Volume 1, Number 3, March 2015 pp. 14-18
ISSN: 2395-3519

International Journal of Advanced Trends in Computer Applications
www.ijatca.com

A HYBRID APPROACH OF PREVENTION OF DDOS ATTACK USING NEURAL NETWORK

[1]Ankita Mangotra
M Tech Student
Rayat and Bahra Group of Colleges
ankita.magotra90@gmail.com
[2]Er. Vivek Gupta
Assistant Professor
Rayat and Bahra Group of Colleges
gupta_vivek1@yahoo.com

Abstract: *DDOS is a type of DOS attack where multiple compromised systems -- which are usually infected with a Trojan -- are used to target a single system causing a Denial of Service (DoS) attack. Victims of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack. This work proposes a Back Propagation Neural Network (BPNN) prevention engine to flag known and unknown attacks from genuine traffic. We have intensively trained the algorithm with real life cases and attacking scenarios (patterns) based on the existing DDoS tools. The more we train the algorithm with up-to-date patterns (latest known attacks), the further we increase the chances of detecting unknown attacks, considering that over training is avoided. This is because BPNN algorithm learns from scenarios and detects zero-day patterns that are similar to what it was trained with. This design is implemented in the MATLAB environment.*

Keywords: *DDOS Attack, Neural Network, Genetic Algorithm.*

I. INTRODUCTION

It seems that we are witnessing a tremendous growth of Internet threats. The emergence of multiple worms [1] and viruses that are propagating by exploiting the numerous vulnerabilities that are discovered day by day, transforms poorly administered computers into a powerful army in the electronic battlefield. The compromised hosts can be remotely controlled to perform various malicious activities like Spam forwarding [2], hosting illegal web sites or Distributed Denial of Service attacks 1. Malicious users that have under their control a large number of compromised hosts are able to launch packet floods towards a victim host or a router with a single command. These packet floods may aim at bandwidth starvation, at overloading a system's IP stack or a router's flow based switching module and are able to make the victim devices unreachable - denying thus service to legitimate users.

The detection of Distributed Denial of Service attacks is vital for the security management of edge networks, especially of university networks and ADSL providers. Poorly administered workstations and servers of academic networks and non-sophisticated users' home computers become the main sources of such attacks. Detection of DDoS attacks near their sources is the most effective approach that has been slightly explored [3], [4]. However, detection is hard even near the victim -destination network- , especially if we monitor non-congested links, which is the case in an overprovisioned ISP backbone. In this case link saturation can't provide us with an anomaly signature. In the same time it would be economically questionable to expect ISP's to perform DDoS detection on many, small and highly utilized customer links and not just at a few points of the over-provisioned backbone.

Given the current technology constraints, the research community has failed to offer to network administrator's reliable and feasible detection methods. The problem is that our sensors have to cope with high data rates which impose constraints on the detection algorithm's complexity. This way, complex processing

techniques like power spectral density estimation [5], clustering algorithms [6] or wavelet analysis [7] are promising but not readily available since they are based on hard to measure metrics (at least in real time) and they involve high processing overhead.

This proposed includes the detection of DDOS attack using genetic algorithm and prevention will be done using neural network.

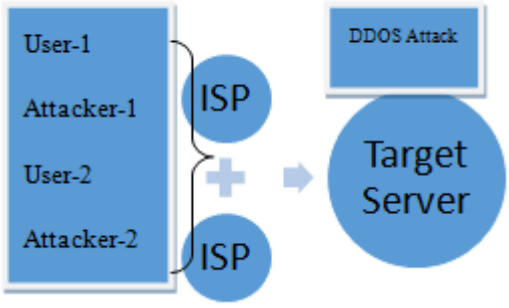

Figure 1.1: *DDOS Attack in Cloud Network*

II. DDOS ATTACKS

Denial of Service (DoS) is a class of attacks where an attacker makes some computing or memory resource too busy or too full to handle legitimate requests, thus denying legitimate users access to a machine [6]. There are different ways to launch DoS attacks:

- Abusing the computers legitimate features.
- Targeting the implementations bugs.
- Exploiting the system's misconfigurations.

DoS attacks are classified based on the services that an attacker renders unavailable to legitimate users.

III. RELATED WORK

Xiao et al. [12] present an approach that uses information theory and GA to detect abnormal network behaviors. Based on the mutual information between network features and the types of network intrusions, a small number of network features are closely identified with network attacks. Then a linear structure rule is derived using the selected features and a GA. The use of mutual information reduces the complexity of GA, and the single resulting linear rule makes intrusion detection efficient in real-time environment. However, the approach considers only discrete features.

Li [13] present to detect network anomalous using Genetic Algorithm. The detection rates may be increased due to quantitative features inclusion. However, no implementation results are available.

Bridges [14] Implemented a method to detect both anomalies and network misuses by combing Genetic Algorithm‟s and Fuzzy data mining technologies. In this method select the most significant network features and locate the best possible parameters of the fuzzy function by using Genetic Algorithm.

Crosbie [15] proposed a methodology to detect network anomalies using Genetic Programming (GP) and multiple agent technology. When the agents are not properly initialized, the training process takes long time. The communication among small autonomous agents is still a problem.

Selvakani [16] Applied Genetic Algorithm to generate rules for training the IDS. Rules are generated for only Smurf (DoS) attack and Warzemaster (R2L) attack. This performance of this methodology detection rate is low. This survey shows that the proposed Intrusion Detection models for R2L, U2R, Probe attacks get low detection rates using KDDCup dataset. This paper studies two types of attacks for each category i.e., DoS, R2L, U2R and Probe. Observed all the features in the KDDCUP Dataset to detect the attacks.

Lu [17] Develop a method to derive a set of classification rules by using Genetic Programming (GP) with help of past data of network. In this method using GP the practical implementation is more difficult due to the system required more data or time.

IV. PROPOSED WORK

The network attacks can be divided in four groups of DDoS, R2L, U2R, and Probe. In the designed IDS, the system can detect DDoS -type attacks, in very high detection rate. In fact, this kind of IDS is responsible for the detection attacks, which can be included in DDoS category. In order to design this type of IDS, we identified DDoS attacks and designed a separate IDS for each one to detect that specific attack. In general, considering the designed IDS, the system will detect DoS attacks in the network (if there is any).

The basic methodology is as follows:

1. During initial phase, feature extraction is done using genetic algorithm and this is done for detection of DDOS attack.

2. For prevention of DDOS attack: During a training/learning phase, the input traffic is source-separated, and fed into a NN, whose

parameters are iteratively re-estimated and established.

3. During the testing phase, the probability of a streamed, source-separated packet sequence of length n is estimated using the trained NN

4. If the probability of the packet sequence is lesser than a threshold probability, then the sequence is declared abnormal.

The experiment were based on the following:

1. During the learning phase, normal traffic was separated at three levels, based on layer 3/4 protocols used, based on destination information, and based on source information. Each stream is subjected to a HMM for the purpose of learning. Therefore, multiple HMMs are trained with the normal traffic.

2. During the testing phase, streaming is done again on all the three levels mentioned above, and the probability of the packet sequence in the stream coming from corresponding trained HMM is estimated, and flagged as anomaly if it falls below a threshold.

V. FLOWCHART

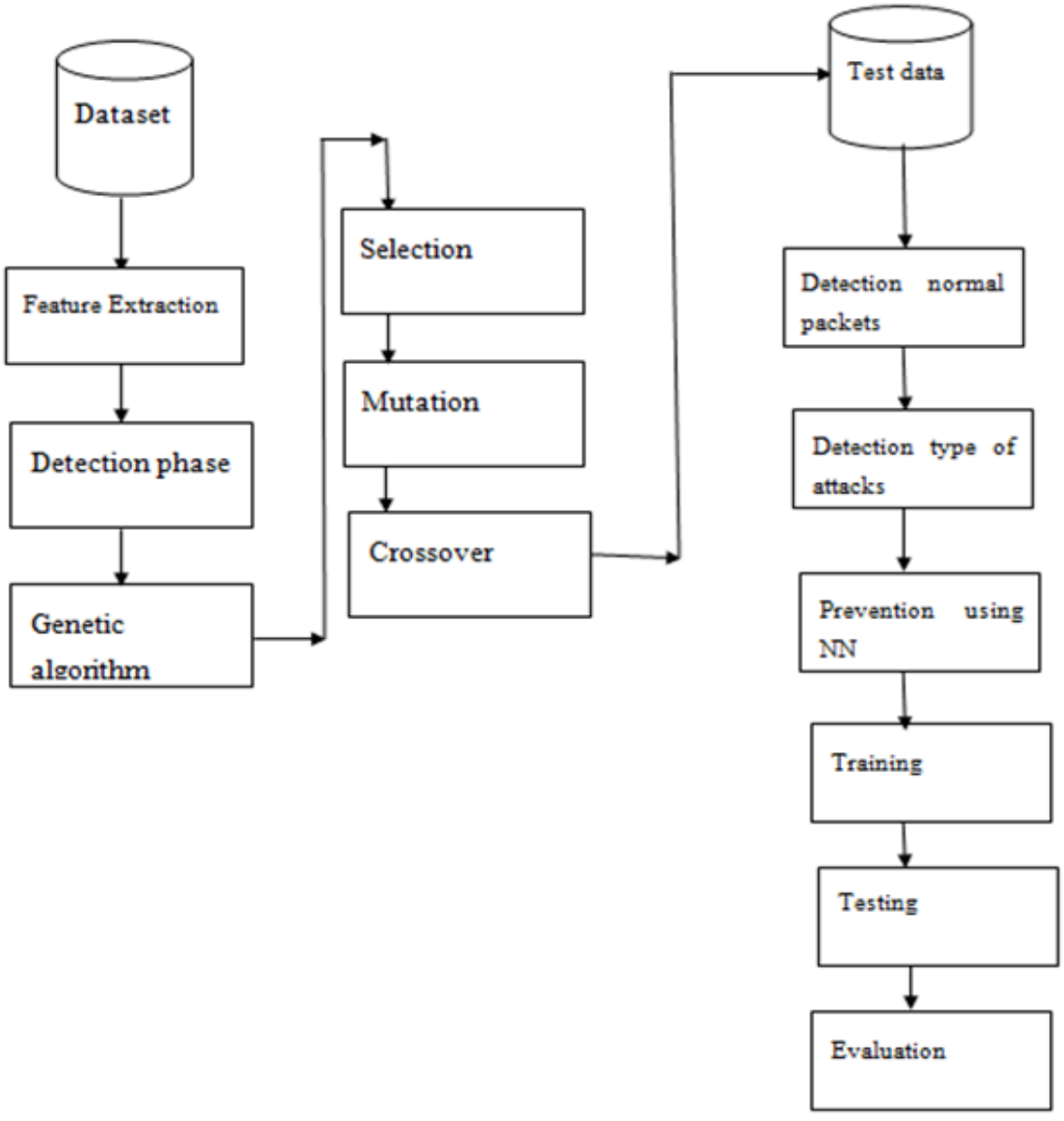

Figure 1-2 *Flowchart*

VI. RESULTS DISCUSSION

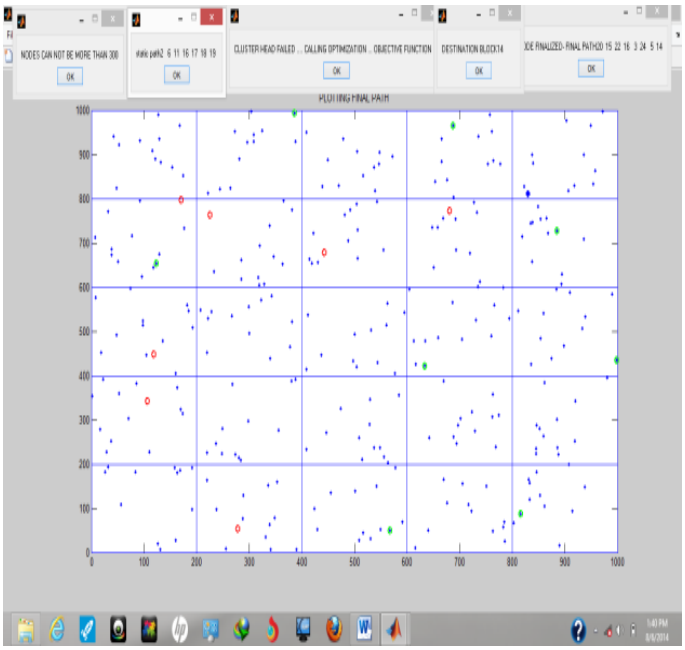

Figure 3: Node movement and failure in network

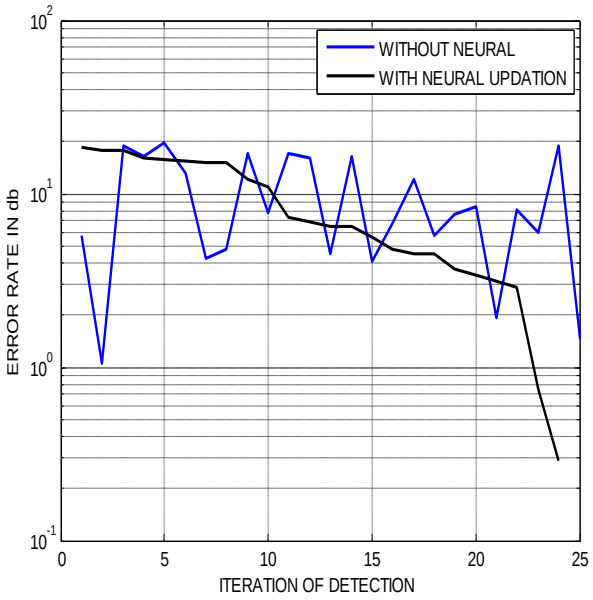

Figure 4: Rate of change of error rate

Above figure, shows the rate of change of the BER versus rate of change of SNR when energy and speed are only the constraints.

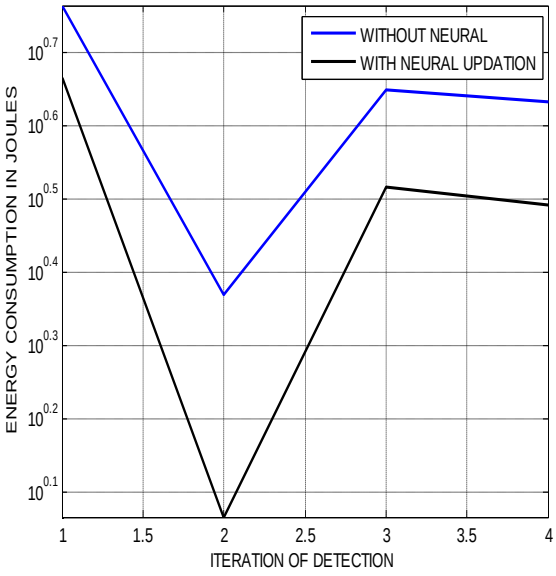

Figure 5: Rate of change of energy consumption

The above figure represents energy consumption in Joules with and without neural network. The graph clearly states that the energy consumption without neural network is more than that of with neural network.

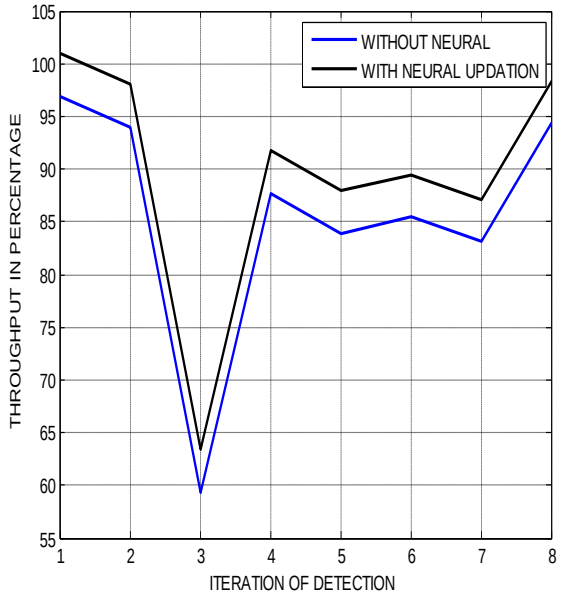

Figure 6: Rate of change of throughput

Above, figure shows the rate of change of the throughput versus change in iteration . It shows that throughput has been increased by 20 %.

CONCLUSION

Artificial Intelligence methods are gaining the most attention at present regarding its ability to learn and evolve, which makes them more precise and efficient in facing the huge number of unpredictable attacks.

Hence in this proposed work methodology based on Genetic Algorithm for detection of Distributed Denial of Service is proposed. The proposed approach aims at gaining maximum detections of the DDoS attacks with minimum false positive rate. Then prevention of DDOS attack will takes place with Neural Network.

REFERENCES

[1] Bhavin Shah, Bhushan H Trivedi, "Artificial Neural Network based Intrusion Detection System", International Journal of Computer Applications" *Volume 39– No.6, February 2012.*

[2] Manoranjan Pradhan, Sateesh Kumar Pradhan, Sudhir Kumar Sahu, "Anomaly Detection using Artificial Neural Network","International Journal of Engineering Sciences & Emerging Technologies, April 2012".

[3] Zahra Moradi1**,** Mohammad Teshnehlab , "Intrusion Detection Model in MANETs using ANNs and ANFIS", *2011 International Conference on Telecommunication Technology and Applications, Singapore*

[4] Mehdi MORADI and Mohammad ZULKERNINE, "A Neural Network Based Ssytem for Intrusion Detection and Classification of Attacks".

[5] Przemysław Kukiełka, Zbigniew Kotulski, "Adaptation of the neural network- based IDS to new attacks detection".

[6] M. Dondo and J. Treurniet, "Investigation of a Neural Network Implementation of a TCP packet Anomaly Detection System", Defence Research and Development Canada, May 2004.

[7] V.Sivakumar1,T.Yoganandh,R.Mohan Das, "Preventing Network From Intrusive Attack Using Artificial Neural Networks", International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 2,Mar-Apr 2012, pp.370-373.

[8] Samaneh Rastegari, M. Iqbal Saripan and Mohd Fadlee A. Rasid, "Detection of Denial of Service Attacks against Domain Name System Using Neural Networks", IJCSI International Journal of Computer Science Issues, Vol. 6, No. 1, 2009.

[9] S. Devaraju, S. Ramakrishnan, " Detection of Accuracy for Intrusion Detection System using Neural Network Classifier", International Journal of Emerging Technology and Advanced Engineering (IJETAE).

[10] Afrah Nazir, " A Comparative Study of different Artficial Neural Networks based Intrusion Detection Systems" International Journal of Scientific and Research Publications, Volume 3, Issue 7, July 2013.

[11] Sudhakar Parate, S. M Nirkhi, R.V Dharaskar, "Application of Neural Forensics for detection of Web Attack using Neural Network", National Conference on Innovative Paradigms in Engineering and Technology(NCIPET-2013).

[12] T. Xiao, G. Qu, S. Hariri, and M. Yousif, "An Efficient Network Intrusion Detection Method Based on Information Theory and Genetic Algorithm", Proceedings of the 24th IEEE International Performance Computing and Communications Conference (IPCCC „05), Phoenix, AZ, USA. 2005. Proceedings of the Sixth International Conference on Software Engineering, Artificial Intelligence, Net.

[13] W. Li, "Using Genetic Algorithm for Network Intrusion Detection". "A Genetic Algorithm Approach to Network Intrusion Detection". SANS Institute, USA, 2004.

[14] Bridges, Susan, Rayford B. Vaughn," Intrusion Detection via Fuzzy Data Mining", In Proceedings of 12th Annual Canadian Information Technology Security Symposium, pp. 109-122, Ottawa, Canada, 2000.

[15] Crosbie, Mark, Gene Spafford,"Applying Genetic Programming to Intrusion Detection", In Proceeding of 1995 AAAI Fall Symposium on Genetic Programming, pp. 1-8, Cambridge, Massachusetts, 1995.

[16] Selvakani S, R.S. Rajesh," Genetic Algorithm for framing rules for Intrusion Detection", IJCSNS, Vol.7, No.11, 2007.

[17] W. Lu, I. Traore,"Detecting new forms of network intrusion using genetic programming", Computational Intelligence Vol.20, Issue 3, 2004, pp. 475-494.