Deep RL-based Volt-VAR Control and Attack Resiliency for DER-integrated Distribution Grids

Graduate Student: Kundan Kumar (kkumar@iastate.edu)
Faculty: Gelli Ravikumar (gelli@iastate.edu)
Department of Electrical and Computer Engineering, Iowa State University

IEEE PES ISGT INNOVATIVE SMART GRID TECHNOLOGIES NORTH AMERICA
PAPER ID: 24ISGT0050

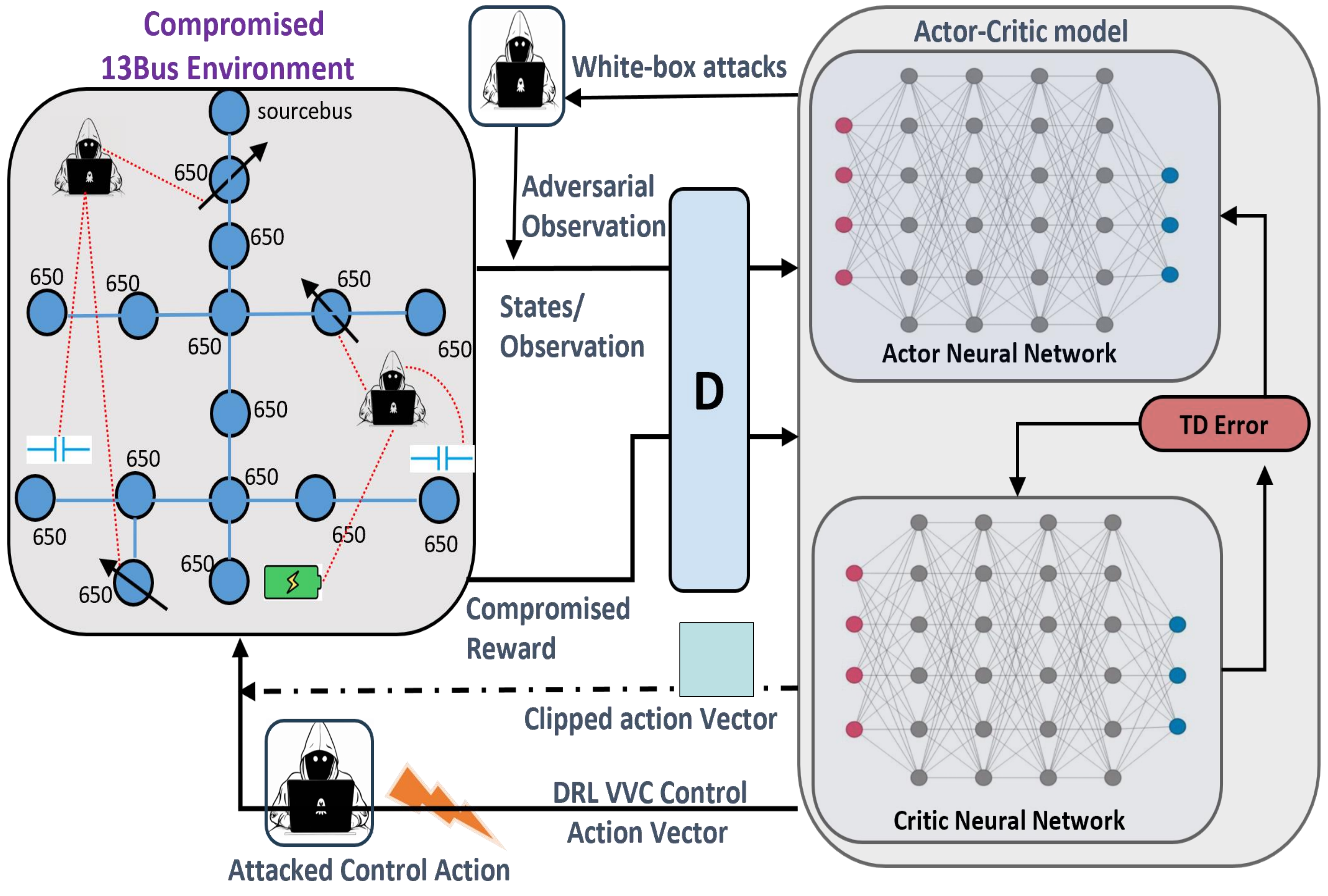
Motivation & Research Objective

- Stealthy adversarial white-box attacks potentially manipulate the control actions of DRL-VVC, jeopardizing the reliability and resilience of the entire power distribution network. It is crucial to protect the control actions of DRL-VVC, which can lead to voltage instabilities, power fluctuations, equipment damage, and cascading failures in distribution grids.

Research Objective:

- ➢ Develop a DRL framework for VVC policies for the distribution grid for regulating bus voltages and optimizing power distribution.
- ➢ Propose a stealthy cyberattack technique on the trained advantage actor-critic (A2C) DRL agent, which compromises the control policies of VVC.
- ➢ Propose a mitigation techniques against stealthy cyber-attacks to enhance grid stability and minimize voltage irregularities in the smart grid.
- ➢ Performed impact analysis to determine the effectiveness of the mitigation technique on the IEEE-13 bus system.

Proposed Methodology

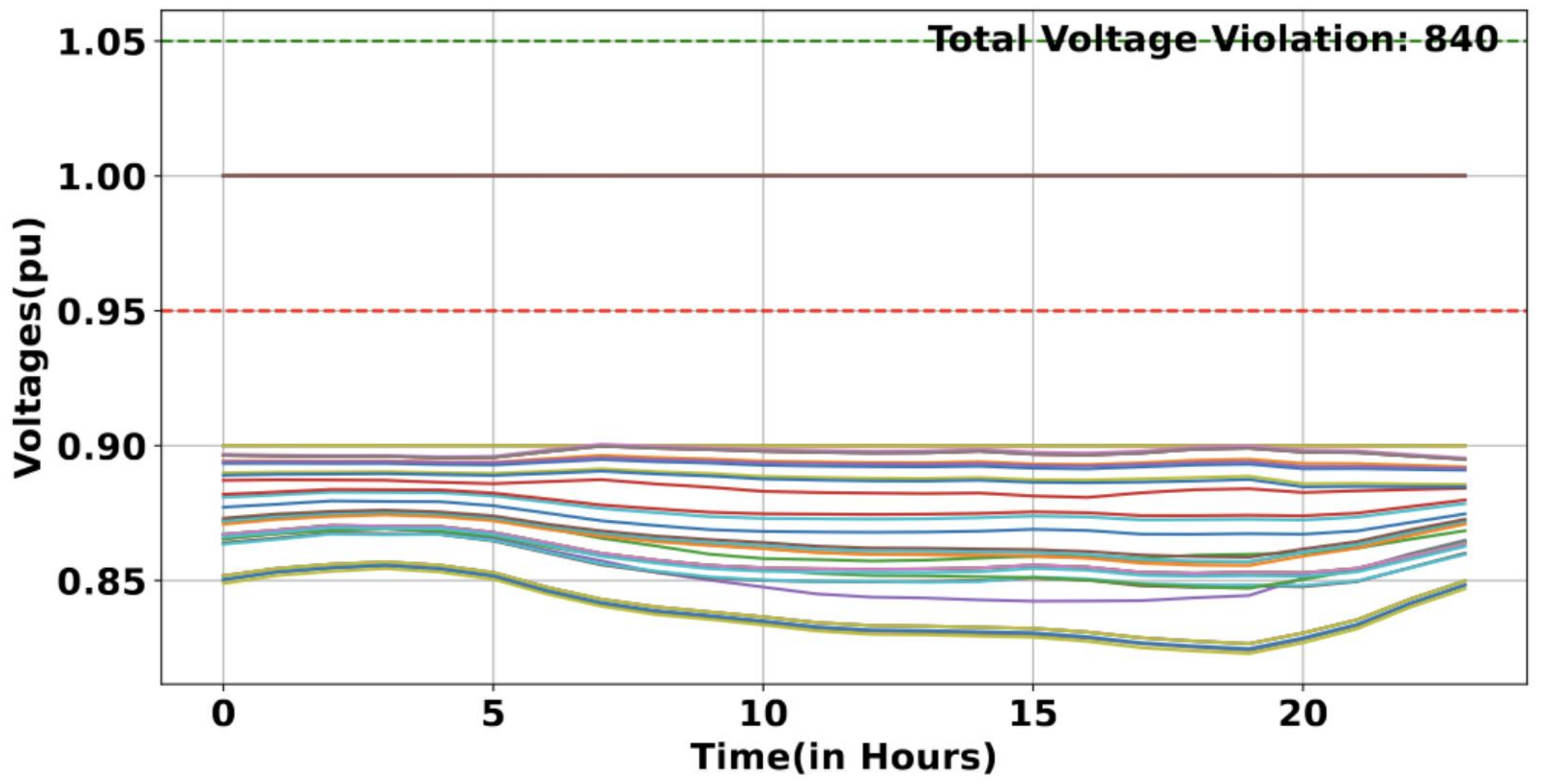


Proposed DRL-based VVC framework for stealthy attack and mitigation

Stealthy Cyberattacks on DRL Model

- Stealthy adversarial white-box attacks are performed by manipulating the control action space of the trained DRL model.
- Performed attacks on the IEEE –13 Bus distribution grid capacitors, regulators, and batteries.

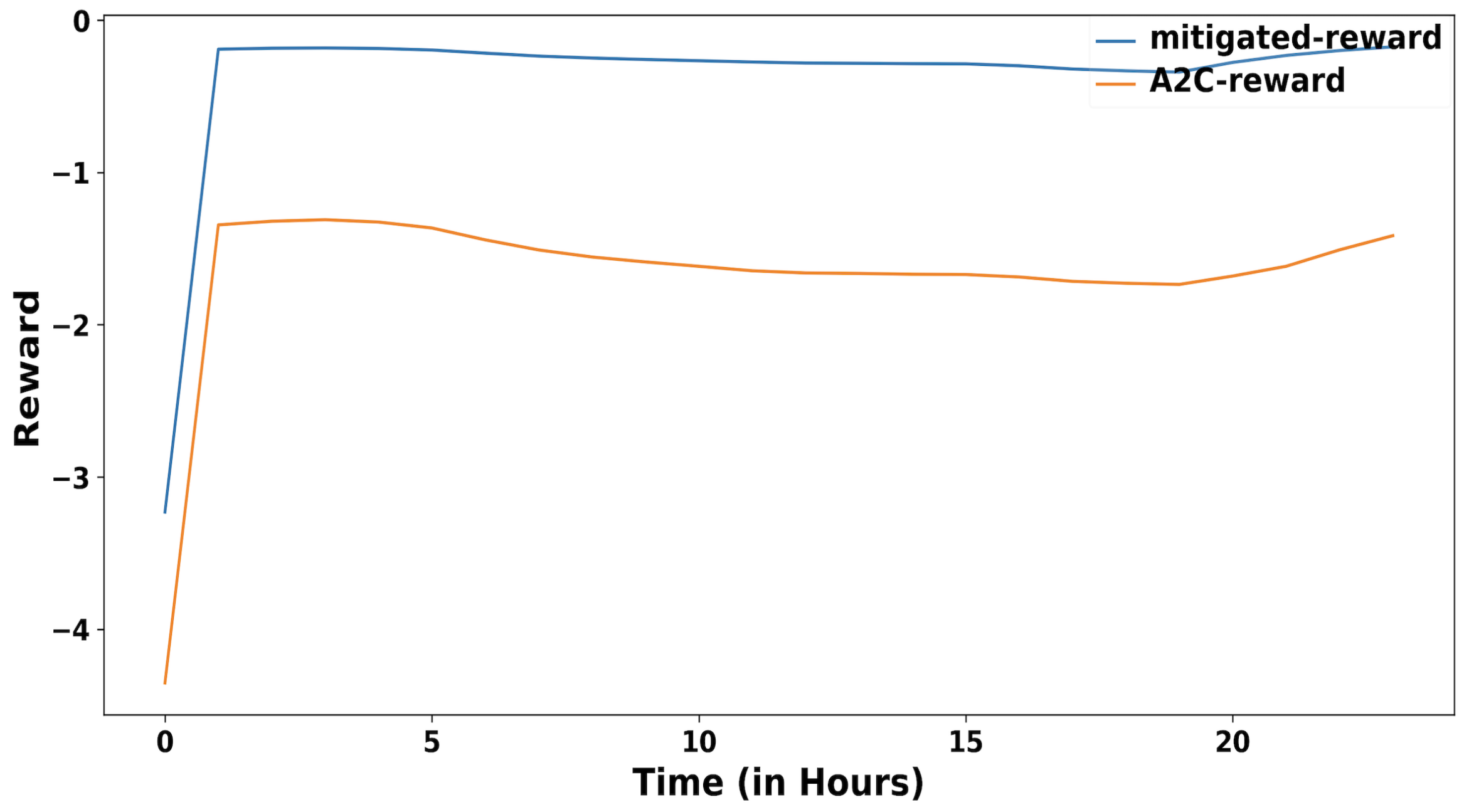
Attack-vector	***Voltage Violations across IEEE-13 Node***
No Attack	11
Attack on Capacitors	49
Attack on Regulators	81
Attacks on Battery	345
Attacks on All of them	840



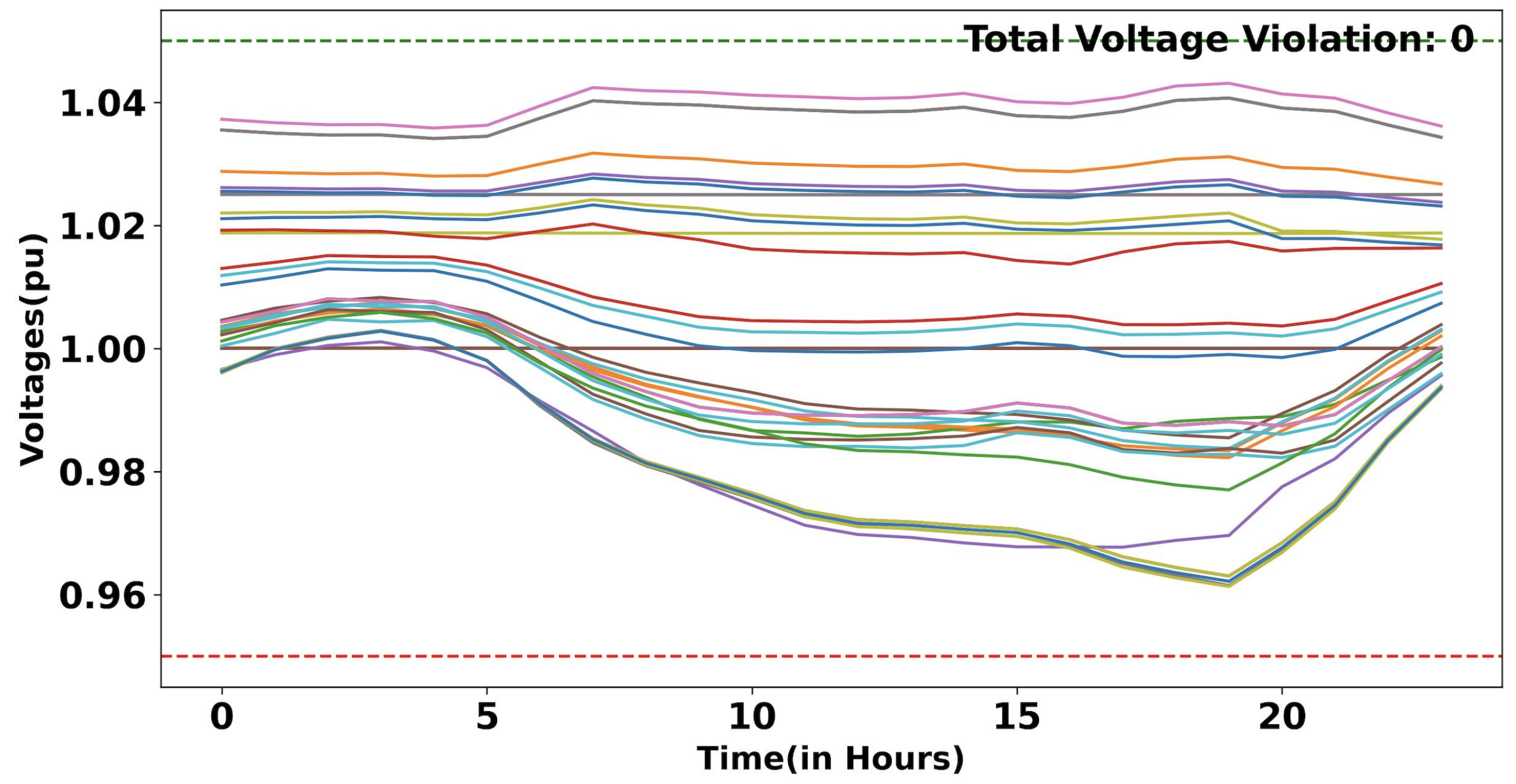
Voltage Violations after adversarial white box attack

Case Study: DRL Action Clipping Mitigation Strategies for Volt-Var Control

- Restrict the DRL action vector within the predefined safe bounds to prevent the agent from taking significant deviations in control actions.
- Performed the effectiveness of mitigation techniques on IEEE –13 Bus distribution grid.



Reward Comparison



Voltage Violations

Observations

- ❖ Adversarial white-box attacks on the deployed DRL model.
- ❖ Action clipping techniques reduce voltage violations.
- ❖ The result shows zero voltage violations on the IEEE-13 Bus.
- ❖ The mitigation techniques improved the reward, making the smart grid more robust to cyber-attack dynamics.

Conclusion and Future Work

- The proposed stealthy cyberattacks on the trained A2C DRL Model and mitigation technique by clipping the action vector.
- Experimental results demonstrate the 100% voltage violation reduction and improved reward function.

Future Work:

- Developing an interpretable DRL model for transparency and trustworthiness of control actions.

References

[1] N. Kato, B. Mao, F. Tang, Y. Kawamoto, and J. Liu, "Ten challenges in advancing machine learning technologies toward 6g," IEEE Wireless Communications, vol. 27, no. 3, p. 96–103, 2020.
[2] G. Ravikumar and M. Govindarasu, "Anomaly detection and mitigation for wide-area damping control using machine learning," IEEE Transactions on Smart Grid, pp. 1–1, 2020.

IOWA STATE UNIVERSITY OF SCIENCE AND TECHNOLOGY

Acknowledgement: This research is funded partly by US NSF Grant # CNS 2105269, US DOE CESER Grant DE-CR000016, and Iowa Energy Center Grant #21-IEC-009.