Abstract

To ensure efficient energy management in power systems, digitalisation and interconnected communication networks are required. The modernisation and development of power systems lead to an increased susceptibility for cyberattacks. Therefore, network intrusion detection systems are employed as an additional security layer. To this end, the anomaly-based machine learning methods, including autoencoder, graph neural network and isolation forest, are analysed. The methods aim to serve as a network intrusion detection system that recognises zero-day-attacks without the need for human supervision. The proposed algorithms are tested on the publicly available UNSW-NB15 network dataset. Furthermore, the performance of these models is evaluated and compared in terms of AUC, f-score, accuracy, recall and precision. The results reveal that the autoencoder model demonstrates the overall best results with an AUC of 0.96908. In short, all three methods exhibit the ability to detect unknown attacks but suffer from a high false-alarm rate.