DDoS Attack Detection using Artificial Neural Network on IoT Devices in a Simulated Environment

Ankit Khatri[1] and Ravi Khatri[2]

[1] Dr B R Ambedkar National Institute of Technology Jalandhar, Punjab, India
[2] Dr B R Ambedkar National Institute of Technology Jalandhar, Punjab, India
ankitk.cs.21@nitj.ac.in, ravik.cs.21@nitj.ac.in

Abstract. The Internet has expanded a lot in terms of its geographical coverage as well as its accessibility, since its inception in the late 20th century. With its rise, the number of devices connected with it are also increasing, especially with the advent of Internet of Things. IoT devices are being utilized in a variety of applications and nowadays, they form the base of crucial Infrastructure of a country as well, due to which they are becoming prime targets to being hacked and attacked for malicious purposes. DoS is one such attack which disrupts the accessibility to the server, restricting access to it for the legitimate users. When it is carried out simultaneously by multiple devices (bots) then the attack is called the DDoS (Distributed denial of service) attack. Due to the increasing vulnerability of IoT devices to such attacks and the impact of them in today's digitized world, it has gathered attention of researchers in this problem domain in the recent past. In this paper, we have focused on the role of Deep Learning for this task. We have proposed an Invasion Detection System based on Machine Learning which leverages the ANN (Artificial Neural Networks) for combating such attacks. The ANN is trained on IP traces data to classify safe and hostile packets, and based on this knowledge it is able to detect a DDoS attack. This framework is tried out in a simulated IoT Environment and is able to achieve significant accuracy.

Keywords: DDoS, Deep Learning, ANN, IoT

1 Introduction

Internet of Things is a Technology which has found applications in a variety of areas [1] and has transformed industries too. It has revolutionized the industries such as Food Production, Health, Manufacturing, etc. and is deeply influencing our lives too. Apart from these industries, it has also become a crucial part of what we call the Critical Infrastructure of a country. Due to its such vast applications, it has also attracted the threat of attacks which can immensely impact the socio-economic security of the nation and also intrude the privacy of its citizens.

IoT basically consists of a network of devices interconnected with each other, the cloud servers and the internal system. These devices collect data which are then sent further for various analysis. With the rise of the Internet, the count of such interconnected devices over the network are also on a high and are thus becoming an influential part of our daily lives. According to some reports [2], the count of such devices is

increasing continuously and is expected to rise by a significant amount in coming years as well.

As the IoT devices use batteries as their source of power [3], they have low processing capabilities. It leads to a lack of security and required defense against Cyber-attacks. The number of attacks on IoT have increased immensely in the recent past. The Attackers generally prefer IoT for performing the assault for a variety of reasons, which puts him/her in a position of advantage.

The attacker may have different motives. The attack may be performed for personal gains, state sponsored assault, business rivalry, etc. These attackers may belong to the same network which is being compromised or may belong to an external network. The difference being, the internal ones [4] have the access and privileges to easily carry out such an attack, whereas the external ones [4] usually carry out the attacks by exploiting the system using malware.

There are a variety of attacks that can be performed on IoT devices which can paralyze the functioning of critical sectors of a nation, and can even lead to war among the conflicting parties. These attacks however can be detected using a variety of means [5].

The assaults on such devices [6] can be User's Privacy Infringement, Malware attack such as Mirai, DoS attacks, Physical tampering, Ransomware attacks, etc.

In this paper, we tackle the menace caused by DDoS attacks which are targeted upon the IoT equipment by providing an IDS centered on the use of Machine Learning. In DDoS attacks, the attacker floods the target host with a massive amount of traffic [7] with an aim to restrict its access for the legitimate users. Various DDoS attacks have occurred in the recent past which have immensely impacted various Big MNCs [8]. For example, the GitHub attack of 2015 [9], Dyn attack [10], the attack on University of Minnesota [11], Websites getting crashed during an uprising in Turkey [12], attack on the White House website [13], etc.

To detect and mitigate such attacks Invasion detection systems are deployed. These systems have existed since the late 20th century and perform their intended task of monitoring the networks for such attacks using various methodologies that evolve continuously with time such as, Machine Learning based Invasion Detection systems, as proposed by [14].

We have discussed an Artificial Neural Network Based IDS in this paper. Our proposed algorithm sniffs the incoming traffic packets, which is then sent to the trained model of ANN for classification of these packets into safe or hostile. The source IP addresses of hostile packets are also revealed for further action.

In this paper, we have discussed various concepts and terminologies in Section 2. In Section 3, we have mentioned the related works. Our Proposed methodology is discussed in Section 4, followed by the observations and results in Section 5. Finally, we have concluded this paper is Section 6.

2 Basic Concepts and Terminologies

2.1 Artificial Neural Networks

In ANN [15] we try to replicate the working of a real human brain. A real human brain contains a huge network of neurons which are interconnected to each other. These neurons are responsible for transferring the impulses from the brain to different parts of the body and vice-versa. In ANN we replicate this process with the use of several layers like an input layer, one or many hidden layers and at the end there is an output layer. The first layer i.e. Input is responsible for taking the inputs either from the user or the environment and passing these inputs onto the next layer. The hidden layers are responsible for performing a mathematical computation of the inputs and the weights associated with the inputs. Then the weighted inputs are passed to an Activation Function which basically transforms the output as per the function used and also tells which node would fire and which node would not fire. Finally, we get the desired output through the output layer. ANNs can be used for various problems like Regression, classification, image recognition etc. We have several advantages of using an ANN like it can perform multiple tasks simultaneously, node failure doesn't result in failure of the whole network, whole of the data is stored within the network, ANN have the ability of giving the results even with incomplete information, etc.

2.2 Invasion Detection System

Invasion to any system refers to gaining unauthorized access to it by a perpetrator with a motive to intrude on the privacy of the network. There may be various types of such intruders, which are broadly categorized into three classes. First one is the Masqueraders who don't have any privileges to access a particular system, but gain such an access by illegitimate means. Second, the Misfeasors, who may be some internal user who misuses the privileges or gains unauthorized access. Third ones are the Clandestine Users who use the credentials of privileged access people of the same network, to steal confidential information [16].
Invasion Detection Systems [17] could be categorized into 2 categories:

- Host Based Invasion Detection System - The Host System is equipped with software-based tools that can analyze and observe all the activities in the system and for possible intruders.
- Network Based Invasion Detection System - The traffic flow is monitored on the complete network to check for possible malicious users trying to intrude in the network by illegitimate means.

The comparison of these Invasion Detection Systems based on certain performance measures are shown in Table I.

These Systems can detect potential threats by identifying patterns which are based on Misuse and Anomaly Invasion. Various methodologies are known for Invasion Detection. Few most widely used ones are based on Statistical Analysis [18], Rule based

Detection [19], Artificial Neural Networks, Protocol Verification [20], etc. In this Paper, we have proposed an Artificial Neural Network based IDS which is trained to effectively classify safe and hostile packets based on the patterns detected in such flooding attacks.

As the IoT devices have limited capacity in terms of storage and computational power, standard IDS may not be suitable for them which are otherwise suitable for highly complex environments. Recent works on the dataset used in The KDD Competition, have shown the potential of using Machine Learning for Invasion detection.

Table 1. Comparison of performance of HIDS and NIDS [21]

Host-based IDS	**Network-based IDS**
Performs well at analyzing the traffic to perceive possible threats	Performs well in analyzing the traffic to perceive possible threats
It performs better for the detection of internal perpetrators	It performs better for the detection of external perpetrators
Performs good in analyzing the magnitude of the damage	Performs poorly in analyzing the magnitude of the damage
Poor reaction to real time threats, but works better for persistent ones	Strong reaction to real time threats
Best for detecting internal intruders	Best for detecting external intruders

2.3 DDoS (Distributed Denial-of-service) attack

In such an attack, numerous systems are utilized to carry out the attack on the target host. It is faster than the DoS attack and difficult to block and trace as well, due to its nature being distributed, i.e. packets are coming simultaneously from multiple devices and from different geographical locations as well. The volume of such attacks is also huge when compared to DoS attacks. These attacks can be classified as Application Layer, Protocol based and Volumetric based attacks. Some of the most common DDoS attacks are - SYN Flood, DNS Amplification, UTP Flood, etc.

3 Literature Review

The term Internet of Things was coined by Kevin Ashton of MIT' in 1999. However, it is yet to reach its maturity level. Numerous researches have already been done in this domain that have contributed immensely for its expansion. A few literature Surveys are as follows:

Kasinathan P. et al. [22] in his IEEE research paper written in 2013 explores "flood attack in an IoT environment". They had proposed a scheme which uses an Invasion detection system to detect the attacks. In their paper they have focused on detecting the UDP flood attacks on the IoT environment. The solution which they proposed was implemented for creating a network-based IDS. They designed a network manager which detected hostile packets based on parameters defined.

Misra et al. [23] developed "A learning automata-based solution to DDoS attacks in IoT networks" in 2011.They developed an architecture that was service-oriented to

shape their solution. It was an automata-based solution. The framework was defined to automatically select the best choice. The drawback of this solution was that no real implementation was done.

Hodo et al. [24] in his paper “Threat analysis of IoT networks Using Artificial Neural Network Invasion Detection System " has shown how ANN could be used in Invasion Detection System. The Model showed a significant accuracy of 99.4 %. It demonstrated that the ANN Algorithm could successfully be used in IDS. However, it lacked any insight on how to prevent such an attack if detected.

Tseung et al. [25] proposed a solution which used the power of Machine Learning along with an auto-learning Bloom Filter to identify and mitigate the DDoS attacks targeted on a network. They have used multiple feature selection and extraction algorithms of Machine Learning like Linear SVM, ANOVA to assess the incoming data packets and extract important features from them. Then the extracted features are kept in a customized feature list. The input data packets and the extracted information associated with them are given to the auto-learning Bloom Filter which identifies and classifies the incoming data packets as Malicious or not. In this way both Machine Learning and Bloom Filter are used to identify such attacks and defend them. There is an issue associated with their approach i.e. the solution proposed by them is not cost-efficient because the feature selection approach used is very computationally expensive, hence may not be suitable for an IoT environment.

Zekri et al. [26] have proposed a machine learning based solution to identify DDoS attacks in a cloud computing environment. They have used the C.4.5 algorithm to design an Invasion Detection System to identify such attacks on a cloud-based environment. They have also used the combination of C.4.5 algorithm with signature identification methods for efficient identification of signatures attacks. A decision tree is generated to automatically and effectively detect such attacks targeted on the cloud environment.

A Support vector machine based detection methodology was proposed by Liao et al. [27]. Their proposed scheme focuses on the similarity among the devices that are part of the Zombie network and carrying out the attack. The request patterns of users are stored and analyzed to detect similarities.

A K-Nearest Neighbor based DDoS attack detection framework was proposed by Xiao et al. [28]. Their methodology is based on the assumption that similar bots and softwares will generate identical traffic. But, one restriction of their study is that even non identical traffic flows can be generated by similar bots.

ANN is used for detection of DDoS attacks in the study conducted by Jie-Hao et al. [29]. They have compared its performance with various other machine learning models. The user traffic is checked for aberrations by the neural network.

The Detection methodology proposed by [30] is based on the analysis of traffic by Radial basis function neural networks. This categorizes the traffic into safe or hostile. The source IP addresses of the hostile traffic are then sent to a different module for filtering. A FCM Cluster Algorithm based methodology is proposed by [31]. A Decision Tree based solution is put forward by [32], which observes the traffic flow to classify safe and hostile packets. Moreover, it also describes the packet flow pattern as well.

An Invasion Prevention System is developed by Li et al. [33], which uses SVM in addition with SNORT so that the accuracy of the overall system is improved.

A different type of neural network is used by Liu et al. [34] which finds applications in areas such as classification, data compression, pattern identification, etc. Here the Data is fed to the neural network in numeral form, which then classifies the packets as safe or malicious and takes further actions. The information about the protocols that are present in the packets are analyzed by a data mining algorithm in the detection scheme proposed by [35].

4 Proposed Methodology

We shall emulate the scenario shown in Fig.1 where IoT devices are connected. A bot shall be created to carry out DDoS Attack on these devices. The server device shall be equipped with DDoS Network Intrusion Detection System to detect the DDoS attack. The IDS would be based on Deep Learning (Artificial Neural Networks), a multilayer perceptron. Our discussed approach uses a simple ANN, the structure of which is depicted in detail below. The server will keep on analyzing the incoming traffic. The ANN will receive the input data through Wireshark with different parameters (Highest layer, Transport layer, Source IP address, Destination IP, Source port, destination port, packet length, target). Once the attack has been carried out on the device, the input data will be analyzed by the trained model of ANN. The input data packets will be analyzed and classified as hostile or normal packets that will define whether the traffic is DDoS traffic or normal traffic. The parameters have been fine-tuned multiple times, so as to achieve a better accuracy. Further details are discussed in the implementation section in a much more detailed manner.

Our Algorithm is trained to classify the number of safe and hostile packets, and based on this knowledge it is able to detect a DDoS attack. This knowledge of having the hostile packets already, the algorithm further exposes the source IP addresses, from where these packets are coming from.

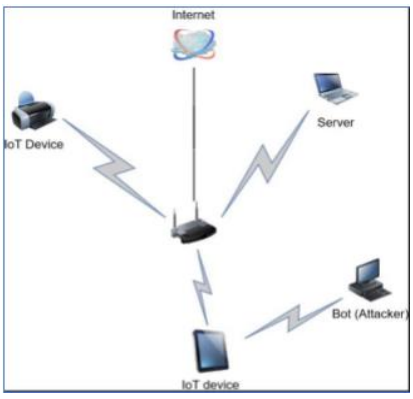

Fig. 1. Depiction of attack on IoT devices in a simulated environment

4.1 Detailed Configuration of our model

A Regular Perceptron is being used by us, which is developed using TensorFlow. We have increased the width of our model to achieve better results. Our Proposed model has the following parameters.
Configuration:

- Layer (Hidden 1): [50 neurons] Fully Connected Layer
- Layer (Hidden 2): [50 neurons] Fully Connected
- Layer (Hidden 3): [50 neurons] Fully Connected
- Output Layer: [2 neurons] One Hot Encoding Layer
- Initialization of the weights: Random / Normal

Activation Function used:
- Hidden Layers: ReLU
- Output Layer: Softmax function

4.2 Workflow and algorithms of Our Proposed methodology

The workflow of our proposed system would include the following parts,

- Sniffing the incoming traffic
- Collecting the Data (Real Time)
- Training our ANN
- Viewing our Data
- Analyzing the Real-Time Traffic
- Graphical presentation of our Model's Architecture

We have trained our model in 30 epochs of 15,000 iterations each. The workflow of our proposed system includes the following phases:

- Sniffing the incoming traffic
  This model captures the packets in real-time and shows detailed information about each of them. We have included the necessary details that need to be displayed in order to analyze the traffic. The Algorithm for that is depicted below in Fig. 2
- Neural Network Trainer
  This algorithm deals with collecting the data at real time and then using that data to train our neural network. Data collected is saved in a file named Data.csv which trains our Artificial Neural Network (ANN). The Algorithm for that is depicted below in Fig. 4
- Real Time Prediction
  This algorithm reads the Live Data csv file and it classifies the traffic as malicious (DDoS) or secure based on our already trained model. This model then prints the Results/Observations using a confusion matrix and classification report. The Algorithm for that is depicted below in Fig. 3

Algorithm 1: Capturing Packets (Sniffing)

This model captures the packets in real-time and shows detailed information about each of them.

Start

```
1.For pkts in capture
2.    If (pkts.TopLayer != 'ARP'):
3.        ip_add = None
4.        ip_layer_name = get_ip_layer_name(pkt)
5.        If (ip_layer_name == 4):
6.            ip_add = pkts.ip_add
7.            End If
8.        Else If (ip_layer_name == 6):
9.            ip_add = pkts.ipv6addr
10.       Display the details about each packet captured
11.           pkt.Top_Layer
12.           packet.trnsprt_layer_name
13.           Time Taken
14.           Layers
15.           Source IP
16.           Destination IP
17.           Length of the Packet
18.       Try displaying Source and Destination Port
19.           Source Port
20.           Destination Port
21.       Except AttributeError
22.           Source Port
23.           Destination Port
24.           End If
25.   Else
26.           ARP = pkt.arp
27.           Display the packet information
28.           End Else
```

Stop

Fig. 2. Algorithm for packet sniffing

Algorithm 3:Real Time Prediction

#This model is used for classifying the traffic as DDoS or normal traffic.This is not used for training purposes.

Input: [Already Saved model, if user wishes to load existing model]

Start

```
1.User inputs name of the Data File.
2.Process the Data (Live Label Encoding)
3.Print the data for viewing
4.Load model and model coefficients
5.predicted_result = model.predict(Input Data)
6.malicious,secure = 0
7.For c in predicted_results :
8.  If c == 1: # replace it as zero so that DDoS attack can be forced
9.          increment malicious packets
10. Else:
11.         increment secure packets
12.         End If
13.   print secure and malicious packets
14.   If No.of malicious Packets > Sum of Both/2 :
15.    print Attack Detected
16.  Else:
17.           print Normal Activity Detected
18.  End If
19. print Confusion Matrix
20. print Classification Report
```

Stop

Fig. 3. Real Time prediction of DDoS attack by an ANN

Algorithm 2: Data collector

```
## This trains our Artificial Neural Network(ANN).

Input: [Already Saved model,  if user wishes to load existing model]


Start
1.User inputs name of Saved Model file
2.Ask user if they want to train a saved algorithm, if no, the new model is created and trained
3.If(load _model== 'Y'):
4.    train= Load_model_saved()
5.    End If
6.Else
7.  Imports the Neural Network Class from Sci-kit learn
8.  train= Classifier(size_of_hidden_layer,activation_function,iter_max,verbose,toI)
    # Setting the parameters of our classifier
    #size_of_hidden_layer = layers that are hidden in the neural net, (6) = single layer 6, (6,6) = Two layers,
each having 6 nodes
    #activation_function = activation function, 'logistic' is equivalent of the sigmoid activation function
    #iter_max = maximum amount of iterations that the model will do
    #Verbose = whether the model prints the iteration and loss function per iteration
    #tol = the decimal place the user wants the loss function to reach
9.Read CSV

#Neural Net Training
12.X =Input (Independent Variables)
13.Y = Dependent Variable
14.Train the model
15.Display predictions
16.malicious = 0, secure = 0
17.For c in predicted_results:
18.         If(c == 1):
19.              increment malicious packets
20.              End If
21.           Else:
22.              increment secure packets
23.              End Else;
24Display secure Packets and malicious Packets
25.Display confusion matrix
27.Store model?
28.If true: then Store Model


Stop
```

Fig. 4. Data collection and training of the neural network

5 Observations and Results

The project consists of two phases: First is the DDoS attack which is performed on an IoT device in a Simulated Environment. And second is its Detection using Deep Learning. The DDoS attacks that we have performed are TCP SYN, Slow Loris, UDP Flood. And each attack is able to take our server down and make the services unavailable to the User. We have achieved satisfactory results in this phase. The test results and the confusion matrix are shown in Fig. 5 and Fig. 6 respectively. Fig. 7 shows the data flow diagram of our proposed methodology.

```
Safe Packets:  162533
Hostile Packets:  99578
Time Taken: 11.340712799999991
Confusion Matrix:
 [[162383    162]
 [   150  99416]]
```

Fig. 5. Confusion matrix

	Control	Normal	TCP	UDP	Combined (TCP)	Combined (UDP)
Total Packets	0	5171	260	21963	11748	15482
Safe	0	5167	0	1	11624	6667
Hostile	0	4	260	21962	124	8815
Percentage	0	0.077354	100	99.99545	1.055498808	56.93708823
DDoS detected	0	0	1	1	0	1
DDoS in Action	0	0	1	1	1	0

Fig. 6. DDoS detection test results

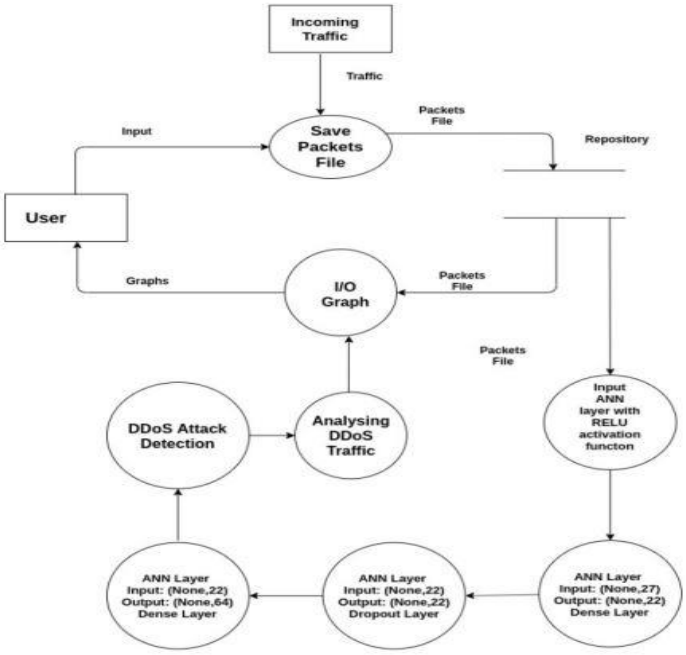

Fig. 7. Data Flow diagram of our proposed methodology

6 Conclusion

The simulated environment we have created successfully performs DDOS Identification and prevention. The ANN could accurately perform and detect SYN flooding attacks with a significant accuracy. The future plans could include modifying this algorithm to identify other DDoS attacks. Moreover, the simulated environment can also showcase methods to filter hostile IP addresses and redirect them to other/fake addresses. Apart from that mitigation strategies can be used, such as blocking the hostile IP addresses using techniques like Bloom Filter. Although, we have detected DDoS

attacks using an ANN in a simulated environment, a real implementation can easily be extracted from this emulation and could be applied in real scenarios.

References

1. Jain, Deeksha & Krishna, P. & Saritha, V.. (2012). A Study on Internet of Things based Applications.
2. D. Evans, “The Internet of Things - How the Next Evolution of the Internet is Changing Everything,” CISCO white Pap., no. April, pp. 1–11, 2011.
3. A. Iqbal, M. A. Suryani, R. Saleem, and M. A. Suryani, “Internet of things (IoT): On-going security challenges and risks,” Int. J. Comput. Sci. Inf. Secur., vol. 14, no. 11, p. 671, 2016.
4. J. Shun and H. a. Malki, “Network Intrusion Detection System Using Neural Networks,” 2008 Fourth Int. Conf. Nat. Comput., vol. 5, pp. 242–246, 2008.
5. SANS institute, “InfoSec Reading Room tu , Application of Neural Networks to Intrusion Detection,” 2001.
6. “Internet of Things: How Much Are We Exposed to Cyber Threats? - InfoSec Resources.” [Online].Available:http://resources.infosecinstitute.com/internet-thingsmuch-exposed-cyber-threats/. [Accessed: 10-Dec2015].
7. S. Sharwood. Github wobbles under ddos attack. http://www.theregister.co.uk/2015/08/26/github_wobbles_under_ddos_attack/, Aug 2015. Accessed: 2018-06-20.
8. L. Garber. Denial-of-service attacks rip the internet. Computer, 33(4):12–17, 2000.
9. The Github Attack, 2015 https://www.wired.com/story/github-ddos-memcached/
10. Ademola, Ojo. (2021). Dyn DDoS Cyber Attack: A Position Paper. 13-20. 10.22624/AIMS/MATHS/V9N1P2.
11. G. C. Kessler. Defenses against distributed denial of service attacks. SANS Institute, 2002, 2000.
12. S. Simpson, S. N. Shirazi, A. Marnerides, S. Jouet, D. Pezaros, and D. Hutchison. An inter-domain collaboration scheme to remedy ddos attacks in computer networks. IEEE Transactions on Network and Service Management, pages 1–1, 2018.
13. D. Evans and D. Larochelle. Improving security using extensible lightweight static analysis. IEEE software, 19(1):42–51, 2002.
14. N. T. T. Van and T. N. Thinh, “Accelerating Anomaly-Based IDS Using Neural Network on GPU,” in 2015 International Conference on Advanced Computing and Applications (ACOMP), 2015, pp. 67– 74.
15. M. Mishra and M. Srivastava, "A view of Artificial Neural Network," 2014 International Conference on Advances in Engineering & Technology Research (ICAETR - 2014), 2014, pp. 1-3, doi: 10.1109/ICAETR.2014.7012785.
16. “What it is Network intrusion detection system? | COMBOFIX.” [Online]. Available: http://www.combofix.org/what-it-is-networkintrusion-detection-system.php. [Accessed: 10-Dec2015].
17. SANS institute, “InfoSec Reading Room tu , Application of Neural Networks to Intrusion Detection,” 2001.
18. J. Shun and H. a. Malki, “Network Intrusion Detection System Using Neural Networks,” 2008 Fourth Int. Conf. Nat. Comput., vol. 5, pp. 242–246, 2008.
19. X. J. A. Bellekens, C. Tachtatzis, R. C. Atkinson, C. Renfrew, and T. Kirkham, “A Highly-Efficient Memory-Compression Scheme for GPU-Accelerated Intrusion Detection Systems,” Proc. 7th Int. Conf. Secur. Inf. Networks - SIN ’14, pp. 302–309, 2014.

20. T. Verwoerd and R. Hunt, Intrusion detection techniques and approaches, vol. 25, no. 15. 2002.
21. H. Kozushko, “Intrusion detection: Host-based and network-based intrusion detection systems,” Sept., vol. 11, 2003.
22. Kasinathan P, et al. "Denial-of-Service detection in 6LoWPAN based Internet of Things." 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). IEEE, 2013.
23. S. Misra, P. V. Krishna, H. Agarwal, A. Saxena and M. S. Obaidat, "A Learning Automata Based Solution for Preventing Distributed Denial of Service in Internet of Things," 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, Dalian, 2011, pp. 114- 122.
24. E. Hodo et al., "Threat analysis of IoT networks using artificial neural network intrusion detection system," 2016 International Symposium on Networks, Computers and Communications (ISNCC), Yasmine Hammamet, 2016, pp. 1-6. doi:10.1109/ISNCC.2016.7746067
25. C. Tseung, K. Chow, and X. Zhang. Anti-ddos technique using self- learning bloom filter. In Intelligence and Security Informatics (ISI), 2017 IEEE International Conference on, pages 204–204. IEEE, 2017.
26. M. Zekri, S. E. Kafhali, N. Aboutabit and Y. Saadi, "DDoS attack detection using machine learning techniques in cloud computing environments," 2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech), 2017, pp. 1-7, doi: 10.1109/CloudTech.2017.8284731.
27. Q. Liao, H. Li, S. Kang, and C. Liu, “Application layer ddos attack detection using cluster with label based on sparse vector decomposition and rhythm matching,” Security and Communication Networks, vol. 8, no. 17, pp. 3111–3120, 2015.
28. P. Xiao, W. Qu, H. Qi, and Z. Li, “Detecting ddos attacks against data center with correlation analysis,” Computer Communications, vol. 67, pp. 66–74, 2015.
29. Jie-Hao, C.; Feng-Jiao, C.; Zhang. (2012) “DDoS defense system with test and neural network”. IEEE International Conference on Granular Computing (GrC), 11-13 Aug. 2012, Hangzhou, China, pp. 38 – 43.
30. R. Karimazad and A. Faraahi, “An anomaly-based method for ddos attacks detection using rbf neural networks,” in Proceedings of the International Conference on Network and Electronics Engineering, 2011, pp. 16–18.
31. R. Zhong and G. Yue, “Ddos detection system based on data mining,” in Proceedings of the 2nd International Symposium on Networking and Network Security, Jinggangshan, China, 2010, pp. 2–4
32. Y.-C. Wu, H.-R. Tseng, W. Yang, and R.-H. Jan, “Ddos detection and traceback with decision tree and grey relational analysis,” International Journal of Ad Hoc and Ubiquitous Computing, vol. 7, no. 2, pp. 121– 136, 2011.
33. H. Li and D. Liu, “Research on intelligent intrusion prevention system based on snort,” in International Conference on Computer, Mechatronics, Control and Electronic Engineering (CMCE), vol. 1. IEEE, 2010, pp. 251–253.
34. J. Li, Y. Liu, and L. Gu, “Ddos attack detection based on neural network,” in 2nd International Symposium on Aware Computing (ISAC),. IEEE, 2010, pp. 196–199
35. N. Gao, D.-G. Feng, and J. Xiang, “A data-mining based dos detection technique.” Jisuanji Xuebao(Chinese Journal of Computers), vol. 29, no. 6, pp. 944–951, 2006.