Technical University of Munich

Thesis B.Sc.

# AI-based Network Anomaly Detection

## Motivation

Cyber-physical systems (CPS) such as automated/autonomous vehicles or factory plants are controlled by networked computers. However, the operational safety of the CPS can only be guaranteed if the security of the networked computers is maintained.
An important step towards this goal is constant host and network monitoring. If anomalies are detected, their cause can either be eliminated or – as an ultima ratio – the CPS can be transferred into a safe state (”switched off”).
In recent years, industry and research have developed various approaches to monitoring hosts and networks for anomaly detection (intrusion detection systems, IDS). These systems often have the property that they generate large amounts of information, which – either automated or by humans – must be correlated and evaluated.
Recently, methods from the field of artificial intelligence (AI), such as Deep Learning, have enjoyed great success in areas such as automatic images analysis or speech recognition. The step to apply AI technology to other problems, such as network monitoring, anomaly detection and the correlation/evaluation of information from ”conventional” IDSs, is obvious. Hence, a broad pool of publications on AI-based methods in this scientific field exists.
In this thesis, we first want to get an overview of the AI technology discussed and investigated by the scientific community and categorize it. We want to evaluate which approaches and methods are most promising. Lastly, based on previous findings, we want to implement and evaluate a simple AI-based tool for network anomaly detection.

## Your Tasks

- Understand the specific requirements of the scenario automotive and industrial networks.
- Perform a literature analysis on the subject of AI-based methods for anomaly detection.
- Design and implement a prototype for AI-based anomaly detection.
- Evaluate your prototype.

## Note

Due to the complexity of the topic, we require that the student has some background on AI. The topic is also broad and can be executed with a direct focus on AI-based network anomaly detection, or AI-based aggregation of information from IDSs.

## Contact

Dr. Holger Kinkelin kinkelin@net.in.tum.de
Christian Lübben luebben@net.in.tum.de