International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-11 Issue-6, May 2022

Detection and Investigation of DDoS Attacks in Network Traffic using Machine Learning Algorithms

Biswajit Mondal, Chandan Koner, Monalisa Chakraborty, Subir Gupta

Abstract*: The Internet of Things (IoT) represents the start of a new age in information technology (IoT). Objects (things) such as smart TVs, telephones, and smartwatches may now connect to the Internet. New services and software improve many consumers' lives. Online lessons based on COVID-9 are also included in child education devices. Multiple device integration is becoming more widespread as the Internet of Things (IoT) grows in popularity. While IoT devices offer tremendous advantages, they may also create network disruptions. This article summarises current DDoS intrusion detection research utilizing machine learning methods. This study examines the detection performance of DDoS attacks utilizing WEKA tools using the most recent NSL KDD datasets. Logistic Regression (LR), Naive Bayes (NB), SVM, K-NN, Decision Tree (DT), and Random Forest (RF) are examples of Machine Learning algorithms. Using K-Nearest Neighbors in the presented assessment (K-NN), accuracy was attained. Finally, future research questions are addressed.

***Keywords*: DDoS Attacks; Internet Of Things; Machine Learning**

I. INTRODUCTION

As computing networks, particularly the internet, grow in size, network attacks are becoming increasingly widespread. The Wannacryransomware infection has caused the internet to be inaccessible in 156 nations. Kaspersky Lab identified botnet-assisted attacks on assets in 69 different countries during the fourth quarter. Furthermore, the botnet-based DDoS attack that lasted the longest happened in the previous quarter (15.5 days, 371 hours)[1][2]. Cybercriminals continually develop tiered distributed denial of service (DDoS) techniques that attack the OSI network and application layers. These attacks employed faked IP addresses to fool source detection and launch a large-scale wave of attacks[3][4]. These attacks are massive, using a considerable percentage of the network's spectrum during peak hours and interfering with the transmission of legitimate packets. Ironically, governments, banks, militaries, and defense forces have all been attacked. DDoS attacks against well-known websites such as Facebook, Twitter, and Wikileaks have resulted in financial losses, service degradation, and lack of access. Services might be swamped or crashed in one of two ways. In floods, the target system becomes excessively sluggish, eventually failing to respond at all. DDOS is a more severe and difficult-to-detect distributed denial-of-service assault. A denial of service attack is referred to as a "Distributed Denial of Service." This article describes a machine-learning technique for detecting and analyzing attacks such as Smurf, UDP flooding, and HTTP flooding[5]. Because there are no particular data sets containing contemporary DDoS assaults on several levels, such as SI-DDoS and HTTP flood, this study was done on a new dataset containing new types of DDoS attacks produced expressly for this purpose. According to the findings of comparing the various classification algorithms, MPL has the most remarkable accuracy rate[6].

Manuscript received on 02 April 2022.
Revised Manuscript received on 05 April 2022.
Manuscript published on 30 May 2022.
* Correspondence Author
Mr. Biswajit Mondal, Department of Computer Science and Engineering, Dr. B. C. Roy Engineering College, Durgapur, West Bengal 713206, India. Email: biswa.mondal@gmail.com
Dr. Chandan Koner, Department of Computer Science and Engineering, Dr. B. C. Roy Engineering College, Durgapur, West Bengal 713206, India. Email: chandan.koner@bcrec.ac.in
Miss. Monalisa Chakraborty, Department of Computer Science and Engineering, Dr. B. C. Roy Engineering College, Durgapur, West Bengal 713206, India.. Email: chakraborty.monalisa6@gmail.com
Dr. Subir Gupta*, Department of Computer Science and Engineering, Dr. B. C. Roy Engineering College, Durgapur, West Bengal 713206, India. Email: subir2276@gmail.com

II. LITERATURE REVIEW

DDoS attacks may be detected and blocked using an application-layer method. SVM was used by them (Support Vector Machine). As a result, it's not clear how accurate the approach is in detecting DDoS attacks at the application layer[7][8][9]. The Ploy Kernel and Sequential Minima Optimization (SMO) could not foresee a distributed denial of service attack. Two sets of data were used in this study. The proposed method was shown to be extremely accurate with a low percentage of false alarms. Another group of academics has developed a method for detecting Denial-of-Service attacks using an artificial neural network (ANN). The technique was tested using the CICIDS2017 dataset[10]. An extra seven layers are proposed by Yadigar Imamverdiyev to cover the machine's input and output levels in a restricted Boltzmann device of the Gaussian-Beroni type. In terms of danger detection, only a few researchers have examined the efficacy of several machine learning methods. They found a number of characteristics that may be tweaked to further improve the algorithms' precision. Several scientists have also proposed a machine learning-based approach for identifying distributed denial of service (DDoS) attacks[11][12]. The suggested system's accuracy and warning categories were evaluated using a variety of machine learning methods.