

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/376621161>

DDoS attack detection and mitigation using deep neural network in SDN environment

Article in *Computers & Security* · December 2023

DOI: 10.1016/j.cose.2023.103661

CITATIONS

0

READS

85

5 authors, including:



[Vanlalruata Hnamte](#)

Mizoram University

23 PUBLICATIONS 87 CITATIONS

[SEE PROFILE](#)



[Ashfaq Ahmad Najar](#)

Central University of Kerala

6 PUBLICATIONS 21 CITATIONS

[SEE PROFILE](#)



[Nhung Nguyen](#)

Viet Tri University of Industry

10 PUBLICATIONS 26 CITATIONS

[SEE PROFILE](#)



[Jamal Hussain](#)

Mizoram University

52 PUBLICATIONS 1,551 CITATIONS

[SEE PROFILE](#)

Journal Pre-proof

DDoS attack detection and mitigation using deep neural network in SDN environment

Vanlalruata Hnamte, Ashfaq Ahmad Najar, Hong Nhung-Nguyen, Jamal Hussain and Manohar Naik S

PII: S0167-4048(23)00571-0
DOI: <https://doi.org/10.1016/j.cose.2023.103661>
Reference: COSE 103661

To appear in: *Computers & Security*

Received date: 22 September 2023
Revised date: 28 November 2023
Accepted date: 13 December 2023



Please cite this article as: V. Hnamte, A.A. Najar, H. Nhung-Nguyen et al., DDoS attack detection and mitigation using deep neural network in SDN environment, *Computers & Security*, 103661, doi: <https://doi.org/10.1016/j.cose.2023.103661>.

This is a PDF file of an article that has undergone enhancements after acceptance, such as the addition of a cover page and metadata, and formatting for readability, but it is not yet the definitive version of record. This version will undergo additional copyediting, typesetting and review before it is published in its final form, but we are providing this version to give early visibility of the article. Please note that, during the production process, errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

© 2023 Published by Elsevier.

DDoS attack detection and mitigation using deep neural network in SDN environment

Vanlalruata Hnamte^{a,*}, Ashfaq Ahmad Najar^b, Hong Nhung-Nguyen^c, Jamal Hussain^a, Manohar Naik S^b

^aDepartment of Mathematics and Computer Science, Mizoram University, Tanhril, Aizawl, 796004, Mizoram, India

^bDepartment of Computer Science, Central University of Kerala, Tejaswini Hills, Periyar, 671320, Kerala, India

^cDepartment of Information Technology, Viet Tri University of Industry, Tien Son Street, Viet Tri City, 29000, Phu Tho Province, Viet Nam

Abstract

In the contemporary digital landscape, the escalating threat landscape of cyber attacks, particularly distributed denial-of-service (DDoS) attacks, has become a paramount concern for network security. This research introduces an innovative approach to DDoS detection leveraging a deep neural network (DNN) architecture rooted in deep learning (DL) principles. The proposed model exhibits a scalable and adaptable framework, enabling meticulous analysis of network traffic data to discern intricate patterns indicative of DDoS attacks. To validate the efficacy of our methodology, rigorous evaluations were conducted using authentic real-world traffic data. The results unequivocally establish the superiority of our DNN-based approach over traditional DDoS detection techniques. This research holds significant promise for bolstering network security, particularly within the dynamic landscape of software-defined network (SDN) environments. The study's findings contribute to the continual refinement and eventual deployment of advanced measures in fortifying digital infrastructure against the evolving threat landscape. Performance metrics, including detection accuracy and loss rates, further emphasize the effectiveness of our approach across different datasets. With detection accuracy rates of 99.98%, 100%, and 99.99% for the InSDN, CICIDS2018, and Kaggle DDoS datasets, respectively, coupled with low loss rates, our DNN-based model demonstrates robust capabilities in mitigating contemporary DDoS threats. This study not only presents a novel DDoS detection approach within SDN infrastructures but also offers insights into practical implications and challenges associated with deploying DNNs in real-world SDN environments. Network security professionals can benefit from the nuanced perspectives provided, contributing to the ongoing discourse on fortifying digital networks against evolving cyber threats.

Keywords: Deep Learning, Deep Neural Network, SDN, DDoS Detection, Distributed Denial of Service Attack, Anomaly Detection

1. Introduction

In an era characterized by an ever-increasing reliance on technology, the significance of cybersecurity has soared to unprecedented heights. With the pervasive adoption of digital communication, the proliferation of the Internet of Things (IoT), the ubiquity of cloud computing, and the omnipresence of mobile devices, the attack surface for cyber threats has expanded exponentially. Cybersecurity, encompassing a multifaceted spectrum of practices, is dedicated to the safeguarding of computer systems and networks against unauthorized access, theft, damage, or disruption of services. The imperative for cybersecurity has escalated in tandem with the evolution of cyber threats, which have grown progressively sophisticated. The ramifications of cyberattacks are profound, encompassing substantial financial losses, severe damage to reputation, and the perilous compromise of sensitive data. These malevolent incursions are

*Corresponding author.

Email addresses: vanlalruata.hnamte@gmail.com (Vanlalruata Hnamte), ishfaqnajar@gmail.com (Ashfaq Ahmad Najar), nhungnguyen.uet@gmail.com (Hong Nhung-Nguyen), jamal.mzu@gmail.com (Jamal Hussain), manoharamen@cukerala.ac.in (Manohar Naik S)