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

Vanlalruata Hnamte
Mizoram University

Ashfaq Ahmad Najar
Central University of Kerala

Nhung Nguyen
Viet Tri University of Industry

Jamal Hussain
Mizoram University

ISSN 0167-4048
ELSEVIER
Computers & Security
The International Source of Innovation for the Information Security and IT Audit Professional
ifip

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

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]

[a]Department of Mathematics and Computer Science, Mizoram University, Tanhril, Aizawl, 796004, Mizoram, India
[b]Department of Computer Science, Central University of Kerala, Tejaswini Hills, Periye, 671320, Kerala, India
[c]Department 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)