Chapter 78
Analysis of Machine Learning and Deep Learning Approaches for DDoS Attack Detection on Internet of Things Network

Aman Kashyap and Ankit Kumar Jain

1 Introduction

The proliferation of Internet-connected devices that exchange services and data without any help of human mediation constitutes today's Internet of things [1, 2]. With this rapid growth of IoT, it often serves severe concerns about safety, notably in the areas of security and privacy. Due to the exploitation of the vulnerabilities in IoT emerging from various obstructions such as restricted resources, not changing default passwords, scarcity of important security protocols, unauthorized access of devices by malicious entities, and, therefore, may take the shape of diverse attacks. A distributed denial of service (DDoS) is a specific type of denial-of-service (DoS) attack targeted at the servers to shut it down partially or completely, by flooding the Internet traffic. The main aim of these types of attacks is to exploit vulnerabilities of the targeted network or server and stop regular traffic flow. DDoS attacks are implemented by compromising the security of non-legacy IoT devices with low security, for example, printers, smart television, smartwatch, etc. The compromised devices are called bots. And the collection of bots creating a network of compromised devices is called a botnet.

In 2016, Web site of a French web host and a security consultant was attacked with the traffic of 1 Tbps and 620 Gbps, respectively. The name of the attack was called Mirai. Moreover, nearly 600,000 of IoT devices were infected for such attack [3]. And when the source code of this famous attack was released publicly, more attacks

A. Kashyap (✉) · A. K. Jain
Department of Computer Engineering, National Institute of Technology, Kurukshetra, Haryana, India
e-mail: aktcse18@gmail.com

A. K. Jain
e-mail: ankit.jain2407@gmail.com

M. Dave et al. (eds.), *Proceedings of the International Conference on Paradigms of Computing, Communication and Data Sciences*, Algorithms for Intelligent Systems,
https://doi.org/10.1007/978-981-15-7533-4_78

followed with an intensity of 1.2 Tbps. The attacks targeted hundreds of famous Web sites like Netflix, Twitter, GitHub, and Reddit. The cyber-security solutions provider recorded one of the biggest DDoS attacks in history in 2019. The attack was targeted on a streaming service client. The attack focused on the application layer, which continues over 13 days with a frequency of 292,000 requests per second. The main reason for such type of attacks discovered by Neustar in its DDoS attack research is the increasing trend of what their researchers refer to as strategic, "low-intensity incursions" that degrade the performance of servers over time. Using these lowball attacks allows hackers to execute longer attacks that fall below the intensity level that would cause DDoS defenses. The number of Internet of things (IoT) devices that are estimated to exist by 2020 is 20.4 billion, according to a press release from Gartner, Int. Because IoT devices (connected devices such as smart thermostats, refrigerators, and even baby monitors) are considered to lack any real IT protection or cyber-security steps, they are vulnerable to hacking, eavesdropping attacks, and DDoS attacks. The researcher from IBM X-Force indicates that more than 80 percent of all observed activity from Mirai botnet variants so far in 2019 targeted media/information services and insurance industries [4].

1.1 Attack Motivation on IoT Devices

The IoT devices are easily targeted because of the deficiency of necessary and important security protocols, which makes them easy targets [5]. The attacker can easily impair an IoT device and can create a botnet of similarly infected devices [6]. The main reasons that allows an attacker to target these devices are as follows-

- *Scarcity of important security protocols*—Most of the IoT devices are not having basic security protocols, and they can be exploited using backdoors.
- *Simple password*—Most of the owner of the IoT devices does not change the default password given by the manufacturer. And exploiting this vulnerability attacker can easily get access to the device.
- *Always connected*—Nearly all IoT devices are continuously connected to the internet. This can become the worst problem as most of the DDoS attacks take subsequently more time for the attack to happen.
- *Cost-effective*—The attacker does not need to maintain highly functional servers for DDoS attack as the IoT devices are very cost-effective as well as easy to hack.
- *Incompetence to reset authorization*—The IoT devices are not able to get the control back once it is attacked. Even the security credential cannot be reset by the manufacturers.

The rest of the paper is structured as follows: In Sect. 2, we discuss attacks on IoT devices using a botnet, overview of frequently used botnets, and statistics of different types of attacks in recent years. In Sect. 3, we review various state-of-the-art works of literature on detecting DDoS attacks and also suggest an approach to mitigate DDoS

attacks on IoT. In Sect. 4, we discuss some open issues and challenges. Finally, in Sect. 5, we conclude our discussion on DDoS attack detection on IoT.

2 Attacks on IoT Network Using Botnet

The Internet of things (IoT) has revolutionized familiar spaces by making them more intelligent. Homes, offices, and cities are just a few of the places where IoT devices gave better visibility, safety, and control. These conveniences, however, came at a cost, traditional cyber threats also found a new arena for attacks and created realities such as IoT botnets. IoT botnets also closely resemble conventional botnets in terms of composition, in that it has two major components. One is the C&C server, from where a threat actor sends orders from and manages the botnet. And the second is independently hacked or infected computers [7]. Several botnet attacks took place in past years, among them BashLite, Mirai, Remaiten, and 3ve are the popular botnets:-

- *BashLite* [7] This malware is also named as Lizkebab, Torlus, and gafgyt. A common malware which mainly aimed at IoT devices based on Linux, for example, cameras and digital video recorders (DVR). DDoS attacks like UDP and TCP flooding attacks can be launch with this botnet along with an HTTP attack with a capacity of 400 Gbps. In 2015, its source code was released, giving more developers an opportunity to improve it.
- *Mirai* [7] Mirai had become the most popular IoT malware in existence when it exploded in 2016. The fact that most of its targets are household IoT devices (home routers, baby monitors, and security cameras) is what made the attack also unparalleled. Due to the low or poor protection on these devices, Mirai was able to hijack devices with the initial list of 64 common usernames and passwords. Since Mirai's source code had been leaked to the public, developers continue to use its code to spawn new variants that have plagued IoT devices over the years.
- *Remaiten* [7] It was released in 2016. It is also known as KTM-RM. It incorporated Tsunami's DDoS features (a Hydra variant) and an improved version of BASHLITE's scanning capacities. Remaiten can download a bot executable for many of the embedded architectures used on these devices once it has gained access to IoT devices, enables the launching of architecture-adapted attacks. Remaiten is remarkable for its complexity and flexibility in the most advanced IoT device architecture.
- *3ve* [8] It was the combination of three different, but related sub-operations, each of which perpetrated ad fraud and could skillfully evade detection. In Q4 of 2018, a month's long investigation conducted by White Ops, Google, and law enforcement which began in early 2017 resulted in an unprecedented takedown of the botnet [9]. It was different from other botnets because it could create a botnet of its own, create false copies, cover up their IP address with proxies, and hijack the IP address of the Border Gateway Protocol (BGP) and sell their bogus ad inventories to advertisers to earn money.

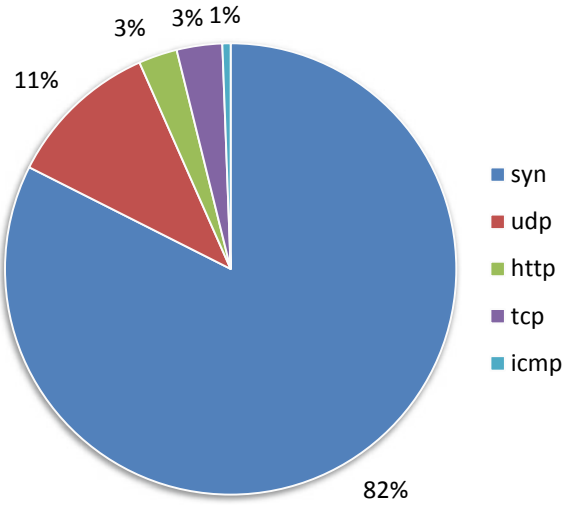

Fig. 1 Distribution of DDoS attacks by duration (hours) in quarter 1 and quarter 2 of 2019

DDoS attacks have become more complex and are now being used as a mixture of several attacks to bypass their victims' defenses. The perpetrator is planned to routinely interrupt the services of the target. The attacker can, for example, launch a single type of attack and let the victim recover it. Once the victim is recovered, a new attack is launched, which forces the victim to deprive users of service. The attacking process is simply repeating. In the second quarter of 2019, among all the DDoS attacks, the most famous attack is still the SYN floods attack with 82.43%. The UDP flood attack is in second place with 10.94%, TCP requests have been lifted to third place with a 3.26% share, while HTTP traffic has dropped to 2.77%. The last position is still the ICMP flood, with a 0.59% share. Figure 1 displays the current distribution of DDoS attacks by duration (hours) in 2019 [10].

3 Machine Learning-Based Approaches for DDoS Attack Defense on IoT

Different types of variation in launching DDoS have been attempted there in the past and still increasing in the present. All such attacks can be broadly categorized into application and infrastructure layer attacks and can be a mixture of two like a Dyn DNS Outage, which was a combination of an application plus protocol-based attack on DNS service that was expanded into a volumetric attack. There have been a number of proposals on defense mechanism against DDoS attack, specifically after seeing its wide range of variations in the recent past years. In [11], the authors generated an IoT dataset, namely Bot-IoT, which consists of legitimate and simulated IoT traffic and attack traffic (including DDoS, DoS, reconnaissance, and information theft) based on a real testbed and compared the dataset with other publicly available

datasets. Among the comparison, the proposed dataset was claimed to be the only dataset containing IoT traces. The authors also developed new features using correlation coefficient and joint entropy techniques. They proposed three machine learning and deep learning algorithms to detect attacks in the extracted dataset (i.e., 5% of the original dataset). Evaluation results of the classifiers were presented, which demonstrate good accuracy. However, the extracted dataset contains imbalanced normal and attack traffic because the number of attack packets is much higher than that of normal packets for three attack types (DDoS, DoS, and reconnaissance).

In [12], for detection of network intrusion on the dataset UNSW-NB 15, a deep learning model was proposed. The model consists of a total of fifty neurons, each of them distributed equally over the hidden layers, i.e., ten neurons per layer. The numbers of feature categories decide the count of the hidden layers, while the numbers of features decode the number of neurons in the model. The learning took place in ten epochs, which tenfold cross-validation on the whole dataset. The threshold is set to ten for the squared sum of the incoming weights per unit. Before training the model, the dataset entries are shuffled randomly, and Gedeon method is used to calculate the importance of features for further process.

In [13], the authors proposed a solution based on machine learning using Bidi long short-term memory recurrent neural network. DDoS attack detection is done by packet flow analysis. The proposed approach focused on text recognition within applications in contrast with other approaches for flow detection. Attack vectors can be predicted using word embedding to identify text. Using UDP flooding and DNS attack, 98 percent accuracy in attack detection was achieved while testing the proposed methodology. For training and validation, the attack type was split. Each model was trained over twenty iterations. Available botnet detection methods based on the detection of the signature of attack flow-based anomaly cannot prevent attacks on the IoT system. The solution proposed provides better accuracy in attacking vector detection by executing the text recognition functions at the packet level.

In [14], the authors proposed an artificial neural network-based approach for monitoring the IoT network. They have created 4000 data samples with the help of Arduino Uno devices to act as their edge devices. Total of 10 of these devices are connected to Raspberry Pi 3 for implementing gateway. Initially, they used only two features (i.e., device ID and sensor value). They decided to create a five-layer network in which three hidden layers were there. They divided the dataset randomly into training and testing data. The trained model did not show valid predictions when tested. Therefore, they added a third input, which is a delay between transmissions. It was measured in ms. The main aim of adding this feature is to detect man-in-the-middle attack by normal delay. They were able to detect the attack input with 99% of the time.

In [15], the authors proposed a feed-forward neural network-based intrusion detection system with backpropagation. With the advantages in mind like distributed computation, learning capabilities, parallelism, adaptability, and fault tolerance of neural network, they have chosen two different datasets. One is the KDD cup 99 dataset, which contains different types of attack and normal attack traffic in different files. They converted symbolic features into numerical features so that it can be used in

training neural network. The second dataset is the Darpa project, which was evolved in MIT University in 1998 to provide a benchmark to intrusion detection system developers to equate their products. The dataset has normal traffic and four categories of attacks, all in TCPdump file. They have created a two-layer feed-forward neural network and randomly assigned weights with 41 inputs in the input layer. The number of inputs depends on the number of features used. Accordingly, the hidden layer and the number of connection features are 35. Since the data was huge, any classic backpropagation algorithm cannot be used; therefore, they have used "trainscg" fast training function. For dataset 1, the learning took place in 599 epochs, and for dataset two, the learning took place in 611 epochs. The results showed that using less data was more suitable as it lowers the computational overhead. The proposed system had achieved good results in the probe and DDoS attacks with an accuracy of 99% and 97.5%, respectively.

In [16], the authors proposed a novel approach to detect IoT malware by conducting malware image classification. They explained, a malware binary might also be reformatted as a sequence of 8 bits, and then it can be further converted to a grayscale image having a pixel value ranging from 0 to 255 and has one channel. Then the resulting image is input into the image classifier. To convert malware binary into the image, the only requirement is to obtain the input vectors of the CNN, i.e., 8-bit vectors. It requires only the reorganization of the malware binaries (without any further preprocessing of the real image). To create a balance in CNN, all the images are rescaled to 64 $\times$ 64 pixels for input. They have used a dataset that has been collected by IoTPOT. The dataset has 500 malware samples. The CNN model was trained on 365 samples from which 45 samples were used for testing purposes. The training and testing samples were divided into four major classes. The configuration used is a light weighted, two-layer convolutional neural network. The number of iteration was 5000 for network training, and the batch size was 32 with a learning rate of 0.0001. The proposed system was able to predict the malware existence with 94.0% accuracy for two-class classification.

In [17], the authors proposed a method named deep defense based on deep learning for identifying DDoS attacks. The dataset they have used is ISCX2012. They have used NVIDIA Tesla M40 GPUs with 12 GB memory, and the experiments were repeated 10 times in order to decrease uncertainty from the datasets. The dataset was divided into a 9:1 ratio for training and testing purposes, respectively. The model they have used is based on the recurrent neural network (RNN) (such as LSTM, GRU). To train the model, they have selected 20 fields of network traffic from the dataset to use them as features in the training model. The aim of LSTM is to overcome an RNN gradient problem and to present the past timestamp using a memory cell. GRU is a simpler version of the conventional LSTM, which, due to fewer parameters, can be trained more easily. To show the last packet's prediction in the entire sequence, the sigmoid function is used in the deep learning model. For capturing local information and the simplification of deep neuron network, a one-dimensional convolutional neural layer was used before recurrent neural layers. The activation function for convolutional neural layers was the rectified linear unit (ReLU), and the kernel size was 3 with a stride of 1. To accelerate deep neural network, a batch normalization

Table 1 Comparison of recently proposed machine learning algorithms for DDoS attack detection

S. No.	Defense techniques	Advantages	Limitation
1	Deep learning-based approach [12]	It can be useful for detecting low rate attack as it looks similar to actual network traffic to the victim	The accuracy of the model is directly proportional to the dataset used for training purposes
2	Bidirectional long short-term recurrent neural network [13]	The method uses text recognition at a packet level, which provides better accuracy	To get high accuracy and precision more memory and resources were used
3	Feed-forward neural network [15]	Neural networks come handy when the dataset is huge, like in this case. The proposed approach showed good results, with 97.5% accuracy	The proposed method may show less accuracy when the data is large as the dataset with fewer data performed better than the one which has large data
4	Malware image classification [16]	The configuration is light weighted, and the accuracy for the two-class classification is 94%	Detailed features are not there to improve the accuracy of the model
5	Artificial neural network [14]	The model ran perfectly on the dataset, and they had created with an error rate of 1%	The dataset created was very limited. The model could perform differently when tested on a large-scale DDoS attack
6	Deep defense based on deep learning [17]	The largest number of window sizes is used to store a longer attack time sequence	Use of older dataset. It may perform not so good for nowadays attack traffic

layer was added after every two recurrent neural layers and every fully connected layer. The model showed an accuracy of 97.99%. Table 1 presents the comparison of different machine learning approaches for detecting DDoS attacks on IoT along with their advantages and limitations.

3.1 Suggestions to Mitigate a DDoS Attack [18]

The process of protecting a target server successfully from a DDoS attack is called DDoS mitigation [18]. By using specifically designed equipment or some mitigation process, an incoming attack can be mitigated by the target victim. There can be four steps to stop DDoS attacks as shown in Fig. 2. The first step is routing the traffic such that it breaks into manageable chunks to prevent denial of service. The second step is detection. It is imperative to distinguish attack traffic from legitimate traffic. The victim should be able to see common attack patterns, and previous data

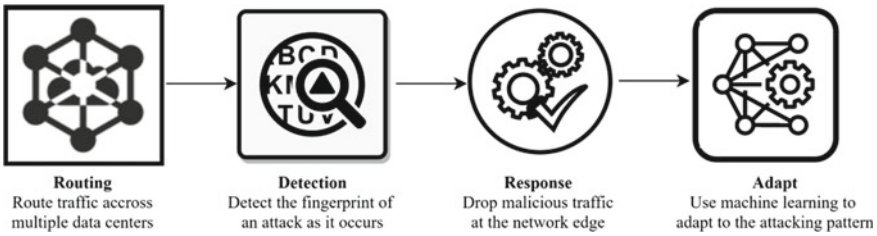

Fig. 2 DDoS Mitigation stages

assist in proper detection. In the next step, the attack protection system responds to the identified threat by dropping malicious attack traffic and allowing the rest of the normal traffic. In the last step, adaptation using machine learning so that the victim can recognize attacks from a certain location, or repeating offending IP blocks, or improper use of any particular protocols. With the adaptation of current attack patterns, a protection system can become stronger to mitigate future attacks [18] Fig. 2.

4 Open Issues and Challenges

One of the main challenges for mitigation methods based on machine learning is the quantity and quality of the dataset. As machine learning approach depends on the dataset for training and testing of the algorithm [19]. Therefore, assuring the exact amount and quality of the data would help deal with new types of attacks and improve the accuracy of the algorithm for the detection of threats. Apart from the studied methods, there is still room for improvement in necessary protocols. The basic line of defense for IoT devices are: update firmware, change default passwords, educate users, and implement a firewall. As suggested in Sect. 3.1, Mitigation of DDoS attack can be in 4 steps, and in the last step, i.e., adaptation is where these challenges are. The results from the above-discussed approaches motivate us to do more research to assess DDoS attack detection in a setting that is more connected to the real world.

5 Conclusion

Most commonly, DDoS attacks do not show any signs at the starting of the attack, but it gradually increases its attack resulting in server shutdown. We have listed reasons and motivations why the attacker chooses IoT devices to create a botnet. We have listed different types of botnet used for creating DDoS attacks. We have focused our studies on machine learning-based solutions as per the current trends. We have presented multiple solutions for defending a DDoS attack on IoT based on machine learning. A comparative analysis of popular machine learning approaches used in recent past years is also discussed along with their advantages and limitations.

Furthermore, we have suggested four steps solution to mitigate future DDoS attacks and adapt from current attacks to be ready for future attacks. We have also discussed open issues and challenges in Sect. 4, which provides an understanding to improve DDoS defense system further. We need a smarter defense than the IoT devices itself.

References

1. Chen K, Zhang S, Li Z, Zhang Y, Deng Q, Ray S, Jin Y (2018) Internet-of-things security and vulnerabilities: Taxonomy, challenges, and practice. J Hardw Syst Secur 2(2):97–110
2. Zhou W, Jia Y, Peng A, Zhang Y, Liu P (2018) The effect of iot new features on security and privacy: new threats, existing solutions, and challenges yet to be solved. IEEE Internet Things J 6(2):1606–1616
3. Kolias C, Kambourakis G, Stavrou A, Voas J (2017) DDoS in the IoT: Mirai and other botnets. Computer 50(7):80–84
4. https://securityintelligence.com/posts/i-cant-believe-mirais-tracking-the-infamous-iot-malware-2/. Last accessed 2020/1/28
5. Lee JH, Kim H (2017) Security and privacy challenges in the internet of things (security and privacy matters). IEEE Consum Electron Mag 6(3):134–136
6. Salim MM, Rathore S, Park JH (2019) Distributed denial of service attacks and its defenses in IoT: a survey. J Supercomputing 1–44
7. https://www.trendmicro.com/vinfo/in/security/news/internet-of-things/into-the-battlefield-a-security-guide-to-iot-botnets. Last accessed 2020/1/28
8. Vishwakarma R, Jain AK (2020) A survey of DDoS attacking techniques and defence mechanisms in the IoT network. Telecommun Syst 73(1):3–25
9. Alert (TA18-331A) 3ve—Major online Ad fraud operation. https://www.us-cert.gov/ncas/alerts/TA18-331A
10. https://securelist.com/ddos-report-q2-2019/91934/. Last accessed 2020/1/29
11. Koroniotis N, Moustafa N, Sitnikova E, Turnbull B (2019) Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset. Future Gener Comput Syst 100:779–796
12. Ge M, Fu X, Syed N, Baig Z, Teo G, Robles-Kelly A (2019) Deep learning-based intrusion detection for IoT networks. In: IEEE 24th pacific Rim international symposium on dependable computing (PRDC), pp 256–25609. IEEE
13. McDermott CD, Majdani F, Petrovski AV (2018) Botnet detection in the internet of things using deep learning approaches. In: 2018 International joint conference on neural networks (IJCNN), pp 1–8. IEEE
14. Canedo J, Skjellum A (2016) Using machine learning to secure IoT systems. In: 14th Annual conference on privacy, security and trust (PST), pp 219–222. IEEE
15. Haddadi F, Khanchi S, Shetabi M, Derhami V (2010) Intrusion detection and attack classification using feed-forward neural network. In: 2010 Second international conference on computer and network technology, pp 262–266. IEEE
16. Su J, Vasconcellos VD, Prasad S, Daniele S, Feng Y, Sakurai K (2018) Lightweight classification of IoT malware based on image recognition. In: IEEE 42nd annual computer software and applications conference (COMPSAC), vol 2, pp 664–669. IEEE
17. Yuan X, Li C, Li X (2017) DeepDefense: identifying DDoS attack via deep learning. In: IEEE International conference on smart computing (SMARTCOMP), pp 1–8. IEEE
18. https://www.cloudflare.com/learning/ddos/ddos-mitigation/. Last accessed 2020/2/4
19. Alpaydin E (2009) Introduction to machine learning. MIT Press, Cambridge