DDOS Detection Using Machine Learning Technique

Chapter · October 2020

DOI: 10.1007/978-981-15-8469-5_5

4 authors:

Sagar Dhanraj Pande
Lovely Professional University
47 PUBLICATIONS **104** CITATIONS
SEE PROFILE

Aditya Khamparia
Babasaheb Bhimrao Ambedkar University
138 PUBLICATIONS **1,459** CITATIONS
SEE PROFILE

Deepak Gupta
Maharaja Agarsain Institute of Technology
245 PUBLICATIONS **3,787** CITATIONS
SEE PROFILE

Dang N. H. Thanh
University of Economics Ho Chi Minh City
93 PUBLICATIONS **830** CITATIONS
SEE PROFILE

DDOS Detection Using Machine Learning Technique

Sagar Pande, Aditya Khamparia, Deepak Gupta, and Dang N. H. Thanh

Abstract Numerous attacks are performed on network infrastructures. These include attacks on network availability, confidentiality and integrity. Distributed denial-of-service (DDoS) attack is a persistent attack which affects the availability of the network. Command and Control (C & C) mechanism is used to perform such kind of attack. Various researchers have proposed different methods based on machine learning technique to detect these attacks. In this paper, DDoS attack was performed using ping of death technique and detected using machine learning technique by using WEKA tool. NSL-KDD dataset was used in this experiment. Random forest algorithm was used to perform classification of the normal and attack samples. 99.76% of the samples were correctly classified.

Keywords DDoS · Machine learning · Ping of death · Network security · Random forest · NSL-KDD

S. Pande · A. Khamparia (✉)
School of Computer Science Engineering, Lovely Professional University, Phagwara, Punjab, India
e-mail: aditya.khamparia88@gmail.com

S. Pande
e-mail: sagarpande30@gmail.com

D. Gupta
Maharaja Agrasen Institute of Technology, New Delhi, India
e-mail: deepakgupta@mait.ac.in

D. N. H. Thanh
Department of Information Technology, School of Business Information Technology, University of Economics Ho Chi Minh City, Ho Chi Minh City, Vietnam
e-mail: thanhdnh@ueh.edu.vn

A. Khanna et al. (eds.), *Recent Studies on Computational Intelligence*,
Studies in Computational Intelligence 921,
https://doi.org/10.1007/978-981-15-8469-5_5

1 Introduction

With the ongoing convergence of data innovation (IT), various data gadgets are turning out to be massively muddled. Associated with one another, they keep on making furthermore spare significant computerized information, introducing a period of big data. However, the probability is extremely high that they may expose significant data as they transmit a lot of it through consistent correspondence with one another. A framework turns out to be more vulnerable as more digital devices are connected. Hackers may additionally target it to take information, individual data, and mechanical insider facts and break them for unlawful additions [1]. Given these conditions, attack detection system (ADS) ought to likewise be more smart and successful than previously to battle attack from hackers, which are continuously evolving. Confidentiality, integrity and availability can be considered as the main pillars of security [2, 3]. All these pillars are discussed below.

1.1 Confidentiality

Confidentiality is also called as secrecy. The motive behind secrecy is to keep sensitive information away from illegitimate user and to provide access to the legitimate user. Along with this, assurance must be given on restricted access of the information.

1.2 Integrity

Integrity means keeping up the data as it is without any modification in the data. Data must be received as it at the receiver end. To provide integrity, file permissions and user access controls can be used. A variety of techniques has been designed to provide integrity, and some of them are as follows: checksums, encryption, etc.

1.3 Availability

Availability can also be called as accessibility. Availability means providing the required data whenever and wherever required by fixing all the issues as early as possible. Sometime, it is difficult to overcome the situation caused by bottleneck condition. RAID is one of the popular techniques used for providing availability. Precaution needs to be taken from the hardware context also. The hardware used must be kept away at secured places. Apart from this, firewalls can be used to prevent from malicious activity.

1.4 DDoS Attack Dynamics

As per the report of Kaspersky [4], growth in the frequency and the size of DDoS attack in the 2018 can be seen. One of the largest DDoS attacks was implemented on GitHub in the month of February, 2018, which consists of 1.3 TBPS of traffic transfer [5].

1.5 DDoS Tools

Various tools are freely available for performing DDoS attack; some of them are listed below [6]

- HULK (HTTP Unbearable Load King)
- GoldenEye HTTP DoS tool
- Tor's Hammer
- DAVOSET
- PyLoris
- LOIC (Low Orbit Ion Cannon)
- XOIC
- OWASP DoS HTTP Post
- TFN (Tribe Flood Network)
- Trinoo.

2 Related Work

Lot of researchers are working on the detection of the most DDoS which has its largest impact in the area of social networking by using deep learning and machine learning techniques. Some of the recent work done in this area is discussed below.

Hariharan et al. [7] used machine learning C5.0 algorithm and have done the comparative analysis of the obtained results with different machine learning algorithms such as Naïve Bayes classifier and C4.5 decision tree classifier. Mainly, the author tried to work in offline mode.

BhuvaneswariAmma N. G. et al. [8] have implemented a technique, deep intelligence. The author extracted the intelligence from radial basis function consisting of varieties of abstraction level. The experiment was carried out on famous NSL KDD and UNSW NB15 dataset, where 27 features were considered. The author claimed to have better accuracy compared to other existing techniques.

Muhammad Aamir et al. [9] implemented feature selection method based on clustering approach. Algorithm was compared based on five different ML algorithms. Random forest (RF) and support vector machine (SVM) were used for training purpose. RF achieved highest accuracy of around 96%.

Dayanandam et al. [10] have done classification based on features of the packets. The prevention technique tries to analyze the IP addresses by verifying the IP header. These IP addresses are used for differentiating spoofed and normal addresses. Firewalls do not provide efficient solution when the attack size increases.

Narasimha et al. [11] used anomaly detection along with the machine learning algorithms for bifurcating the normal and attacked traffics. For the experiment, real-time datasets were used. Famous naive Bayes ML algorithm was used for classification purpose. The results were compared with existing algorithms like J48 and random forest (RF).

J. Cui et al. [12] used cognitive-inspired computing along with entropy technique. Support vector machine learning was used for classification. Details from switch were being extracted from its flow table. The obtained results were good in terms of detection accuracy.

Omar E. Elejla et al. [13] implemented an algorithm for detecting DDoS attack based on classification technique in IPv6. The author compared the obtained results with five different famous machine learning algorithms. The author claimed that KNN obtained the good precision around 85%.

Mohamed Idhammad et al. [14] designed entropy-based semi-supervised approach using ML technique. This implementation consists of unsupervised and supervised compositions, among which unsupervised technique gives good accuracy with few false-positive rates. While supervised technique gives reduce false-positive rates. Recent datasets were used for this experiment.

Nathan Shone et al. [15] implemented deep learning algorithm for classification of the attack. Along with this, it used unsupervised learning nonsymmetric deep autoencoder (NDAE) feature. The proposed algorithm was implemented on graphics processing unit (GPU) using TensorFlow on famous KDD Cup 99 and NSL-KDD datasets. The author claimed to obtain more accurate detection results.

Olivier Brun et al. [16] worked in the area of Internet of Things (IoT) to detect the DDoS attack. The author implemented one of the famous deep learning techniques, i.e., random neural network (RNN) technique for detection of the network. This deep-learning-based technique efficiently generates more promising results compared to existing methods.

3 Implementation of DDoS Attack Using Ping of Death

While performing ping of death attack, the network information needs to be gathered, and to achieve this, ipconfig command can be used. In Fig. 1, the detailed information of the network is gathered after giving ipconfig command. As soon as the network information is gathered, we can start performing the ping of death attack on the IP address.

Enter the following command to start the attack:

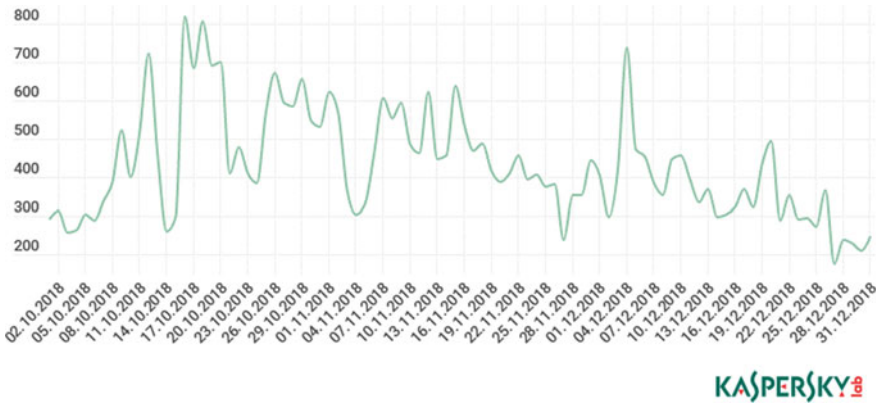

Fig. 1 DDoS attacks dynamics in 2018 [4]

```
ping-t –l 65500 XX.XX.XX.XX
```

- "ping" command transfer the data packets to the target
- "XX.XX.XX.XX" is the IP address of the target
- "−t" means sending packets repeatedly
- "−l" specifies the data packet load to be sent to the target.

Figure 2 shows the packet information after performing ping of death attack; this attack will continue till the target resources are exhausted. The primary goal of this

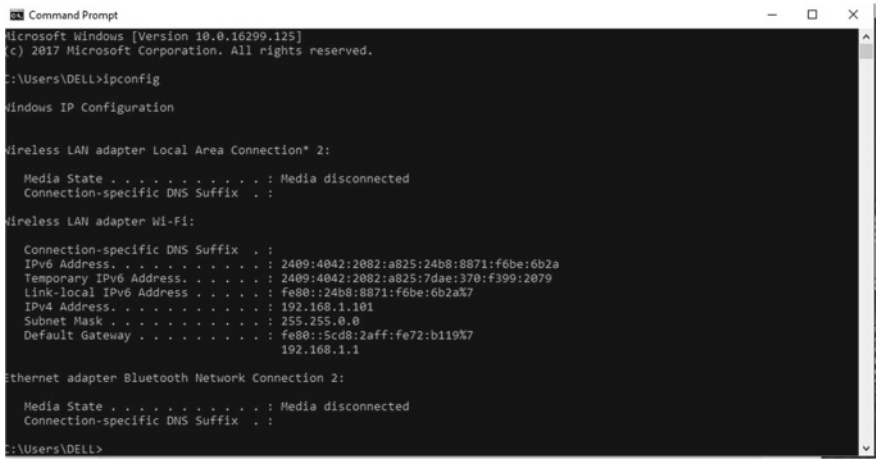

Fig. 2 Details of the network obtained using ipconfig

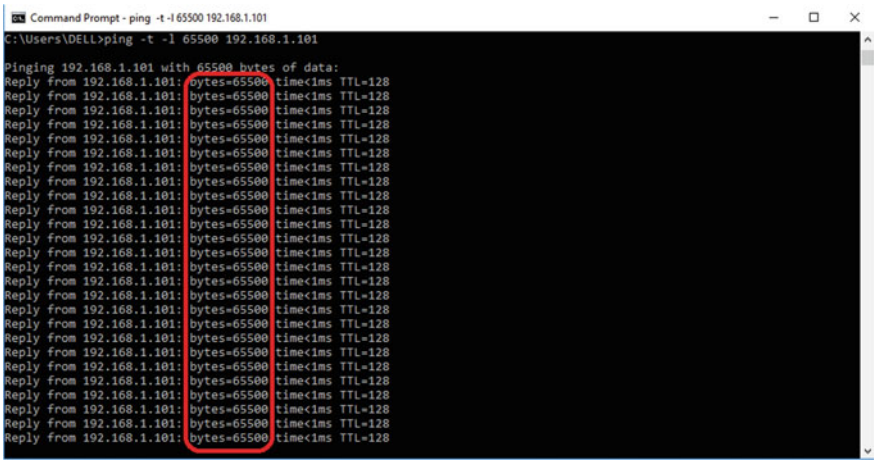

Fig. 3 Packets transfer after implementing ping of death

type of DDoS attack is to utilize all the CPU memory and exhaust it. In Fig. 3, clearly we can see that before starting the attack, the performance graph was linear, and as soon as the attack is started, the spikes are visible. Figure 4 signifies that CPU is being utilized as much as possible, and this will continue till the complete network is exhausted. Details of the memory consumption, CPU utilization, uptime, etc., can be seen in Figs. 3, 4 and 5.

4 DDoS Detection Using Machine Learning Algorithm

Random forest (RF) is one of the popular machine learning techniques which is used for classification developed by Leo Breiman [3]. The random forest produces different decision trees. Each tree is built by an alternate bootstrap test from the first information utilizing a tree classification algorithm. NSL-KDD dataset was used for this experiment [16]. The experiment was performed using a laptop with Windows 10 64-bit operating system, Intel (R) Core (TM) i5-2450 M CPU@ 2.50 GHz, having 8.00 GB RAM. Total instances used for training were 22,544, and the dataset consists of attributes 42. Random forest was used for training the model. 8.71 s was building time of the model, and 1.28 s was the testing time of the model. This experiment was carried out using Weka 3.8 tool. Table 1 provides the summary of the instances after classification using random forest. Table 2 shows the performance evaluation using various parameters. Table 3 consists of confusion matrix using normal & attack classification.

- **Accuracy**: It measures the frequency of the attack instances of both classes correctly identified.

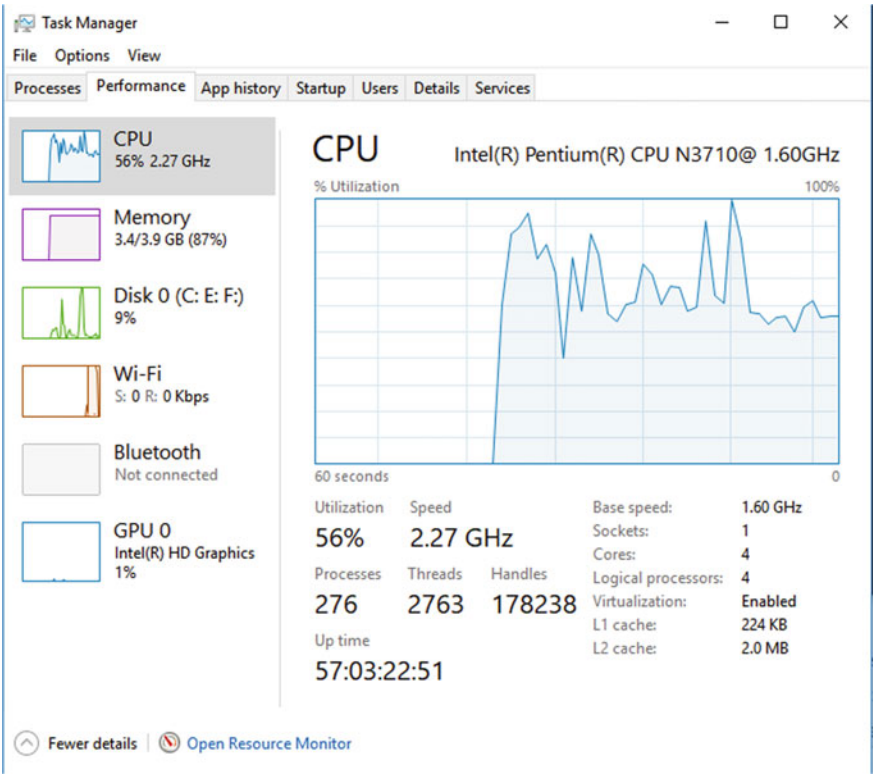

Fig. 4 CPU specifications before the attack

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FN} + \text{FP} + \text{TN}}$$

- **Precision**: It is the ratio of the number of related attacks that were identified to the total number of unrelated and related attacks that were identified. Also known as positive predictive value.

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}$$

- **Recall**: This is the ratio of the number of related attacks to the total number of related attacks received and also known as positive sensitive value.

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

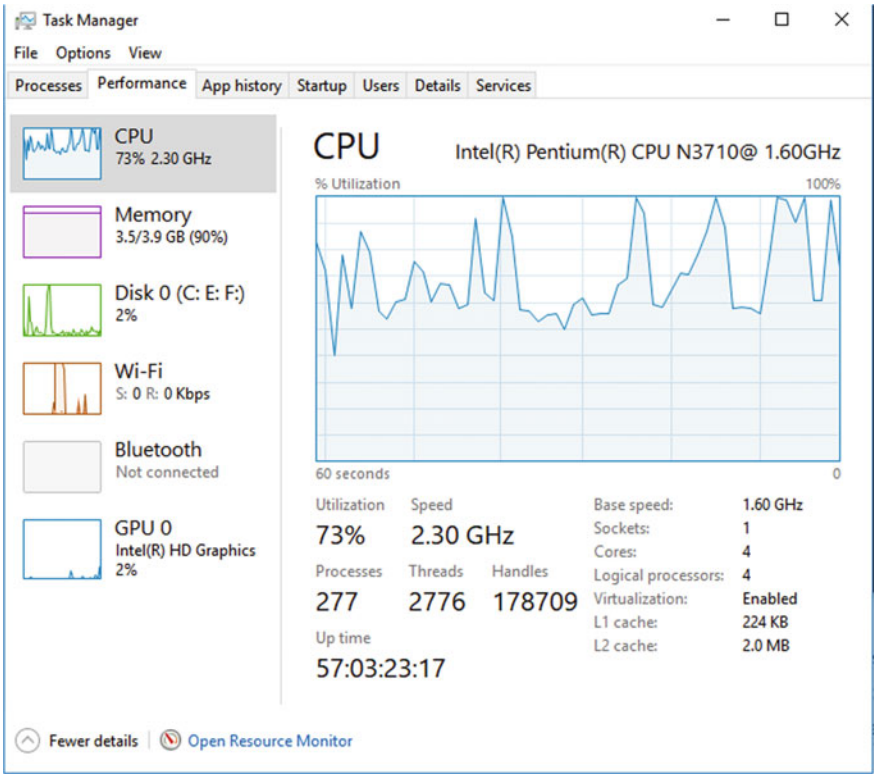

Fig. 5 CPU specifications after the attack

Table 1 Classification summary

Correctly classified attack instances	22,490	99.7605%
Incorrectly classified attack instances	54	0.2395%

Table 2 Performance evaluation

TP rate	FP rate	Precision	Recall	Class
0.998	0.002	0.997	0.998	Normal
0.998	0.002	0.998	0.998	Attack

Table 3 Confusion matrix

a	b	Classification
9689	22	a = normal
32	12,801	b = attack

5 Conclusion

In this paper, several ongoing detection techniques for DDoS attack are discussed, especially using machine learning techniques. Along with this, list of freely available DDoS tools is also discussed. Command-based ping of death technique was used to perform DDoS attack. Random forest algorithm was used to train the model which resulted into 99.76% of correctly classified instances. In future, we will try to implement deep learning technique for the classification of the instances.

References

1. Ganorkar, S. S., Vishwakarma, S. U., & Pande, S. D. (2014). An information security scheme for cloud based environment using 3DES encryption algorithm. *International Journal of Recent Development in Engineering and Technology, 2*(4).
2. Pande, S., & Gadicha, A. B. (2015). Prevention mechanism on DDOS attacks by using multi-level filtering of distributed firewalls. *International Journal on Recent and Innovation Trends in Computing and Communication, 3*(3), 1005–1008. ISSN: 2321–8169.
3. Khamparia, A., Pande, S., Gupta, D., Khanna, A., & Sangaiah, A. K. (2020). Multi-level framework for anomaly detection in social networking, Library Hi Tech, 2020. https://doi.org/10.1108/LHT-01-2019-0023.
4. https://www.calyptix.com/top-threats/ddos-attacks-101-types-targets-motivations/.
5. https://www.foxnews.com/tech/biggest-ddos-attack-on-record-hits-github.
6. Fenil, E., & Mohan Kumar, P. (2019). *Survey on DDoS defense mechanisms.* John Wiley & Sons, Ltd. https://doi.org/10.1002/cpe.5114.
7. Hariharan, M., Abhishek, H. K., & Prasad, B. G. (2019). DDoS attack detection using C5.0 machine learning algorithm. *I.J. Wireless and Microwave Technologies, 1*, 52–59 Published Online January 2019 in MECS. https://doi.org/10.5815/ijwmt.2019.01.06.
8. NG, B. A., & Selvakumar, S. (2019). Deep radial intelligence with cumulative incarnation approach for detecting denial of service attacks. *Neurocomputing.* https://doi.org/10.1016/j.neucom.2019.02.047.
9. Aamir, M., & Zaidi, S. M. A. (2019). Clustering based semi-supervised machine learning for DDoS attack classification. *Journal of King Saud University—Computer and Information Sciences*, Production and hosting by Elsevier, https://doi.org/10.1016/j.jksuci.2019.02.0031319-1578/_2019.
10. Dayanandam, G., Rao, T. V., BujjiBabu, D., & NaliniDurga, N. (2019). DDoS attacks—analysis and prevention. In H. S. Saini, et al. (Eds.), *Innovations in computer science and engineering, Lecture notes in networks and systems* 32. © Springer Nature Singapore Pte Ltd.https://doi.org/10.1007/978-981-10-8201-6_1.
11. NarasimhaMallikarjunan, K., Bhuvaneshwaran, A., Sundarakantham, K., & Mercy Shalinie, S. (2019). DDAM: Detecting DDoS attacks using machine learning approach. In N. K. Verma & A. K. Ghosh (Eds.), *Computational Intelligence: Theories, Applications and Future Directions—Volume I, Advances in Intelligent Systems and Computing, 798*, https://doi.org/10.1007/978-981-13-1132-1_21.
12. Cui, J., Wang, M., & Luo, Y., et al. (2019). DDoS detection and defense mechanism based on cognitive-inspired computing in SDN. *Future Generation Computer Systems.* https://doi.org/10.1016/j.future.2019.02.037.
13. Elejla, O. E., Belaton, B., Anbar, M., Alabsi, B., & Al-Ani, A. K. (2019). Comparison of classification algorithms on ICMPv6 based DDoS attacks detection. In R. Alfred et al. (Eds.*), Computational Science and Technology, Lecture Notes in Electrical Engineering 481.*, Springer Nature Singapore Pte Ltd.https://doi.org/10.1007/978-981-13-2622-6_34.

14. Idhammad, M., Afdel, K., & Belouch, M. (2018). Semi-supervised machine learning approach for DDoS detection.*Applied Intelligence.* . Springer Science+Business Media, LLC, part of Springer Nature 2018. https://doi.org/10.1007/s10489-018-1141-2.
15. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence, 2*(1).
16. Brun, O., Yin, Y., & Gelenbe, E. (2018). Deep learning with dense random neural network for detecting attacks against IoT-connected home environments. *Procedia Computer Science, 134*, 458–463, Published by Elsevier Ltd.