DDoS Mitigation System using eBPF and ML Models

Project Team:

- U Chandra Sekhar - 23BCE9222
- SK Kaif Sharif - 23BCE9393
- J Hari Kiran - 23BCE9389

Under the guidance of: Dr. D SanthaDevi

Table of Contents

1. INTRODUCTION

1.1 Overview

Distributed Denial of Service (DDoS) attacks represent a critical threat to network infrastructure, overwhelming systems with illegitimate traffic and exhausting resources. Modern attacks have evolved from megabit-scale to multi-terabit attacks, with the proliferation of IoT botnets enabling devastating volumetric floods.

Traditional mitigation approaches face fundamental challenges:

- **High Detection Latency:** Minutes to hours response time
- **False Positives:** Legitimate traffic blocked alongside attacks
- **Limited Scalability:** Struggles at multi-million packet-per-second rates
- **High Cost:** Expensive hardware solutions prohibitive for SMEs

Our Solution: A novel hybrid architecture combining:

- **Kernel-level filtering:** eBPF/XDP for ultra-fast packet processing
- **ML Classification:** Random Forest trained on CIC-DDoS-2019 dataset
- **Statistical Anomaly Detection:** Baseline comparison and flash crowd detection
- **Hybrid Decision-Making:** Integrated statistical and ML evidence

1.2 DDoS Attack Taxonomy

1.2.1 Classification by Layer

Volumetric Attacks (L3-L4):

- Objective: Bandwidth exhaustion
- Examples: UDP floods, ICMP floods, DNS amplification
- Impact: Network saturation (millions of pps)

Protocol Attacks (L3-L4):

- Objective: Resource exhaustion (CPU, memory, connections)
- Examples: SYN floods, fragmentation attacks
- Impact: Connection table exhaustion, server crashes

Application Layer Attacks (L7):

- Objective: Application/database crashes
- Examples: HTTP floods, Slowloris, query floods
- Impact: Application overload (low pps, high computational cost)

1.2.2 Target Attack Types

Attack Type	Layer	Detection Metric
SYN Flood	TCP	High SYN/ACK ratio
UDP Flood	UDP	Random port targeting
DNS Amplification	Application	Large packet sizes
HTTP Flood	Application	Repetitive patterns
ICMP Flood	Network	High ICMP rate

2. LITERATURE SURVEY

2.1 SDN-Based DDoS Detection Approaches

2.1.1 Ensemble Online Machine Learning in SDN

Abdulsalam Ahmed Alzahrani et al. [1] proposed enhancing DDoS attack detection and mitigation in Software-Defined Networking (SDN) using ensemble online machine learning models. Their approach utilized:

- **Dataset:** Custom-generated dataset using SDN testbed
- **Technique:** Ensemble Online Machine Learning
- **Attack Types:** Dynamic DDoS, Zero-Day attacks
- **Key Features:** Real-time, on-known signatures
- **Results:** Achieved SDN-LRFDOS Zero Day, DDOS OML, BAL (93.5PML-Based Ensemble), and online training capability

This work demonstrates the effectiveness of ensemble methods in SDN environments but is limited to SDN-specific architectures.

2.1.2 NetFlow-Based Detection with GA-SVM

Hind et al. [2] developed NetFlow-GA-SVM based DDoS detection system utilizing:

- **Technique:** NetFlow + GA-SVM (Genetic Algorithm + Support Vector Machine)
- **Dataset:** Dataset not publicly available

- **Attack Types:** DDoS flooding
- **Key Features:** Standard feature extraction
- **Limitations:** Dataset availability restricts reproducibility

The GA-SVM hybrid shows promise but faces scalability challenges in high-throughput environments.

2.1.3 Machine Learning Chain Technology

Santos et al. [3] investigated machine learning chain technology for DDoS detection:

- **Technique:** ML chain technology (multi-model pipeline)
- **Dataset:** CIC-IDS-2017
- **Attack Types:** DDoS attacks
- **Key Features:** Internal Dataflow, IDS, and portscan-aware data scraper
- **Findings:** Multi-model pipeline enhanced detection but increased processing overhead

This demonstrates the benefits of multi-stage ML pipelines but highlights latency concerns.

2.1.4 Modular Architecture for LDDoS

Jawahar et al. [4] proposed MLDB (Machine Learning-Based LDDoS Detection):

- **Technique:** JetBPF, REP TREE, RF (Random Forest, J48 [Decision Tree])
- **Dataset:** CIC-DoS
- **Attack Types:** LDDoS (Low-rate DDoS)
- **Key Features:** Modular architecture with ML models
- **Results:** Demonstrated effective detection of stealthy low-rate attacks, but limited to benchmark dataset scenarios

2.1.5 Performance Metrics Evaluation

Pande Dias et al. [5] evaluated two models - Decision Tree (DT) and Support Vector Machine (SVM):

- **Technique:** Combination of inferential statistics, feature normalization (Z-norm), and SVM/DT classification
- **Dataset:** KDDCUP DataSet
- **Attack Types:** DDoS
- **Key Features:** Performance metrics evaluation
- **Findings:** Curated dataset but not comparable with other benchmarks; DT outperformed SVM in most cases

2.1.6 SDN Intrusion Detection

Sudari et al. [6] developed IDS for SDN using multiple ML approaches:

- **Technique:** DT (IF, LR, OB-DRB SDN, LSVC)
- **Dataset:** SDN Intrusion Dataset
- **Attack Types:** Various intrusions
- **Key Features:** Contains 6 traffic categories, 23 intrusion fields, three normal activities
- **Results:** Network function virtualization focused, comprehensive feature set

2.1.7 SL Model and Bagging Tree Algorithm

Saied et al. [7] implemented supervised learning with bagging:

- **Technique:** SL Model and Bagging tree algorithm
- **Dataset:** DARPA and NSDM dataset
- **Attack Types:** Protocol DDoS
- **Key Features:** Standard flow features
- **Findings:** Good detection but failed to classify other zero-stage DDoS as seen in advanced scenarios

2.1.8 XGBoost for Traffic Differentiation

Wang et al. [8] applied extreme gradient boosting for SYN flood detection:

- **Technique:** ML models for traffic differentiation using XGBoost
- **Dataset:** Custom dataset
- **Attack Types:** TCP, UDP, ICMP flooding, Slowloris, GoldenEye
- **Key Features:** Fine-grained and coarse-level features (BGP, DH) for geo-anomaly detection
- **Results:** XGBoost demonstrated superior performance; dataset with geographic context

2.2 Advanced ML and Deep Learning Approaches

2.2.1 Mininet-Based RTU Classification

Al-Qahtani et al. [9] developed real-time DDoS detection using deep learning:

- **Technique:** Data Collection and preprocessing using Mininet-RTU
- **Dataset:** Custom dataset
- **Attack Types:** DDoS
- **Key Features:** Layered approach: Building network, Open Flow and RTU SDN Controller, HyperLedger Fabric
- **Results:** Utilized MTU, SDN Controller-based architecture; real-time capability

2.2.2 Precision Tree-Based Detection

Chen et al. [10] proposed privilege escalation detection:

- **Technique:** Precision Tree-based approach using Decision Tree (DT)
- **Dataset:** Custom dataset
- **Attack Types:** privilege escalation
- **Key Features:** eBPF flow monitoring
- **Findings:** Demonstrated eBPF can be used for user-space data gathering but lacks real-time kernel-level decision making; detection verification layer choke points in concurrent systems

2.2.3 Network Layer Packet Filtering

Bui et al. [11] implemented real-time detection using eBPF:

- **Technique:** Packet filtering at network layer using eBPF
- **Dataset:** Custom dataset

- **Attack Types:** volumetric attacks
- **Key Features:** Network layer packet filtering
- **Results:** Offers execution overhead performance but lacks comprehensive ML integration

2.3 eBPF and XDP-Based Solutions

2.3.1 Flow-State Management with eBPF

Chen et al. [12] (Not specified from table) explored eBPF for flow state management.

2.3.2 Decision Tree with In-Kernel eBPF

Bui et al. [13] integrated machine learning directly into kernel space:

- **Technique:** A flow-based IDS using Machine Learning in eBPF
- **Dataset:** Custom dataset
- **Attack Types:** DDoS, general signatures
- **Key Features:** Flow state (pkt/bytes/timestamp) from Single eBPF maps
- **Results:** 100K pkt/s on user-space, full GBF ML in-kernel analysis; demonstrates potential but throughput below production requirements

2.3.3 XDP Learning-Based Framework

Bui et al. [14] proposed Framework Based on Machine Learning and eBPF:

- **Technique:** BILSTM classifier (Bidirectional LSTM)
- **Dataset:** Production traffic traces
- **Attack Types:** DDoS, Network threats
- **Key Features:** Flow data (pkt/bytes/timestamp)
- **Results:** Real-time-only capture; Detect. Utilizes high-efficiency and time-series analysis

2.3.4 ANOVA Feature Selection

Chen et al. [15] investigated distributed denial of service attacks with ANOVA:

- **Technique:** DT, RF, SVM, TwoSDM
- **Dataset:** CIC-DDS-2017
- **Attack Types:** DoS, DDoS
- **Key Features:** ANOVA-F best selection, filtering/reduction
- **Results:** eBPF kernel bypass; TCPdump tool key tree main (dimension/centrality/safety); demonstrates statistical feature selection improves ML performance

2.3.5 Federated Learning for Collaborative Detection

Chen et al. [16] proposed privacy-preserving DDoS detection:

- **Technique:** Federated Learning
- **Dataset:** Production traces
- **Attack Types:** Large-scale DDoS
- **Key Features:** Packet/flow classification features

- **Results:** IDP firewalls; collaborative-improved domain accuracy-defensives without centralized data sharing

2.4 Research Gap Analysis

Category	Best Performance	Limitation	Our Contribution
SDN-Based ML	93.5% accuracy [1]	SDN-specific, not general-purpose	General Linux kernel integration
NetFlow Detection	Good accuracy [2]	Dataset unavailable, offline	Real-time, public dataset (CIC-DDoS-2019)
eBPF Flow Monitoring	Real-time capable [10]	No ML integration	Full ML + eBPF hybrid
eBPF + ML	100K pps [13]	Low throughput	Target 5M+ pps with XDP
Feature Selection	ANOVA-based [15]	Separate from deployment	Integrated feature extraction pipeline

Primary Gap: No comprehensive system integrates **eBPF/XDP kernel-level filtering** with **ML classification** achieving both **high throughput (5M+ pps)** and **high accuracy (95%+)** with low false positives (<2%).

Our Novel Contribution:

1. **Hybrid Architecture:** Seamless eBPF/XDP + Random Forest integration
2. **High Performance:** Kernel-level filtering preserves multi-million pps throughput
3. **Intelligent Classification:** ML-based detection with statistical validation
4. **Practical Implementation:** Complete system with evaluation on real datasets

---

REFERENCES

SDN-Based DDoS Detection and Mitigation

[1] **A. Sebbar and K. Zkik**, "Enhancing Resilience against DDoS Attacks in SDN-based Supply Chain Networks Using Machine Learning," *2023 9th International Conference on Control, Decision and Information Technologies (CoDIT)*, Rome, Italy, 2023, pp. 230-234.
📄 **DOI:** 10.1109/CoDIT58514.2023.10284387
🔗 **IEEE Xplore:** https://ieeexplore.ieee.org/document/10284387
🔑 **Keywords:** Machine learning algorithms, Scalability, Supply chains, DDoS, Random Forest, SDN
📊 **Focus:** DDoS resilience in SDN-based supply chain networks using ML algorithms

[2] **S. Marleau, P. Rahman and C. Lung**, "DDoS Flood Detection and Mitigation using SDN and Network Ingress Filtering - an Experiment Report," *2024 IEEE 4th International Conference on Electronic Communications, Internet of Things and Big Data (ICEIB)*, Taipei, Taiwan, 2024, pp. 67-72.
📄 **DOI:** 10.1109/ICEIB61477.2024.10602663
🔗 **IEEE Xplore:** https://ieeexplore.ieee.org/document/10602663

🔑 **Keywords:** DDoS attacks, Network ingress filtering, SDN, Mininet, Ryu Controller
📊 **Focus:** Experimental DDoS flood detection using SDN controller and network ingress filtering

[3] **J. E. Varghese and B. Muniyal**, "Trend in SDN Architecture for DDoS Detection - A Comparative Study," *2021 IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER)*, Nitte, India, 2021, pp. 170-174.
📄 **DOI:** 10.1109/DISCOVER52564.2021.9663589
🔗 **IEEE Xplore:** https://ieeexplore.ieee.org/document/9663589
🔑 **Keywords:** DDoS, SDN, Comparative study, SDN architecture, DDoS detection
📊 **Focus:** Comparative analysis of SDN architectural trends for DDoS detection

[4] **N. M. Yungaicela-Naula, C. Vargas-Rosales, J. A. Perez-Diaz, E. Jacob and C. Martinez-Cagnazzo**, "Physical Assessment of an SDN-Based Security Framework for DDoS Attack Mitigation: Introducing the SDN-SlowRate-DDoS Dataset," *IEEE Access*, vol. 11, pp. 46820-46831, 2023.
📄 **DOI:** 10.1109/ACCESS.2023.3274577
🔗 **IEEE Xplore:** https://ieeexplore.ieee.org/document/10113577
🔑 **Keywords:** SDN, Dataset, Deep learning, Slow-rate DDoS, IDS, IPS
📊 **Contribution:** Introduces **SDN-SlowRate-DDoS Dataset** for slow-rate DDoS attack detection in SDN environments

[5] **R. Sanjeetha, K. N. A. Shastry, H. R. Chetan and A. Kanavalli**, "Mitigating HTTP GET FLOOD DDoS attack using an SDN controller," *2020 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT)*, Bangalore, India, 2020, pp. 6-10.
📄 **DOI:** 10.1109/RTEICT49044.2020.9315608
🔗 **IEEE Xplore:** https://ieeexplore.ieee.org/document/9315608
🔑 **Keywords:** DDoS attack, SDN, Blacklist, Flow table, OpenFlow
📊 **Focus:** HTTP GET Flood mitigation using SDN controller with flow table and blacklist mechanisms

---

eBPF/XDP-Based DDoS Protection

[6] **K. Živanović and P. Vuletić**, "Kernel-Level DDoS Protection Using eBPF in IoT Networks," *2025 33rd Telecommunications Forum (TELFOR)*, Belgrade, Serbia, 2025, pp. 1-4.
📄 **DOI:** 10.1109/TELFOR67910.2025.11314317
🔗 **IEEE Xplore:** https://ieeexplore.ieee.org/document/11314317
🔑 **Keywords:** Filtering, DoS, eBPF, XDP, IoT, MQTT, Kernel-level protection
📊 **Focus:** Kernel-level DDoS protection in IoT networks using eBPF filtering algorithms

[7] **Y. Zhang, H. Wang and P. Gao**, "Research on Efficient Packet Filter Technology Based on eBPF," *2025 IEEE 8th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, Guiyang, China, 2025, pp. 891-894.
📄 **DOI:** 10.1109/IAEAC65194.2025.11165810
🔗 **IEEE Xplore:** https://ieeexplore.ieee.org/document/11165810
🔑 **Keywords:** Packet filter, eBPF, XDP, Efficient processing, Real-time systems
📊 **Focus:** Efficient packet filtering optimization using eBPF/XDP for real-time processing

[8] **S. Remya et al.**, "eBPF-Based Runtime Detection of Semantic DDoS Attacks in Linux Containers," *IEEE Access*, vol. 13, pp. 169178-169219, 2025.
📄 **DOI:** 10.1109/ACCESS.2025.3614389

🔗 **IEEE Xplore:** https://ieeexplore.ieee.org/document/10847389
🔑 **Keywords:** eBPF, Linux, DDoS attack, Docker, CODA, Container security, Real-time detection
📊 **Focus:** Runtime detection of semantic DDoS attacks in containerized environments using eBPF monitoring