Analysis of the deep one-class classification procedure applied on network anomaly detection tasks

Michael Heichler

[1]) First affiliation

michael.heichler@fom-net.de

[2]) 1st reviewer

Prof. Dr. Thomas Wiebringhaus

[2]) 2nd reviewer

Dr. Oliver Schmidts

Network traffic anomaly detection is critical for cybersecurity, yet most machine learning classifiers require labeled training data, which remains scarce and costly to obtain in this domain. Existing anomaly detection approaches struggle with tabular network traffic logs, as supervised learning methods prove ineffective due to the rarity of labeled examples and the dynamic nature of emerging threats. This thesis evaluates deep one-class classification, specifically DeepSVDD, to address the gap between available methods and the growing need for unsupervised anomaly detection in tabular network environments.

DeepSVDD was applied to publicly available network traffic datasets, with preprocessing techniques addressing data irregularities and self-supervised learning improving feature representation. Model performance underwent evaluation using standard metrics (precision, recall, and F1-score) and cross-validation.

Results show that DeepSVDD detects anomalies in known network traffic patterns with improved accuracy and robustness. However, self-supervised learning on tabular data poses challenges, such as the generation of irrelevant features that hinder generalization to unseen datasets. The model performs well on training data but struggles with novel or unknown traffic patterns.

Findings indicate that deep one-class classification procedures excel at characterizing known behaviors but often miss novel anomalies. Robust anomaly detection depends on accurate modeling of familiar behaviors and the inclusion of mechanisms for domain adaptation. Hybrid approaches that combine deep learning with traditional statistical methods and incorporate domain adaptation strategies can enhance generalization across diverse network environments.