Application of Machine Learning for Prevention of Attacks on IoT Devices by using Classification of IoT Traffic Patterns

Problem Statement

The Internet of Things (IoT) refers to an ongoing trend of connecting all kinds of physical objects to the internet. The IoT brings the power of the internet, data processing and analytics to the real world of physical objects. Attackers may attempt to exploit vulnerabilities in application protocols, including Domain Name System (DNS), Hyper Text Transfer Protocol (HTTP) and Message Queue Telemetry Transport (MQTT) that interact directly with back-end database systems. Successful exploitation of one or more of these protocols can result in security breaches. Machine Learning is seen as an alternative method to defend against malware, botnets and other attacks. A promising approach to vulnerabilities of IoT devices is to embed solutions at the network-level, whereby network traffic to/from IoT devices is monitored to ensure they operate normally and detect abnormal behaviours. This research shows that how machine learning and deep learning techniques can be used to efficiently detect and classify malicious attacks on IOT devices.

Background

The raise in the amount of Internet applications and the appearance of modern technologies such as the Internet of Things (IoT) are followed with new and recent efforts to invade computer networks and systems. As compared to other networks, IoT nodes have low capacity and limited resources, and do not have manual controls and are thus more prone to attacks by intruders, raising the need to develop strict security solutions based on networks. IoT services operate via network protocols, such as DNS, HTTP and MQTT, in the TCP/IP model. Attackers generally seek to identify and exploit vulnerabilities and limitations in these protocols, for example using various deception approaches. Botnets can be used to perform Distributed Denial-of-Services (DDoS) attacks, steal data, send spam, and allows the attacker to access the device and its connection.

Methodology

Step 1: Data collection and analyses

It involves the capturing real botnet traffic mixed with normal traffic and background traffic and stored in the form of PCAP files.

Step 2: Data preprocessing and feature extraction

This step involves separating the IoT traffic from whole network traffic and then extracting the features such as time-stamp, source & destination IP address, source & destination port numbers, protocol used, total uploaded and downloaded bytes.

Step 3: Training and experimentation on datasets

In this step building a deep neural network with binary classifier which can efficiently classify attack traffic and benign traffic of an IOT network.

Step 4: Deployment and analysis on real life scenario

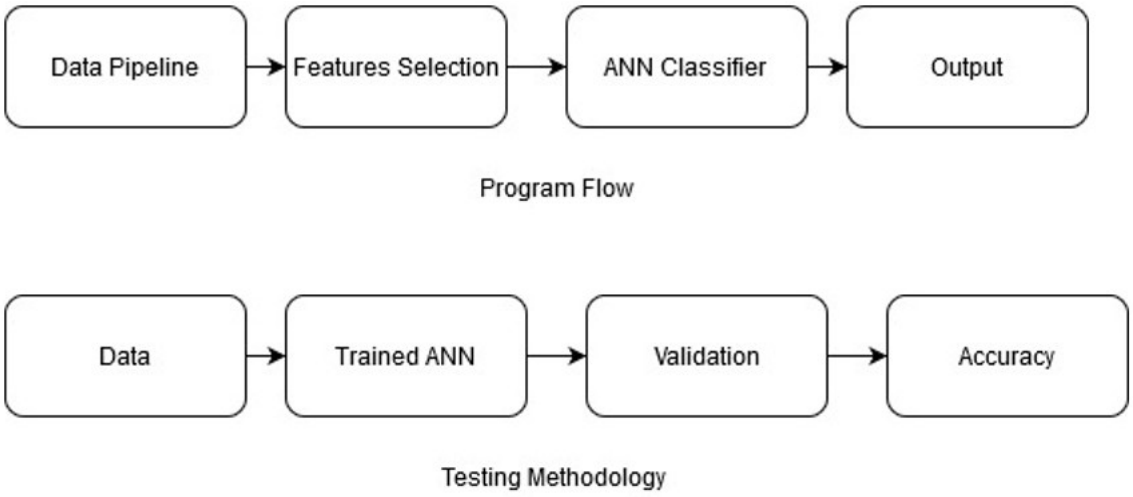

Figure 1: Training and Testing of neural network model for classification of attacks on IoT

Figure 1 shows the proposed methodology for the classification of attacks and benign traffic of IoT devices by analysing the network traffic characteristics.

The training and testing of attacks and benign IoT traffic data over deep neural network with binary classifier and achieved good results for prediction of attacks and benign traffic from IoT devices. The real life scenarios leveraged the further improvements in the methodology used.

Experimental Design

Dataset

We used the CTU dataset for IOT with labelled data from https://www.stratosphereips.org/datasetsiot23. These attacks are performed on real IOT devices. The IoT-23 dataset consists of twenty three captures (called scenarios) of different IoT network traffic. It has 20 malware captures executed in IoT devices, and 3 captures for benign IoT devices traffic. The data collected is of maximum 24 hours and captured total flows are 12629968.

Evaluation Measures

Evaluation is measured in terms of Accuracy, Precession, Recall, F1 Score, and Errors performed on malicious IoT traffic.

Software Requirements

- Basic knowledge of Python/Java
- Exposure to Linux environment.

Hardware Requirements

- NVIDIA GPU