Enhancing DDoS Detection and Mitigation in Software-Defined Networks: A Literature Survey

[1]Avinash Rajendra Deshpande, [2]Tarun Prabhu, [3]Dr. Jagruthi H

[3]Associate Professor
Information Science and Engineering
B.N.M. Institute of Technology, Bengaluru.

Abstract- **This literature survey explores the landscape of Distributed Denial of Service (DDoS) detection and mitigation techniques tailored for Software-Defined Networks (SDNs). In the face of escalating DDoS threats, particularly within the dynamic environment of SDNs, the necessity for effective detection and mitigation strategies is paramount. Through a comprehensive examination of existing research, this paper elucidates the diverse array of methodologies employed for detecting and mitigating DDoS attacks in SDNs, spanning from traditional to emerging approaches. By analysing the strengths, limitations, and comparative efficacy of these techniques, this survey aims to provide insights into the evolving strategies for fortifying SDNs against DDoS assaults. Additionally, it identifies existing gaps and potential avenues for future research, with the goal of fostering advancements in DDoS defence mechanisms within SDN infrastructures.**

Keywords: **DDoS, Deep Learning, Machine Learning, Software Defined Networks.**

1. INTRODUCTION

The advent of Software-Defined Networks (SDNs) has ushered in a new era of network management characterized by unprecedented flexibility and efficiency. By separating the control plane from the data plane, SDNs consolidate network intelligence, enabling dynamic and programmable network configurations. However, this architectural shift has also unveiled a critical vulnerability: susceptibility to Distributed Denial-of-Service (DDoS) attacks. These attacks exploit the centralized control and dynamic nature of SDNs, posing a significant threat to the availability and integrity of network services. Traditional defence mechanisms often struggle to keep pace with the evolving tactics of cyber adversaries within SDN environments, necessitating the development of proactive and adaptive defence mechanisms. In response, this research proposes leveraging deep learning algorithms to fortify SDN resilience against DDoS attacks, aiming to develop an intelligent system capable of real-time detection and mitigation.

The primary aim of this literature survey paper is to explore the landscape of DDoS detection and mitigation techniques within SDNs, with a specific focus on the application of deep learning algorithms. By synthesizing existing research, this paper seeks to identify key trends, challenges, and opportunities in bolstering SDN security. Through comprehensive analysis and evaluation in realistic SDN environments, this research endeavours to contribute to the advancement of SDN security, ultimately safeguarding network services from the evolving threats posed by DDoS attacks.

2. LITERATURE SURVEY

In [1], the author presents a pioneering hybrid deep learning algorithm tailored to combat DoS/DDoS attacks within the framework of software-defined networks (SDNs). As SDNs gain traction for their centralized control and adaptability, they concurrently attract cyber threats, underscoring the urgency for robust defense mechanisms. Detecting such attacks in SDNs proves challenging due to the complex nature of network traffic. To address this challenge, the researchers devised a hybrid deep learning strategy amalgamating three distinct algorithms. Their method exhibited remarkable accuracy rates, reaching 99.81% and 99.88% across two diverse datasets, validated through both reference-based analysis and practical experimentation. This research marks a significant stride in network security, particularly within SDNs, promising enhanced resilience against DoS/DDoS threats. Given the pivotal role of SDNs in contemporary network infrastructures, safeguarding them from attacks assumes paramount importance to preserve the availability and integrity of network resources. In essence, this study underscores the efficacy of a hybrid deep learning approach for detecting DoS/DDoS attacks in SDNs, charting a compelling trajectory for future research endeavors in this domain.

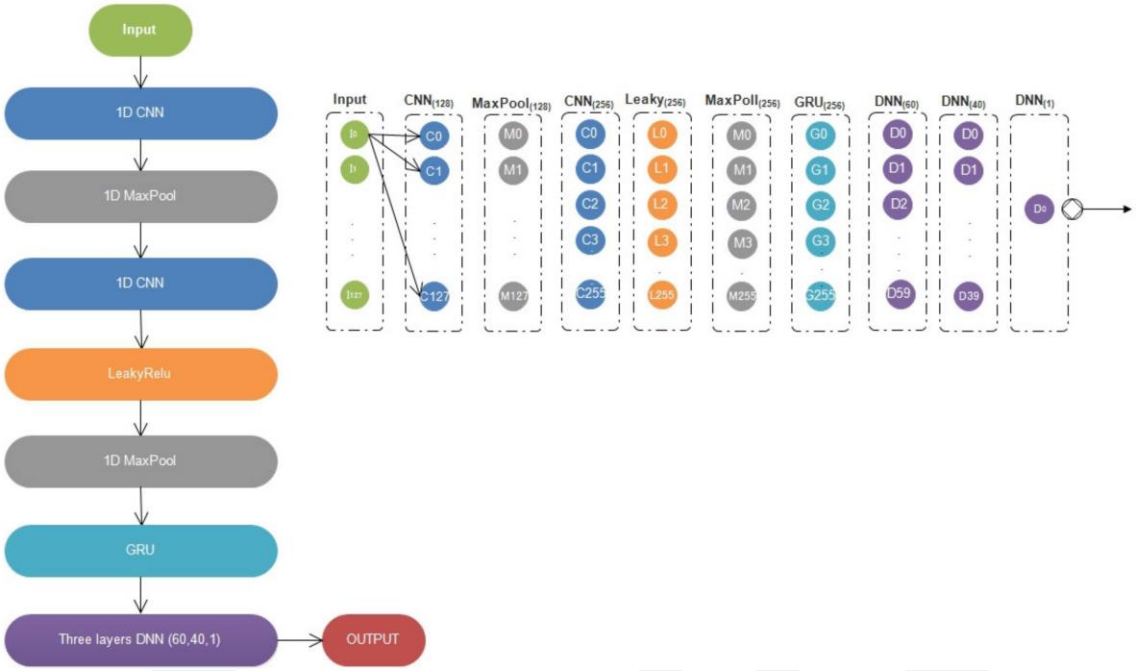

Figure 1. Hybrid model through a high-level and traditional neural network representation.

In [2], the authors present an inventive strategy for detecting and mitigating DoS/DDoS attacks within software-defined networks (SDNs) using conditional entropy. Diverging from conventional methods reliant on single entropy metrics, which often struggle to differentiate attack traffic from normal network activity, this approach augments accuracy by conducting a comprehensive analysis of attack features and entropy parameter variations. By establishing novel criteria for state determination and harnessing entropy value distributions in non-attack scenarios, the authors markedly enhance the precision of attack detection. Through extensive numerical analysis, they substantiate the efficacy of their methodology, showcasing its adeptness in distinguishing between normal and abnormal network behaviour, thereby elevating overall attack detection accuracy in SDNs. This research represents a significant advancement in SDN security, offering a refined approach to combating DoS/DDoS threats and fortifying network resilience. As SDNs continue to play a pivotal role in modern network infrastructures, safeguarding them from attacks becomes increasingly imperative to ensure uninterrupted network operations and resource availability. Consequently, this study underscores the potential of leveraging conditional entropy for bolstering SDN security and sets a compelling direction for further exploration in this field.

Proposed Method

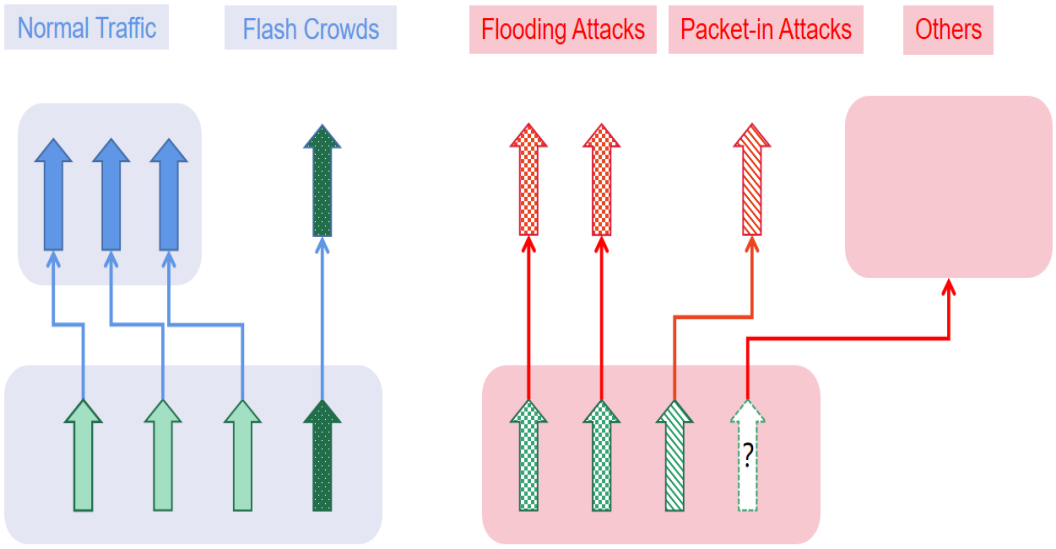

Figure 2: Proposed Detection Method

The author in [3] a novel approach for detecting and defending against DoS/DDoS attacks in software-defined networks (SDNs) by employing a Joint Self-Attention mechanism and SVM classification. With SDN architecture allowing centralized network management, the threat of DDoS attacks is amplified due to the separation of control and forwarding planes. To mitigate this risk, the paper introduces a high-precision attack detection method that combines self-attention mechanisms and support vector machines. A trigger mechanism is deployed at both control and data layers to initiate initial attack detection, followed by detailed screening of network data using the proposed mechanism and SVM. The control plane leverages OpenFlow protocol features to issue flow tables for precise classification results and initiate attack defense. Experimental results demonstrate the effectiveness of the trigger mechanism in reacting to attacks with minimal load and the accuracy of the detection mechanism, achieving a precision rate of 98.95% with a low false alarm rate of 1.04%. Additionally, the defence strategy enables timely recovery of network characteristics, showcasing the efficacy of the proposed approach in combating DoS/DDoS attacks in SDNs.

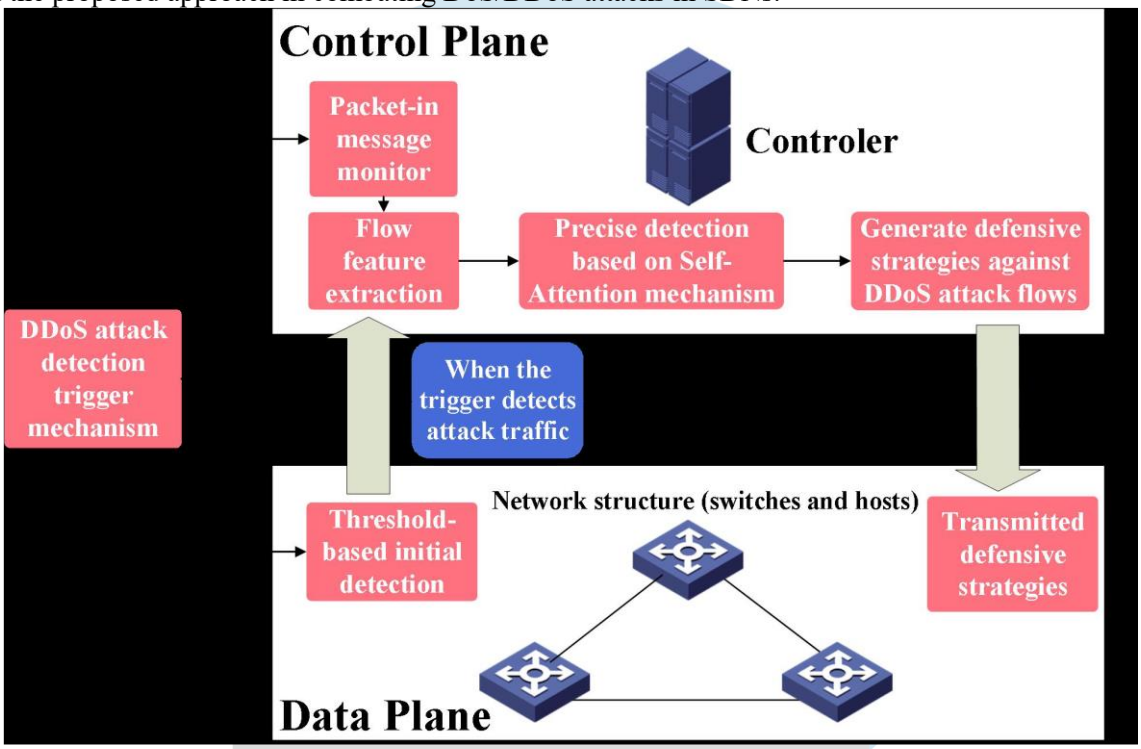

Figure 3. Selfattention-SVM detection defense mechanism model structure.

In [4], the author introduces machine learning methodologies tailored for detecting and mitigating DoS/DDoS attacks within software-defined networks (SDNs). SDNs, heralded for their transformative impact on network dynamics, facilitate programmability of network elements, centralized monitoring, and expedited, large-scale network operations. Nonetheless, this paradigm shift also exposes networks to a spectrum of security vulnerabilities, including the peril of complete network shutdown due to DDoS assaults. In response to this looming threat, the paper advocates for the adoption of machine learning techniques to swiftly identify and counter such attacks. By rigorously evaluating various methods for detecting DDoS attacks and optimizing classification accuracy within SDNs, the proposed system demonstrates remarkable efficacy, with the Decision Tree (DT) algorithm achieving an impressive 99.90% accuracy in DDoS attack detection. This research underscores the significance of integrating machine learning into SDN security frameworks, offering a potent arsenal for fortifying network resilience and thwarting malicious incursions. As SDNs continue to reshape modern network infrastructures, safeguarding them against evolving cyber threats assumes paramount importance, making this study a pivotal contribution to the field of SDN security.

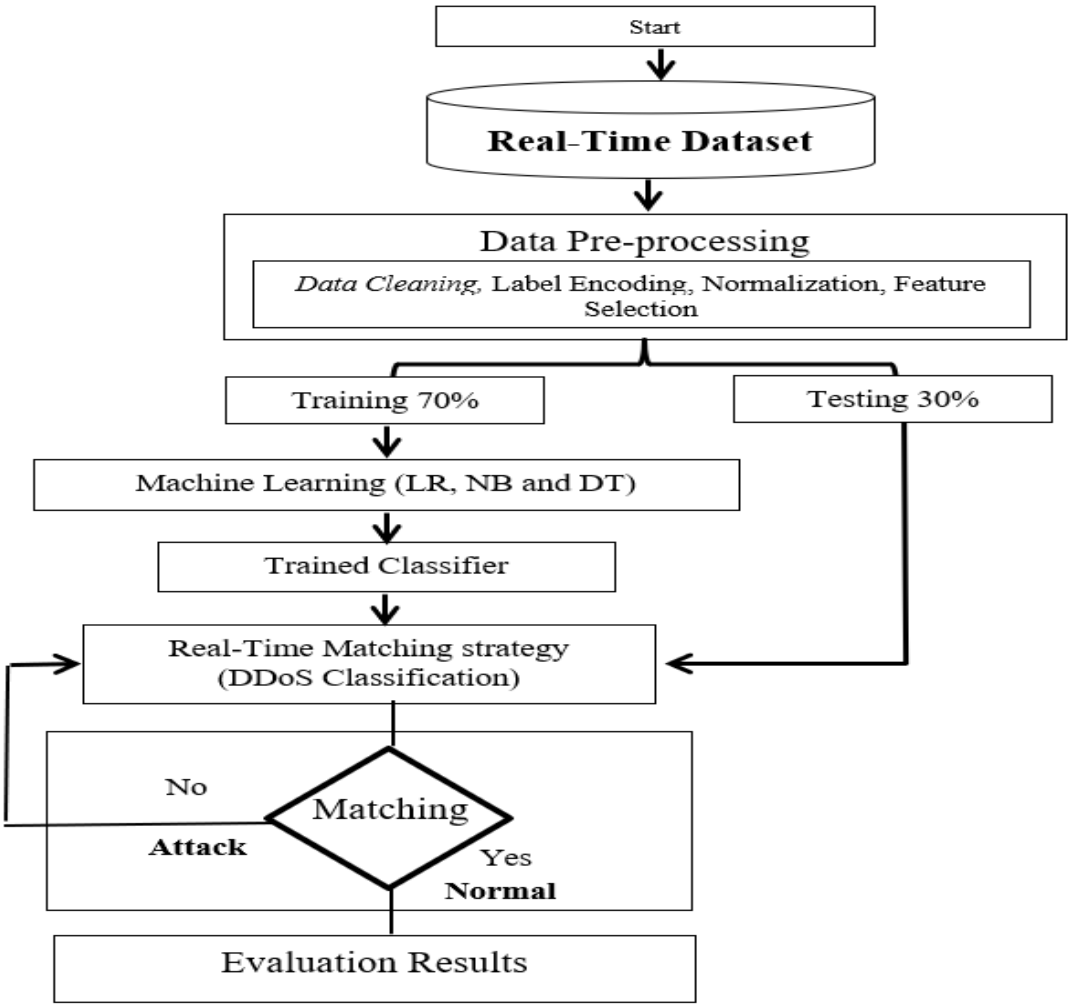

Figure 4. The proposed machine learning system model

In [5], the author introduces machine learning algorithms, notably Decision Trees and Support Vector Machines (SVM), tailored for the detection and mitigation of DoS/DDoS attacks within software-defined networks (SDNs). SDNs, distinguished by their capacity for virtual construction and dynamic adaptation of hardware components, diverge from traditional fixed connections, rendering them susceptible to DDoS threats. These attacks, orchestrated by multiple coordinated systems targeting a single server simultaneously, pose a formidable menace to the internet ecosystem. Within SDNs, where the control layer serves as a centralized nexus connecting application and infrastructure layers, software governs devices in the infrastructure layer, amplifying the vulnerability to DDoS assaults.

The proposed methodology harnesses Decision Trees and SVM to discern malicious traffic patterns. Test outcomes underscore the superior accuracy and detection rates offered by both algorithms, reaffirming their efficacy in combating DDoS attacks within SDNs. This research underscores the pivotal role of machine learning in bolstering SDN security, offering a potent arsenal for fortifying network resilience and mitigating the impact of malicious incursions. As SDNs continue to redefine the landscape of network architectures, safeguarding them against evolving cyber threats emerges as a pressing imperative, making this study a significant contribution to the field of SDN security.

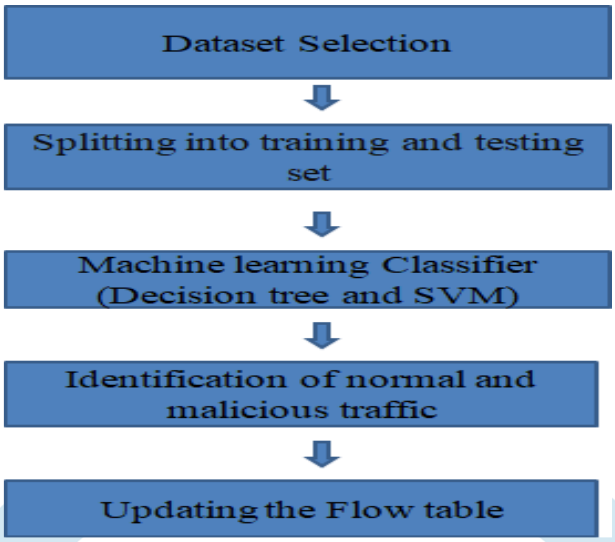

Figure 5. System Diagram

REFERENCES:

[1] Hybrid Deep Learning Approach for Automatic DoS/DDoS Attacks Detection in Software Defined Networks by Hani Elubeyd and Derya Yiltas-Kaplan.

[2] A DDoS Attack Detection Method Using Conditional Entropy Based on SDN Traffic by Qiwen Tian and Sumiko Miyata.

[3] Joint Selfattention-SVM DDoS Attack Detection and Defense Mechanism Based on Self Attention Mechanism and SVM Classification for SDN Networks, by Wanying MAN, Guiqin YANG, Shurui.

[4] DDoS attack detection in software defined networking controller using machine learning techniques by Abbas Jasem Altamemi, Aladdin Abdulhassan, Nawfal Turki Obeis.

[5] Detection of Distributed Denial of Service Attacks in SDN using Machine learning techniques by K.Muthamil Sudar, M. Beulah, P.Deepalakshmi, P.Nagaraj, P. Chinnasamy.