ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 6, June 2019

Identification of DOS attack Identification in Distributed Environment using Deep Learning

Vaishnavi Dande , Dr.Mrs.A.M. Deshmukh

Savitribai Phule Pune University, Pune, India

ABSTRACT : As the complexity of Internet is scaled up, it is likely for the Internet resources to be exposed to Distributed Denial of Service (DDoS) flooding attacks on TCP-based Web servers. There has been a lot of related work which focuses on analyzing the pattern of the DDoS attacks to protect users from them. However, none of these studies takes all the flags within TCP header into account, nor do they analyze relationship between the flags and the TCP packets. To analyze the features of the DDoS attacks, therefore, this paper presents a network traffic analysis mechanism which computes the ratio of the number of TCP flags to the total number of TCP packets. In this work we propose a system DDOS identification system using deep learning approach. This work initially carried out NS2 has design vitreous cluster network, each cluster having a cluster head as well as some cluster members. Each cluster number should we generate or sense random data and send to cluster head. Here we need to check each packet flow with packet features. Basically kddcup99 data set is the well-known intrusion detection data set to detect the malicious activity based on the DOS attack. Around seven sub types has been categorized in proposed system. The system contains training phase it is already holds some background knowledge as well as policy under the network security for system. Recurrent neural network (RNN) as used to generate the runtime weight between received data by cluster head with background policies. According to generator distance system will decide the desired packet is normal or abnormal. In experimental analysis we had shown various type of dos attack with accuracy rate in network simulator-2 environment.

KEYWORDS: DDOS, Deep Learning, Recurrent Neural Network, Malicious Network environment, NIDS, HIDS

I. INTRODUCTION

To understand the options of DDoS attacks, we have a tendency to introduce the analysis mechanism of the DDoS attacks in 2 settings: the traditional internet server with none attack and also the Web server with the DDoS attacks. In these settings, we have a tendency to live TCP flag rates, which ar expressed in terms of the quantitative relation of variety of TCP flags to the entire number of TCP packets. as an example, the quantity of SYNs drastically will increase just in case of SYN flooding attacks that is that the commonest DDoS attacks. In consequence, the increasing variety of SYNs indicates the chance of the DDoS attacks. Our analysis mechanism calculates the TCP flag rates and provides the premise of the DDoS attacks detection in a very TCP-based network surroundings.

In this work proposed DOS attack detection and defense mechanism using machine learning approach. The runtime data set has generated from different sensor nodes and collected by middleware authority as well as receiver not respectively. The background knowledge has already generated by system before execution of simulation and during the data receiving phase checks dynamically with each data packet. The recurrent neural network best deep learning approach has implemented to monitor the proposed system malicious environment. Finally system categorized each packet as a normal for abnormal respectively on their specific extracted features set.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 6, June 2019

II. LITERATURE SURVEY

According to Tariq Ahamad et. Al. [1] Large amounts of research have been conducted to improve IDS using artificial neural networks. The research proved that the network data traffic can be filtered and modeled more efficiently using artificial neural networks. Using artificial neural network proved itself as more advantageous as it take a thorough conscientious, perfect and accurate training, validation and top level testing phases before it is applied to the networks to detect malicious data and network attacks. Neural network (also known as artificial neural network) is an information processing model that is based and inspired from the human nervous system like the human brain does for humans by Z. F. Chen in [2]. The most important characteristic feature of this model is its unique structure of the system that processes the information. It consists of numerous exceptionally interconnected processing nodes (neurons) that work simultaneously to solve the specified problems which are defined by I. F. Akyildiz and I. H. Kasimoglu in [3].

According to N. Bulusu et. Al. [4] System also shows the real mathematical form of a neural network neuron. Neural networks, like humans do, learn by examples. Neural network is configured for a particular application, such as data classification or recognizing patterns through a learning process. The learning process in humans requires synaptic connections adjustments between the neurons and same is the case with neural networks as well. With the extra ordinary character of deriving meaning from complex and indefinite data, neural networks can be used to recognize and detect the patterns that are exceptionally complicated to be even observed or detected by humans and even by computer techniques proposed by E. Shih et. Al. in [5]. According to Tariq Ahamad, Abdullah Aljumah [6] the modern network world suffer due to security and threat vulnerabilities despite being from different origin or manufacturer or for different purpose and on the ground level, it is truly difficult technically and economically not feasible as far as both creating and maintaining such systems and to ensure that both the network and the associated systems are not susceptible to threats and attacks [6].

IDS is a special security tool that is being used by the network experts to keep the network safe and secure from network attacks which can come from many different sources by Abdulaziz Aldaej and Tariq Ahamad in [7]. It has emerged as one of the basic and powerful tool in order to deal with data security and availability issues over the communication networks. These attacks have a major influence of the networks and the systems as they include network performance, data security, loss of intellectual property by K. K Gupta and et. El. In [8] and a real liability for the compromised notes or networks data and that is why need a powerful IDS illustrates the architecture of IDS. The data packets received from the internet is forwarded to the processing unit where the format of the data is changed in order to make it compatible with the associated IDS and eventually the data packets are categorized as an attack or normal [9] which is defined by Tariq Ahamed Ahanger.

According to M. A. Pérez del Pino et. Al. The normal data packet re allowed to pass through but the attack data packets as identified as attack type and are kept in the attack table and the alarm is raised and the defense procedure is invoked [10]. After training process, a neural network can be treated as an expert one in the class or group information that has been given for analysis. This expert system can answer ―what if‖ questions. There are other advantages of neural networks which include Adaptive learning, Self organization, Real time operation, redundant information coding, etc. by Eugene Y et. Al. in [11]. Neural networks learn by examples and cannot be programmed to accomplish any specific job [12] by A. D. Wood and J. A. Stankovic. These examples need to be selected correctly and delicately otherwise the precious time of the system will get wasted or the network might work improperly

III. PROPOSED SYSTEM

The proposed RNNbased system combines parameters from KDD CUP 99 dataset such as duration, protocol type, service, flag, srcbyte, destbytes, land, is guest login, count, srv count of flows at each router to distinguish DDoS from flash crowd. In this way, our novel approach aims to improve the global security level and is the best solution to DDOS

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 6, June 2019

attacks in theory. Also our novel tracing system is used to trace the sources of the DDoS attack .It will detect the subtypes of DDoS attack such as flood attack, amplification attack, smurf, fraggle attack etc.

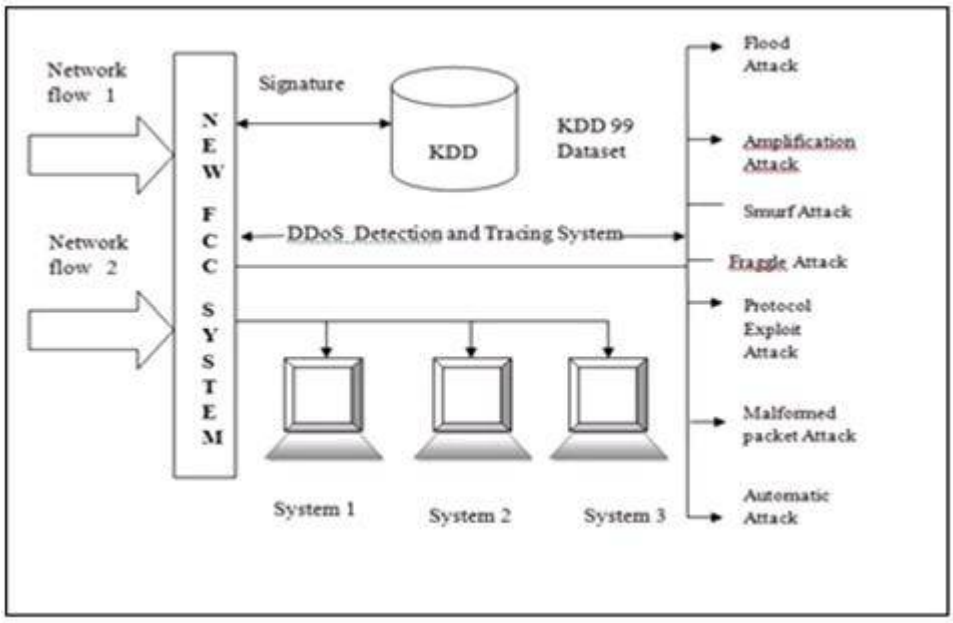

Figure 1: Proposed system architecture diagram

In the proposed system figure 1 shows the proposed system architecture, here we used runtime flash based attack generation technique which will runtime generate thousand of null packets and post in victims port. Our proposed classification based RNN algorithm will detect such malicious behavior ip as well as packets, and eliminate such connection.

Algorithm Design

Recurrent Neural Network

Input : Training Rules Tr[], Test Instances Ts[], Threshold T.
Output : Weight w=0.0
Step 1 : Read each test instance from (TsInstnace from Ts)
Step 2 : $TsIns = \sum_{k=0}^{n} \{Ak \dots An\}$
Step 3 : Read each train instance from (TrInstnace from Tr)
Step 4 : $TrIns = \sum_{j=0}^{n} \{Aj \dots \dots Am\}$

Step 5 : *w = WeightCalc(TsIns, TrIns)*

Step 6 : if (w >= T)

Step 7 : Forward feed layer to input layer for feedback FeedLayer[] ← {Tsf,w}

Step 8 : optimized feed layer weight, Cweigt ← FeedLayer[0]

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 6, June 2019

Step 9 : Return Cweight

Dataset Description

The inherent drawbacks in the KDD cup 99 dataset [4] has been revealed by various statistical analyses has affected the detection accuracy of many IDS modeled by researchers. It contains essential records of the complete KDD data set. There are a collection of downloadable files at the disposal for the researchers.

Table 1: Dataset Description

No	Name of the file	Description
1	KDDTrain+.ARFF	The full KDD train set with binary labels in ARFF format
2	KDDTrain+.TXT	The full NSL-KDD train set including attack-type labels and difficulty level in CSV format
3	KDDTrain+_20Percent.ARFF	A 20% subset of the KDDTrain+.arff file
4	KDDTrain+_20Percent.TXT	A 20% subset of the KDDTrain+.txt file
5	KDDTest+.ARFF	The full NSL-KDD test set with binary labels in ARFF format
6	KDDTest+.TXT	The full NSL-KDD test set including attack-type labels and difficulty level in CSV

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 6, June 2019

		format
7	KDDTest-21.ARFF	A subset of the KDDTest+.arff file which does not include records with difficulty level of 21 out of 21
8	KDDTest-21.TXT	A subset of the KDDTest+.txt file which does not include records with difficulty level of 21 out of 21

IV. RESULTS

In this section we present the evaluation of proposed system as well as existing system. After describing our experimental setup, we quantitatively evaluate the analysis with respect to the different parameter used such as throughput, packet delivery ratio, cost, and time. We run our experiments in NS2 simulator version 2.35 that has shown to produce realistic results. NS simulator runs TCL code, but here use both TCL and C++ code for header input. In our simulations, we use Infrastructure based network environment for communication. For providing access to the wireless network at anytime used for the network selection. WMN simulate in NS2 .TCL file show the simulation of all over architecture which proposed. For run .TCL use Eval Vid Framework in NS2 simulator it also help to store running connection information message using connection pattern file us1. NS2 trace file .tr can help to analyze results. It supports filtering, processing and displaying vector and scalar data. The results directory in the project folder contains us.tr file which is the files that store the performance results of the simulation. Based on the us.tr file using xgraph tool we execute graph of result parameters with respect to x and y axis parameters. Graphs files are of .awk extensions and are executable in xgarph tool to plot the graph.

The below figure shows average accuracy of proposed system in the initial experiment. The threshold has changed according to their data flow and it shows detection accuracy based on a respective threshold. The optimum threshold based on below figure 2 will be 0.75.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 6, June 2019

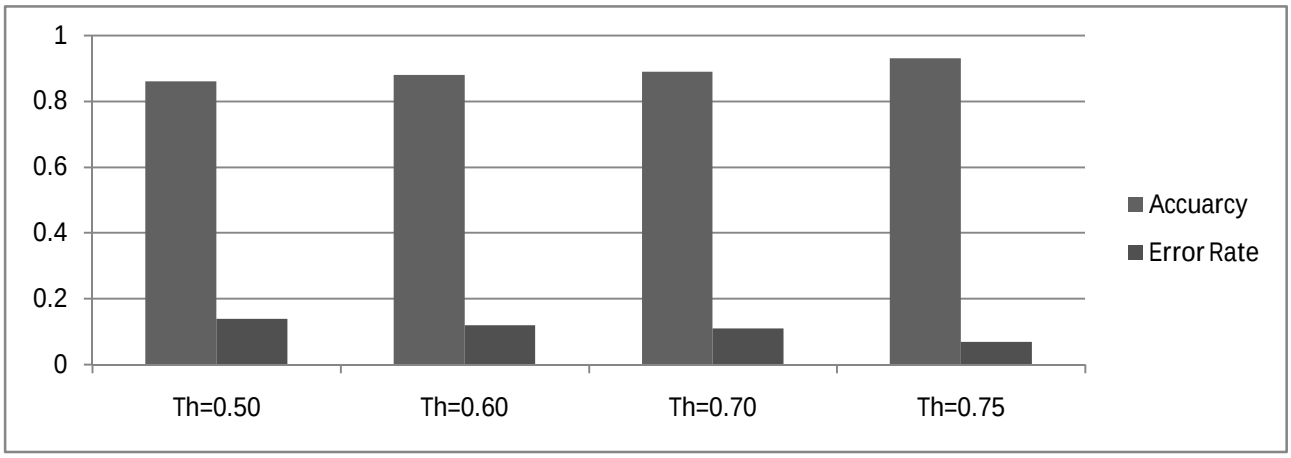

Figure 2: DOS attack detection accuracy with various threshold

The below figure 3 shows the each sub attack detection accuracy of dos attack, most of sensor nodes generates empty packets and sent it to receiver continuously, this event can be generated flash attack which is sometime having some malicious contents which will be harmful fall victim machine. In below figure 3 it illustrates detection accuracy for each sub attack under the DOS.

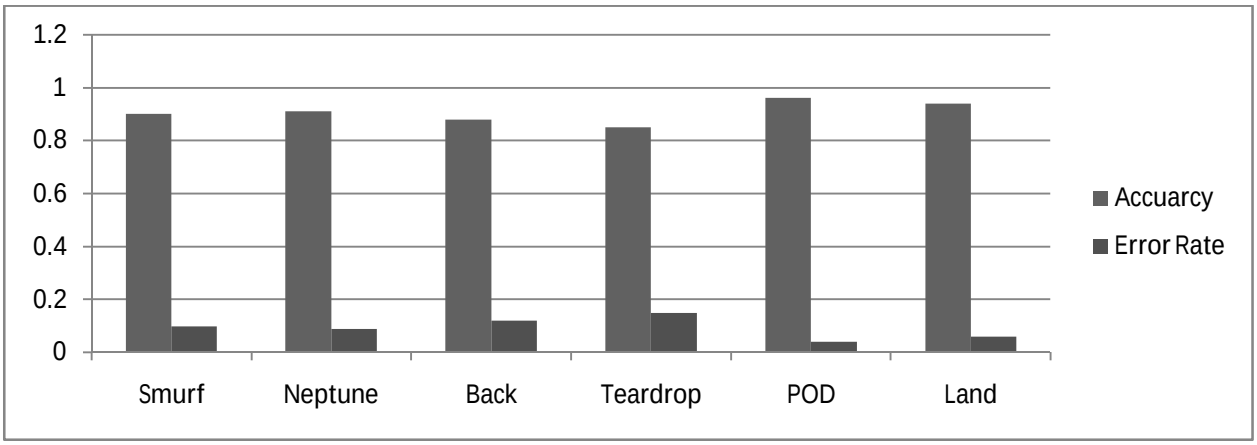

Figure 3: DOS subtype detection accuracy of proposed system

V. CONCLUSION

As Internet is a wide network used to combine different sectors. It carries number of information services and resources which exchange large amount of traffic over the Internet every day. All these services should be maintained properly so that user can access it as per their requirement. If all these services not maintained properly, definitely it will create problems. As the numbers of Internet users are increasing, the threats to it are also increasing. So protection against different software attacks and threats is one of the key challenges to maintain data integrity and privacy. Among them, Distributed Denial of Service (DDoS) and Flash Crowd attacks are the two major events. To maintain security and stability, it is very important to differentiate DDoS attack from flash crowd and trace the sources of the attack in large amount of traffic in network.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 6, June 2019

VI. FUTURE WORK

To implement the proposed system with another network defense mechanism in real time environment as well as need to do who proposed experiment in various network data sets like ISCX, Botnet, WSNTrace etc.

REFERENCES

[1] Tariq Ahamad, Abdullah Aljumah," Hybrid Approach Using Intrusion Detection System", International Journal of Engineering Research & Technology, Vol. 3 Issue 2, February - 2014.
[2] Z. F. Chen, P. D. Qian and Z. F. Chen, ―Application of PSO-RBF Neural Network in Network Intrusion Detection‖, 2009 3rd International Symposium on Intelligent Information Technology Application, pp.362-
364, 2009
[3] I. F. Akyildiz and I. H. Kasimoglu, ―Wireless sensor and actor networks: research challenges,‖ to be published Ad Hoc Networks, 2004.
[4] N. Bulusu, D. Estrin, L. Girod and J. Heidemann, ―Scalable coordination for wireless sensor networks: self-configuring localization systems International Symposium on Communication Theory and Applications (ISCTA), Ambleside, UK, July 2001.
[5] E. Shih, S. Cho, N. Ickes, R. Min, A. Sinha, A. Wang and A. Chandrakasan, ―Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks,‖ Proceedings of ACM MobiCom, Italy, pp:272-286, July 2001.
[6] Tariq Ahamad, Abdullah Aljumah,"Detection and Defense Mechanism against DDoS in MANET", Indian Journal of Science and Technology, Vol 8, No. 33, Dec 2015.
[7] Abdulaziz Aldaej and Tariq Ahamad, ―AAODV (Aggrandized Ad Hoc on Demand Vector): A Detection and Prevention Technique for Manets‖ International Journal of Advanced Computer Science and Applications(IJACSA), 7(10), 2016. http://dx.doi.org/10.14569/IJACSA.2016.071018 .
[8] K. K Gupta, B. Nath, and R. Kotagiri,―Layered Approach Using Conditional Random Fields for Intrusion Detection,‖ IEEE Transactions on Dependable and Secure Computing, Vol. 7, No. 1, pp. 35-49, Jan 2010.
[9] Tariq Ahamed Ahanger," An Effective Approach of Detecting DDoSUsing Artificial Neural Networks", IEEE international Conference on Wireless Communications, Signal Processing and Networking March 2017.
[10 M. A. Pérez del Pino, P. García Báez, P. Fernández López, and C. P. Suárez Araújo, ―Towards Self-Organizing Maps based Computational Intelligent System for Denial of Service Attacks Detection‖, INES2010, 14th International Conference on Intelligent Engineering Systems, pp. 151-157, Spain, May 5–7, 2010.
[11] Eugene Y. Vasserman and Nicholas Hopper, ―DOS flooding: Draining Life from Wireless Ad Hoc Sensor Networks‖, IEEE Transactions on mobile computing, Vol. 12, No. 2, February 2013.
[12] A. D. Wood and J. A. Stankovic, ―Denial of Service in Sensor Networks,‖ IEEE Computer, pp:54-62, 2002.