

Attack Graph Model for Cyber-Physical Power Systems Using Hybrid Deep Learning

Alfan Presekal¹, Alexandru Ștefanov¹, Vetrivel Subramaniam Rajkumar¹, Peter Palensky¹

¹Delft University of Technology

Electrical power grids are vulnerable to cyber attacks, as seen in Ukraine in 2015 and 2016. However, existing attack detection methods are limited. Most of them are based on power system measurement anomalies that occur when an attack is successfully executed at the later stages of the cyber kill chain. In contrast, the attacks on the Ukrainian power grid show the importance of system-wide, early-stage attack detection through communication-based anomalies. Therefore, in this paper, we propose a novel method for online cyber attack situational awareness that enhances the power grid resilience. It supports power system operators in the identification and localization of active attack locations in Operational Technology (OT) networks in near real-time. The proposed method employs a hybrid deep learning model of Graph Convolutional Long Short-Term Memory (GC-LSTM) and a deep convolutional network for time series classification-based anomaly detection. It is implemented as a combination of software defined networking, anomaly detection in communication throughput, and a novel attack graph model. Results indicate that the proposed method can identify active attack locations, e.g., within substations, control center, and wide area network, with an accuracy above 96%. Hence, it outperforms existing state-of-the-art deep learning-based time series classification methods.