Avin Saxena 202111015
K. Anamithra 202111041
Shriram Ashok Birajdar 202111078
Vaishali Bhagwani 202111085
Yeshwanth Vatti 202111086

Indian Institute of Information Technology Vadodara - International Campus Diu

---

PROJECT

DDoS Prediction System: A Study on Detection and Impact on 5G Networks

---

Course Instructor: Bhupendra Kumar

Contents

Abstract

Distributed Denial of Service (DDoS) attacks represent one of the most persistent threats to the stability and reliability of modern communication networks. The rapid advancement of 5G technologies, characterized by ultra-reliable low-latency communication (URLLC), massive machine-type communication (mMTC), and enhanced mobile broadband (eMBB), has significantly expanded the attack surface, increasing the complexity and volume of network traffic. This study presents a machine-learning-based predictive system designed to detect and mitigate DDoS attacks in real-time. By combining anomaly detection techniques with real-time monitoring, the proposed solution minimizes detection latency and enhances response capabilities. A user-friendly dashboard enables network administrators to analyze traffic patterns and take corrective actions swiftly. Experimental results validate the system's efficiency, highlighting its critical role in safeguarding 5G networks.

1 Introduction

The rapid adoption of 5G networks is transforming the global digital landscape. Offering unprecedented data speeds, low latency, and vast connectivity potential, 5G supports diverse applications ranging from autonomous vehicles to smart cities and advanced IoT systems. However, this technological revolution comes with significant cybersecurity challenges, particularly in combating Distributed Denial of Service (DDoS) attacks.

DDoS attacks involve overwhelming a network with illegitimate traffic, rendering it inoperable for legitimate users. In the context of 5G networks, the challenges of detecting DDoS attacks are amplified by increased traffic volumes, heterogeneous device ecosystems, and low-latency requirements. Traditional detection systems, reliant on predefined attack signatures, fail to adapt to the dynamic nature of modern threats.

This study introduces a machine-learning-driven system specifically designed to detect and predict DDoS attacks in real-time, offering a scalable and efficient solution for modern networks.

1.1 Motivation

The motivation behind this project stems from the critical role 5G networks play in modern communication infrastructures. A disruption due to DDoS attacks could result in catastrophic consequences for critical sectors like healthcare, autonomous transportation, and industrial IoT systems. This work seeks to leverage machine learning to enable proactive detection, ensuring 5G systems remain resilient to evolving threats.

1.2 Research Objectives

The key objectives of this study are:

- Develop a scalable and robust machine-learning framework for real-time DDoS detection in 5G networks.
- Evaluate the effectiveness of machine learning algorithms like Random Forest, K-Nearest Neighbors (KNN), and Naive Bayes for anomaly detection.

- Build a user-friendly and dynamic dashboard for data visualization and proactive threat mitigation.
- Enhance the overall cybersecurity framework for 5G networks through predictive analytics.

2 System Design and Architecture

2.1 Overview

The system is built with a modular design to ensure scalability and seamless integration with existing network infrastructures. It consists of three main components: data collection and preprocessing, machine learning, and visualization and mitigation.

The Data Collection and Preprocessing component captures real-time network traffic from various sources, cleans the data, and extracts relevant features such as IP addresses, protocol types, and traffic volume. This structured data is then prepared for analysis.

The Machine Learning Module uses algorithms like Random Forest, K-Nearest Neighbors (KNN), and Naive Bayes to classify network traffic and identify anomalies. The machine learning models analyze the preprocessed data in real-time to detect potential DDoS attacks. These models are continuously updated to adapt to new threats, ensuring the system remains effective.

The Visualization and Mitigation Module provides a user-friendly interface for network administrators. It displays real-time traffic data, highlighting any anomalies detected by the machine learning models. Administrators can view traffic patterns and take corrective actions, such as blocking malicious IPs or adjusting firewall settings, to mitigate attacks.

Together, these components form a robust, scalable system for real-time DDoS attack detection and mitigation, tailored for the unique demands of 5G networks.

2.2 Workflow

The system operates through a structured and efficient workflow, ensuring seamless data processing and accurate DDoS detection. The first step is Data Ingestion, where real-time network traffic is captured from multiple sources within the network infrastructure. This includes data from various network nodes, enabling the system to monitor traffic across different segments of the network simultaneously.

Next, in the Preprocessing stage, the raw traffic data is cleaned and essential features are extracted. These features include IP addresses, protocol types (such as TCP and UDP), and traffic volumes, all of which are critical for detecting patterns indicative of DDoS attacks. The preprocessing step ensures that the data is structured and suitable for further analysis by machine learning algorithms.

In the Model Training and Prediction phase, machine learning models are employed to classify the traffic and identify any anomalies. The models, trained on historical data, analyze the preprocessed input to predict potential threats in real-time. This predictive capability allows the system to detect attacks before they cause significant disruption.

Finally, the Visualization stage displays the results on an intuitive dashboard. This dashboard allows administrators to easily interpret the analysis and make informed deci-

sions about mitigating threats, ensuring a timely and efficient response to potential DDoS attacks.

3 Machine Learning Models

3.1 Feature Selection

Effective feature selection is critical for improving prediction accuracy and computational efficiency. The following features were utilized:

- Source and Destination IP Addresses
- Protocol Type (e.g., TCP, UDP)
- Packet Frequency and Volume
- Anomaly Labels

3.2 Algorithms Evaluated

Three machine learning models were tested:

- **Random Forest:** Achieved the highest accuracy due to its ability to handle complex interactions.
- **KNN:** Suitable for smaller datasets but computationally intensive for real-time scenarios.
- **Naive Bayes:** Demonstrated fast processing times but struggled with data heterogeneity.

The system is composed of several key components that work together to provide efficient DDoS detection. The Machine Learning Module uses algorithms like Random Forest and KNN to classify network traffic, identifying anomalies that could indicate potential DDoS attacks. The Visualization and Mitigation Module displays real-time traffic data on a user-friendly dashboard, enabling administrators to take swift action, such as blocking malicious IP addresses or adjusting firewall settings.

3.3 Performance Metrics

Performance was evaluated using accuracy, precision, recall, and F1-score. Results showed the Random Forest model achieving the best overall performance with an accuracy of 97.5%.

Model	Accuracy	Precision	Recall	F1-Score
Random Forest	97.5%	96.8%	98.3%	97.5%
KNN	94.2%	93.1%	95.6%	94.3%
Naive Bayes	89.7%	87.5%	91.2%	89.3%

Table 1: Performance Metrics of ML Models

4 Frontend Development

The frontend of the DDoS prediction system is built using React.js to provide a dynamic, responsive user interface, and Flask to handle backend processing. It is designed to offer an intuitive and interactive experience for network administrators. One of the key features is Dataset Upload, allowing users to easily upload network traffic datasets for model training directly through the interface. Once the data is uploaded, the Model Training feature enables users to initiate and monitor the training of machine learning models, offering real-time feedback on the training process.

The Traffic Analysis section provides administrators with detailed insights into network traffic patterns, helping them understand normal and abnormal behaviors. This is coupled with the Anomaly Detection Results, which visually displays the outcomes of the model's predictions. By presenting the results clearly, the system allows administrators to easily interpret potential threats and make informed decisions to mitigate DDoS attacks, ensuring quick and efficient responses to network anomalies.

5 Experimental Results

The system was evaluated using simulated datasets, and the outcomes highlighted the effectiveness of the model in detecting DDoS anomalies.

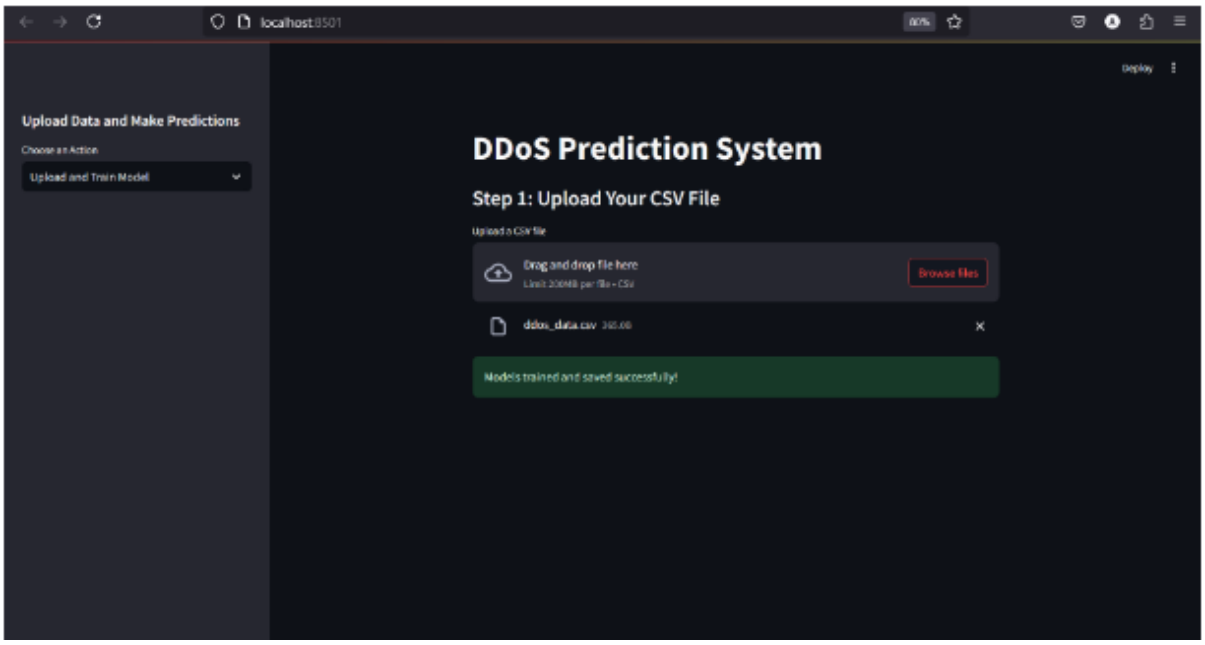

Figure 1: Model Training Interface

6 Contributions

The project was completed collaboratively by the team:

- **Avin Saxena** and **Vaishali Bhagwani** were responsible for conducting the research on the dataset, performing data analysis, and building the system architecture. They laid the foundation for the project by selecting the right dataset,

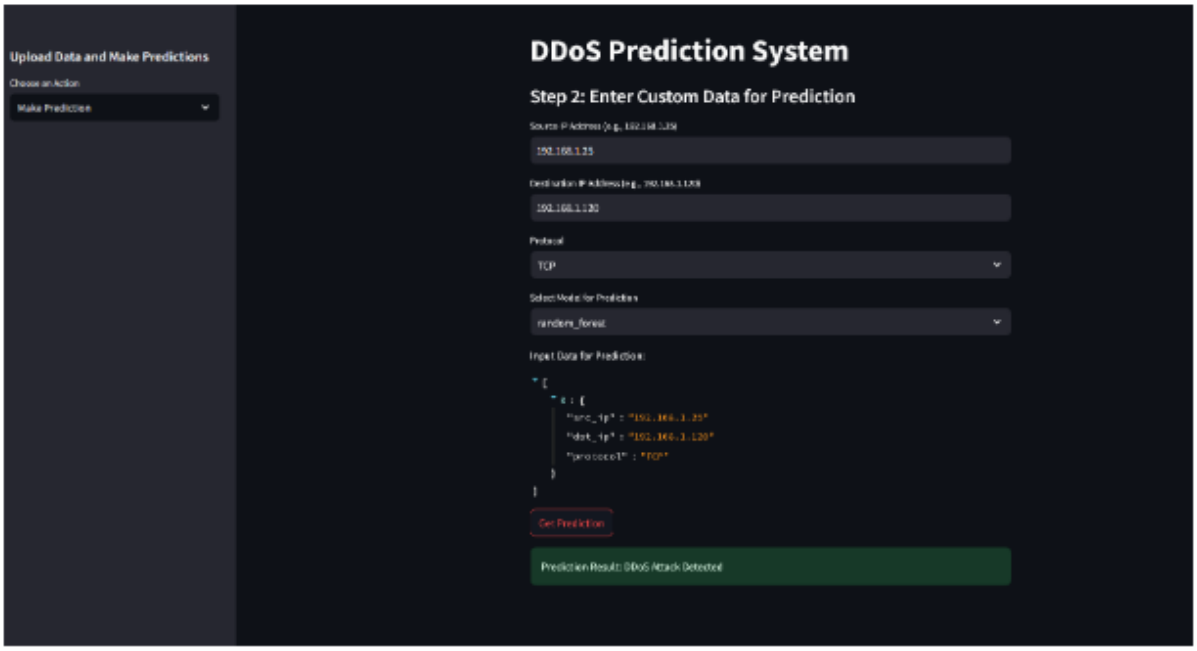

Figure 2: Prediction Interface

ensuring its quality, and designing the architecture to accommodate the system's components efficiently.

- **K. Anamithra** handled the entire frontend development of the system. This involved designing and implementing a dynamic, user-friendly interface using React.js, ensuring the system was intuitive for network administrators to upload datasets, monitor traffic, and visualize prediction results.

- **Yeshwanth Vatti** focused on training the machine learning models and working on the backend development. He trained models like Random Forest, KNN, and Naive Bayes, optimized them for better performance, and integrated them into the backend to ensure real-time prediction capabilities.

- **Shriram Ashok Birajdar** worked alongside **Yeshwanth Vatti** in assisting with the backend development. He helped implement the data processing pipeline, integrated machine learning models into the system, and ensured smooth communication between the backend and frontend components.

Each team member played a crucial role in delivering a comprehensive solution to detect and mitigate DDoS attacks in 5G networks.

7 Conclusion and Future Work

The DDoS Prediction System demonstrates high accuracy and scalability, addressing the unique challenges posed by 5G networks. Future enhancements will include support for multi-vector attacks and automated threat mitigation strategies.

Acknowledgment

We would like to express our sincere gratitude to Bhupendra Kumar Sir for his invaluable guidance, support, and encouragement throughout the duration of this project. His insights and expertise were instrumental in shaping the direction of the project, and his constant feedback helped us refine our approach. We greatly appreciate his mentorship, which significantly contributed to the successful completion of this project.