Assessing the Impact of Electric Vehicles on Grid Stability: A Case Study of ERCOT System

Fariha Hakim Sneha[1], Yilu Liu[1,2]
[1] The University of Tennessee, Knoxville [2]Oak Ridge National Laboratory

Abstract

This study examines the impact of electric vehicle charging on the ERCOT grid using an industry-level PSSE model with 10,948 buses. It aims to determine the system's threshold for simultaneous EV charging before instability or collapse occurs. Additionally, the study explores cybersecurity risks posed by remote manipulation of EV charging stations.

Grid Impact

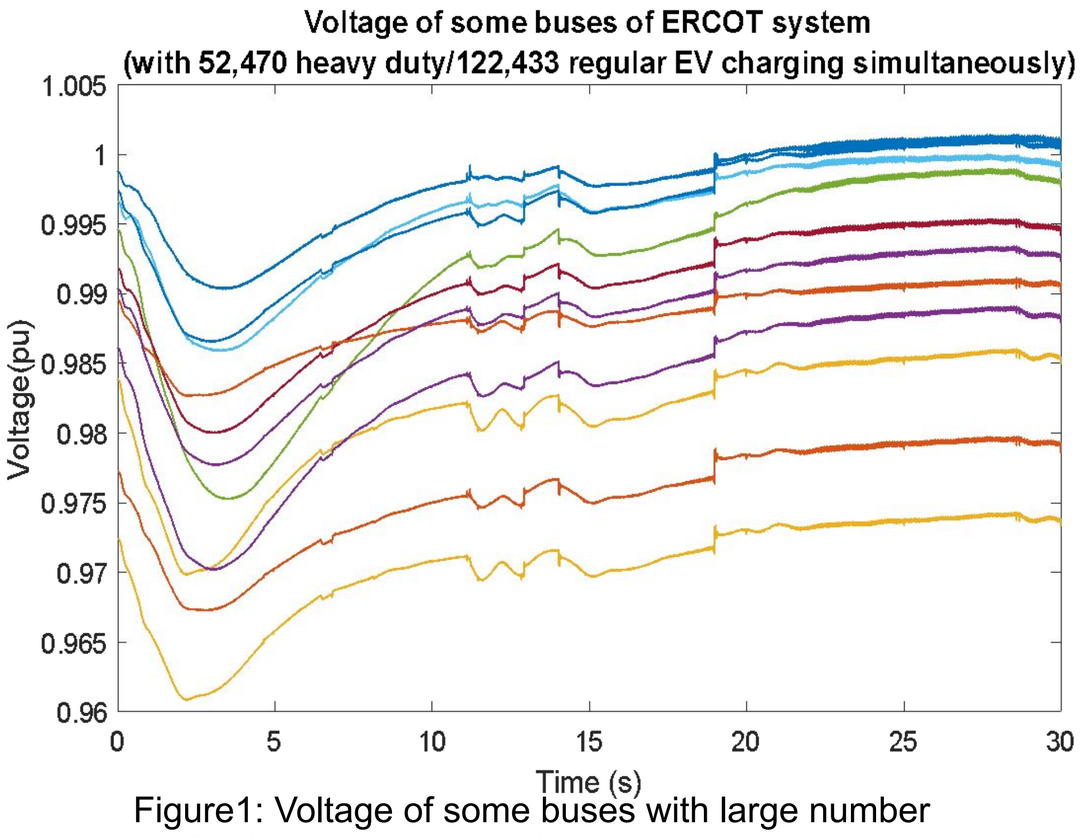

Figure1: Voltage of some buses with large number of EV chargers connected to grid

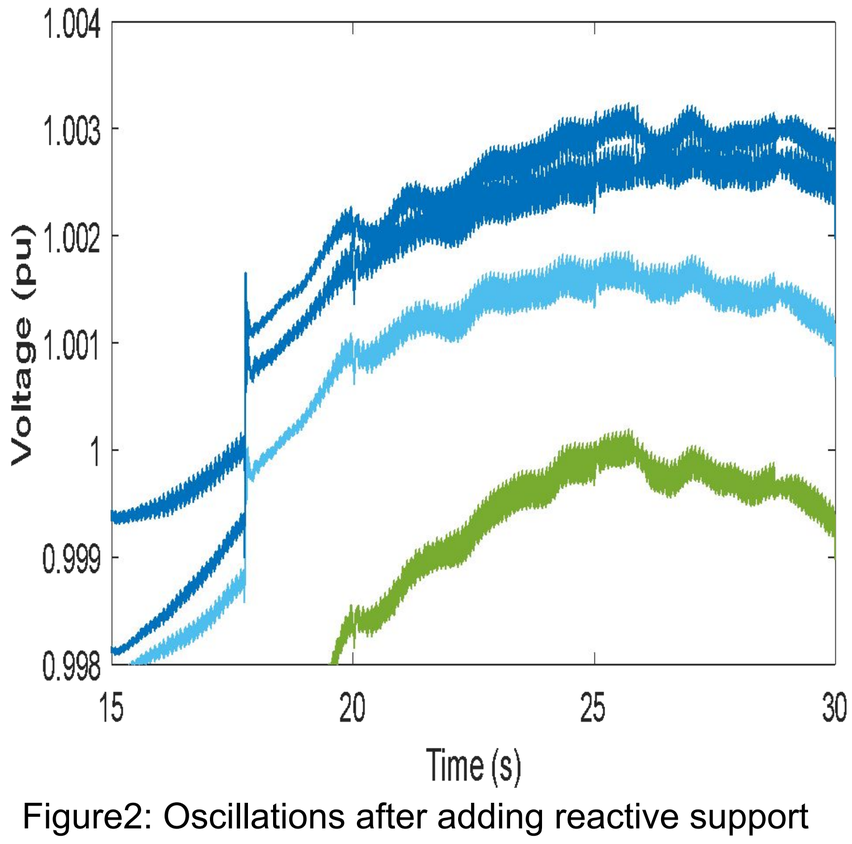

Figure2: Oscillations after adding reactive support

- EV charging is modelled as constant power load and distributed evenly among all the buses.
- Maximum additional load that can be simultaneously added to each bus is 1.514496 MW. Once this saturation point is reached, the simulation fails to converge, indicating its inability to accommodate any further EV charging.
- At this saturation point, the total additional power is calculated as 16,581 MW.
- Assuming that heavy-duty electric vehicles consume 350 kW and regular electric vehicles consume 150 kW, the maximum number of heavy-duty electric vehicles that can be charged simultaneously is calculated as 47,374 (16,581 MW / 350 kW), while the maximum number of regular electric vehicles that can be charged simultaneously is calculated as 110,540 (16581 MW / 150 kW).
- With additional reactive support, these numbers can be increased. Figure 2 illustrates the voltage condition with reactive support and increased EV chargers. Increasing reactive support can create oscillations, as depicted in Figure 2.

Cyber Threat

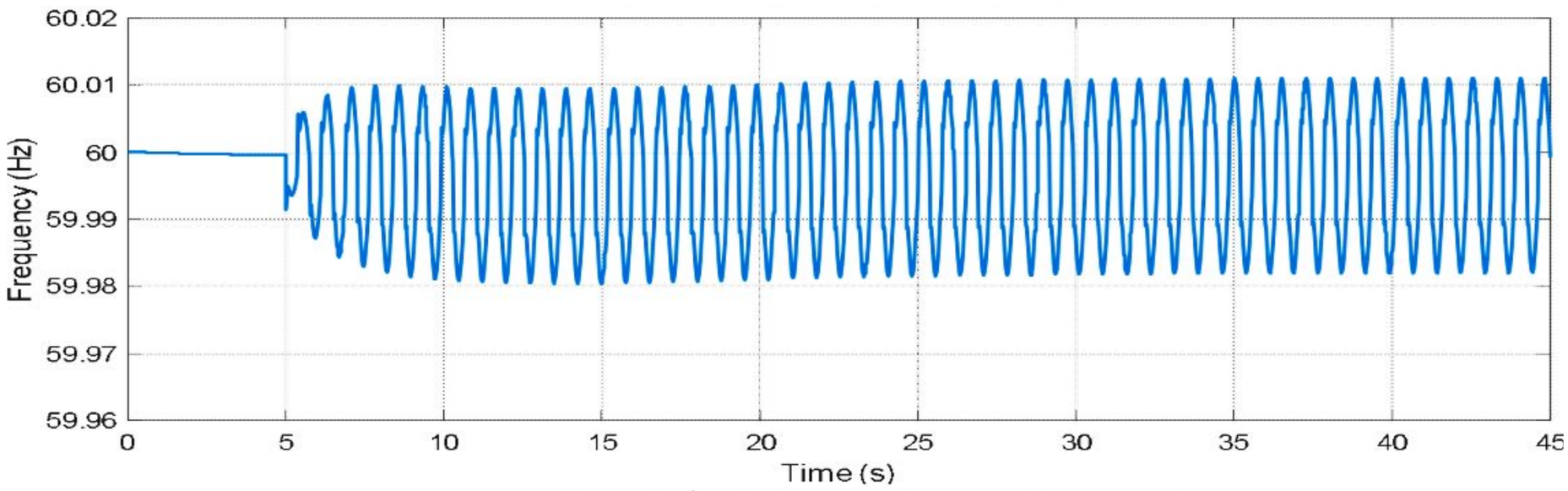

Figure3: Oscillations in cyber attacking scenario

Attackers may exploit vulnerabilities by switching EV chargers on and off from the grid, inducing grid oscillations. To test the grid impact due to such cyber attacks, a case is considered when 700 regular EV chargers are connected. The EV chargers are switched on and off at 0.38-second intervals(synchronizing the system's dominant mode) to mimic such cyber attack scenario. This results in 30 mHz peak-to-peak oscillations which is displayed in Figure 3.

Conclusion

This study highlights the risks associated with the increasing demand for EV charging and emphasizes the importance of addressing cybersecurity concerns in grid management.