CSCE 623 Project Proposal

Marvin Newlin

2 May 19

Network Intrusion Detection Systems (NIDS) are in important aspect of cybersecurity in modern networks. One important task of many NIDS is being able to detect malicious traffic among the benign traffic.

For the project, we will address the task of detecting malicious traffic. The machine learning task we plan to accomplish is classification of the data as benign or malicious. The dataset we will be using is a labelled dataset, thus this will be a supervised learning classification task.

The dataset we will be using is the CICIDS2017 dataset described in [1]. This dataset is in the form of a network packet capture. There are many features within the dataset like the standard Source/Destination IP address, Source/Dest port number, timestamp, and protocol. The dataset also contains summary statistics of the dataset for each labelled flow. These are the features that we will focus on for the classification task. The features that we will be utilizing are displayed in table 1 below.

**Table 1: Summary statistical features and formats of the CICDS2017 dataset**

|  |  |
| --- | --- |
| **Feature** | **Format** |
| Flow duration (seconds) | float |
| Number of bytes in the flow | float |
| Number of forward packets/second | float |
| Number of backward packets/second | float |

There are two research questions that we hope to answer in this project:

1. Can we successfully classify traffic as benign or malicious using the features from Table 1?
2. What features from Table 1 are most important for classifying traffic as benign or malicious?

The CICIDS2017 dataset is contained in CSV files and as such is easily importable into code. The data is already formatted and the summary statistical features we will be using are ready to be plugged into a matrix. There are a large number of features that will not be utilized from this dataset so in pre-processing these features will be dropped. Since there may be large differences in the scales of each feature, we will normalize the data in the pre-processing stage.

The CICIDS2017 dataset is split up into 10 files based on specific attacks and contains truth labels for the benign and malicious traffic. We will be utilizing a single file from this dataset, specifically the Web Attacks file from the dataset. This specific file contains approximately 170,000 observations in which there is benign traffic and malicious traffic. As the name indicates all of the malicious traffics are web attacks, but the specific type of attack is beyond the scope of the course.

As mentioned earlier, there will be two classes for the classification task, benign and malicious. Since we will be performing supervised classification, we will use standard classification performance measures. The main performance metrics for the classification will be Accuracy, Precision, Recall, and F-Measure.

Future research will be focused on the metrics for evaluation of the similarity between synthetically generated and real data. The eventual goal is to be able to generate synthetic data that is not only syntactically similar to real data, but also semantically similar. This first step of classification allows us to develop a framework in which we can test some different metrics for evaluation of similarity.

REFERENCES

[1] I. Sharafaldin, A. Habibi Lashkari, and A. A. Ghorbani, “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization,” in *Proceedings of the 4th International Conference on Information Systems Security and Privacy*, 2018, pp. 108–116.

Link: <https://www.unb.ca/cic/datasets/ids-2017.html>