Ministry of Higher Education and Scientific Research

University of Babylon

information technology collage

Information Security Department

Study: morning

Network attack detection system using Machine Learning

A Graduate Project Submitted to the department of Information Security of the College of Information Technology, University of Babylon, in Partial Fulfillment of the Requirements for the Bachelor's degree in the Information Security of Information Technology.

By

Teba Hassan Khalil

Supervisor name

Lect. Dr. Mohammed Ibrahim Kareem

Abstract

This document describes a network attack detection system (NIDS) utilizing machine learning algorithms for network traffic classification. The system leverages a pre-existing dataset containing network traffic features labeled as either normal or attack traffic. The code explores the performance of various machine learning models, including Logistic Regression, Random Forest, Support Vector Machines (SVM) with different kernels, Decision Trees, Naive Bayes, and K-Nearest Neighbors (KNN).

The system employs data preprocessing techniques such as label encoding and feature scaling to prepare the data for machine learning algorithms. It then performs dimensionality reduction using Principal Component Analysis (PCA) to visualize the data in a two-dimensional space.

The evaluation focuses on measuring the accuracy, precision, and recall of each machine learning model. Additionally, for selected models, the system generates decision boundaries to visually represent the classification process.

The code incorporates a user interface that allows users to choose individual models for evaluation or run all models sequentially. It also offers the option to execute the evaluations in parallel using multiprocessing for potentially faster processing times.

This work highlights the potential of machine learning for network attack detection. While the provided code serves as a starting point, further research could involve exploring additional algorithms, hyperparameter tuning, and incorporating real-time network traffic analysis.