Review

Not peer-reviewed version

A Brief Research in Machine Learning-Driven Classification of DDoS Attacks in SDN Environment

Shirmohammad Tavangari *

Posted Date: 22 August 2023

doi: 10.20944/preprints202308.1589.v1

Keywords: SDN; Machine Learning; Algorithms; Network

Review

A Brief Research in Machine Learning-Driven Classification of DDoS Attacks in SDN Environment

Shirmohammad Tavangari

University of British Columbia, ElectricalandComputerEngineering Faculty,
2332 Main Mall, Vancouver, BC Canada V6T 1Z4, s.tavangari@alumni.ubc.ca

Abstract: In the landscape of network management, software-defined networking (SDN) technology emerges as a dynamic approach, facilitating efficient network configuration for improved performance and monitoring, akin to the agility of cloud computing rather than traditional methods. However, its centralized structure exposes SDN to various attack vectors. Distributed Denial of Service (DDoS) attacks, particularly, pose a significant threat to SDN. This study employs machine learning algorithms and Network Traffic Classification Analysis (NCA) to classify SDN traffic as potential attacks. Notably, Decision Trees (DT) out shine other algorithms with a flawless 100% classification success, spotlighting their supremacy. Through this research, a robust path toward fortified SDN security takes form, where technological prowess and strategic intelligence unite for enhanced defense.

Keywords: SDN; machine learning; algorithms; network

Introduction:

Software-Defined Networking (SDN) is an approach to networking that uses software-based controllers or application programming interfaces (APIs) to communicate with underlying hardware infrastructure and direct traffic on a network. .[1] This model differs from that of traditional networks, which use dedicated hardware devices (i.e., routers and switches) to control network traffic. .[2] SDN can create and control a virtual network – or control a traditional hardware – via software. While network virtualization allows organizations to segment different virtual networks within a single physical network, or to connect devices on different physical networks to create a single virtual network, software-defined networking enables a new way of controlling the routing of data packets through a centralized server. .[3]

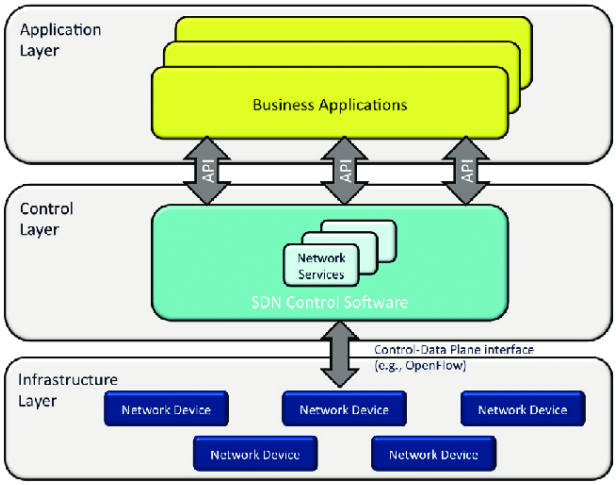

Figure 1. SDN architecture.

The contrast between SDN and traditional networking primarily centers on their infrastructure. SDN opts for a software-based architecture, diverging from traditional networking's hardware-centric approach. Empowered by its software-driven control plane, SDN offers notable flexibility. [4,5] Administrators can centrally manage the network, configure settings, allocate resources, and scale capacity—eliminating the need for extra hardware. At its core, SDN decouples software from hardware, relocating the traffic-routing control plane to software while retaining the data-forwarding data plane in hardware. [6,7] This enables comprehensive network programming and management, surpassing device-

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 22 August 2023 doi:10.20944/preprints202308.1589.v1

specific limitations. A quintessential SDN architecture comprises Applications, Controllers, and Networking devices. Though distributed, these elements contribute to a cohesive framework. SDN's agility suits emerging trends like edge computing and the Internet of Things, which demand rapid data transfer across remote nodes. [8]

However, SDN's potency exposes it to vulnerabilities. Notably, Distributed Denial of Service (DDoS) attacks stand out. DDoS aims to overwhelm targeted servers, services, or networks with massive Internet traffic, disrupting operations. In SDN, these attacks manipulate new flows to flood the control plane, OpenFlow switches, and SDN controller's bandwidth, leading to network failure. [9] Countering these threats while leveraging SDN's transformative capabilities poses a critical challenge. [10]

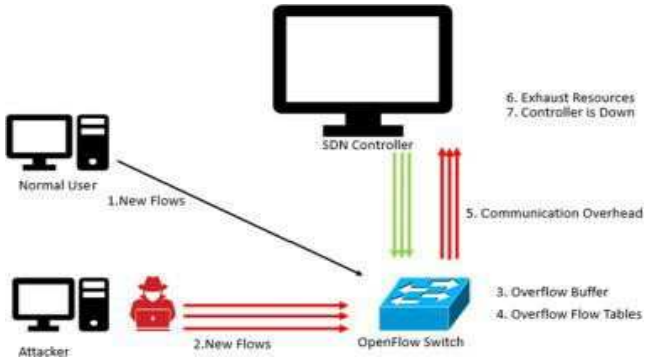

Figure 2. DDoS Attacks in SDN.

In this context, my focus centers on Software-Defined Networking (SDN), striving to establish a streamlined hybrid model bolstered by Network Traffic Classification Analysis (NCA) and the prowess of machine learning techniques. [11] This endeavor aspires to forge novel and efficient network architecture for the next generation. [12,13]The pivotal objective revolves around detecting Distributed Denial of Service (DDoS) attacks through the lens of machine learning. This involves leveraging various flow characteristics, including packet size, arrival and response times, packet rates, and packets per flow, among others. The aim is to discern whether network traffic adheres to normal behavior or manifests as potential threats. [14,15] Interestingly, DDoS attacks frequently exhibit a uniform average packet size. Furthermore, their attack traffic showcases a remarkable surge in bit rate, leading to swift arrival times at the target machine. [16] Attackers meticulously exploit these attributes to exhaust the resources of the target machine, thereby incapacitating its functionality and incapacitating its ability to serve its intended purpose. [17]

Methods:

1- Dataset:

DDoS attack SDN Dataset: 22 Features**.**

2- Machine Learning (ML):

Decision Tree, Artificial Neural Network, KNN

Formula:

FS->2*Tp/2*Tp+Fp+Fn

Ac->Tp+Tn/Tp+Tn+Fp+Fn

Sp-> Tn/Tn+Fp

 doi:10.20944/preprints202308.1589.v1

Expriments:

Within this scope, I endeavor to elucidate the array of machine learning techniques employed in this context, encompassing Artificial Neural Networks, K-Nearest Neighbors (K-NN), and Decision Trees. The dataset under scrutiny comprises a comprehensive feature set spanning 22 distinct attributes. Following rigorous training utilizing the Network Traffic Classification Analysis (NCA) algorithm, a judicious feature selection process ensues. Features boasting an index value exceeding 1.11 are systematically chosen for further analysis. Subsequently, these selected features are subjected to classification by means of machine learning methodologies, harnessing identical hyperparameters as employed in the inaugural experimental phase. The culmination of these experimental endeavors yields highly promising outcomes across the spectrum of classification algorithms. Notably, the Decision Tree (DT) algorithm achieves a remarkable accuracy rate of 100%, underscoring its prowess. Parallelly, the K-NN, Artificial Neural Network (ANN), and Support Vector Machine (SVM) algorithms exhibit impressive accuracy levels, registering at 98.12%, 98.67%, and 97.25% respectively. To encapsulate the results, Receiver Operating Characteristic (ROC) curves are portrayed for all machine learning methods, offering a visual depiction of their performance (see Figure 6). The amalgamation of these findings engenders an insightful perspective on the efficacy of various machine learning paradigms in this domain.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 22 August 2023 doi:10.20944/preprints202308.1589.v1

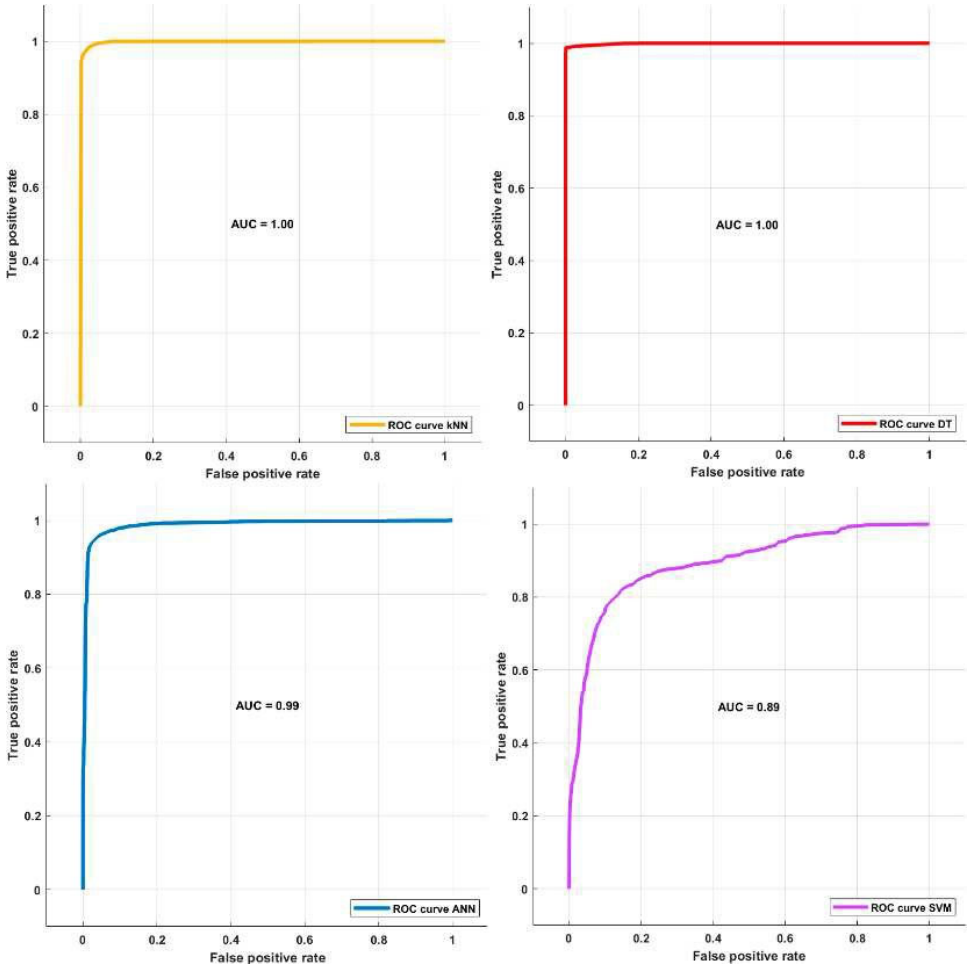

Figure 3. ROC curves of all ML models.

Tip 1:

In our approach, we meticulously curated a feature subset for integration into machine learning algorithms. Specifically, we employed the Network Traffic Classification Analysis (NCA) to meticulously cherry-pick 11 key attributes out of a total of 22. These chosen features encompass a spectrum including "dt," "dur," "Flows," and others, forming the foundation for our subsequent machine learning endeavors.

Tip 2:

One remarkable facet that underscores our feature selection process is the incorporation of weights. To elucidate, each feature carries a distinct weight, contributing to the overall significance of the feature set. For instance, "dt" bears a weight of 2.11, "dur" holds a weight of 1.05, and "Flows" commands a substantial weight of 7.45, thus intricately weaving a tailored architecture of attributes.

Tip 3:

Our journey extends to unveiling the outcomes engendered by machine learning models, sans the feature selection methodology. In this realm, our models emerge as follows: Decision Tree (DT) achieves an astonishing specificity rate of 99.23%; K-Nearest Neighbors (KNN) presents an accuracy score of 94.28%; while the Artificial Neural Network (ANN) boasts an accuracy of 96.95%. These results underscore the proficiency of our models in a comparative context, accentuating the significance of both feature selection and algorithmic performance.

Conclusions:

Leveraging the NCA algorithm, I unveil the utmost pertinent attributes via a meticulous feature selection process, ultimately fostering performance-enhancing classification. Subsequent to rigorous preprocessing and refined feature curation, the dataset is subjected to classification via k-Nearest Neighbors (kNN), Decision Tree (DT), and Artificial Neural Network (ANN). Impressively, the experimental outcomes underscore DT's supremacy in accuracy (Ac), distinctly outperforming alternative algorithms, and achieving an impeccable 100% classification attainment. This resounding accomplishment further underscores DT's prowess as a preeminent classifier within this context, exemplifying its aptitude in achieving precision and reliability in classification tasks.

Refrences:

1- D.B.Rawat, S.R.Reddy. Software defined Networking Architecture , Securityand Energy Efficiency : A Survey. IEEE(Sep2017).DOI: https://doi.org/10.1109/COMST.2016.2618874

2- Karan.B.V, Narayan.D.G, P.S.Hiremath. Detection of DDoS Attacks in Software Define Networking. IEEE(July 2018).DOI: https://doi.org/10.1109/CSITSS.2018.8768551

3- K.Sagar Sahoo, A.Iqbal, P.Maiti, B.Sahoo. A Machine learning approach for predicting DDoS traffic in Software DefineNetwork. IEEE(Sep2018). DOI:https://doi.org/10.1109/ICIT.2018.00049

4- Y.Yang,S.Li,P.Zhang.Data-Drivenaccidentconsequenceassessmentonurbangaz pipeline network based on machine learning. Elsevier (March 2022). https://doi.org/10.1016/j.ress.2021.108216

5- A.R.Mohammad, S.A.Mohammad, D.Cote, S.Shirmohammadi. Machine learning- based Network status detection and fault localization. IEEE (July 2021). https://doi.org/10.1109/TIM.2021.3094223

6- H.Aldabbas. Efficient Bandwidth Allocation in SDN-Based Pear to Peer Data Streaming Using Machine learning Algorithm.Springer. Nov 2022. https://doi.org/10.1007/s11227-022-04929-y

7- S.Tavangari, S.T.Kulfati. Review of Advancing Anomaly Detection in SDN Through Deep Learning Algorithms. *Preprints* 2023, 2023081089.https://doi.org/10.20944/preprints202308.1089.v1

8- B.Sarma, R.Kumar, T.Tuithung. Machine Learning Enabled Network and Task Management in SDN Based Fog Archicture. Springer. May 2023. https://doi.org/10.1016/j.compeleceng.2023.108705

9- A.Mozo, A.Karamchandi,L.D.L.Cal, S. Gomez-Canaval,A.Pastor, L.Gifre. A Machine Learning –Based Cyberattack Detector For a Cloud-Based SDN Controller. MDPI. April 2023. https://doi.org/10.3390/app13084914

10- L.M.halman, M.J.F. Alenazi, MCAD: A Machine Learning Based Cyberattacks Detector in Software-Defined Networking(SDN) for healthcare Systems. IEEE. April 2023. https://doi.org/10.1109/ACCESS.2023.3266826

11- A.Sharma, H.S.Chauhan, H.Kaur, H.Babbar. Analysis of DDoS Attacks in Software Defined Networking Using Machine Learning. IEEE. April 2023. https://doi.org/10.1109/IITCEE57236.2023.10090959

12- R.R.Sekar, AM.Jenny, D.Sreshta, M.Vikas. Prediction of Distributed Denial of Service Attacks in SDN Using Machine Learning Techniques. IEEE. August 2023. https://doi.org/10.1109/CONIT59222.2023.10205887

13- A.Sahbi, F.Jaidi, A.Bouhoula. Machine Learning algorithms For Enhancing intrusion Detection Within SDN/NFV. IEEE. July 2023. https://doi.org/10.1109/IWCMC58020.2023.10183024

14- K.Puranik , K.Patil, G.Ghaligi, R.Jannu. A Two-Level DDoS Attack Detection Using Entropy and Machine Learning in SDN . IEEE. August 2023. https://doi.org/10.1109/CONIT59222.2023.10205776

15- K.M.Sudar, P.Deepalakshmi, A.Singh, P.N.Srinivasu. TFAD:TCP Flooding Attack Detection in Software-Defined Networking Using Proxy-Based and Machine Learning- Based Mechanisms.Springer. 2023. https://doi.org/10.1007/s10586-022-03666-4

16- **R. Anusuya, M. Ramkumar Prabhu, Ch. Prathima, J. R. Arun Kumar**. Detection of TCP, UDP and ICMP DDOS attacks in SDN Using Machine Learning approach. Journal Survey in fisheries Sciences.2023. https://doi.org/10.17762/sfs.v10i4S.1117

17- Shinde, A.R., Bendale, S.P. (2023). Evolution of Quantum Machine Learning and an Attempt of Its Application for SDN Intrusion Detection. In: Pandey, R., Srivastava, N., Singh, N.K., Tyagi, K. (eds) Quantum Computing: A Shift from Bits to Qubits. Studies in Computational Intelligence, vol 1085. Springer, Singapore. https://doi.org/10.1007/978-981-19-9530-9_22