World Academy of Science, Engineering and Technology
International Journal of Electrical and Computer Engineering
Vol:18, No:12, 2024

A Deep Reinforcement Learning-Based Secure Framework against Adversarial Attacks in Power System

Authors : Arshia Aflaki, Hadis Karimipour, Anik Islam

Abstract : Generative Adversarial Attacks (GAAs) threaten critical sectors, ranging from fingerprint recognition to industrial control systems. Existing Deep Learning (DL) algorithms are not robust enough against this kind of cyber-attack. As one of the most critical industries in the world, the power grid is not an exception. In this study, a Deep Reinforcement Learning-based (DRL) framework assisting the DL model to improve the robustness of the model against generative adversarial attacks is proposed. Real-world smart grid stability data, as an IIoT dataset, test our method and improves the classification accuracy of a deep learning model from around 57 percent to 96 percent.

Keywords : generative adversarial attack, deep reinforcement learning, deep learning, IIoT, generative adversarial networks, power system
Conference Title : ICEPE 2024 : International Conference on Electrical and Power Engineering
Conference Location : Dubai, United Arab Emirates
Conference Dates : December 23-24, 2024