Multi-Class Classification for Network Traffic Analysis

Hepple Xi

Problem Statement:

Modern computer networks are increasingly targeted by a wide range of sophisticated cyber-attacks that compromise data integrity, availability, and security. Traditional intrusion detection systems struggle to detect cyber-attacks due to their reliance on static methods. This project proposes a machine learning-based multi-class classification model to distinguish between benign and malicious network traffic, enhancing the accuracy and adaptability of detection, thereby contributing to a more secure and resilient cyberspace.

Objectives:

- To understand and preprocess the network traffic dataset for classification tasks.
- To develop and compare several machine learning models for multi-class classification.
- To evaluate the models and identify the most effective for real-world applications.

Dataset:

UNSW-NB15 dataset:(https://research.unsw.edu.au/projects/unsw-nb15-dataset)

ML methods:

- ***Support Vector Machines***
- ***Random Forest***
- ***XGBoost***
- ***Neural Network***

Reference:

1. Moustafa, Nour, and Jill Slay. "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)."Military Communications and Information Systems Conference (MilCIS), 2015. IEEE, 2015.
2. Moustafa, Nour, and Jill Slay. "The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set." Information Security Journal: A Global Perspective (2016): 1-14.