Case Study: ARIMA for Anomaly Detection in DDOS Attacks

Ben Harris

DS 4002: Prototyping – 4/28/2025

Context

You are a data scientist at a cybersecurity firm and your client's servers are under attack! A Distributed Denial of Service (DDoS) attack is flooding their servers with traffic, and your job is to intervene before serious, costly damage is done. Your supervisor has tasked you with developing a model to detect these attacks early before they spiral out of control.

Mission

In this case study, you will use real Amazon Web Services CloudWatch data on CPU utilization, inbound network traffic, and request counts to detect anomalies that may signal a DDoS attack. You will construct a statistical model using time series data and evaluate its performance across these distinct server metrics. If successful, you will be able to spot and mitigate the damage from cyber attacks.

Your job is to replicate and evaluate an ARIMA model for anomaly detection. You will submit a reproducible script along with reports on the dataset and the model's effectiveness. Through this case study you will learn technical skills as well as good data and communication practices.

Link to the Github repository: **https://github.com/harrisvben/arima_ddos_detection**