Machine Learning for Network Security

by Tanja Zseby (TU Wien)

The protection of communication networks against new and unexpected attacks remains a challenging task. Machine Learning provides powerful methods to distinguish between benign and suspicious network traffic. However, several challenges have to be addressed to apply machine learning in the field of network security. Data sets are often unbalanced, unlabeled and outdated. Results are network and attack specific and difficult to generalize. Feature sets are limited by resource constraints and traffic encryption. Explainability is valuable and the operation in adversarial environments is inevitable.

In this talk I introduce challenges and approaches for applying supervised and unsupervised machine learning methods to network security with a focus on the detection of malware communication in network traffic. I address important aspects in the processing steps, such as data pre-processing, feature selection, choice of machine learning methods and the calculation of appropriate performance metrics and point out challenges regarding reproducibility and comparability of results.