International Journal of Research in Engineering, Science and Management
Volume-2, Issue-10, October-2019
www.ijresm.com | ISSN (Online): 2581-5792

Detection of DoS and DDoS Attacks using Neural Network

Tuhina Jayanta Banerjee[1], Seema Shah[2]

[1]*Student, Department of Computer Science Engineering, Mukesh Patel School of Technology Management and Engineering, NMIMS University, Mumbai, India*

[2]*Professor & Chair Person, Department of Computer Science Engineering, Mukesh Patel School of Technology Management and Engineering, NMIMS University, Mumbai, India*

***Abstract*: In this paper, there are many techniques reviewed which detects the Denial of Services (DoS) attack and Distributed Denial of Services (DDoS) attack over a network, server or device and the new technique of detection of DoS and DDoS using neural network is proposed. In DoS and DDoS attacks, the attacker may not have any specific mindset to manipulate or steal the data, but these attacks can lead to volume traffic which will lead to the denial of service for the legitimate user. Neural network is known for its effectiveness and efficiency and is quite comprehensive which proves to be one of the reliable techniques in the aspect of detection. The model proposed can predict the trend of normal network traffic, identify the abnormal traffic caused by DDoS and DoS hit over a network.**

***Keywords*: Denial of Service attack, Distributed Denial of Service attack, Neural Network, Detection**

1. Introduction

The intensive growth of computer networks has led to the growth of the internet environment too. This growth of internet environment has led to a massive cybersecurity issue. Cybersecurity could be an issue targeted to any electronic information system, infrastructure, computer network or personal computer equipment using a variety of methods to hack, change or kill data or information system. Cybersecurity leads to a great loss at times, for an organization or individual. According to [1], the second quarter of 2019 appeared to be richer than the first in terms of high-profile Distributed Denial of Service (DDoS) attacks. The need for a defense against Denial of Service attacks is gaining its importance and it's a difficult task at the same time.

A DoS is a technique in cyber-attack where the genuine users are unable to access data or other resources and tools due to the actions of a malicious activities. Unlike other kinds of attacks, the primary motive of a DoS attack is not to steal information but to slow or take a website down. An attack method of denial of service can be achieved with the use of only one computer. One of the most common threats to IT security are DoS and DDoS. These attacks can be carried out by individual as well as organized group, so-called "hacktivists", since they do not require major resources.

Using several computers and internet connections, network attacks overwhelm the target asset. DDoS attacks are often global attacks that are spread via botnets. Botnets are just a group of computers used to send huge amounts of requests, simultaneously changes generate many source IP addresses to prevent the routing, identification and any blockage. Distributed Denial of Service attack is quiet an achieving for the attacker as the botnets can generate and send huge amounts of requests at the same which will make the server at the victim side to crash, this feature of DDoS makes the detection of DDoS complicated yet necessary to prevent any further malicious disrupts.

Nowadays every computer can easily get connected to the cloud which is preferable in terms of storage and security. The cloud storage allows to store a huge amount of data, this has also given the attackers the confidence to penetrate in the network and make it busy for the other legitimate users. This led to a great terror for the organizations as this might result in degraded reputation of an organization. As the dealing is with the data the security is the first concern taken care for.

Neural networks are the information processing systems that are designed and implemented to mimic the human brain. The main objective of neural network research is to create a computational brain modeling tool to perform different computational task at a faster rate than traditional system [10]. On the other hand, if we talk about the neural networks one of its advantages is to handle variant data set. So, the combination of neural network and cybersecurity in terms of detecting the attack can prove to be a best combination as in during the training period we can analyze the model by applying a huge number of data set and its combination. This data set can include a data packet's signature inputs.

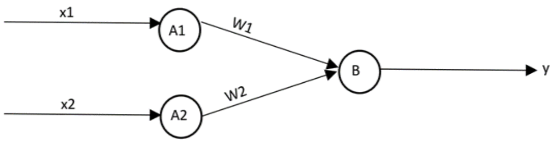


Fig. 1. Architecture of a neural network

Fig. 1, shows the simple architecture of a neural network.

In Section II, the related work of the referred papers which uses different methods of detection of attacks and the overview regarding the topic and the technology of the proposed method is discussed. Section III is an overview of DoS and DDoS it's challenges and effects. Section IV specifies the role of neural network. Section V gives the proposed method to detect the attack using a neural network. Section VI discusses the proposed method and section VII gives the conclusion.

2. Related work

Haining Wang [2], proposed a simple and robust mechanism, called change-point monitoring (CPM), to detect denial of service (DOS) attacks. The core of CPM is based on the inherent network protocol behavior and is an instance of the sequential change point detection. To make the detection mechanism insensitive to sites and traffic patterns, a nonparametric cumulative sum (CUSUM) method is applied, thus making the detection mechanism robust, more generally applicable, and its deployment much easier. CPM does not require per-flow state information and only introduces a few variables to record the protocol behavior.

Mallesham Dasari [3] proposed a real time detection of Medium Access Control (MAC) layer attacks in IEEE 802.11 wireless networks. There can be different kinds of Denial of Service (DOS) attacks observed at the MAC layer such as misbehavior and selfish attacks. The malicious nodes manipulate the MAC protocol parameters such as a back-off time, network allocation vector value and short inter frame space, or flood the network with huge volume of dummy packets. With this, the attacker's node captures entire network bandwidth causing legitimate nodes not communicate with other nodes, consequently decreasing the throughput of the nodes significantly.

Ms. Supriya S. Thakare [4] proposed a system that makes use of multivariate correlation analysis (MCA) technique which extracts the geometrical correlation between network traffic. This geometrical correlation is used for detecting DoS attack. Triangle area-based technique to used enhance and speedup the MCA process. KDD cup 99 dataset is for examining the effectiveness of the proposed system. To increase the detection rate and to reduce the complexity of the proposed system a subset of features of the record is used. This subset is used in the whole detection process.

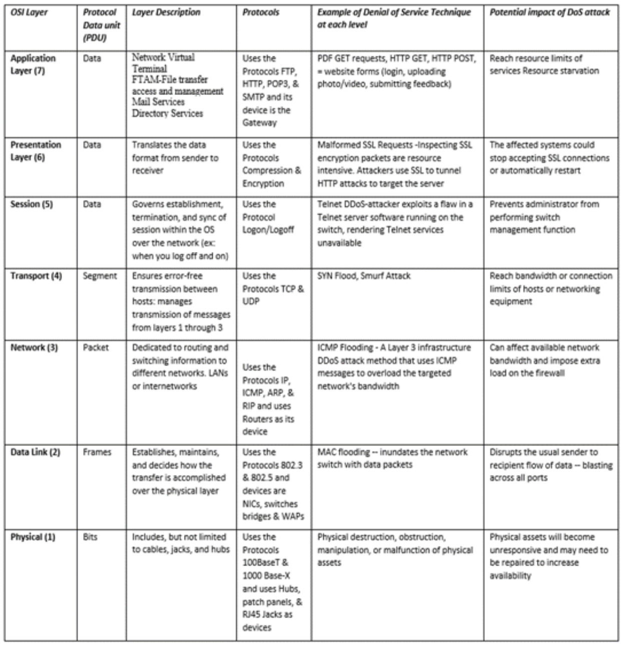
Rajendra Patil [5], proposed a design an efficient security framework which is protocol specific Multithreaded Network Intrusion Detection System (PM-NIDS) aiming at detecting DoS/DDoS attacks in the cloud. Here, the incoming packets are separated according to the protocol and queued for further processing.

M. Maheshwari [6], proposed an Attacked Packet Detection Algorithm (APDA) which is used to detect the DOS (Denial-of-Service) attacks before the verification time. It minimizes the overhead delay for processing and enhances the security in VANET.

There are various such techniques used to detect DoS and DDoS attack over network, device or sever. This paper uses neural network for the detection of DoS and DDoS.

3. Overview of DoS AND DDoS attacks

DoS and DDoS can hit at any layer of the OSI (Open System Interconnection) model with different type of attacks. OSI model is a model that characterizes and standardizes the communication functions in a telecommunication network. After attack there is an impact at the victim side (the server, host or the device).



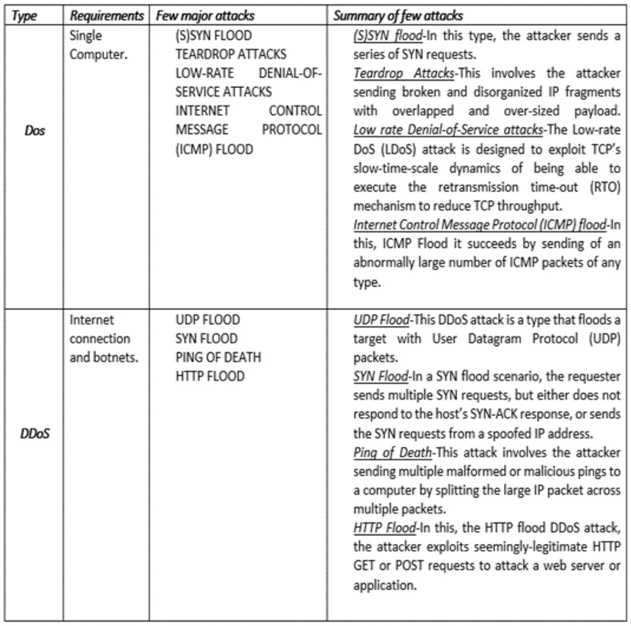
OSI Layer	*Protocol Data unit (PDU)*	*Layer Description*	*Protocols*	*Example of Denial of Service Technique at each level*	*Potential impact of DoS attack*
Application Layer (7)	Data	Network Virtual Terminal FTAM-File transfer access and management Mail Services Directory Services	Uses the Protocols FTP, HTTP, POP3, & SMTP and its device is the Gateway	PDF GET requests, HTTP GET, HTTP POST, = website forms (login, uploading photo/video, submitting feedback)	Reach resource limits of services Resource starvation
Presentation Layer (6)	Data	Translates the data format from sender to receiver	Uses the Protocols Compression & Encryption	Malformed SSL Requests -Inspecting SSL encryption packets are resource intensive. Attackers use SSL to tunnel HTTP attacks to target the server	The affected systems could stop accepting SSL connections or automatically restart
Session (5)	Data	Governs establishment, termination, and sync of session within the OS over the network (ex: when you log off and on)	Uses the Protocol Logon/Logoff	Telnet DDoS-attacker exploits a flaw in a Telnet server software running on the switch, rendering Telnet services unavailable	Prevents administrator from performing switch management function
Transport (4)	Segment	Ensures error-free transmission between hosts: manages transmission of messages from layers 1 through 3	Uses the Protocols TCP & UDP	SYN Flood, Smurf Attack	Reach bandwidth or connection limits of hosts or networking equipment
Network (3)	Packet	Dedicated to routing and switching information to different networks. LANs or internetworks	Uses the Protocols IP, ICMP, ARP, & RIP and uses Routers as its device	ICMP Flooding - A Layer 3 infrastructure DDoS attack method that uses ICMP messages to overload the targeted network's bandwidth	Can affect available network bandwidth and impose extra load on the firewall
Data Link (2)	Frames	Establishes, maintains, and decides how the transfer is accomplished over the physical layer	Uses the Protocols 802.3 & 802.5 and devices are NICs, switches bridges & WAPs	MAC flooding -- inundates the network switch with data packets	Disrupts the usual sender to recipient flow of data -- blasting across all ports
Physical (1)	Bits	Includes, but not limited to cables, jacks, and hubs	Uses the Protocols 100BaseT & 1000 Base-X and uses Hubs, patch panels, & RJ45 Jacks as devices	Physical destruction, obstruction, manipulation, or malfunction of physical assets	Physical assets will become unresponsive and may need to be repaired to increase availability

Fig. 2. Attack possibilities

Fig. 2. gives the brief about the type of attacks at every level, also the brief of the protocols used at each layer and its impact [9].

Dos attack is a type of an attack where the malicious host attempts to make the machine or the other devices inaccessible to its intended users by disrupting the normal functioning of the system. Usually, it typically functions by over flooding a specific device upon demand by the same client, resulting in the denial of service to another additional user. The two attacks require a single computer to launch an attack.

Distributed denial-of-service(DDoS) attacks are increasingly common in today's cyber-space. DDoS type of an attack is like other DoS attacks, but the primary difference is the traffic flooding which turns down a victim's server or system originates from many sources rather than one. Distributing the attack across multiple zombie sources increases the damage which makes it harder to identify the malicious party behind the attack. These zombie sources together form botnet.



Type	*Requirements*	*Few major attacks*	*Summary of few attacks*
Dos	Single Computer.	(S)SYN FLOOD TEARDROP ATTACKS LOW-RATE DENIAL-OF-SERVICE ATTACKS INTERNET CONTROL MESSAGE PROTOCOL (ICMP) FLOOD	*(S)SYN flood*-In this type, the attacker sends a series of SYN requests. *Teardrop Attacks*-This involves the attacker sending broken and disorganized IP fragments with overlapped and over-sized payload. *Low rate Denial-of-Service attacks*-The Low-rate DoS (LDoS) attack is designed to exploit TCP's slow-time-scale dynamics of being able to execute the retransmission time-out (RTO) mechanism to reduce TCP throughput. *Internet Control Message Protocol (ICMP) flood*-In this, ICMP Flood it succeeds by sending of an abnormally large number of ICMP packets of any type.
DDoS	Internet connection and botnets.	UDP FLOOD SYN FLOOD PING OF DEATH HTTP FLOOD	*UDP Flood*-This DDoS attack is a type that floods a target with User Datagram Protocol (UDP) packets. *SYN Flood*-In a SYN flood scenario, the requester sends multiple SYN requests, but either does not respond to the host's SYN-ACK response, or sends the SYN requests from a spoofed IP address. *Ping of Death*-This attack involves the attacker sending multiple malformed or malicious pings to a computer by splitting the large IP packet across multiple packets. *HTTP Flood*-In this, the HTTP flood DDoS attack, the attacker exploits seemingly-legitimate HTTP GET or POST requests to attack a web server or application.

Fig. 3. Summary of different types of attacks

Effects are faced by the legitimate users as the sever is been flooded with full of requests, and it becomes completely inaccessible. In addition, the outcome from such an attack, an organization may find its customers turning to competitors due to a loss of confidence resulting from the bad publicity. Financial and travel service firms and various e-commerce Web sites are frequent targets of DDoS attacks.

4. Role of neural network in detection of DoS and DDoS

It becomes a challenging task to differentiate whether it is a multiple request by the legitimate user or the flooded attempts by the attacker. In DDoS attacks it leads to disturbance of the networking sites, it simply breaks down the network or website applications by flooding with requests. The DDoS types of an attack involves botnet which are the set of multiple sources used to establish the attack, thereby it involves many IP addresses. The attackers, here tries to hang up the machine or website or the network as a whole with multiple request because of which the legitimate users cannot get a genuine request granted and it leads to the denial of service. DDoS is again a complex and sophisticated form of DoS, where the botnets are distributed globally. To analyse a complex type of an attack neural network gives a good backup which can be used to detect the attacks and respond accordingly. Neural network, which is a mimic of the human brain neural system acts very intelligently in a required situation when trained well. Neural network is well comprehensive option when there is a need of detection.

5. Proposed method of the neural network used for detection

The proposed method differentiates between normal traffic and abnormal traffic. For it will require to check every packet arrives at the destination site. To differentiate the type of traffic, the model uses the neural network to detect whether every IP packet sent is a genuine or a spoofed and then forwards it to the destination host. The model will be set up at every start of the server of host or device as per the requirement. Every IP packet will have to cross the neural network by default to reach the destination. The neural network would be configured at the start of the server as a wall. Before configuring the neural network will have to be trained and tested. The training of the neural network requires a data set. The data set comprises of the features of an IP packet; features will be extracted by the CICFlowmeter [8] from the sampled pcap files. Matlab will be used for the simulation of neural network. The neural network will be trained and tested. The neurons were assigned with some random weights; the assigned values will be as small as possible to minimize error. Fig. 4, illustrates the block diagram of the entire process.

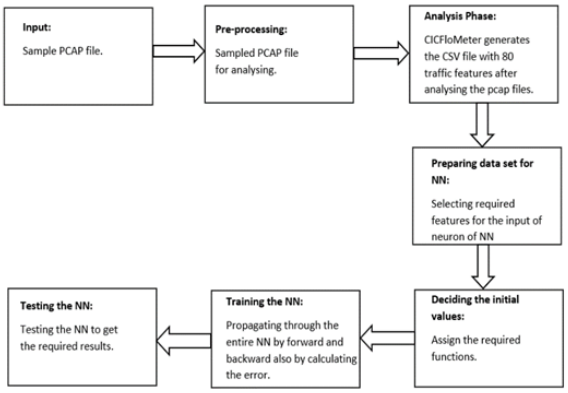

Input:
Sample PCAP file.
Pre-processing:
Sampled PCAP file for analysing.
Analysis Phase:
CICFloMeter generates the CSV file with 80 traffic features after analysing the pcap files.
Preparing data set for NN:
Selecting required features for the input of neuron of NN
Deciding the initial values:
Assign the required functions.
Training the NN:
Propagating through the entire NN by forward and backward also by calculating the error.
Testing the NN:
Testing the NN to get the required results.

Fig. 4. Block diagram

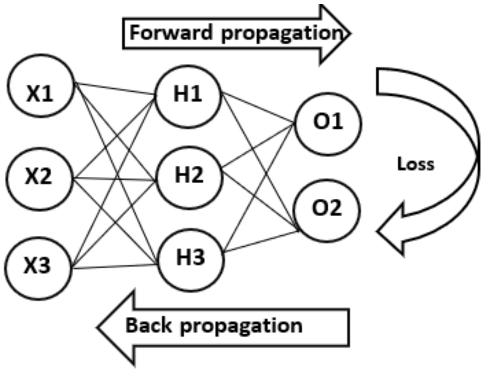


Fig. 5. Testing and training of the neural network

Fig. 5, represents the training and the testing phase of the neural network, firstly the network is subjected to the training data and the data would cross the entire neural network for their prediction (features of the IP packet) to be calculated. The input data would be passed through the layers in such a way that all the neurons apply the conversion to the information they receive from the neurons from the previous layer and sending it to the next layer. At the last layer will contain the result of the input data. Now the loss function will be used to estimate the error and compare with the expected result, the weights of the neurons will affect the system in this level. Thus, the weights will be changed accordingly until a better result is achieved. When the error is found the entire system would be back propagated to the start layer and traverse again till the output. This process would repeat until the expected result is achieved. The activation function would be used to propagate the output forward.

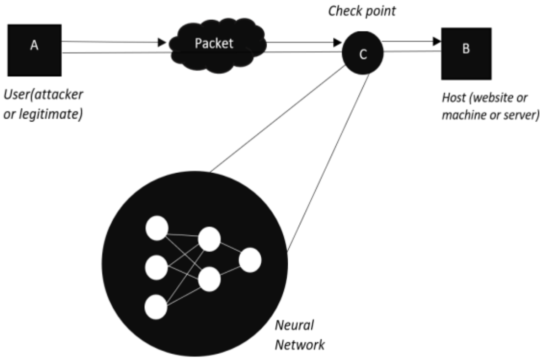


Fig. 6. Architecture of the proposed method

Fig. 6 illustrates the configuration of the neural network at the start of the required server as the wall. Before the packet reaches the destination host the packet will cross the neural network and gets detected whether it's a genuine or a spoofed packet. If the packet turned to be a spoofed packet the packet would be discarded, whereas if the packet is genuine it would be sent to the destination. For analyzing every packet, the neural network will check the features of an IP packet. "A" is the user from where the packet would move, the source. "B" is the destination. "C" would be the check point the neural network will be configured for analysis.

Requirements:

CiCFlowMeter, Matlab, sampled .pcap files.

A. Use of CICFlowMeter for pcap file analysis

The PCAP files are data files created using the program and they contain the packet data of a network. These files are mainly used in analyzing the network characteristics of a certain data. They are stored using an extension ".pcap".

CICFlowMeter [8] is a network traffic flow generator distributed by CIC to generate 84 network traffic features. It reads pcap file and generate a graphical report of the features extracted and also provides a csv file of the report. It is an open source application written in Java and can be downloaded from Github. Its source codes can be integrated to a project as it offers more flexibility in terms of choosing the features you want to calculate, adding new ones, and also having a better control of the duration of the flow timeout.

CICFlowMeter generates Bidirectional Flows (Biflow), where the first packet determines the forward (source to destination) and backward (destination to source) directions, hence the 84 statistical features such as Duration, Number of packets, Number of bytes, Length of packets, etc are also calculated separately in the forward and reverse direction. The output of the application is the CSV file format with six columns labelled for each flow, namely Flow ID, Source IP, Destination IP, Source Port, Destination Port, and Protocol with more than 80 network traffic features. Note that TCP flows are usually terminated upon connection teardown (by FIN packet) while UDP flows are terminated by a flow timeout. The flow timeout value can be assigned arbitrarily by the individual scheme, e.g. 600 seconds for both TCP and UDP.

6. Discussion of the proposed method

After the neural network is designed it will be configured at the network, server or device as a wall which will detect every packet it receives. The packet would travel through the neural network and this network would analyze the features of the packet. If the packet is malicious then the packet would be blocked by the NN as per the design, if the packet is genuine it will be moved the respective destination. Also, if the IP packet features are genuine and many numbers of failed or unsuccessful URL request attempts are encountered by the same IP then that particular IP would be blocked but for a limited time. The threshold point of attempting would be finalized by the organization depending upon the context. The neural network configured would be in the form of a device at the network. This device would require a ram for the operation, this ram would be adjusted as per the requirement. Also, the position of the NN could be changed from decentralized to a centralized device or otherwise as per the need. This complete NN would be an independent device which would have database along. This database would store every IP packet traverses through it. This method would prevent the server from crashing due to the flood created or generated.

7. Conclusion

Now a days every computer can be connected to the cloud for a better and spacious storage option, so it has become very obvious for the attackers that most of the data of any organization could possibly be found in the cloud. Thus, clouds are been attacked very often.

After the study about the DoS and DDoS attack, it has proved to be of a great loss for an organization. The attackers produce some truly staggering volumes of traffic, which stops the legitimate users to enter the connection. This non-approachable situation of an organization leads to the growth and establishment of many competitors. DDoS or DoS attackers are not necessarily hackers, but manipulation or steal of data is not a necessary or wanted task of the attacker, they can also attack the host and can also be successful by just stopping the access of the site for a long time. At this date none of the organization would require to get a hit by DDoS or DoS type of attacks.

References

[1] Kaspersky lab-DDoS reports.

[2] Haining Wang, Danlu Zhang and K. G. Shin, "Change-point monitoring for the detection of DoS attacks," in *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 4, pp. 193-208, Oct.-Dec. 2004.

[3] M. Dasari, "Real time detection of MAC layer DoS attacks in IEEE 802.11 wireless networks," *2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, 2017, pp. 939-944.

[4] S. S. Thakare and P. Kaur, "Denial-of-service attack detection system," *2017 1st International Conference on Intelligent Systems and Information Management (ICISIM)*, Aurangabad, 2017, pp. 281-285.

[5] Rajendra Patil, Harsha Dudeja, Snehal Gawade, Chirag Modi,"Protocol Specific Multi-Threaded Network Intrusion Detection System (PM-NIDS) for DoS/DDoS Attack Detection in Cloud." 9th ICCCNT 2018 July 10-12, 2018, IISC, Bengaluru Bengaluru, India.

[6] S. RoselinMary, M. Maheshwari and M. Thamaraiselvan, "Early detection of DOS attacks in VANET using Attacked Packet Detection Algorithm (APDA)," *2013 International Conference on Information Communication and Embedded Systems (ICICES)*, Chennai, 2013, pp. 237-240.

[7] Kevin Gurney 1997, UCL Press Limited 11 New Fetter Lane London EC4P 4EE

[8] CICFlowMeter by UNB Canadian University of Cybersecurity.

[9] DDoS Quick Guide- National Cybersecurity and Communications Integration Center

[10] S. N. Sivanandam, S. N. Deepa, "Principles of Soft Computing," Wiley India Pvt. Ltd.