Detection Attack DOS Using Reinforcement Learning

Abstract

In light of the increasing prevalence of Denial-of-Service (DoS) attacks, robust detection mechanisms have become essential to ensure the availability and reliability of computer networks. This thesis proposes a novel intrusion detection approach that leverages Reinforcement Learning (RL) to identify and mitigate DoS attacks. The RL agent learns optimal detection policies by interacting with a simulated network environment, continuously improving its performance through reward-based feedback. Key network traffic features are extracted and used as state inputs for the agent, enabling it to distinguish between benign and malicious activity. The model is evaluated in benchmark datasets such as CSE-CIC-IDS2018, demonstrating high detection accuracy, low false positive rates, and adaptability to evolving attack patterns. Compared to traditional machine learning classifiers, the RL-based system shows improved response and decision-making capabilities under dynamic network conditions. Future research will explore the integration of this system into real-time network infrastructures and the enhancement of its scalability for broader threat detection.

Keywords: Intrusion Detection Systems (IDS), Denial-of-Service (DoS), Reinforcement learning (RL), CSE-CIC-IDS2018, Cybersecurity, Network Traffic Analysis.

Contents

Chapter 1

Intrusion Detection System (IDS)

1.1 Security Fundamentals

Introduction

Security fundamentals refer to the essential principles, concepts, and practices that form the foundation of information security. These fundamentals encompass a wide range of technical and organizational measures aimed at protecting sensitive information and systems from unauthorized access, theft, damage, or other forms of compromise.

Key security fundamentals include Confidentiality, Integrity, Availability, Authentication, Authorization, Encryption, Risk Management, Incident Response, and Disaster Recovery. Together, these principles establish the basis of a comprehensive information security program, enabling organizations to effectively safeguard their critical information assets and maintain the trust of stakeholders.[**?**]

1.1.1 Core Security Concepts

Network security encompasses strategies and technologies to protect systems from cyber threats, particularly Denial of Service (DoS) attacks that aim to disrupt service availability. Several core principles serve as the foundation for secure systems.

CIA Triad

Confidentiality Confidentiality ensures that sensitive information is only accessible to authorized users. Techniques such as encryption, user authentication, and access control policies prevent unauthorized data access. While DoS attacks do not typically aim to breach confidentiality directly, successful exploitation may lead to indirect confidentiality violations if attackers cause service misconfigurations or force failovers to insecure states.

Integrity Integrity guarantees that data is accurate and unaltered. It is maintained through cryptographic hash functions, checksums, and digital signatures that validate whether data has been tampered with. During a DoS attack, integrity may be compromised by interrupting legitimate updates or corrupting processes due to system overload.

Availability Availability ensures that services and systems remain accessible to legitimate users at all times. This principle is the primary target of DoS attacks, which flood networks or services with excessive requests, causing slowdowns or complete denial of access. Maintaining availability involves redundancy, load balancing, and proactive mitigation strategies like rate limiting and firewalls.

Figure 1.1: Principles of information security

Source: [?]

Extended Security Principles

Non-repudiation Non-repudiation guarantees that an entity cannot deny having performed a particular action, such as sending a message or initiating a transaction. This is enforced through digital signatures and secure logging mechanisms. In the context of DoS attacks, non-repudiation helps trace attack origins and supports legal accountability.

Authenticity Authenticity confirms that data, communications, or users are genuine and not forged. Authentication protocols, digital certificates, and cryptographic techniques are used to ensure that data comes from trusted sources. This is crucial for filtering legitimate traffic from spoofed attack traffic in DoS scenarios.

Accountability Accountability ensures that all actions within a system can be traced to responsible users or processes. It involves logging, auditing, and monitoring to track behavior. Accountability is vital for forensic analysis after a DoS attack and for strengthening defenses against future intrusions.

1.2 Denial-of-Service (DoS) Attacks

Introduction Denial-of-Service (DoS) attacks aim to make a system or network resource unavailable to its intended users by overwhelming it with excessive traffic or exploiting protocol-level vulnerabilities. These attacks can disrupt services, degrade performance, or completely shut down access. The most common types include:

1.2.1 Volumetric Attacks

Volumetric attacks aim to saturate a target's bandwidth by generating an overwhelming amount of traffic. This often involves amplification techniques or high-rate packet floods. Common examples include UDP floods and DNS amplification attacks, which leverage misconfigured servers to multiply traffic directed at the victim [**?**].

In a UDP flood, attackers send large numbers of spoofed UDP packets to random or specific ports, consuming bandwidth and processing power. DNS amplification uses small queries to open resolvers with the victim's IP address, causing them to return large responses to the victim.

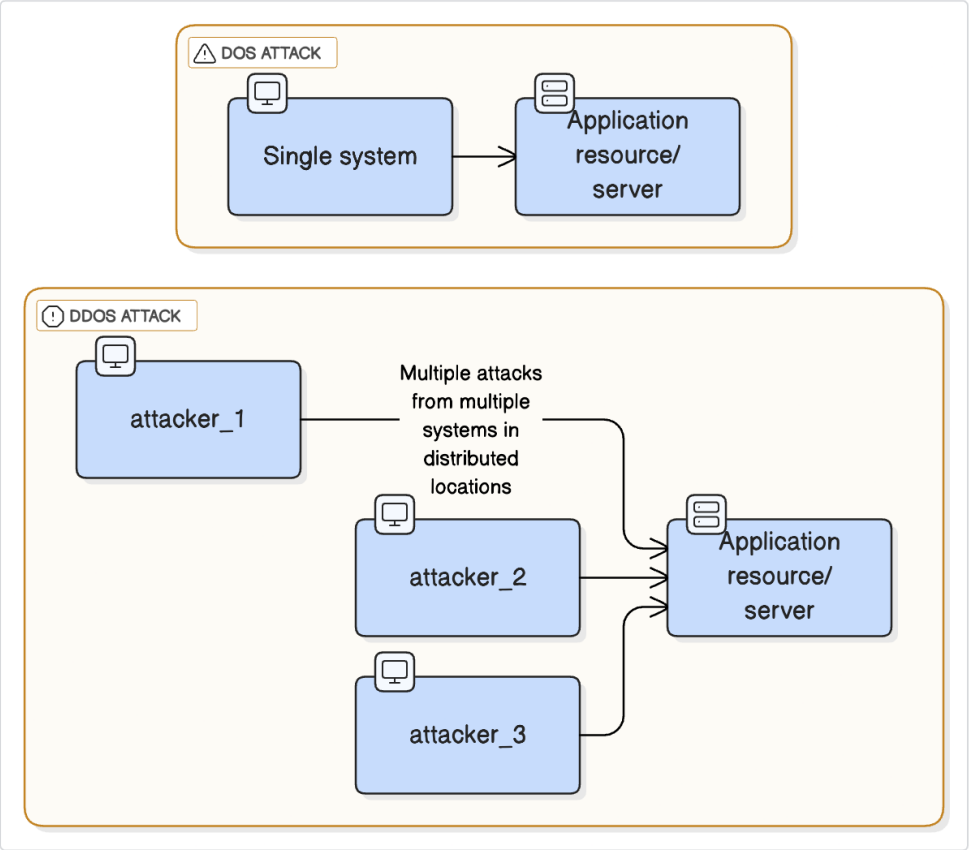

Figure 1.2: DoS and DDoS Attack Traffic Comparison

A notable example is the Mirai botnet, which infected hundreds of thousands of insecure IoT devices to coordinate massive traffic streams toward its targets [**?**]. The goal of volumetric attacks is to clog network links (Gbps or Tbps scale), preventing legitimate access.

1.2.2 Protocol Attacks

Protocol attacks exploit weaknesses in Layer 3/4 protocols (network or transport layer) to exhaust server or network resources. Unlike volumetric attacks, they do not require high bandwidth but instead consume stateful resources like connection tables or CPU cycles [**?**].

A classic example is the TCP SYN flood, where attackers send numerous SYN packets without completing the handshake, filling the server's connection queue [**?**]. ICMP floods and Ping of Death attacks exploit the Internet Control Message Protocol to crash or freeze systems by sending malformed or excessive traffic.

Other examples include fragmentation attacks (e.g., Teardrop), which send overlapping IP fragments to crash reassembly logic, and ACK/FIN floods that exhaust firewall state tables.

1.2.3 Application Layer Attacks

Application-layer (Layer 7) attacks generate traffic that appears legitimate at the application level but consumes excessive server resources such as CPU, memory, or threads [**?**]. These attacks are difficult to detect because they mimic real user behavior.

HTTP GET/POST floods can overwhelm web servers by triggering costly operations. A well-known example is Slowloris, which sends partial HTTP headers slowly to hold open many connections and exhaust the web server's pool [**?**]. Other examples include RUDY (R-U-Dead-Yet) attacks and HTTP floods targeting dynamic or database-backed content.

1.2.4 Distributed Denial-of-Service (DDoS)

DDoS attacks use multiple compromised machines (botnets) to launch coordinated attacks, making them harder to block and vastly more powerful than single-source DoS attacks [**?**].

Botnets like Mirai leverage IoT devices to simultaneously launch volumetric or protocol-based attacks. Reflective amplification (e.g., using open DNS/NTP servers) further increases traffic impact. Mitigation requires upstream filtering, rate-limiting, and often third-party scrubbing services.

1.2.5 Network Traffic Analysis

Mitigating DoS/DDoS attacks relies on monitoring and anomaly detection. This involves establishing a baseline of normal network behavior and identifying deviations in volume, protocol use, or source IPs [**?**, **?**].

Anomaly-based intrusion detection systems (IDS) can flag unusual spikes, connection patterns, or TCP flag anomalies. Signature-based systems match known attack patterns. Flow analysis tools (e.g., NetFlow, sFlow) help detect irregular byte/packet rates or unusual source-destination pairs.

Advanced methods include machine learning to classify deviations. Once detected, defenses such as rate limiting, traffic shaping, or redirection to mitigation services are employed to maintain availability.

1.3 Intrusion Detection Systems (IDS)

An **Intrusion Detection System (IDS)** is a cybersecurity solution designed to monitor network or system activities for malicious actions or policy violations. Upon detecting such activities, the IDS typically alerts system administrators or integrates with centralized security tools like Security Information and Event Management (SIEM) systems to facilitate a coordinated response [**?**].

1.3.1 IDS Architecture

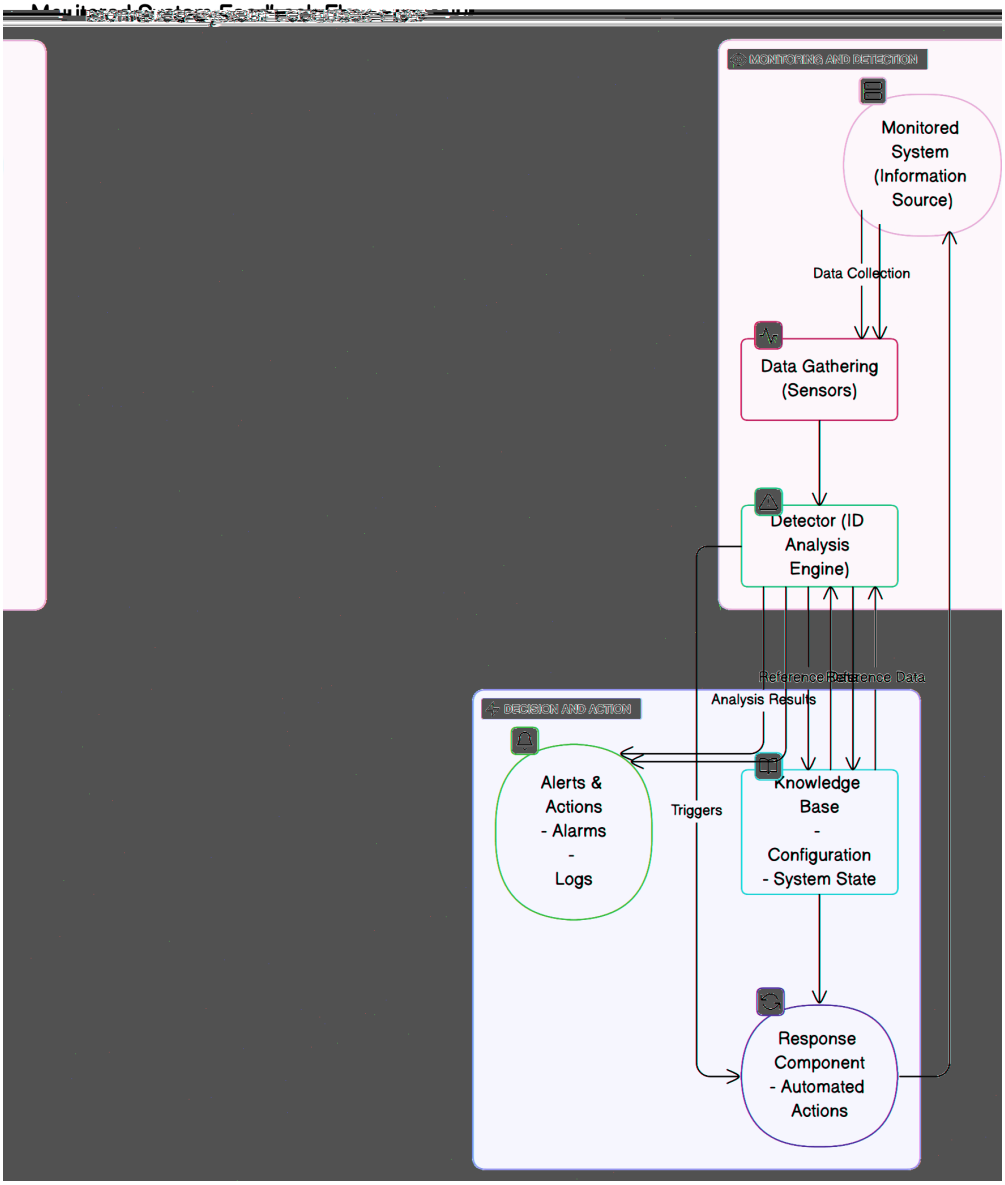

Figure 1.3: Network-based Intrusion Detection System (NIDS) Architecture

Modern IDS platforms implement modular architectures with several key components:

- **Sensors:** are the front line of an IDS, deployed at strategic network chokepoints—such as mirror (SPAN) ports, network taps, or virtual interfaces in cloud environments—to collect raw traffic data. They capture full packet streams, flow records, or application logs and often include built-in filters or sampling mechanisms to reduce noise in high-volume settings. By pre-processing and forwarding only relevant events, sensors ensure the IDS receives a representative yet manageable dataset, enabling visibility into lateral movement, data exfiltration, and denial-of-service attempts without overwhelming the analysis layer.

- **Analysis Engines:** Analysis Engines form the IDS's "brain," taking the sensor-collected data and

applying a mixture of rule-based and intelligent techniques to detect threats. Traditional pattern-matching engines compare payloads against known attack signatures, while statistical or machine-learning analyzers establish behavioral baselines and flag deviations. Protocol analyzers dive deep into application-level conversations—HTTP, DNS, SMB, etc.—to spot malformed requests or anomalous sequences. By correlating events across multiple sensors and data sources, the engine can piece together multi-stage attacks (e.g., a scan followed by an exploit) and prioritize alerts based on risk.

- **Knowledge Base:** The Knowledge Base underpins all detection logic by maintaining up-to-date signatures, behavioral profiles, and historical datasets. Signature databases are refreshed with the latest threat intelligence feeds, while anomaly detectors continuously refine their statistical models using both live traffic and feedback on past alerts. In more advanced platforms, machine-learning feedback loops incorporate security analyst verdicts—true positive, false positive—to retrain the system, improving accuracy over time. This shared repository ensures that the IDS can recognize both known exploits and subtle shifts in normal network behavior.

- **Response Systems:** Response Systems close the loop between detection and defense. Once the analysis engine assigns a confidence score to an event, the response component generates alerts—pushing them into dashboards, SIEMs, or ticketing systems—and, where policies allow, triggers automated countermeasures. High-confidence detections might invoke firewall rule updates, IP blacklists, or host quarantines, while lower-confidence events are routed to alert managers for human review. Integrated visualization tools help security teams triage incidents rapidly, and orchestration connectors enable the IDS to participate in broader security workflows, ensuring a coordinated, efficient reaction—especially critical when facing large-scale DoS or DDoS onslaughts.

For DOS attack detection, these components must operate with high efficiency and scale to process enormous traffic volumes during attack scenarios.

1.3.2 IDS Types and Functionality

Intrusion Detection Systems serve as the primary monitoring and detection layer for network security threats, including DOS attacks:

- **Network-based IDS (NIDS):** A Network-based Intrusion Detection System (NIDS) is a monitoring solution placed at key junctions within a network—often on a mirrored switch port or network tap—where it passively captures and inspects all passing traffic. Unlike host-based agents, a NIDS doesn't rely on software installed on individual machines; instead, it reconstructs network sessions and analyzes packet headers and payloads in real time. It uses signature-based detection (comparing packets against a database of known attack patterns) and anomaly-based detection (profiling normal traffic volumes, protocols, and behavioral baselines) to spot suspicious or malicious activity—such as port scans, denial-of-service floods, SQL injection attempts, or data exfiltration. When the NIDS flags a potential intrusion, it generates an alert that can be logged centrally, forwarded to a Security Information and Event Management (SIEM) system, or used to trigger automated defenses (e.g., instructing a firewall to block the offending IP). Because it sees all traffic crossing its monitored segment, a properly tuned NIDS provides broad visibility into attacker reconnaissance and network-level exploits—though it can be blind to encrypted payloads unless integrated with SSL/TLS decryption, and it may generate false positives if thresholds or signatures aren't carefully calibrated. By complementing host-based sensors and other controls, a NIDS forms a crucial layer in a network's defense-in-depth strategy.

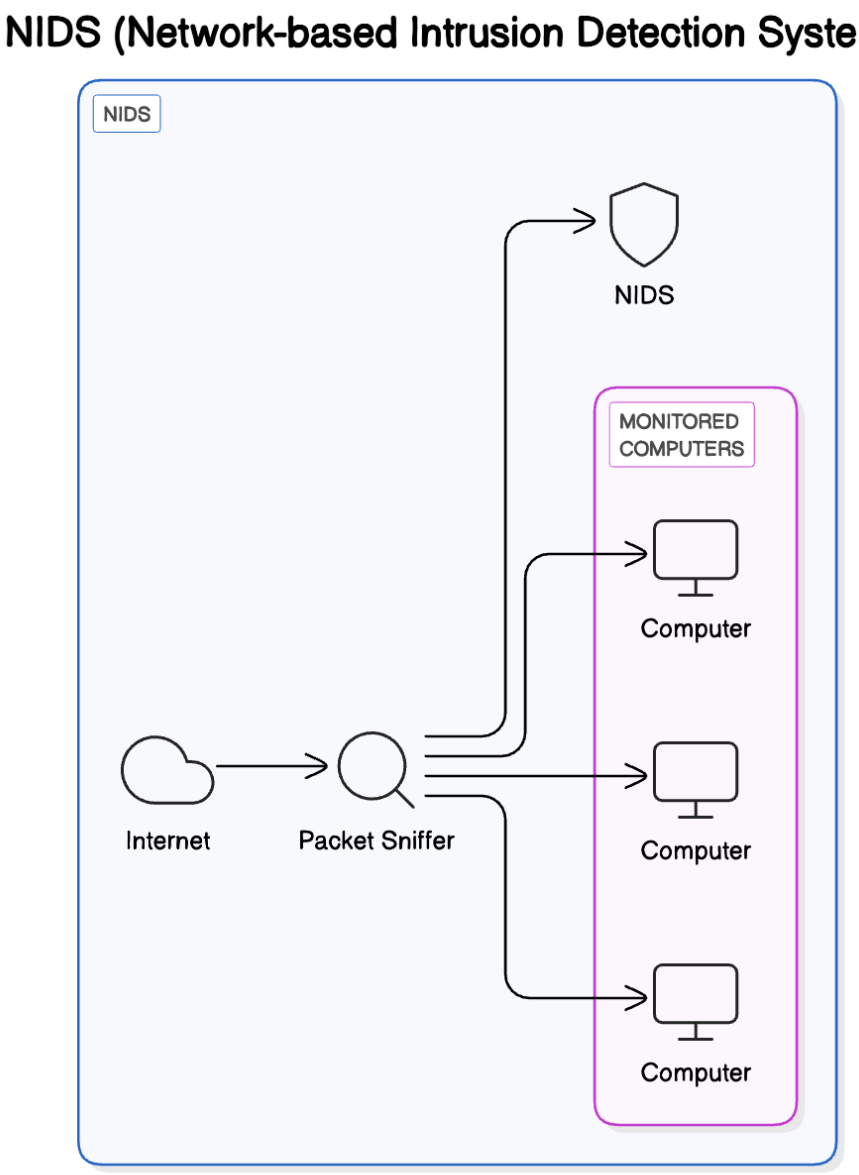

Figure: Network-based Intrusion Detection System (NIDS) Architecture

- **Host-based IDS (HIDS):** A Host-based Intrusion Detection System (HIDS) operates at the level of individual endpoints or servers, offering deep visibility into system-specific activities. Instead of analyzing network traffic, HIDS monitors internal events such as system calls, file integrity changes, registry modifications, user logins, and local log files. This allows it to detect unauthorized alterations, privilege escalations, malware activity, and localized impacts of denial-of-service (DoS) attacks that may not be evident from a network perspective. By focusing on what happens inside the host, HIDS provides rich contextual information—such as which process triggered a suspicious action or which user account was involved—which is crucial for forensic analysis and containment. However, its scope is inherently limited to the device it protects, offering little visibility into lateral movement or network-wide attack patterns. Common examples of HIDS tools include OSSEC, Tripwire, and Wazuh.

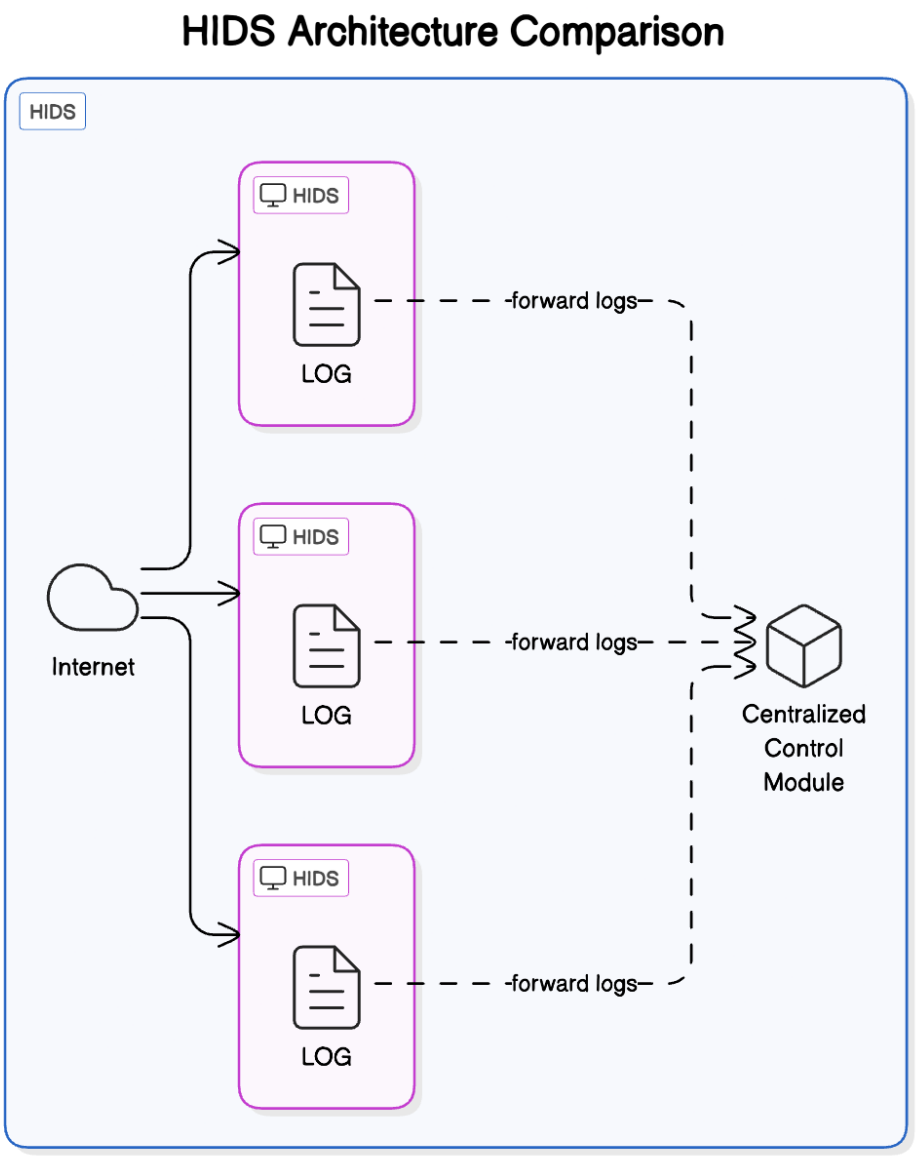

Figure: Network-based Intrusion Detection System (NIDS) Architecture

- **Detection Methodologies:**
  - **Signature-based:** Matches observed traffic against known attack patterns (signatures)
    - Highly effective for known attacks with clear signatures
    - Requires regular signature updates
    - Ineffective against zero-day or modified attacks
    - Examples: SYN flood patterns, known botnet command signatures
  - **Anomaly-based:** Establishes baselines of normal behavior and flags significant deviations
    - Can detect previously unknown attack vectors
    - Requires training period to establish accurate baselines
    - Typically generates more false positives than signature-based systems
    - Examples: Traffic volume spikes, unusual protocol distributions

- **Hybrid Systems:** Combine signature and anomaly detection approaches
  - Leverage strengths of both methodologies
  - Use signatures for known threats and anomaly detection for novel attacks
  - Implement weighted alert systems for confidence scoring
  - Reduce false positives through correlation of multiple detection methods

Limitations of Traditional IDS for DOS attack detection include:

- Difficulty processing high-volume traffic during attacks
- Challenges distinguishing flash crowds from attacks
- Limited adaptation to evolving attack techniques
- High false-positive rates with anomaly detection
- Resource consumption during high-traffic periods

These limitations necessitate AI-driven approaches like reinforcement learning that can adapt to evolving threat landscapes.

1.4 Classification in Security Contexts

1.4.1 Classification Paradigms

Classification forms the foundation of automated threat detection, organizing network traffic into categories for analysis and response:

Binary Classification: The simplest approach for distinguishing between normal and attack traffic. This method provides clear decision boundaries for basic filtering with low granularity but high processing efficiency. It is essential for initial traffic triage during high-volume attacks, offering straightforward pass/block decisions and benign/malicious categorization.

Multi-class Classification: A more sophisticated approach that distinguishes between multiple attack types, enabling targeted responses for specific threats. While requiring more complex models and training data, this method supports detailed attack attribution and can differentiate between various attack vectors such as SYN floods, HTTP floods, and DNS amplification attacks.

Hierarchical Classification: An organized approach that structures threats in a tree-like format, enabling progressive refinement of classifications. This method balances processing efficiency with detection detail and supports multi-stage detection pipelines. For example, traffic can be progressively classified as: Traffic → Attack → DOS → Protocol-based → SYN Flood.

Multi-label Classification: An advanced approach that assigns multiple categories to a single traffic flow, recognizing attacks with multiple characteristics. This method identifies complex attack campaigns and supports sophisticated response orchestration. For instance, traffic can be simultaneously classified as "volumetric," "distributed," and "amplification."

Classification outcomes drive security responses, determining whether traffic should be allowed, throttled, redirected, or blocked entirely.

What is Machine Learning?

Machine learning (ML) is a branch of artificial intelligence (AI) focused on enabling computers and machines to imitate the way that humans learn, to perform tasks autonomously, and to improve their performance and accuracy through experience and exposure to more data.

According to UC Berkeley, the learning system of a machine learning algorithm can be broken down into three main parts:

1. **A Decision Process:** In general, machine learning algorithms are used to make a prediction or classification. Based on some input data, which can be labeled or unlabeled, the algorithm produces an estimate about a pattern in the data.

2. **An Error Function:** An error function evaluates the prediction of the model. If there are known examples, an error function can make a comparison to assess the accuracy of the model.

3. **A Model Optimization Process:** If the model can fit better to the data points in the training set, then weights are adjusted to reduce the discrepancy between the known example and the model estimate. The algorithm repeats this iterative "evaluate and optimize" process, updating weights autonomously until a threshold of accuracy has been met.

Source: https://www.ibm.com/think/topics/machine-learning

1.4.2 Machine Learning Techniques

Modern security systems leverage diverse machine learning approaches for traffic classification:

Supervised Learning

Supervised learning involves training on labeled datasets where the "ground truth" classifications of attacks are already known. This approach allows models to learn from past data and make accurate predictions on new, unseen inputs. Common algorithms used in supervised learning include Random Forests, which are ensembles of decision trees that offer robust classification; Support Vector Machines (SVM), which are effective at identifying decision boundaries between different types of network traffic; Neural Networks, including multi-layer perceptrons and deep learning architectures capable of recognizing complex patterns; and Gradient Boosting methods like XGBoost, which are known for their high-performance classification capabilities. Supervised learning is especially useful in scenarios such as detecting known attacks using labeled training data, identifying specific types of attacks, analyzing the importance of different features, and deploying models in production environments where minimizing false positives is crucial.

Unsupervised Learning

Unsupervised learning focuses on uncovering patterns and structures within data that has not been labeled. This approach is especially useful when dealing with vast amounts of network traffic where manual labeling is impractical or impossible. Techniques commonly used in unsupervised learning include clustering methods such as k-means and DBSCAN, which group similar traffic patterns together based on statistical similarity. Anomaly detection methods like Isolation Forest and One-Class SVM are effective for identifying outliers that may indicate potential security threats. Dimensionality reduction techniques such as Principal Component Analysis (PCA) and t-Distributed Stochastic Neighbor Embedding (t-SNE) are used to simplify complex traffic data, making it easier to analyze. Autoencoders, a type of neural network, learn representations of normal traffic behavior and can highlight anomalies when deviations occur. Unsupervised learning is particularly valuable for identifying novel attack patterns, establishing baselines for normal behavior, detecting zero-day attacks, and categorizing traffic without the need for prior labeling.

Semi-Supervised Learning

Semi-supervised learning bridges the gap between supervised and unsupervised approaches by combining a small amount of labeled data with a much larger pool of unlabeled data. This method reduces the need for extensive manual labeling while still achieving reasonable accuracy in classification. It is especially beneficial in cybersecurity contexts where labeled attack data may be scarce, but large amounts of raw traffic data are available. Techniques in this category include self-training classifiers, where the model iteratively labels new data based on its predictions, and label propagation methods, which spread label information across a data

graph based on similarity. Semi-supervised learning is particularly valuable in dynamic and evolving threat landscapes, where continuous adaptation to new types of attacks is required without exhaustive annotation efforts.

These approaches also form the foundation for reinforcement learning systems, which build upon the outcomes of classification tasks to develop and refine optimal security policies.

Chapter 2

Reinforcement Learning Applications: A Comprehensive Guide

2.1 Introduction to the Reinforcement Learning Approach

Reinforcement Learning (RL) is a branch of machine learning that focuses on how agents can learn to make decisions through trial and error to maximize cumulative rewards. Unlike supervised learning, where models learn from labeled data, RL involves learning optimal behaviors through interactions with an environment, receiving feedback in the form of rewards or penalties based on actions taken. This approach enables agents to discover strategies that yield the highest long-term benefits, making RL particularly effective for tasks involving sequential decision-making, such as robotics, game playing, and autonomous systems. Reinforcement Learning provides several key advantages over traditional DoS detection approaches:
Source: Adapted from GeeksforGeeks: What is Reinforcement Learning

2.2 Introduction to Deep Q-Learning

Deep Q-Learning is a powerful extension of the traditional Q-Learning algorithm that leverages deep neural networks to approximate the Q-value function. In standard Q-Learning, an agent maintains a Q-table that maps state-action pairs to expected future rewards. However, this becomes impractical for environments with large or continuous state spaces. Deep Q-Learning addresses this limitation by using a deep neural network, known as a Q-network, to estimate Q-values directly from raw input states.

In reinforcement learning, the agent interacts with the environment in discrete time steps. At each step t, the agent observes a state s_t, selects an action a_t, receives a reward r_t, and transitions to a new state s_{t+1}. The goal is to learn a policy π that maximizes the expected cumulative reward over time.

The Q-value function $Q(s, a)$ represents the expected return of taking action a in state s and following the policy thereafter. In Deep Q-Learning, the Q-network is trained to minimize the difference between the predicted Q-value and the target Q-value, which is computed using the Bellman equation:

$$Q(s\_t, a\_t) = r\_t + \gamma \max\_a' Q(s\_t + 1, a'; \theta^-) \tag{2.1}$$

Here, γ is the discount factor, θ are the parameters of the current Q-network, and θ^- are the parameters of a target network that is periodically updated to stabilize training.

To improve learning stability and efficiency, Deep Q-Learning introduces two key techniques:

- **Experience Replay:** Stores past experiences in a replay buffer and samples mini-batches randomly during training to break correlations between consecutive samples.
- **Target Network:** Uses a separate, periodically updated target network to compute the target Q-values, reducing oscillations and divergence.

Deep Q-Learning has been successfully applied to various complex decision-making tasks, such as playing Atari games directly from raw pixels, demonstrating its potential in handling high-dimensional input spaces.

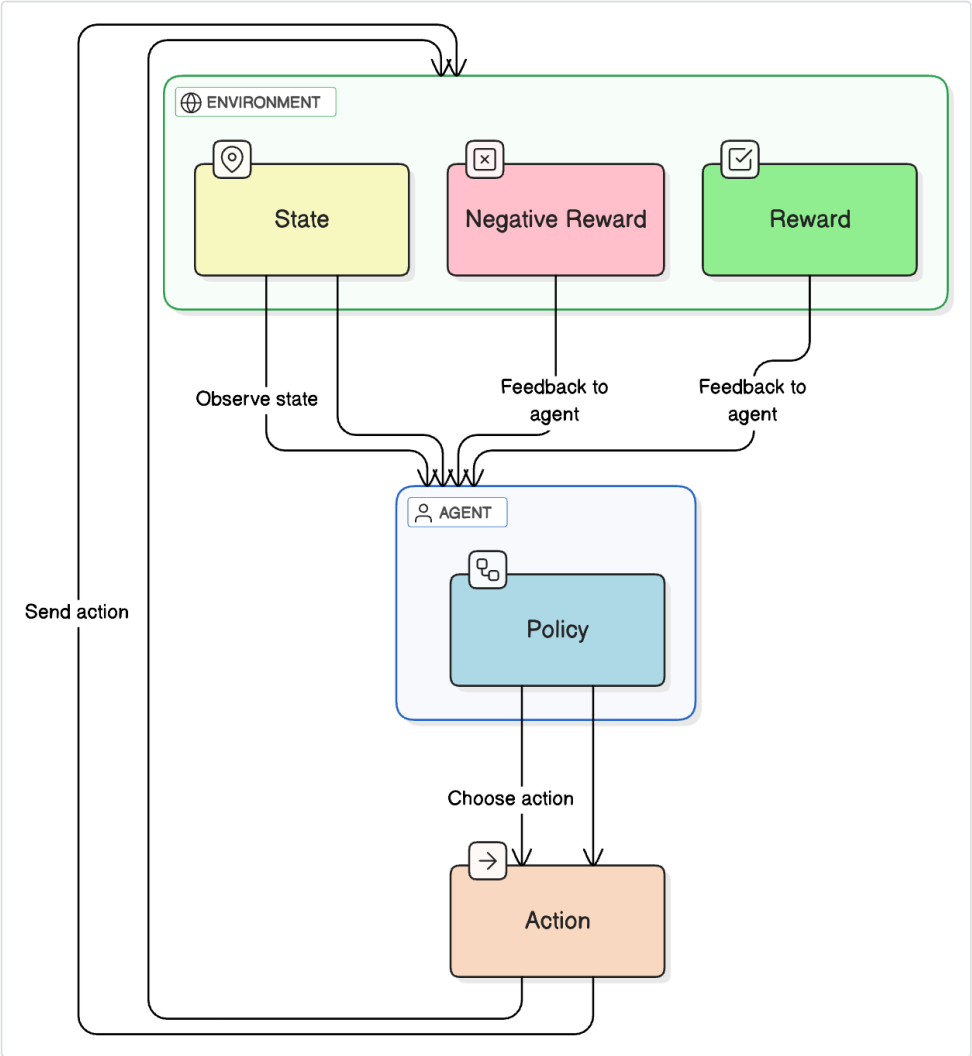

Figure: Basic Components of Reinforcement Learning

2.3 Environment Modeling for DoS Detection

The foundation of any RL application is a well-designed environment that accurately represents the problem domain. For DoS detection, this environment must model network traffic patterns and attack scenarios in a way that enables effective learning.

2.3.1 State Space Design

The state space in a reinforcement learning (RL) framework for Denial-of-Service (DoS) detection encodes the essential characteristics of network traffic that the agent uses to make decisions. A well-designed state space should reflect a comprehensive yet efficient representation of the network environment, enabling the RL agent to distinguish between normal and malicious activity. This design typically integrates four categories of features: traffic volume metrics, statistical distribution properties, temporal behavior indicators, and content-based descriptors. Each category offers a unique perspective on the nature of the traffic, contributing to a robust and informative state representation.

Traffic volume features quantify the scale and frequency of network activity. These include metrics such as packets per second, bytes per second, flow initiation rates, and the number of concurrent connections. These indicators are particularly useful for detecting volumetric DoS attacks, which are characterized by sudden spikes in traffic volume designed to overwhelm network resources. By monitoring these patterns, the RL agent can quickly recognize and react to abnormal surges in activity.

Statistical distribution features capture how traffic attributes are spread across various dimensions. Entropy values of source and destination IP addresses, protocol usage percentages, port distributions, and packet size variation are key indicators in this category. These features help identify anomalies that are not necessarily reflected in overall traffic volume but manifest as irregularities in distribution patterns, such as a high concentration of traffic targeting a specific port or originating from a narrow set of addresses.

Temporal pattern features provide insight into the evolution of traffic over time. By analyzing short-term trends, comparing current behavior to historical baselines, or evaluating periodicity, the agent can detect subtle or persistent attack patterns. Features such as time-of-day normalization or trend analysis allow the RL agent to differentiate between expected daily fluctuations and genuinely suspicious behavior, such as traffic bursts that align with known attack schedules.

Content-based features delve into the specifics of packet content and header information. This includes identifying protocol anomalies, unusual header field values, payload characteristics (when available), and application-layer request patterns. Such features are crucial for detecting more sophisticated attacks that may not exhibit volume or distribution anomalies but instead exploit specific protocol vulnerabilities or payload structures.

A critical aspect of state space design is balancing informativeness with efficiency. High-dimensional state representations can slow down learning and lead to overfitting. To mitigate this, techniques like feature selection, dimensionality reduction, and hierarchical representations can be employed. These methods help retain the most relevant features while reducing computational overhead, ultimately enhancing the agent's learning performance and scalability.

2.3.2 Action Space Definition

The action space defines the set of all possible decisions or interventions that the reinforcement learning (RL) agent can make in response to observed network conditions. In the context of DoS detection systems, these actions are typically organized into three main categories: detection-related, response-related, and adaptive actions. Each category serves a distinct role in enabling the agent to not only identify malicious activity but also to react appropriately and adjust its behavior over time.

Detection-related actions allow the agent to classify the nature of incoming traffic. These may include flagging traffic as normal, marking it as a potential DoS attack with low confidence, confirming it as a high-confidence DoS event, or requesting additional inspection to reduce uncertainty. These actions contribute to the agent's ability to differentiate between benign and malicious behavior with varying degrees of certainty.

Response-related actions are used to enforce protective measures against suspicious or confirmed attack traffic. These actions include allowing traffic to proceed unimpeded, rate-limiting suspected malicious flows, blocking specific traffic patterns known to be harmful, or redirecting traffic for more detailed analysis by external systems. Such actions form the core of the system's active defense mechanism, enabling real-time mitigation of ongoing threats.

Adaptive actions provide the agent with the ability to adjust its operational parameters in response to evolving threat landscapes. This includes actions such as modifying monitoring sensitivity, tuning feature extraction processes, escalating suspicious cases to human analysts, or gathering additional contextual data to refine future decision-making. These adaptive strategies are essential for maintaining long-term performance in dynamic environments.

The granularity of the action space plays a critical role in determining both the learning efficiency and the practical utility of the RL system. An overly coarse action space may restrict the agent's responsiveness and lead to underfitting, whereas an excessively fine-grained space can increase the complexity of the learning problem and slow convergence. Therefore, careful design of the action space is essential to strike an optimal balance between expressiveness and tractability.

2.3.3 Reward Function Design

The reward function plays a pivotal role in shaping the learning behavior of the reinforcement learning (RL) agent, guiding it toward effective and efficient DoS detection strategies. A well-crafted reward function must strike a balance between multiple, often competing objectives such as detection accuracy, operational efficiency, and timely response.

In terms of detection accuracy, the agent is incentivized through positive rewards for correctly identifying attacks, while being penalized for false positives and false negatives. These penalties and rewards may be further weighted based on the severity of the detected attack and the agent's confidence in its classification. This ensures that the agent not only learns to detect attacks but also to assess their impact and act accordingly.

Operational efficiency is also integral to the reward function. Small penalties may be applied to account for resource consumption, including computational overhead and bandwidth usage. Additionally, time-based rewards can encourage early detection, while excessive inspection of normal traffic or inefficient use of mitigation mechanisms can incur penalties. These components help align the agent's behavior with real-world constraints and performance expectations.

A typical structure for the reward function may take the following form:

$$R(s, a, s') = w_1 \times \text{DetectionAccuracy} + w_2 \times \text{TimeToDetect} + w_3 \times \text{ResourceEfficiency} \tag{2.2}$$

In this formulation, *DetectionAccuracy* reflects the correctness of the classification, considering true positives, false positives, and false negatives. *TimeToDetect* quantifies the latency in identifying an attack, and *ResourceEfficiency* evaluates how judiciously the system utilizes its resources during detection and response. The weights w_1, w_2, w_3 are tunable parameters that allow the system to prioritize objectives based on organizational or operational goals.

Careful calibration of the reward function is essential to ensure that the agent develops policies that are not only accurate and robust but also practical within the resource constraints and real-time requirements of modern network environments.

2.3.4 Environment Dynamics

The environment dynamics define the mechanisms through which state transitions occur in response to the agent's actions. In the context of DoS detection, these dynamics are influenced by both the underlying traffic patterns and the mitigation strategies employed by the agent. State transitions are often governed by probabilistic rules that reflect how network traffic evolves over time. For instance, specific traffic behaviors may be more or less likely to follow certain patterns, such as bursty traffic or sustained high-volume flows indicative of an ongoing attack.

The agent's actions directly impact the state evolution. For example, blocking suspicious traffic may lead to a reduction in attack volume, altering the observable state characteristics. Similarly, redirecting traffic for analysis or applying rate limits can change flow distributions and entropy metrics within the network. It is also important to consider temporal aspects of the environment; the effects of certain actions may not be immediately visible. For instance, a rate-limiting policy might only manifest noticeable changes after a delay, as the network adapts or the attacker responds.

Modeling these dynamics accurately is essential for realistic simulation and effective training of reinforcement learning agents. It allows the agent to learn how its actions influence the environment and adjust its policy accordingly to achieve robust and adaptive DoS detection performance.

2.3.5 Challenges in Applying RL to Security Domains

While reinforcement learning (RL) holds significant potential for enhancing cybersecurity systems, its application to security contexts—particularly DoS detection—presents several unique challenges. One major hurdle is the high dimensionality of the state space. Network traffic generates vast and complex feature sets, requiring sophisticated representation and dimensionality reduction techniques to ensure tractable learning.

Another difficulty lies in the delayed nature of rewards. In many cases, the outcome of a security-related decision—whether it successfully prevented an attack or caused unintended side effects—may only

become clear after a considerable time delay. This complicates credit assignment and policy evaluation. Moreover, rewards in the security domain tend to be sparse; attack events are relatively rare in comparison to the continuous stream of benign network activity, making it difficult for the agent to gain useful feedback consistently.

Safety during the learning process is also a critical concern. Exploration, a core part of RL, must be managed carefully to avoid compromising system integrity. Unlike in traditional domains, erroneous actions in security systems can have severe consequences. Compounding this is the adversarial nature of the environment—attackers actively adapt their strategies to bypass detection mechanisms, forcing RL agents to learn in a moving target setting.

To address these challenges, structured educational frameworks and simulation environments can be employed. These offer controlled scenarios where RL techniques can be gradually introduced and refined before deployment in production systems.

2.3.6 Advantages of RL for DoS Detection

Despite the complexities involved, RL brings numerous advantages to the domain of DoS detection. One of the most notable is adaptability. Unlike rule-based systems that require manual updates, RL agents can dynamically adjust to novel attack strategies and traffic behaviors. This makes them particularly well-suited for rapidly evolving threat landscapes.

RL also enables contextual decision-making, where responses are informed by the broader network state rather than isolated events. This holistic approach helps reduce false positives and improve detection accuracy. Moreover, RL frameworks can be designed to balance multiple, sometimes conflicting objectives—such as maximizing detection rates while minimizing the impact on normal traffic—through multi-objective optimization.

A proactive defense posture is another key benefit. By interacting continuously with the environment, RL agents can learn to anticipate and preempt attack progression rather than merely reacting to already-occurred incidents. This ongoing interaction fosters continuous improvement, allowing the system to refine its policies over time and maintain effectiveness even as network conditions and attack techniques evolve.

Chapter 3

Architectural Blueprint of a DQN-Powered DDoS Detection System

3.1 Introduction

This chapter provides a detailed examination of the architectural design and implementation of a Distributed Denial of Service (DDoS) detection system leveraging a Deep Q-Network (DQN).

We will systematically deconstruct the entire pipeline, beginning with the foundational steps of dataset acquisition and preprocessing. From there, we explore the critical process of feature engineering required to transform raw network data into a format suitable for a neural network.

The core of our discussion will focus on the DQN model itself: its underlying neural network architecture, the Q-learning algorithm that drives its decision-making, and the mechanisms that enable it to learn and adapt to evolving threat landscapes.

3.2 Comprehensive Data Preprocessing Pipeline

The primary dataset for this research is the CIC-DDoS2019, developed by the Canadian Institute for Cybersecurity (CIC). This dataset is exceptionally relevant as it captures a comprehensive set of contemporary DDoS attack vectors. It includes both reflection-based attacks that exploit UDP protocols (such as DNS, NTP, and SSDP amplification) and connection-based TCP floods (like SYN and ACK attacks). This diverse attack landscape is integrated with realistic, multi-protocol benign traffic profiles, including common application-layer protocols like HTTP, HTTPS, and FTP. This composition ensures the data closely simulates a real-world network environment, making it an ideal benchmark for evaluating modern intrusion detection systems.

The raw data, provided in PCAP format, was processed using the CICFlowMeter-V3 tool to generate labeled network flows. Each flow is uniquely identified by its 5-tuple (source/destination IP addresses, ports, and protocol). From these raw flows, CICFlowMeter extracts a rich set of over 80 statistical and time-based features. These include metrics such as flow duration, forward and backward packet counts, packet length statistics (min, max, mean), and flow I/O rates (bytes/sec). Crucially for supervised learning, each generated flow is explicitly labeled as either 'Benign' or with its specific attack type (e.g., 'DrDoS_NTP'), providing the ground truth for training our model.

This phase is paramount for ensuring the model's robustness and performance, as it involves meticulously cleaning and preparing the raw dataset. Our focus here is on retaining only high-quality, relevant samples, thereby mitigating noise and irrelevant features that could lead to overfitting and reduced detection accuracy.

3.2.1 Step 1: Data Cleaning

The initial phase focuses on cleaning the dataset to ensure its quality and integrity. This involves three key actions:

1. **Handling Null Values:** The dataset is first inspected for any missing or null values. Rows containing such values are dropped entirely. This step is crucial to prevent computational errors during model training and to ensure that the model learns from complete, high-quality samples.

2. **Dropping Irrelevant Features:** Certain features in the dataset, such as `Flow ID`, `Source IP`, `Destination IP`, `Source Port`, and `Timestamp`, are removed. These features are unique to each specific flow and do not represent generalizable patterns of an attack. Including them would introduce noise and create a high risk of overfitting, where the model memorizes specific instances from the training data rather than learning the underlying behavior of attacks.

3. **Numeric Conversion:** All remaining feature values are converted to a numeric data type. Machine learning models, and particularly neural networks like the DQN, require numerical input for their mathematical operations. This step ensures that all data, including any encoded categorical features, is in a format that the model can process.

3.2.2 Step 2: Binary Label Transformation

To simplify the detection task, the problem is framed as a binary classification problem. The multi-class labels present in the original dataset are converted into a binary format:

- Traffic labeled as **'BENIGN'** is mapped to the value **0**.
- Traffic representing any type of attack (e.g., 'DrDoS_NTP', 'SYN', 'UDP-lag') is mapped to the value **1**.

This transformation allows the model to focus on the fundamental task of distinguishing any malicious activity from normal network behavior.

3.2.3 Step 3: Feature Selection using Random Forest Classifier

Feature selection is a critical process for reducing the dimensionality of the dataset, which in turn reduces model complexity, decreases training time, and mitigates the risk of overfitting. For this task, we utilize the **Random Forest Classifier**.

Random Forest is an ensemble learning method that constructs a multitude of decision trees during training. It provides a built-in measure of feature importance, which reflects the degree to which each feature contributes to improving the purity of the nodes in the trees. The process is as follows:

1. A Random Forest Classifier is trained on the cleaned dataset.

2. The `feature_importances_` attribute of the trained model is used to extract an importance score for each feature.

3. Features are ranked based on these scores, and only the top-ranked features that contribute most significantly to the model's predictive power are retained for subsequent steps.

3.2.4 Step 4: Data Normalization

After feature selection, the data is normalized to ensure that all features contribute equally to the model's learning process. We employ **Min-Max normalization**, which scales each feature to a fixed range between 0 and 1.

This technique is essential for neural networks, as it prevents features with larger numeric ranges from dominating the learning process and helps stabilize the gradient descent optimization, leading to faster convergence. The Min-Max normalization formula for a feature X is given by Equation **??**.

$$X_{\text{normalized}} = \frac{X - X_{\min}}{X_{\max} - X_{\min}} \tag{3.1}$$

where:

- $X_{\text{normalized}}$ is the scaled value.
- X is the original feature value.
- $X_{\min}$ is the minimum value of the feature in the dataset.
- $X_{\max}$ is the maximum value of the feature in the dataset.

3.2.5 Step 5: Dataset Balancing with Random Undersampling

The CICDDoS2019 dataset exhibits a significant class imbalance, with a much larger proportion of attack traffic compared to benign traffic. Training a model on such an imbalanced dataset would bias it towards the majority class (attacks), leading to poor detection performance for the minority class (benign traffic) and a high false positive rate. amine To address this, we apply **random undersampling**. This technique balances the class distribution by reducing the number of samples from the majority class. Specifically, we randomly select and remove samples from the 'attack' class until its size matches the number of samples in the 'benign' class. While this method risks discarding potentially useful information from the majority class, it is effective in creating a balanced dataset that enables the model to learn the distinguishing characteristics of both classes with equal importance. The result is a model that is more robust and accurate in classifying both attack and benign traffic.

Bibliography

[1] IBM, *Security Fundamentals?*,
https://www.linkedin.com/pulse/fundamentals-security-slammghana/

[2] CIA, *Principles of Information Security.*
Available at: https://www.cleanpng.com/png-information-security-confidentiality-availability-1373941/

[3] Fidelis Security, *Understanding DoS and DDoS Attacks*,
https://fidelissecurity.com/blog/dos-ddos-attacks

[4] Imperva, *Denial of Service (DoS) Attack*,
https://www.imperva.com/learn/ddos/denial-of-service/

[5] NETSCOUT, *Slowloris Attack*,
https://www.netscout.com/blog/asert/slowloris-attack

[6] MDPI, *Anomaly-based Detection of DDoS Attacks Using Machine Learning*,
https://www.mdpi.com/2076-3417/10/3/1052

[7] IBM, *What is an Intrusion Detection System (IDS)?*,
https://www.ibm.com/think/topics/intrusion-detection-system

[8] Wikipedia, *Intrusion Detection System*,
https://en.wikipedia.org/wiki/Intrusion_detection_system

[9] Fortinet, *What is Intrusion Detection Systems (IDS)? How does it Work?*,
https://www.fortinet.com/resources/cyberglossary/intrusion-detection-system

[10] TechTarget, *What Is an Intrusion Detection System (IDS)?*,
https://www.techtarget.com/searchsecurity/definition/intrusion-detection-system

[11] TechTarget, *Dataset Difinition*,
https://www.unb.ca/cic/datasets/ddos-2019.html