*THINK INDIA JOURNAL*

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

# A Review on Detection of DDOS Attack Using Machine Learning and Deep Learning Techniques

**[1, *]Sagar Dhanraj Pande, [2]Aditya Khamparia**

[1, 2]School of Computer Science Engineering, Lovely Professional University, Phagwara,

Punjab, INDIA.

Email: [1]sagarpande30@gmail.com, [2]aditya.khamparia88@gmail.com

**Abstract:**

One of the most serious threat to network security is Denial of service (DOS) attacks. When this attack is performed in distributed manner it can create more disaster. Lot of research has been carried for the detection of this attack. In this various techniques has been studied and discussed. Primary focus was given to machine learning and deep learning techniques.

**Keywords**: DDOS, Deep Learning, Machine Learning, KDD,Detection.

## INTRODUCTION

There are numerous assaults on Network Infrastructure today. These consist of assaults for the accessibility (availability) of the system, and on the privacy and integrity of the system packets. Distributed Denial of Service (DDoS) attacks are assaults focusing on the accessibility of systems, which utilizes the benefits from getting access of different assault source machines.

### Distributed Denial of Service (DDOS) Attack

Accessing seveal systems by using command and control (C & C) and trying denial of the service from the user side can be called as DDOS attack. The main motive of the intruder is to bring down the system or the server by sending repeated and continuous requests of the pages.

### DDOS Implementation

Basically DDOS tries to again access to the systems and server by implanting Command and Control(C & C) technique. Systems which are affected by C & C are called as Botnet or Zombie. The person who control the botnet systems are known as Botmaster. Figure 1 depicts the operational working of DDOS attack.

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

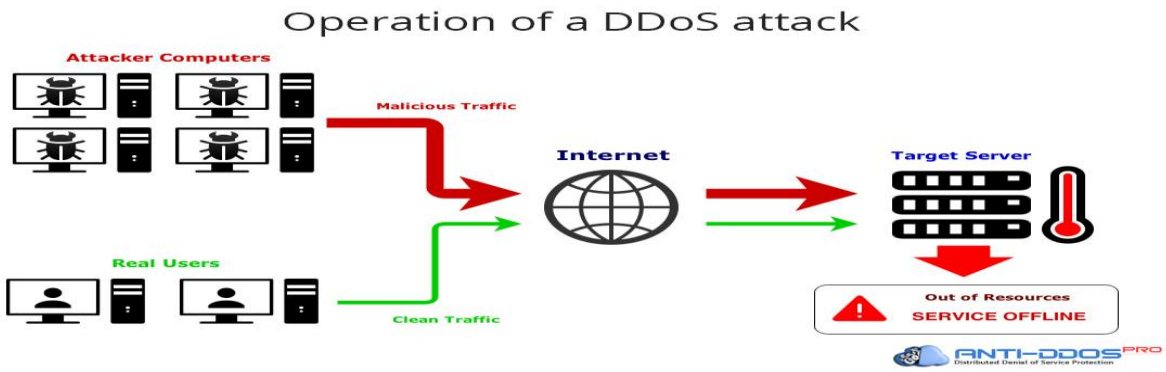



Figure 1: Operational Working of DDOS attack [1]

In the Figure 2, various types of DDOS attacks along with their occurrence are shown.

A definitive point of the assailant is to fill up assets anddestroy them. The real focal point of a HTTP flood DDOS assault is toward creating assault traffic that intently reproduces authenticity of a human client. Subsequently it ends up more diligently for an unfortunate casualty to separate among authentic and assault traffic. As a result of this sort of assaults, the server ends up inaccessible to authentic clients. Figure 3 & 4 Signifies recent attack & its sizes.

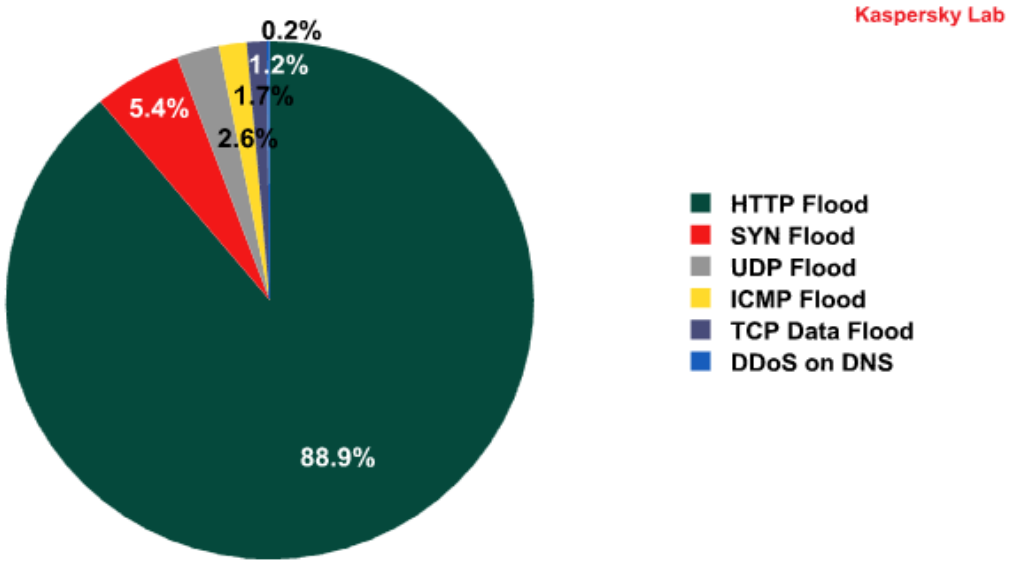
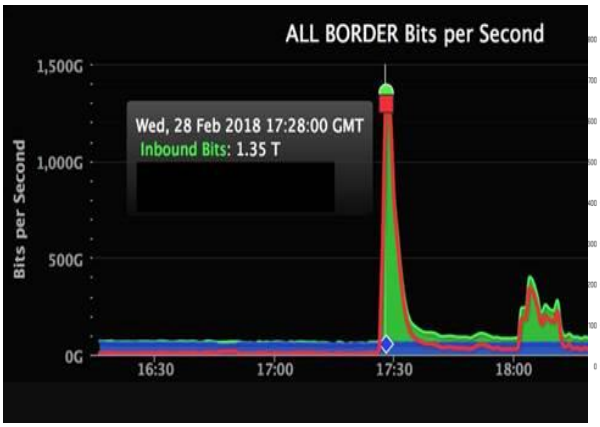



Figure 2: Type of DDOS attacks [2]

ISSN: 0971-1260
Vol-22-Issue-16-August-2019



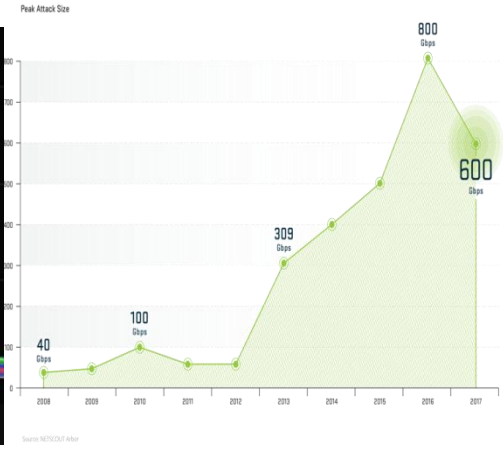




Figure 3: DDOS attack on GITHUB [4] Figure 4: DDOS attack size from 2008 to 2017 [5]

**History of DDOS [6, 7, 8]**

David Dennis was the first person to performed DDOS attack in the 1974[8].

Table 1: History of DDOS attack

| Sr. No | Attack Year | Attack Targets |
|---|---|---|
| 1 | 1998 | Morris worm |
| 2 | 1990, 1990 | IRC chat floods |
| 3 | 2000 | Yahoo |
| 4 | 2001 | Code red worm attacks |
| 5 | 2002 | DNS root servers |
| 6 | 2003 | Al-Jazeera |
| 7 | 2004 | SCO |
| 8 | 2005 | E-bay |
| 9 | 2006 | Storm pay battling |
| 10 | 2007 | Estonian |
| 11 | 2008 | Georgia president Web site |
| 12 | 2009 | Iranian Government Web sites, Facebook, Twitter, and Google, Russian blog |
| 13 | 2010 | Wordpress.com |

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

| | | |
|---|---|---|
| 14 | 2011, 2012 | Sony |
| 15 | 2013 | South Korean Web sites, Spamhaus |
| 16 | 2014 | JP Morgan |
| 17 | 2015 | Github |
| 18 | 2016 | RIO Olympics |
| 19 | 2017 | Melbourne IT |
| 20 | 2018 | Github |

## RELATED WORK

Various researchers has studied and implemented detection technique on DDOS attack mainly by using advanced techniques some of them are discussed below.

Rohan Doshi et. al [9] suggested to use feature selection technique for network behavior specific IoT based DDOS detection. Based on proper feature selection high detection accuracy results can be obtained. The comparison is done with various ML algorithms along with neural networks. The results obtained were based on flow based approach.

Alekhya kaliki et. al [10] designed a unique machine learning based bio inspired technique. This method uses the anomaly detection approach for detecting App based DDOS attack. The main influence was given to the http flooding attack. The famous CAIDA dataset were used for the experimentation.

Chuanhuang Li et. al [11] implemented Deep learning based method in Software-Defined Network (SDN) for detection and prevention from DDOS attack. Sequence of traffic was generated and analyzed. The method reduces the dependency on availability of the datasets.

Muna AL-Hawawreh et. al [12] designed deep learning technique for IICSs using anomaly detection method. The designed model was trained and validated using obtained TCP/IP packets information. Preprocessing has been done on famous datasets like NSL-KDD and UNSW-NB15. Feed forward neural system was designed to obtained improvised results

Xiaoyong Yuan et. al [13] implemented a system using recurrent deep neural network (RNN) for analyzing network traffic and to monitor the network activities. The experiment was carried out on famous datasets and author claimed to obtained improvised results.

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

Kim et al. [14] implemented Deep Neural Network (DNN) for analyzing the network traffic. The method was implemented on famous KDD datasets. Accuracy obtained and claimed by the author was 99%.

Indraneel Sreeram et. al[15] designed ddos detection algorithm which tries to utilize the features of bat algorithm. This method primarily focused on App based DDOS attack. The Famous CAIDA dataset was used to carry out the experiment. The accuracy results obtained was high compared to existing work.

Marwane Zekri et.al [16] implemented C 4.5 based machine leaning algorithm to prevent the DDOS attack. Other ML algorithms were compared and results obtained were claimed to more accurate.

Hossein Hadian Jazi et. al [17] focuses primarily on application layer based DDOS attacks. For implementing the framework nonparametric CUSUM algorithm was used. Subset of system traffic was used for carrying out the detection experiment. The experiment carried out results into minimizes error rate and maximize detection accuracy.

. Abebe Abeshu Diro et. al [18] designed a framework based on Deep learning algorithm for detecting attack on IoT. Traditional machine learning algorithms were compared with this model. Distributed attack detection was compared with centralized system which was further concluded to be efficient approach based on the obtained results.

Syed Ali Raza Shah [19] implemented a hybrid approach for designing intrusion detection systems (IDS). This hybrid approach consists of SVM and fuzzy logic methods. The name given to the two IDS was Snort and Suricata. Along with firefly algorithm the SVM gives better results.

Hodo *et al.* [20] has given an exhaustive survey on Network intrusion detection systems (NIDS). The author has thoroughly discussed various deep learning techniques. Most promising results were also discussed.

Niyaz *et al.* [21] proposed a deep learning system which uses customized traffic for generating the results. The experiment has shown that binary classification (99.82%) obtained high accuracy rate along with 8-class classification (95.65 %.).

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

Lee *et al.* [22] implemented auto encoder based on unsupervised method for semiconductor manufacturing. The designed framework was named as Stacked de-noising Auto-encoder (SdA). Compared to existing approach accuracy obtained was increased by 14%. Also layer 4 results were claimed to be more promising.

Similarly, Tang *et al.* [23] designed network flow based method for detecting DDOS attack in the available network traffic. NSL-KDD dataset was used for the experimentation purpose and the accuracy claimed was more than 75% while considering 6 basic features.

M.S. Hoyos et. al [24] implemented supervised method which uses machine learning Support Vector Machines (SVM) for classification. The HTTP header was analyzed after the network traffic was captured. The author claimed to achieve 99 % accuracy rate compared to traditional approaches.

Elike Hodo et. al [25] designed a technique based on deep learning technique for performing threat analysis. An Artificial Neural Network (ANN) based deep learning algorithm was used with supervised version for carrying out the experiment. They tried to analyze IP traces for the detection and classified the normal and attack packets in the IoT based network. Promising results of 99.4% accuracy rate were achieved.

Kang and Kang [26] deep learning based DDN method. The classification was carried out based on unsupervised DBN and the results were obtained on famous datasets. The obtained results show that more accuracy in the detection rate was achieved.

Wang *et al.* [27] implemented a technique based on JavaScript which uses 3 layers SDA along with the linear regression. The experiment was carried out on famous dataset. The claimed to obtained high true positive frequency along with second highest false positive frequency amongst the compared existing approach.

## CONCLUSION

Even though lot of methodologies has been designed to detect DDOS attack with high accuracy still there are lot of areas where improvements can be done. These areas may include dependency on human operator, lack of freely available datasets, long training and computing time, lot of preprocessing of datasets etc. Still there are lots of areas which need to be focused upon.

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

**REFERENCE**

[1] https://anti-ddos.pro/en/ddos-attacks.html

[2] https://securelist.com/ddos-attacks-in-q2-2011/36394/

[3] https://www.foxnews.com/tech/biggest-ddos-attack-on-record-hits-github

[4]https://www.technologyreview.com/the-download/610405/github-just-suffered-the-worlds-biggest-ddos-attack-it-barely-blinked/

[5] https://blog.apnic.net/2018/04/03/the-ddos-threat-landscape-in-2017/

[6] https://security.radware.com/…/DDoS_Handbook/DDoS_Handbook.pdf.

[7] ShwetaTripathi, Brij Gupta, Ammar Almomani, Anupama Mishra, Suresh Veluru, Hadoop Based Defense Solution to Handle Distributed Denial of Service (DDoS) Attacks", Journal of Information Security, 2013, 4, 150–164.

[8] G. Dayanandam, T. V. Rao, D. Bujji Babu and S. Nalini Durga,DDoS Attacks—Analysis and Prevention, © Springer Nature Singapore Pte Ltd. 2019 H. S. Saini et al. (eds.), Innovations in Computer Science and Engineering, Lecture Notes in Networks and Systems 32, https://doi.org/10.1007/978-981-10-8201-6_1

[9] Rohan Doshi, Noah Apthorpe, Nick Feamster , Machine Learning DDoS Detection for Consumer Internet of Things Devices, 2018 IEEE Symposium on Security and Privacy Workshops, DOI 10.1109/SPW.2018.00013.

[10] Alekhya kaliki1, K Munivara Prasad, Machine Learning based Application Layer DDoS attack detection using Firefly Classification Algorithm, International Journal of Pure and Applied Mathematics, Volume 118 No. 17 2018, 635-645.

[11] Chuanhuang Li, Yan Wu, Xiaoyong Yuan, Zhengjun Sun, Weiming Wang, Xiaolin Li, Liang Gong, Detection and defense of DDoS attack–based on deep learning in OpenFlow-based SDN, Int J Commun Syst. 2018, 31:e3497, https://doi.org/10.1002/dac.3497

[12] Muna AL-Hawawreh , Nour Moustafa , Elena Sitnikova, Identification of malicious activities in industrial internet of things based on deep learning models, Journal of Information Security and Applications, © 2018 Elsevier Ltd. https://doi.org/10.1016/j.jisa.2018.05.002 2214-2126

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

[13]Xiaoyong Yuan, Chuanhuang Li, Xiaolin Li, DeepDefense: Identifying DDoS Attack via Deep Learning, 978-1-5090-6517-2/17/$31.00 ©2017 IEEE.

[14]Jin Kim, Nara Shin, Seung Yeon Jo and Sang Hyun Kim, Method of Intrusion Detection using Deep Neural Network, 978-1-5090-3015-6/17/$31.00 ©2017 IEEE.

[15] Indraneel, S., Praveen Kumar Vuppala, V., HTTP Flood attack Detection in Application Layer using Machine learning metrics and Bio inspired Bat algorithm, Applied Computing and Informatics (2017), doi: https://doi.org/10.1016/j.aci.2017.10.003.

[16] Marwane Zekri, Said El Kafhali, Noureddine Aboutabit and Youssef Saadi, DDoS Attack Detection using Machine Learning Techniques in Cloud Computing Environments, 2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech),IEEE, doi:10.1109/CloudTech.2017.8284731.

[17] Hossein Hadian Jazi, Hugo Gonzalez, Natalia Stakhanova, Ali A. Ghorbani, Detecting HTTP-based Application Layer DoS attacks on Web Servers in the presence of sampling, Computer Networks (2017), doi: 10.1016/j.comnet.2017.03.018

[18] A.A. Diro, N. Chilamkurti, Distributed attack detection scheme using deep learning approach for Internet of Things, Future Generation Computer Systems (2017), http://dx.doi.org/10.1016/j.future.2017.08.043

[19] S. P. Shashikumar, A. J. Shah, Q. Li, G. D. Clifford, and S. Nemati, “A deep learning approach to monitoring and detecting atrial fibrillation using wearable technology,” in Proc. IEEE EMBS Int. Conf. Biomed. Health Informat, FL, USA, 2017, pp. 141–144.

[20] E. Hodo, X. J. A. Bellekens, A. Hamilton, C. Tachtatzis, and R. C. Atkinson, Shallow and deep networks intrusion detection system: A taxonomy and survey, Submitted to ACM Survey, 2017, [Online]. Available: http://arxiv.org/abs/1701.02145

[21] Q. Niyaz, W. Sun, and A. Y. Javaid, A deep learning based DDOS detection system in software-defined networking (SDN), Submitted to EAI Endorsed Transactions on Security and Safety, In Press, 2017, [Online]. Available: http://arxiv.org/abs/1611.07400

[22] H.-W. Lee, N.-R. Kim, and J.-H. Lee, “Deep neural network self-training based on unsupervised learning and dropout,” Int. J. Fuzzy Logic Intell. Syst., vol. 17, no. 1, pp. 1–9, Mar. 2017. [Online]. Available:http://www.ijfis.org/journal/view.html?doi=10.5391/IJFIS.2017.17.1.1

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

[23] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking," in Proc. Int. Conf. Wireless Netw. Mobile Commun., Oct. 2016, pp. 258–263.

[24] Manuel S. Hoyos Ll, Gustavo A. Isaza E, Jairo I. Vélez and Luis Castillo O , Distributed Denial of Service (DDoS) Attacks Detection Using Machine Learning Prototype, S. Omatu et al. (eds.), DCAI, 13th International Conference, Advances in Intelligent Systems and Computing 474, © Springer International Publishing Switzerland 2016, DOI: 10.1007/978-3-319-40162-1_4

[25] Elike Hodo, Xavier Bellekens, Andrew Hamilton, Pierre-Louis Dubouilh, Ephraim Iorkyase, Christos Tachtatzis and Robert Atkinson, Threat analysis of IoT networks Using Artificial Neural Network Intrusion Detection System, 978-1-5090-0284-9/16/$31.00 ©2016 IEEE .

[26] M.-J. Kang and J.-W. Kang, "Intrusion detection system using deep neural network for in-vehicle network security," PLoS One, vol. 11, no. 6, Jun. 2016, Art. no. e0155781.

[27] Y.Wang,W.-D. Cai, and P.-C.Wei, "A deep learning approach for detecting malicious JavaScript code," Security Commun. Netw., vol. 9, no. 11, pp. 1520–1534, Jul. 2016.