Contribution ID: **40** Type: **Poster**

Autoencoder-Based Anomaly Detection in Network Traffic

Friday 13 September 2024 09:00 (20 minutes)

Due to the continuously increasing number of resources and data available in the cloud, the threats related to the security of computer networks and IT systems are critical. Threat detection systems based on deep neural networks and anomaly detection are trained on data related to normal activity so that the network can recognize unusual patterns and behaviors in the event of an attack or an attempt to infiltrate a given IT infrastructure. This paper presents the results of developing a neural network based on an autoencoder for anomaly detection in network packet data. The network was trained on data from the HIKARI-2021 dataset. The autoencoder aims to learn representations of normal network traffic and associate this type of traffic with a minimal reconstruction error. The obtained results were compared with those achieved by authors of other works. High accuracy and sensitivity were achieved, at the cost of rather low precision, resulting in many false-positive results. The obtained results were compared with those achieved by authors of other works. To improve the network's ability to detect anomalies, an attempt was made to enhance it by using an error threshold as a vector. The results obtained in the study indicate very high values for individual components of the vector, which results in low network accuracy. Single deviations in the training data can cause disturbances in selecting values for these components, leading to high values for classifying a given record as an anomaly. This problem can be resolved by changing the method of calculating the individual components of the vector, using only a subset of features, and deriving multiple vectors, one for each class separately, which has been described and analyzed in more detail.
Index Terms—anomaly detection, deep learning, cybersecurity, autoencoder, threat detection

Author: KORNISZUK, Krzysztof

Co-author: SAWICKI, Bartosz (Warsaw University of Technology)

Presenter: SAWICKI, Bartosz (Warsaw University of Technology)

Session Classification: Session 6 - Poster Session B