or equipment damage. The protection system components (i.e., relay switches) are activated with an *activation delay* when the voltage, frequency, and current of a bus crosses

979-8-3503-6927-4/24/$31.00 ©2024 IEEE
DOI 10.1109/ICCPS61052.2024.00038

a *static safety threshold* flagging faults like short circuits, voltage failure, etc. Activation delay for an *under voltage protection* (UVP) unit $\tau = \frac{k}{1-V/V_{th}}$, where k is the inverse time constant, V_{th} is the threshold value for under-voltage load shedding (UVLS) and V is the line voltage.

Proposed Attack Model: We propose an LAA model that attacks the *least stable bus* in a grid during peak consumption time. The stability of power system buses are indicated by stability indices and during peak consumption time, stability index is close to stability margin. We use *Fast Voltage Stability Index (FVSI)* [4] as bus stability index. A bus is unstable when *FVSI* exceeds the stability margin 1 (i.e. *FVSI* > 1). The bus with higher FVSI consumes more reactive power. A small increase of power demand at these buses can cause decrease in voltage across the loads, as the generation unit fails to meet this increase in the line current.

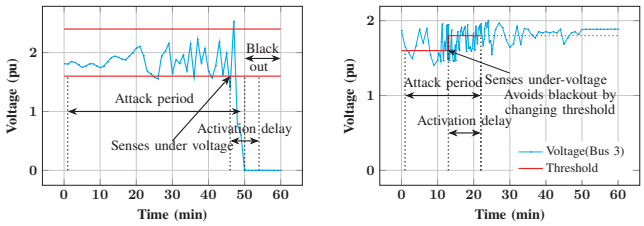
We consider that the attacker selects the most vulnerable bus with the highest FVSI and targets IoT-controlled internet-connected large-scale HVAC units connected to the bus. The heat flow $\frac{dQ}{dt}$ from HVAC heater units is directly proportional to $(T_{sp} - T_r)$ where, T_{sp}, T_r are the set-point and ambient room temperature respectively. Therefore, the *heat cost* required to reduce the difference between ambient and set-point temperatures is $\int_0^t \frac{dQ}{dt} dt$. The proposed LAA falsifies multiple temperature sensor data in HVAC units of a building to increase *heat cost* while remaining stealthy, but the demand grows significantly [2].

III. Motivating Example

We simulate an IEEE-14bus system under LAAs (as mentioned in the previous section) launched at bus 3. Fig. 2(a) plots the per unit (pu) voltage of bus 3 (V_3) in y-axis against time in the x axis. As can be seen, the existing protection scheme senses the voltage drop when V_3 goes below the lower voltage protection threshold of $V_{th} = 1.6pu$ (the red line at the bottom), i.e., at 46 mins when $(V_3 = 1.4pu) < V_{th}$. Considering the inverse time constant of the UVP system $k = 1$, $\tau = 8$ mins. Therefore, the UVP in bus 3 will activate after 8 mins following sensing, i.e. at 54 mins. As we can see in Fig. 2(a), V_3 steeply drops before the UVP is activated. Therefore, the attacker becomes successful in causing blackouts in the grid before getting detected. To counter such attacks, we propose an adaptive UVP that adaptively updates the threshold voltage V_{th}. We demonstrate this in Fig. 2(b) that has the same axes and plots as Fig. 2(a). In Fig. 2(b), we can see that the proposed APS senses the ripples and increases the under-voltage threshold V_{th} from $1.6pu$ to $1.8pu$. Once the threshold is increased, the proposed protection scheme checks if $V_3 < V_{th}$. The new activation delay corresponding to the updated V_{th} is 9 mins. Therefore, the UVP activates at 22 mins and sheds the load before the attacker causes drops in the line voltage.

IV. Problem Formulation & Concluding Remarks

Our LAA model maintains line voltage within static protection thresholds as shown in the Fig 2(a). To counter



(a): LAA under SOTA (b): LAA under APS

such attacks, we propose an adaptive strategy that reduces the activation delay of protection systems as shown in Fig 2(b).

We formulate the APS at i^{th} bus as an RL agent aps that observes the frequency $freq_i$, voltage V_i, rate-of-change of voltage $\frac{dV_i}{dt}$ and area under the power demand curve ϵ_i of some i-th bus with maximum FVSI. Therefore the observation of the defender agent $obs_{aps} = \langle freq_i, V_i, \frac{dV_i}{dt}, \epsilon_i \rangle$ (see the sky-coloured box in Fig. 1). The action of the agent aps is to add bias ΔV_{th} to the existing threshold V_{th} of the voltage protection system. The reward R_{aps} reduces activation delay when $\frac{dV_i}{dt}$ is greater than the threshold, i.e., $R_{aps} = (y \times w_1) - ((1-y) \times w_2)$. Here, y is a binary variable that evaluates to 1 when any of the parameters in obs_{aps} is beyond their safe limits, it is 0 otherwise, and $w_1,\ w_2 \in \mathbb{R}$. Accordingly, for agent aps the reward/penalty becomes w_1/w_2. Agent aps is built around a Simulink model of the power system, and trained in a competitive MARL environment (see Fig. 1), along with an attacker agent laa trying to perform possible LAAs (see red-coloured box in Fig. 1).

The objective of the laa agent's action is to decrease the ambient room temperature value by ΔT in order to increase power consumption, i.e., its action $act_{laa} = \Delta T$. The agent laa observes the following grid parameters, $obs_{laa} = \langle freq_i, V_i, \epsilon_i \rangle$. Its reward $R_{laa} = (x \times w_1') - ((1-x) \times w_2')$, where x is a binary variable that evaluates to 1 when any of the parameters of obs_{laa} is outside safety limits, and to 0 otherwise, $(w_1', w_2' \in \mathbb{R})$. Accordingly, for agent laa, the reward/penalty becomes w_1'/w_2'. Note that to constrain the attacker's actions from impeding the frequency protection systems by causing any sudden surges in power consumption, we limit ϵ_i with a constant threshold.

We set up MARL training with the above-mentioned agents, laa and aps. The action of the former depends on the past action of the latter since they act in the same environment, and the converse is also true. This ensures the protection system aps changes the threshold whenever an attack is injected by laa. In future, we intend to formulate the competing RL agents in the form of a Markov game to ensure *best response equilibrium* and investigate other learning algorithms.

References

[1] S. Maiti *et al.*, "Targeted attack synthesis for smart grid vulnerability analysis," in *ACM CCS*, 2023.

[2] S. Soltan *et al.*, "{BlackIoT}:{IoT} botnet of high wattage devices can disrupt the power grid," in *USENIX*, 2018.

[3] C. Shekari *et al.*, "{MaDIoT 2.0T}:{IoT} modern high-wattage iot botnet attacks and defenses," in *USENIX*, 2022.

[4] R. Maharjan *et al.*, "Voltage stability index for online voltage stability assessment," in *NAPS*, 2025.