IOT Device Identification Using Machine Learning Techniques

Idan Mosseri, Dean Eckert

# Abstract

In this work we apply machine learning algorithms on IOT network traffic data for accurate identification of devices. In order to train and evaluate the classifier, data was collected from different IOT devices. Using supervised learning, we trained a classifier being able to distinguish between a specific use and the rest. The overall IoT classification accuracy of our model is 99.281%.

# Introduction

The “Internet of Things” (IOT) relates to networks of physical devices and items embedded with electronics, sensors, actuators, software and connectivity which enables the communication between these devices and their exchange of data.

In recent years, more organizations allow IOT devices to be connected to their networks which might impose a security threat to these networks. Hence, organizations must be able to identify which devices are connected to their networks and whether these devices are considered legitimate and do not impose a risk.

Leveraging network traffic in order to identify devices in general has been gaining in popularity in previous works. Specifically, there is an increasing interest in the domain of IOT device identification due to the importance of identifying such devices in an organizational environment (in terms of security).

In this work, we address the challenge of identifying an IOT device by analyzing its high-level network traffic data using machine learning techniques. We would like to develop a method for identifying such device, even if its IP address has been spoofed (which can be done easily) and to allow us identify an abnormal behaviour which may indicate which device is in-use.

Since we can’t rely on the IP address as an identifier of the device (since this value can be spoofed), we would like to analyze the traffic’s high-level data (which means the metadata and traffic statistics, rather than analyzing the content).

**Research questions:** This research proposes a novel approach in order to identify IOT devices using their network traffic data and analysis made using machine learning techniques. Specifically, we focus on the following question: Is it possible to identify an IOT device using machine learning techniques by analyzing its high-level network traffic data?

**Summary of contributions:**

# Related Work