Yixiao Wang

Tsinghua University , China

Reasearch

Previous research

- Improving the performance of traffic classifiers in an unstable network environment. Unstable network environment will cause changes in the features extracted by classifiers and descend of performance, which can be tackled by self-supervised learning methods proposed by us. The paper <Rosetta: Enabling Robust TLS Encrypted Traffic Classification in Diverse Network Environments with TCP-Aware Traffic Augmentation> has been accepted by the 32nd USENIX Security Symposium(USENIX Security 23 Summer).
- Proposing attacks that change cipher suit in TLS communication to confuse the defender and try to cope with them. We proved the feasibility of the attacks against CNN-based models(Deep packet, Deep fingerprinting), RNN-based models(BERT, FS-NET) and so on. We also tried a similar self-supervised method to solve the problem.

Current research

- Measurement of the application of deep models in the real world. Existing deep learning models for classifying network packets all focus on a single setting dataset. We proposed that there are multiple factors through the network stack that influence the accuracy of deep models. So we are trying to measure the extent of the influence. We are working on a paper for CCS 2023.
- Jamming attack in IoT. Recently I joined a research group interested in attacks in IoT. We are now focusing on jamming attacks in Helium networks.