Volume No:3, Issue No:6 (June-2018)
ISSN No : 2455–7595 (Online)
International Journal of Research in Management Studies
A Peer Reviewed Open Access International Journal
www.ijrms

Automated DDOS Attack Detection in Network using Machine Learning

Dr. Farha Anjum[1] M Pushpalatha[2] M Prabhakar[3] B Sirisha[4]

[1]Professor, Dept.of ECE, Siddhartha Institute of Engineering & Technology, Ibrahimpatnam, Hyderabad, Telangana, India.
[2]Assistant professor, Dept.of ECE, Siddhartha Institute of Engineering & Technology, Ibrahimpatnam, Hyderabad, Telangana, India.
[3]Assistant professor, Dept.of ECE, Siddhartha Institute of Engineering & Technology, Ibrahimpatnam, Hyderabad, Telangana, India.
[4]Student, Dept.of ECE, Siddhartha Institute of Engineering & Technology, Ibrahimpatnam, Hyderabad, Telangana, India.

Abstract:
DDoS attack is a major Internet security problem-DoS is that lots of clients simultaneously send service requests to certain server on the internet such that this server is too busy to provide normal services for others. Attackers using legitimate packets and often changing package information, so that traditional detection methods based on feature descriptions is difficult to detect it. So, the paper utilizing the combination of the neural network and the support vector machine presents the detection and the classification method for the DDOS attacks in the telecommunication network. The performance evaluation using the network simulator-2 enables to have the enhanced detection accuracy for the proposed method.

Keywords: internetwork, machine learning, distributed denial of service, cyber threats, detection accuracy, neural network, support vector machine.

1. INTRODUCTION

The rapid progress in the telecommunication that is in the form of the computer networks, the internet, the telephone network etc. has led to the evolution of the communication, causing the network to shift from the wired medium to the wireless medium. Playing a vital role in the connecting the entire world the telecommunication networks are capable of storing and conveying a huge set of information in the form of voice and the text that are sensitive as well as non-sensitive. The storage and the communications of the sensitive information's make them liable to many cyber-attacks [1]. The security threats that are keeping on increasing day by day makes necessary for the armed forces against the risk that are progressing. One such is the distributed denial service in short known as the (DDOS). The distributed denial of services causing the service denial in the host and the infrastructures of the internet necessitates the well-established examining and the observing to detect and neutralize the attacks [2], as they are continuously changing due to the evolving network behavior, techniques and the desires of the attackers. They DDOS are structured to overrun the targets with the traffic and stop the correct functioning of the resources in the network. They manage to stop the proper functioning of the network by directing thousands of hosts that are in a bot net to concurrently send traffic to the target in order to by-pass the activities of the target and causing complications in detecting the hosts of the attacks.

Cite this article as: Dr.Farha Anjum, M Pushpalatha, M Prabhakar & B Sirisha, "Automated DDOS Attack Detection in Network using Machine Learning", International Journal of Research in Management Studies, Volume 3 Issue 6, 2018, Page 14-20.

Volume No:3, Issue No:6 (June-2018)
ISSN No : 2455–7595 (Online)
International Journal of Research in Management Studies
A Peer Reviewed Open Access International Journal
www.ijrms

The researches were proceeded to detect these attacks, where David et al in 2015 proposed a flow-based entropy to detect the attacks by enumerating the difference in the flow count of the entropy at each time calculating its mean to note down its increase and decreased based on the verge set. These DDOs attacks are been even provided as the paid services by the company named booters, to many other companies prevailing in the market [3] and further there are other approaches of distributed attacks that are masked under the regular traffic, the ANN and the BGP were developed to detect the known and the unknown attacks and the application layer attacks respectively to segregate the corrupt traffic flow from the genuine one [4]. They paper also proposes a DDOS detection technique in the telecommunication network using the machine learning techniques to elude the hacking of the sensitive information's in the form of the text and the voice.

The remaining paper is arranged with the related works in the section 2, proposed work in the section 3 and the results in the section 4 and the conclusion in the section 5.

2. RELATED WORKS

Obaidat et al [5] the book presents the basics and the performance validation of the computer and the telecommunication networks. Padopoulos et al [6] presents the coordinated suppression caused by the concurrent attacks with the techniques to prevent the DDOS applying the watchdog at the edge networks causing a swift detection and the neutralizing the attacks and the Nazario, Jose et al [7] presents the evolution of the distributed attacks, the mitigation strategies etc. Shields, et al [8] the paper provides the main aspects of the prevailing DDOS and the frame work of the future attacks. Mansfield et al [9] the author visualizes the DDOS is developing as a political weapon as it is becoming more complex and sophisticated nowadays. David, et al [10] imposes a flow-based examination and the fast entropy method to detect the distributed denial of service attacks. Santanna et al [11], the author presents the mitigation techniques available in order to identify the perfect booter to follow to elude the DDOS in large concerns. Saied, et al [12] employs the ANN in detecting the unknown and known DDOS attacks and segregates the genuine traffic from the corrupt. Zhao et al [13] the application layer-distributed denial of service with the swift and the appropriate detection of the attacks. Dousti et al [14] a border gateway protocol for the purpose of the reducing the effects of the distributed denial of service was proffered. Newman et al [15] the author discusses the DDOS attacks with the short duration and low volume that are left unnoticed. Mathews et al [16] the security achieved using the machine learning is discussed in the paper.

3. PROPOSED WORK

The distributed denial service detection is the steps in identifying or segregating the attacks from the traffic that is normal. The most fundamental goal of the distributed denial of service is to restrict an access to the service, by denying the services to the legal users. The distributed-DOS are of prevailing in variety of types and are becoming more and more sophisticated each day. The attacks could not be prevented by just identifying and blocking a single IP address as the DDOS commanding multitude of hosts from different sources to direct their traffic to the destination. The inspiration behind these attacks might be due to the

Volume No:3, Issue No:6 (June-2018)
ISSN No : 2455–7595 (Online)
International Journal of Research in Management Studies
A Peer Reviewed Open Access International Journal
www.ijrms

disagreement in the ideology, to bring down the market of the competitors, for extorting of money, and to hack the secrets of the information's of the rivals in the market.

These DDOS attacks are classified into three types as the volume-based attacks, protocol attacks and the application layer attacks. The table .1 given below shows the types of the DDOS attacks and some of the attacks prevailing in the market today.

Table .1 Types of DDOS Attacks.

Distributed Denial of service	Types of Attacks	Description	Prevailing common Attacks in the Market
	Volume based	Uses a high traffic to drown the bandwidth of the network.	SYN Flood UDP Flood HTTP Flood
	Protocol based	Concentrates on utilizing the resources of the server	PING of Death Smurf Attack Fraggle Attack Slow Loris
	Application based	they are the most sophisticated serious types of attacks that deteriorates the web applications	NTP Amplification Advanced Persistent DOS Zero Day DDOS attacks.

The types of attacks are categorized based on the quantity in the traffic and the vulnerabilities that are exploited. The initial step in avoiding the Distributed Denial of Service is by detecting the occurrence. So, the paper aims in developing a machine learning module for the detecting of the distributed denial of service attacks.

3.1. METHODOLOGY FOR DDOS DETECTION

The proposed methodology can be taken as two strides as the memory module and the learning module, utilizes the combination of the neural network and the Support vector machine (CNSVM) in identifying the distributed DOS in the telecommunication networks. Initially this all begins with the extraction of the information's based on the traffic (T), the packet size (P_s), IP address of the source and the destination (IP_{sD}), the port address (Po_{add}) etc. Once the information are gathered they are analysis and evaluated, by using this the inbound traffic of the network, the normal packet size, the $IP_{sD}$and the Po_{add} of the legal users are extracted, the extracted features are used in training the CNSVM to classify the normal from traffic flow from the distributed denial of service. The fig.1 below shows the flow of the proposed process in identifying the distributed denial of the service.

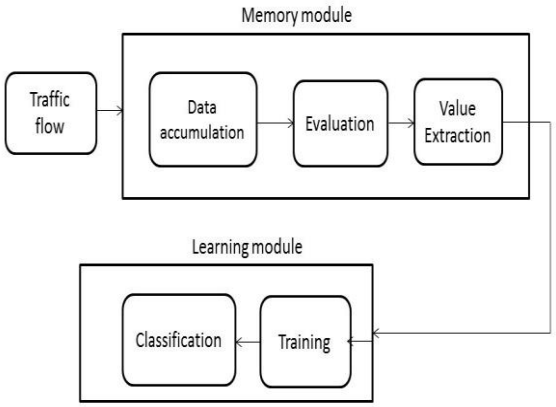

Fig .1 Proposed Flow Diagram

The traffic flow of the network is monitored and the information regarding the major resources that are liable of being attacked are accumulated once accumulated they are evaluated applying the quadratic entropy to identify the normal and the abnormalities in the traffic flow, the packet size, the IP spoofing and the port scan attack. The value extracted based the evaluation is segregated as the normal and the abnormal values by comparing them with the threshold values set. The lower drop thresholds are sets so as to prevent the attacks that affecting the services of the network to its legal users. These above steps are performed in the memory module the information extracted

Volume No:3, Issue No:6 (June-2018)
ISSN No : 2455–7595 (Online)
International Journal of Research in Management Studies
A Peer Reviewed Open Access International Journal
www.ijrms

are stored manually by the manager of the network. The stored information is utilized by the learning model to training the combined neural network support vector machine to classify the normal traffic from the attacks that is based on the volume, protocols and the application.

3.2. STEPS IN THE DETECTION OF THE DISTRIBUTED-DOS

This section presents the steps involved in the proposed methodology in detecting the distributed denial of services, using the quadratic entropy in evaluating the data accumulated and the combination of the neural networks and the support vector machine in identifying the attacks in the telecommunication network.

1. The behavior of the traffic (T), and the packet size (P_s), are accumulated form the traffic that flows into the network.
2. The data accumulated are evaluated using the quadratic entropy $H(B) =$

$$-\log \sum^{n} x_{=1}, \quad \text{where} P_x = b_x/n$$

$$\{ nimal \quad for \quad concentrated\ samples$$

where B is the set of behavior of the traffic, and b_x

$$0 \quad for \quad identical\ samples$$

represents the behavior of the traffic at the particular instant.

3. The evaluated values are extracted, by comparing with the threshold set (TH_{values}), based on the inbound traffic flow and the packet size and stored manually by the network manager.
4. The data extracted are used as the training set for the CNSVM
5. Based on the training the combined neural network support vector machine identifies the abnormalities in the network is determined using the equation $\sum_{l=1}^{i}(a_l - a_l)\, S(\pi(\cdot\ (X_l \mid \theta), \pi(X \mid \theta)) + b$, where the a represents the values of traffic status, $\pi(X_l \mid \theta)$ is the mapping done by the NN, θ is the vector containing the weights.
6. Classifies the normal from the abnormal.
7. The training is done on the periodic bases based on the extracted information that are stored manually in the network.

The step above enables to identify the distributed denial of services; the regular training enables to have an accurate classification of the normal and the abnormal traffic status leading to enhanced detection accuracy. The fig.2 shows the combined neural network and the support vector machine for the classification of the normal and the abnormal traffic status.

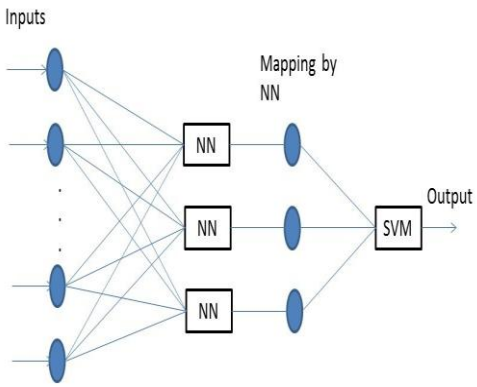

Fig .2 The Combined Neural Network Support Vector Machine

The training and the classification algorithm for the proposed method of the combined neural network and the support vector machine for the classification of the distributed denial of service

Volume No:3, Issue No:6 (June-2018)
ISSN No : 2455–7595 (Online)
International Journal of Research in Management Studies
A Peer Reviewed Open Access International Journal
www.ijrms

for enhancing the detection accuracy is presented below in the fig. 3

Input , traffic behavior T, P_s, IP_{sD} and Po_{add}
Output Attack Detection
Start
For all the behavior gathered
//apply quadratic entropy //
Evaluate the information gathered
Extract information
If $(T, P_s, IP_{sD}$ and $Po_{add} < TH_{values})$ then
Normal
Else
Abnormal
Store manually in the network
// training using the CNSVM//
Initialize SVM
Initialize NN
For all the extracted values
begin
Train SVM and the NN
Stop
For the incoming traffic
Begin
Apply CNSVM classifier
Stop
stop

Fig .3 Proposed Algorithm

The algorithm details the steps involved in the process of the detecting applying the machine learning techniques. This method of detecting the distributed denial services applying the machine learning prevents the network from being overwhelmed, obvious source attacks, time-out half connections and the spoofing through the IP and the Port scan attacks.

4. RESULTS

The evaluation of the proposed combined neural network and the support vector machine to enumerate the accuracy of the detection based on the true positive, false positive, false negative and the false positive conditions is performed for a number of traffic flow ranging up to 1000, the table. 2 below gives the simulation parameters used.

Table.2 simulation Parameters

Parameter	Value
Packet Type	UDP/TCP
Window Size	100
Time Window (Traffic Flow Requisition)	50 seconds
Traffic Flow	Up to 1000
Payload	None
Packets Size	1024 bytes

The proposed method applied for the telecommunication network; ensure the enhancement in the detection accuracy thus reducing the number of attacks that affect the traffic flow. The fig.4 below shows the average time taken in the detection of the distributed denial of service. The performance evaluation of the SVM, NN and the CNSVM shows that the proposed method has a reduced detection time compared to the support vector machine, and neural network.

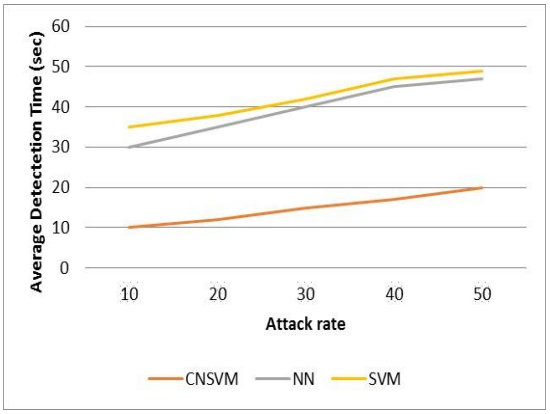

Fig .4 Average Detection Time

The fig .5 below gives the detection percentage of the proposed method in comparison with the support vector machine and the neural networks, the proposed method shows an detection of the DDOS in terms of improved accuracy, precision, recall, and f-measure.

Volume No:3, Issue No:6 (June-2018)
ISSN No : 2455–7595 (Online)
International Journal of Research in Management Studies
A Peer Reviewed Open Access International Journal
www.ijrms

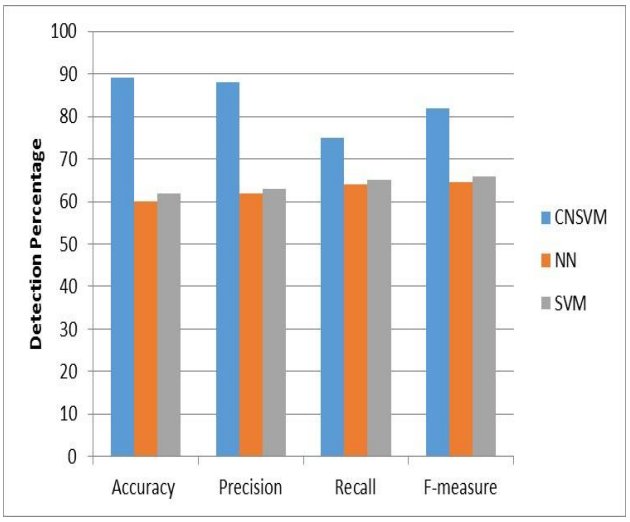

Fig.5.Comparison of DDOS detection

Based on the results shown in fig .5 for the detection accuracy and the comparison in it with the other prevailing methods of SVM and NN, the proposed CNSVM shows an 40% enhanced detection of the distributed denial service. The proposed method could be utilized in the telecommunication network to avoid the service denial to the legal users caused by the distributed denial service.

5. CONCLUSION

The paper with the aim of detecting the distributed denial service in the telecommunication network proceeds with the accumulation of the information regarding the behavior of the traffic to have the knowledge based on the inbound traffic of the network. the information collected are evaluated using the quadratic entropy and the abnormal and the normal are segregated by applying a lower drop thresholds since this is time consuming to be performed each time, the machine learning process combining the SVM and the NN is trained and used in the classification of the normal and the abnormal in the further traffic flow that is directed towards the network , this reduces the time in detection and increases the accuracy in detection , when compared to the classification using the NN and SVM separately. The additional abnormal detected are included to the learning module by regular periodic training. The performance evaluation and the comparison of the CNSVM and the SVM and the NN shows that the proposed method has a 40% improved accuracy than the prevailing methods.

References

[1] Aikaterini Mitrokotsa, Christos Douligeris, “Detecting Denial of Service Attacks Using Emergent Self-Organizing Maps”, IEEE International Symposium on Signal Processing and Information Technology 2005, pp 375-380.

[2] Fox, Kevin L., Henning, Rhonda R., and Reed, Jonathan H. (1990). “A Neural Network Approach Towards Intrusion Detection”. In Proceedings of the 13th National Computer Security Conference

[3] Morteza Amini, Rasool Jalili and Hamid Reza Shahriari, “RTUNNID: A practical solution to real-time network-based intrusion detection using unsupervised neural networks”, Computers & Security Volume 25, Issue 6, Elsevier Inc, September 2006, pp 459-468. [20] Rodes, B., Mahaffey,J., & Cannady, J. “Multiple Self Organizing Maps”. 23rd Security Information System (2000).

[4] Obaidat, Mohammed S., and Noureddine A. Boudriga. "Fundamentals of Performance Evaluation of Computer and Telecommunications Systems." (2010).

[5] Papadopoulos, Christos, Robert Lindell, John Mehringer, Alefiya Hussain, and Ramesh Govindan. "Cossack: Coordinated suppression of simultaneous attacks." In Proceedings DARPA

Information Survivability Conference and Exposition, vol. 1, pp. 2-13. IEEE, 2003.

[6] Nazario, Jose. "DDoS attack evolution." Network Security 2008, no. 7 (2008): 7-10.

[7] https://media.kasperskycontenthub.com /wpcontent/uploads/sites/43/2018/ 03/07185213/ Kaspersky_Teleco m_Threats_2016.pdf

[8] Shields, Clay. "What do we mean by Network Denial of Service." In Proceedings of the 2002 IEEE Workshop on Information Assurance and Security, vol. 4. 2002.

[9] Mansfield-Devine, Steve. "The growth and evolution of DDoS." Network Security 2015, no. 10 (2015): 13-20.

[10] David, Jisa, and Ciza Thomas. "DDoS attack detection using fast entropy approach on flow-based network traffic." Procedia Computer Science 50 (2015): 30-36.

[11] Santanna, Jose Jair, Ricardo de O. Schmidt, Daphne Tuncer, Anna Sperotto, Lisandro Z. Granville, and Aiko Pras. "Quiet Dogs Can Bite: Which Booters Should We Go After, and What Are Our Mitigation Options?." IEEE Communications Magazine 55, no. 7 (2017): 50-56.

[12] Saied, Alan, Richard E. Overill, and Tomasz Radzik. "Detection of known and unknown DDoS attacks using Artificial Neural Networks." Neurocomputing 172 (2016): 385-393.

[13] Zhao, Yuntao, Wenbo Zhang, Yongxin Feng, and Bo Yu. "A classification detection algorithm based on joint entropy vector against application-layer DDoS attack." Security and Communication Networks 2018 (2018).

[14] Dousti, Ramin Ali, Frank Scalzo, and Suresh Bhogavilli. "Automated ddos attack mitigation via bgp messaging." U.S. Patent Application 15/273,510, filed March 22, 2018.

[15] Newman, Sean. "Under the radar: the danger of stealthy DDoS attacks." Network Security 2019, no. 2 (2019): 18-19.

[16] Mathews, Alex. "What can machine learning do for information security?." Network Security 2019, no. 4 (2019): 15-17.