

Netano - AI Network Analyzer: A Thesis for Network Traffic Analysis

Netano - AI Network Analyzer

Leveraging Artificial Intelligence for Real-Time Network Security and Monitoring

Course: Computer Networks

January 2025

Netano - AI Network Analyzer: A Thesis for Network Traffic Analysis

Abstract

The Netano - AI Network Analyzer is a real-time network traffic analysis tool powered by artificial intelligence. Designed to detect anomalies, predict protocols, and analyze hotspots, the system uses advanced clustering and anomaly detection techniques. This thesis explores the implementation, dataset, and results of Netano, focusing on its application in network monitoring, intrusion detection, and traffic classification. By processing 50,000 logs stored in MongoDB, Netano demonstrates how AI can transform raw network data into actionable insights.

1. Introduction

1.1 Background

The increasing complexity of computer networks has necessitated advanced tools for traffic monitoring and security. Traditional methods struggle to process large-scale, real-time data effectively. Netano bridges this gap by combining AI models with a real-time network traffic monitoring system.

1.2 Objectives

- Analyze network traffic to detect anomalies.
- Classify and predict protocols accurately.
- Identify network hotspots, including top destinations and protocols.
- Provide real-time insights using a modern React + FastAPI stack.

2. Dataset

2.1 Overview

The dataset used for this project consists of approximately 50,000 network logs captured using Wireshark on

Netano - AI Network Analyzer: A Thesis for Network Traffic Analysis

a Kali machine over one hour. Each log contains fields such as:

- Time: Timestamp of the traffic.
- Source/Destination: IP addresses of the sender and receiver.
- Protocol: Protocol used in the communication (e.g., TCP, ARP, TLS).
- Length: Size of the traffic packet.
- Info: Additional information about the packet.

2.2 Dataset Structure

Field	Description
Time	Timestamp of the traffic
Source	IP address of the sender
Destination	IP address of the receiver
Protocol	Protocol used in the packet
Length	Size of the traffic packet
Info	Additional packet details