International Journal of Distributed Artificial Intelligence
Volume 14 • Issue 1

An Intelligent Model for DDoS Attack Detection and Flash Event Management

Oreoluwa Carolyn Tinubu, Federal University of Agriculture, Abeokuta. Nigeria*
Adesina Simon Sodiya, Federal University of Agriculture, Abeokuta, Nigeria
Olusegun Ayodeji Ojesanmi, Federal University of Agriculture, Abeokuta, Nigeria
Emmanuel Oyeyemi Adeleke, Federal University of Agriculture, Abeokuta, Nigeria
Ahmad Alfawwaz Timehin, Federal University of Agriculture, Abeokuta, Nigeria

ABSTRACT

Distributed Denial of Service (DDoS) attacks are the foremost security concerns on the internet. DDoS attacks and a similar occurrence called Flash Event (FE) signify anomalies in the normal network traffic, requiring intelligent interventions. This study presents the design and implementation of an intelligent model for the detection of application-layer DDoS attacks and the prevention of service degradations during FE. A Multi-Layer Perceptron (MLP) classifier was used for detecting DDoS attacks on application servers. The FE management system consists of asynchronous processing of requests on a First-In, First-Out (FIFO) basis. A demo application was set up wherein HTTP flood attack was launched and a flash event was simulated. The experimental results clearly show that the MLP classifier in comparison with other machine learning classifiers performs best in terms of speed and accuracy. Also, the evaluation of the FE management system shows a great reduction in service degradation. This reflects that the designed model is capable of averting service unavailability on the web.

KEYWORDS

Classifier, DDoS Attack, Detection, Flash Event, Machine Learning, Multi-Layer Perception (MLP)

INTRODUCTION

The increase in adoption and versatility of the Internet has influenced an exponential rise in cyber attacks. These attacks on the cyber space have severe impacts on the real world (Ghanbari & Kinsner, 2022). A core threat to cyber security is the Distributed Denial of Service (DDoS) attacks (Yang & Hespanha, 2021). DDoS attacks are coordinated attacks on the availability of services on the Internet (Singh & Gupta, 2016). DDoS attacks are malicious attempts by cybercriminals to make web services, network resources or host machines inaccessible to intended users through a flood of useless packets. Cloud-hosted servers are highly susceptible to DDoS attacks (Alqahtani & Gamble,

DOI: 10.4018/IJDAI.301212 *Corresponding Author

2015; Chaudhary *et al.,* 2018). The availability of computing resources is a fundamental characteristic of cloud computing amongst other security necessities (Agrawal & Tapaswi, 2017).

DDoS attacks aim to disrupt networks, applications or web-based services (Dhingra & Sachdeva, 2018). DDoS attacks by overwhelming target servers with floods of bogus traffic consume resources that could service legitimate users. Unlike a traditional Denial of Service (DoS) attack which involves a single machine, modern DDoS attacks involves the use of thousands or millions of zombies, each flooding the server in order to deny access to services by legitimate users. DDoS attacks can easily be launched on web applications, as operating systems and Internet protocols are often prone to vulnerabilities.

DDoS attacks are launched through remotely controlled, well-coordinated and widely dispersed zombies' botnet devices in a network (Khalaf *et al.,* 2019). Typically, the process of executing a DDoS attack involves a botmaster identifying vulnerable hosts on a network, compromising the hosts with malware, controlling the hosts (the attacker executes code on the hosts without the knowledge of the hosts), and launching the attack (Behal *et al.,* 2019). With evolving technologies such as Internet-of-Things (IoT) and cloud computing, malicious agents can launch massive volumes of DDoS attacks. These launched attacks exhaust the processing and connectivity resources of the target systems resulting in partial or total unavailability (Yusof *et al.,* 2019).

Flooding DDoS attacks can be launched on the Network/Transport and Application layers through protocols as UDP, ICMP, TCP and HTTP (Sharafaldin *et al.,* 2019). Network/Transport (layer 3/4) DDoS attacks are intended to deplete the victim's network resources as bandwidth and the processing capacity of routers, thereby disrupting the legitimate user's connectivity. On the other hand, Application (layer 7) DDoS attacks are intended to exhaust the server's resources like CPU, sockets, memory, input/output bandwidth, causing disruption in the processing of genuine user's requests. Nowadays, Application-layer DDoS attacks occur more frequently (Behal *et al.,* 2021).

Despite several research efforts geared towards the detection and mitigation of DDoS attacks, these attacks are increasing in volume and severity (Sangodoyin *et al.,* 2018). The frequency of the attacks is tremendously increasing and has become one of the biggest menaces to Internet-connected systems (Shidaganti *et al.,* 2020). DDoS attacks are continually evolving causing service interruptions that results in huge financial losses (Rios *et al.,* 2021). Popular websites such as Netflix, Twitter, GitHub, Airbnb, PayPal, Spotify, The New York Times, Amazon, eBay, BBC, Reddit, CNN and Yahoo have fallen victims to flooding-based DDoS attacks, having severe impacts on the organizations and the users. An effective defense mechanism against DDoS attacks is yet to be developed by security agents (Gaurav *et al.,* 2022; Khalaf *et al.,* 2019).

Also, the delivery of online services can be degraded by an influx of traffic from genuine users (Bhatia, 2016). In Flash Events (FE), numerous legitimate users simultaneously access a website, leading to a reduced performance of the web server and denial of services (Bhandari *et al.,* 2016; da Silva *et al.,* 2022). An FE is an overload condition where a server experiences a sudden surge in traffic resulting from a large number of requests from legitimate clients. This exponential increase in legitimate traffic is often caused by newsworthy events such as new products launch by big brands as Microsoft, Apple or Samsung, football world cup or Olympics and unforeseen events like natural disasters or terrorist attacks and breaking news.

Flash crowds attempt to access a server concurrently, thereby causing an unexpected flooding (Saravanan *et al.,* 2016). An FE may overwhelm a server and generate a DDoS type of occurrence resulting in either complete crash or delay of responses (Chawla *et al.,* 2016). Behal & Kumar (2017) likened a Flash Event to a high-rate DDoS attack. Thus, both DDoS attacks and Flash Events can be categorized as degrading and disruptive occurrences.

In this study, an intelligent cloud-based model for the detection of application-layer DDoS attacks and the management of Flash Events (FE) is developed. The proposed architecture uses a Software-Defined Networking (SDN) in a cloud environment as modern cloud environments are powered by SDNs for the networking components. A machine learning algorithm, the Multi-Layer Perceptron