Detection of Distributed Denial of Service Attacks Using Artificial Neural Networks

Abdullah Aljumah
College of Computer Engineering and Sciences
Prince Sattam Bin Abdulaziz University, KSA

***Abstract*—Distributed Denial of Services (DDoS) is a ruthless attack that targets a node or a medium with its false packets to decline the network performance and its resources. Neural networks is a powerful tool to defend a network from this attack as in our proposed solution a mitigation process is invoked when an attack is detected by the detection system using the known patters which separate the legitimate traffic from malicious traffic that were given to artificial neural networks during its training process. In this research article, we have proposed a DDoS detection system using artificial neural networks that will flag (mark) malicious and genuine data traffic and will save network from losing performance. We have compared and evaluated our proposed system on the basis of precision, sensitivity and accuracy with the existing models of the related work.**

Keywords*— *Distributed Denial of Services (DDoS); ANN; IDS

I. Introduction

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 [1]. 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 [2]. 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 [3] and a real liability for the compromised notes or networks data and that is why need a powerful IDS? Fig. 1 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 [4]. 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 [5].

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[6].

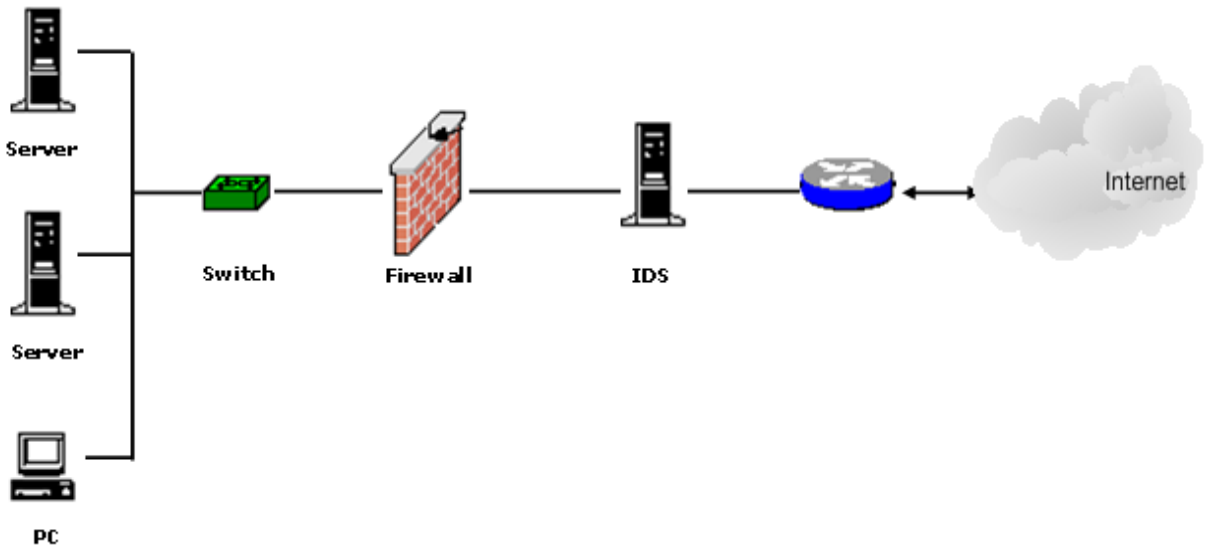


Fig. 1. Intrusion detection system.

II. Artificial Neural Network

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 [7]. 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 [8]. Fig. 2 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 [9]. The learning process in humans requires synaptic connections adjustments between the neurons and same is the case with neural networks as well.

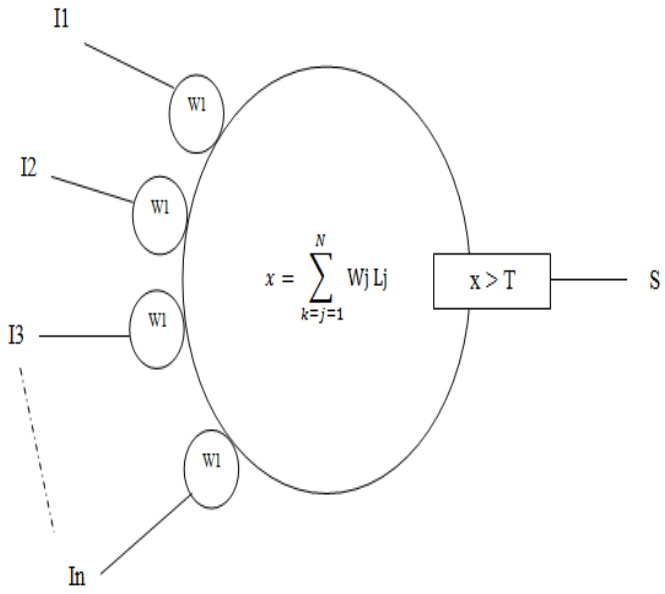


Fig. 2. Block diagram of an artificial neuron.

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 [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. [11]. Neural networks learn by examples and cannot be programmed to accomplish any specific job [12]. 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.

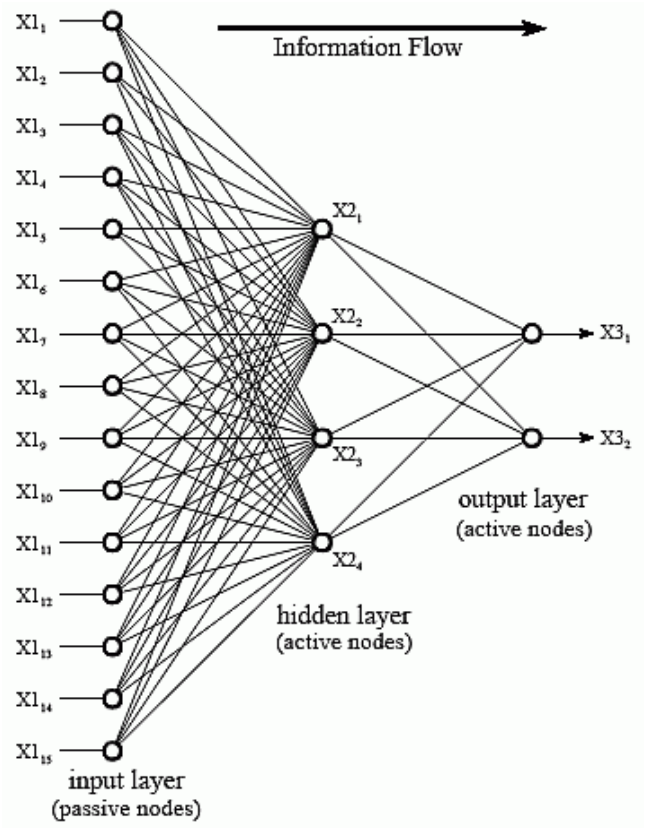


Fig. 3. Architecture of the neural network.

Neural network mainly have three categories of layers which include Input layer, Hidden Layers and output layers. Fig. 3 illustrates the basic architecture of the neural network. This is the most common architecture of neural networks. The input nodes are input nodes and rest of the nodes are active nodes. The input layer nodes are connected to hidden layer nodes and the hidden layer nodes are connected to output units. The action of this neural network is decided by the weight that is put on hidden layer nodes. The main job of the input nodes is to represent the raw information that is received by the network. This input and the weight on the connections between hidden nodes and input nodes decide the action of the hidden layer units. This action or activity of the hidden layer nodes and the weight between output layer nodes and the hidden layer nodes decide the performance and the behavior of the output layer nodes.

III. DDos

Denial of Service (DoS) attacks is a deliberate, malicious, criminal attempt to deprive legitimate network users from using their network resources. DoS affect service providers in many aspects, most notably crippling availability of services provided by them. DDoS themselves are not powerful enough to bring down any web service in present computational resources scenario. A more sophisticated scalable and distributed attack evolved out of DoS is DDoS or Distributed

Denial of Services. It was first reported by Computer Incident Advisory Capability (CIAC) in somewhere around summers of 1999 [20]. Since then almost all DoS attacks were somehow of distributed characteristics.

To sabotage any website by DDoS there are broadly two methods, first and primitive one is to send packet with morphed packed to confuse routing protocols also known as vulnerability attack [21]. Second and somewhat advance and more sophisticated mechanism involve attempts of either one or both of following (a) at network/transport layer attack flooding web server to exhaust bandwidth, router processing capability and hence paralyzing connectivity to the legitimate user [21]; (b) attack at application layer for depriving legitimate user with services by consuming server resources of provider website, e.g. sockets, memory, disk I/O, etc. [22].

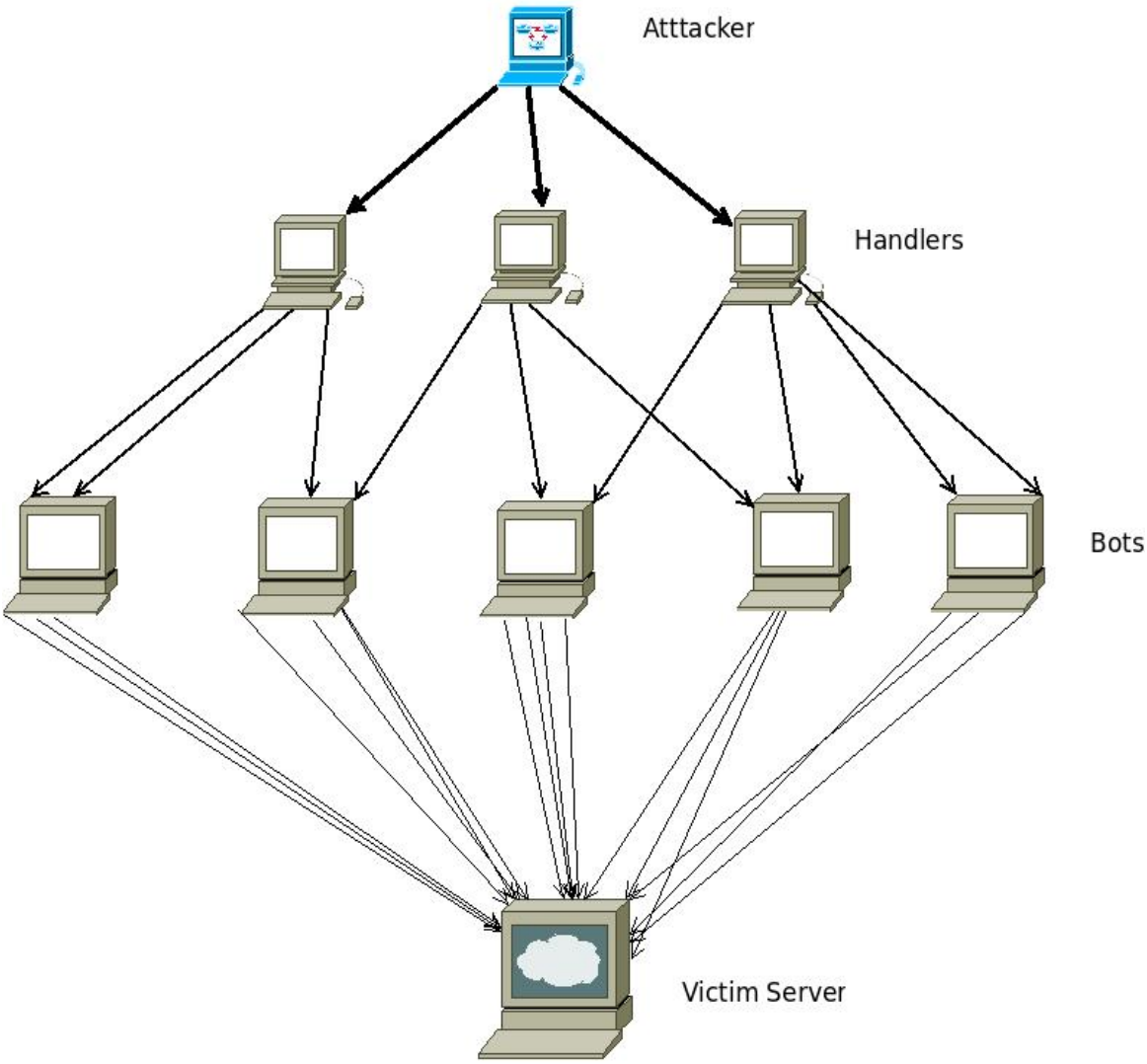
Usually attacker seldom acts directly, rather a series of pre compromised nodes are chosen by him to launch attack on behalf of him, known as Botnets or simply Bots or Zombies (Fig. 4(a)). Attacker may have gain access to these computers by any means of infection [19].

A more recent trend is to magnify the amplitude of attack so as overwhelm victim even with enormous amount of resources, a way to get it is "DNS Amplification" (Fig. 4(b)).

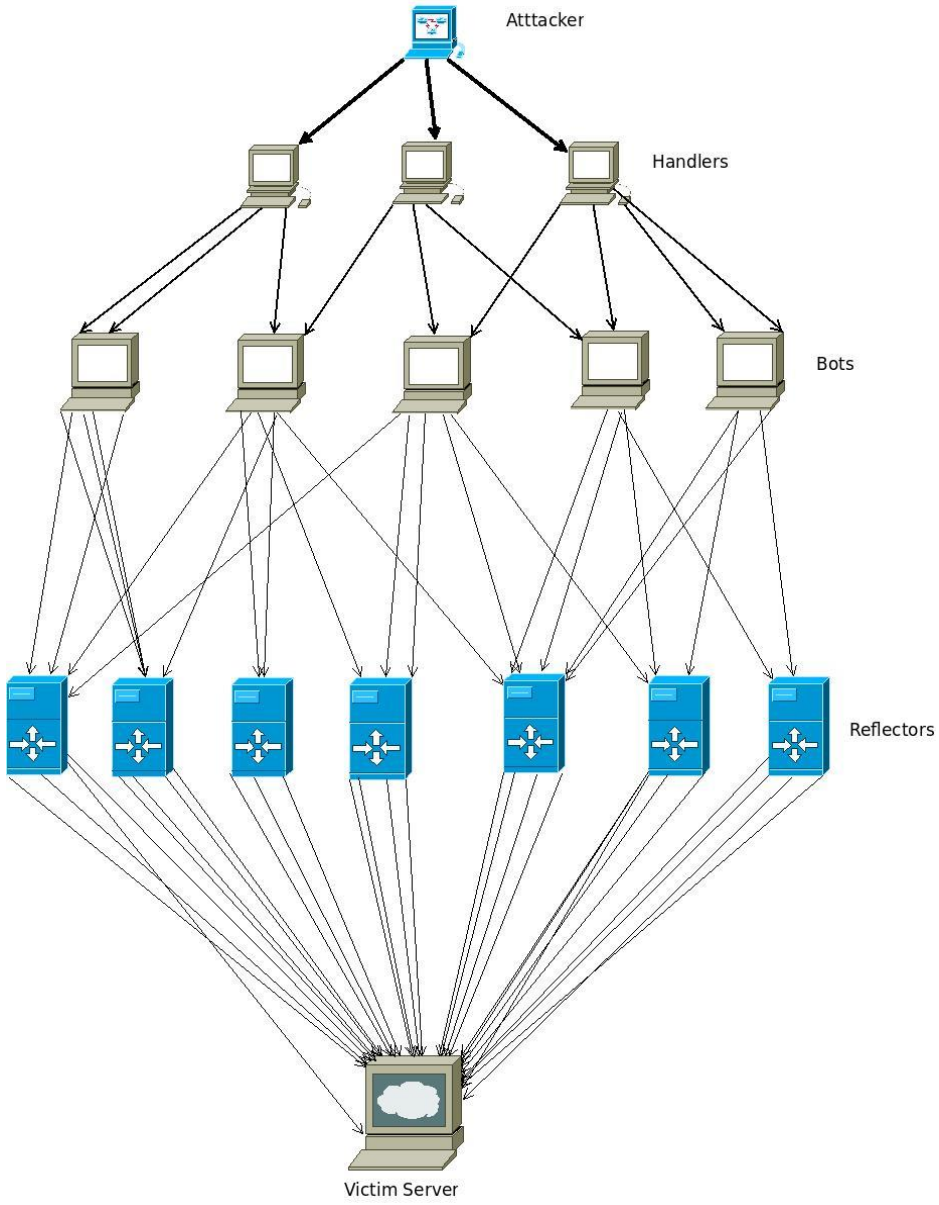
A. Role of Amplifiers/Reflectors

DNS amplification is a phenomenon where a small query is amplified several folds as this amplified query with much larger payload than original one is then directed to victim server. Amplification of usually 70 folds is achieved easily [18].

DNS amplification a kind of reflective attack where spoofed IP of victim server is used for DNS query, in return victim server is flooded with large number of UDP packets.



(a)



(b)

Fig. 4. (a) Direct DDoS attack; (b) Reflexive DDoS attack.

IV. Consequences of DDos

Effects of DDoS attacks on business installation are immediately reflected as Revenue Losses, with loss rate going as high as $ 300K/hour for service outage hours [13]. With advent of time, cost to mitigate DDoS attacks kept ever rising, in a survey by Forrester Research survey of Canadian decision-makers, DDoS attacks were declared most expensive with average cost associated with a typical DDoS reaching well beyond $ 100,000 per security incident [14].

Besides being attacked is direct blow onto market reputation of any e-commerce website. In their findings, Bell Canada mentioned, 67% corporate say DDoS cause negative impact to customers, 56% say it critically impacts the brand name while 55% are concerned with negative effects on customer relations [15].

Al though, DDoS attacks are not meant for theft, but recently there has been shift in DDoS activities with stealing of user data, customers information, intellectual properties, etc. while enterprise resources were busy in mitigation of DDoS and related effects, known as Smoke-Screen effect. In the transitional time when IT experts of target organization are busy to bring back critical application. On line, attacker try to bypass security checks and get away with crucial business data, e.g. during DDoS attack on Carphone Warehouse, while internal team was busy with DDoS mitigation, hackers stole personal and banking details of 2.4 million people [16]. In their security report, Kaspersky Lab has published, 26% of DDoS attacks end up with Data Loss [17].

V. Related Work

With the use of ANN for the detection of DDOS attacks by Jie-Hao and Ming [24] in which the results where compared with output and the decision tree, ANN, Bayesian and entropy. The researchers recognize the user demands for any particular resource on the involved system and their control data. Moreover, the samples of such identifications were sent to the attack detection system for any vulnerabilities.

Liu, Gu and et al. established a system called Learning Vector Quantization (LVQ) neural networks to identify attacks [25]. The technique is supervision type of quantization, which can be used for further procedures such as pattern recognition, data compression and multi-class classifications. Furthermore, the inputs where supplied to neural networks as data sets in the form of numerical calculations.

Akilandeswari and Shalinie [26], proposed a Probabilistic Neural Network Based Attack Traffic taxonomy in order to detect various DDOS attacks. In contrast, the authors mainly focused on distinguished between Flash Crowd Event from Denial of Service Attacks. Moreover, their work also involved the use of Bayes decision rule for Bayes interference coupled with Radial Basis Function Neural Network (RBFNN) for precisely classifying the DDOS attack traffic and the legitimate traffic.

Siaterlis & Maglaris [27] came up with a procedure of single network characteristics to mitigate the attacks. With the use of data fusion algorithm with Multi-layer Perceptron (MLP) in which the inputs where initialized from various non-active measurement which were available on the network, and hence the data combined with the traffic which were generated from the experimenters itself.

Joshi, Gupta and Misra [28] used a design consideration of neural network in order to detect zombie systems which were fueling the DDOS attacks. The main motive to their initiative was to figure out the connection between the zombie computer and sample entropy. The entire process workflow comprises on the predictions with the help of feed-forward neural network. Another objective for their research is to utilize the current infra for detecting and mitigating such attacks.

Badishi, Yachin & Keidar [29] used an approach of cryptography and authentication to defend DDOS attacks from affecting network resources and services. A very close approach proposed by Shi, Stoica and Anderson [30], However, DDOS attacks are detected using a different technique called puzzling mechanism.

Hwang and Ku [31] proposed a distributed technique to mitigate DDOS attacks. The mitigation system called Distributed Change-point Detection (DCD), which primarily reduces the risk of such attacks. The researcher suggests using non-parametric CUSUM (Cumulative Sum) algorithm to identify any major or minor variations in the network traffic. The team also focused on the initial source of the attack for detection.

A group of author [32]-[34] proposed a system of packet-marking and entropy in which each packet is marked on every router involved in communication in order to track the source of the packet. However, a number of techniques proposed by some authors used ANN or infrastructure to defend against DDOS attacks, where as a couple of them identified the source of the attack. In contrast, none of them describes any unknown or zero day attacks labeled as high or low risk attacks. Hence, our main objective is to detect and mitigate unknown DDOS attacks and differentiate our proposed solution from the authors of [25]-[28].

VI. Conceptual Framework

If deployed properly the DDoS detectors can minimize the strength of an attack. The DDoS detectors prevent the malicious packet from reaching the target after detection by analyzing the network for abnormal behavior or the abnormalities in the network. It is important for DDoS detectors to allow legitimate packets to pass through and reach the destination. So, it is extremely important for the detection system to be explicitly precise and checked against every possible and imaginable patterns and cases. Most commonly TCP, ICMP and UDP are used because of ease in practicality, implementation and documentation. The yearly report of Proplexic explained that these protocols are used by most attackers to launch most of the DDoS attacks. Since we have used ANN (artificial neural networks) for our detection mechanism where it's precision predominantly depend on the quality of the algorithm training and the associated datasets and patterns used. The patters include packet source address, sequence numbers and ID along with port numbers of source and destination, all these entities of packets are used for training the ANN. Based on our analysis and experimental verification, maximum number of zombies installed to oppose the operating system libraries in order to generate genuine packets that the installed zombie agents use their integrated built-in libraries. This is just to help the attackers in manipulation and forging the message throughout the attack.

Hence, it is easily possible to study the main properties of authentic packets that are created by authentic applications and can be easily compared with fake packets that are created by the attack tools and feed them as input patterns to train the artificial neural networks. We launched difference kinds of DDoS attacks at distinct levels in order to select the different patterns for input to the artificial neural networks by creating an elite network infrastructure in unanimous and solitary environments. We studied the results very carefully and compared them with authentic traffic in order to verify the characteristic patterns that distinguish authentic traffic from the attack traffic. This segment of the process demanded thorough comprehension of how distinctive protocol interchange data or do the communications. The java neural network simulator accepts the authentic and malicious pattern in a specified format because the data sets are designed and assembled to accommodate both types of patterns. However 79% of the datasets are used in training the algo and 21% are used to ratify the process of learning. The input entities are normalized in order to increase the capability in delicate applications like the one we have where exact detection is extremely important otherwise if applied directly will lead to vanquish the impact of smaller values because normalization has positive effect on artificial neural network's training and performers.

A normal artificial neural network is made up of three layers i.e. input layer, an output layer, and a hidden layer, the datasets and patterns are given through input nodes for the learning process. These input attributes indicate the main pattern that distinguishes the genuine traffic from the attack traffic. Then we selected three different structures of topological artificial neural networks having three layers each i.e., input layer, output layer and hidden layer. But every topological artificial neural network structure will have different number of nodes as shown in Table 1.

TABLE I. NO. OF INPUT AND OUTPUT NODES FOR ICMP, TCP AND UDP

Topological ANN structure	No. of input nodes	No. of hidden nodes
ICMP	3	4
TCP	5	4
UDP	4	3

However the computation process deals with hidden nodes regarding input and output nodes. A single node is used as output layer to represent 1 or 0 for attack and normal traffic, respectively. Fig. 5 displays the TCP topological artificial neural network structure, Fig. 6 displays ICMP topological artificial neural network structure and Fig. 7 displays the UDP topological artificial neural network structure. Selecting an appropriate learning algo, invoking function and number of hidden nodes where chosen on the early experiments where the accurate results were provided by Back Propagation and Sigmoid. Bidirectional associative memory, Elliot, Sigmoid and Softmax are used as functions while the comparison was between Quick-Prop, Back Propagation, Bidirectional Associative Memory, Back Prop Weight Decay, Back Prop thru time (16, 17, 18).

Our experiment shows 98.5% accuracy in selected topological structures when sigmoid invoking function is paired with Back Propagation as shown in Table 2.

TCP topological structure's input layers as shown in Fig. 4 is composed of five nodes with TCP sequence, source IP address, source port number, destination port number and flags.

ICMP topological structure is shown in Fig. 5 where ICMP ID and sequence number, source IP address are the input nodes.

TABLE II. COLLECTIVE RESULTS OF LEARNING ALGO, INVOKING FUNCTION, HL

Protocol	Learning Algorithm	Invoking Function	No. of Hidden Nodes	Detection Accuracy and CPU Usage	Best Results
TCP	Back Propagation	Sigmoid, Elliot, BAM, Softmax	One or more Hidden Nodes	98.6% and 66%-CPU Utilization	Best Recorded With 4 hidden nodes using Sigmoid.
UDP	Back Propagation	Sigmoid, Elliot, BAM, Softmax	One or more Hidden Nodes	98.6% and 69%-CPU Utilization	Best Recorded With 3 hidden nodes using Sigmoid.
ICMP	Back Propagation	Sigmoid, Elliot, BAM, Softmax	One or more Hidden Nodes	98.5% and 70%-CPU Utilization	Best Recorded With 4 hidden nodes using Sigmoid.

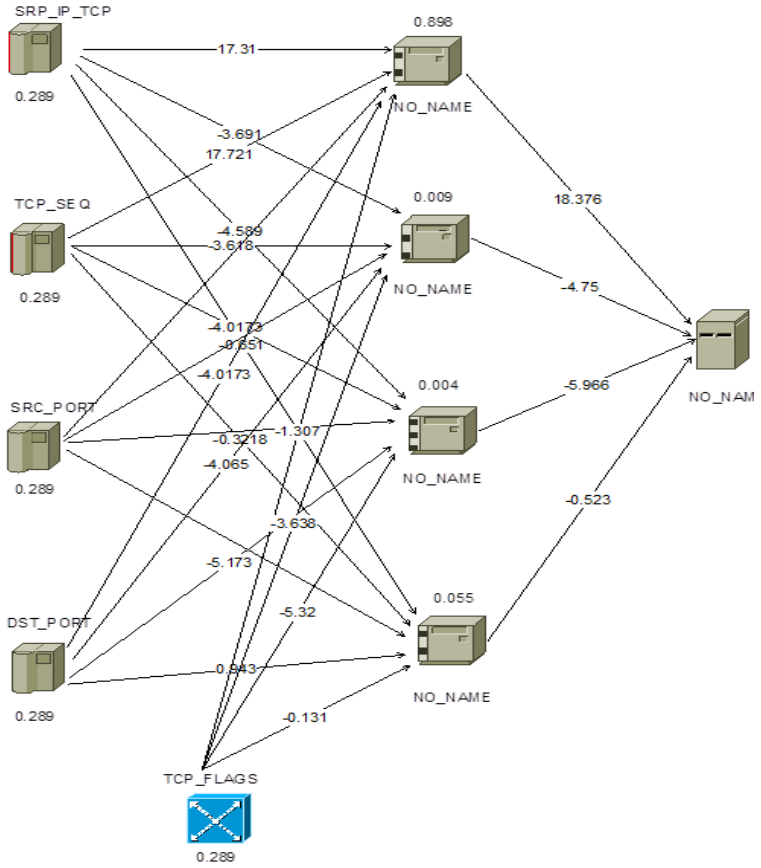


Fig. 5. ANN TCP topological structure.

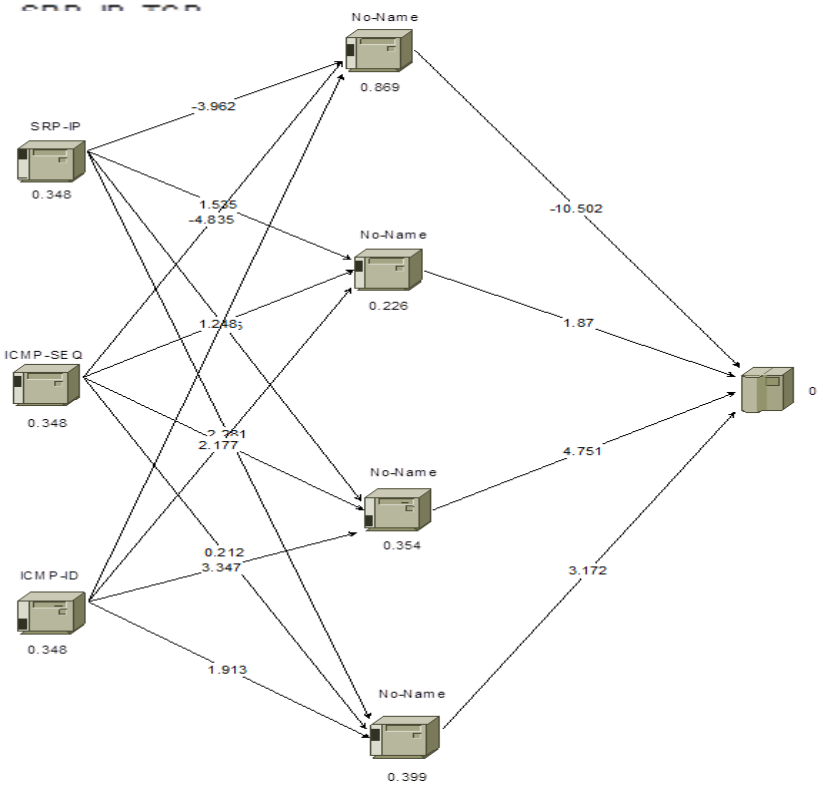


Fig. 6. ANN ICMP topological structure.

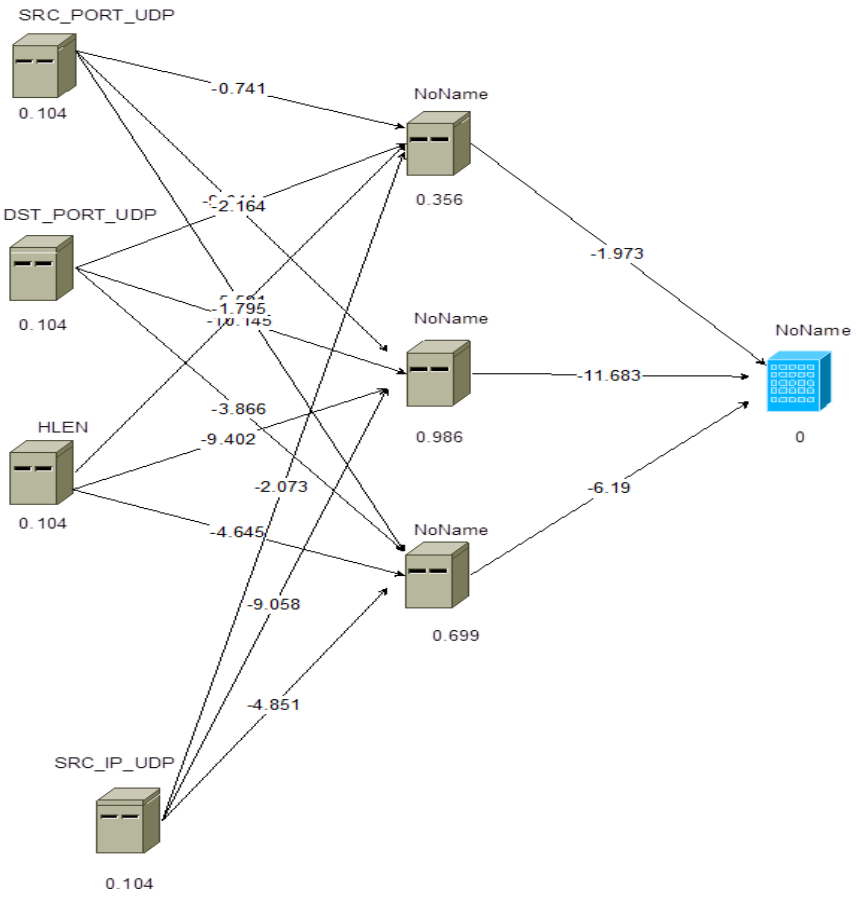


Fig. 7. ANN UDP topological structure.

UDP topological structure is shown in Fig. 6 where UDP source port, UDP destination port, Packet size and source IP address are the input nodes.

The supervised Back Propagation uses the weight that is represented by the numbers between the nodes to calibrate and learn by the patterns (examples). So if we provide more new pattern then it would be better in detecting the attacks. The algorithm keeps on changing the numbers between the nodes (Weight) till the desired result is obtained (having flag either 1 or 0). Fusing all the artificial neural network's as single application against instances can be deficient in availability if the system breaks down technically. Thus, if one instance is technically unavailable or down (for example an instance that detects TCP attack), the other two still will be present to detect TCP and ICMP attacks.

In the meantime, instigating artificial neural network instances separately for every protocol bestows improved maintenance, more control to analyze and to train the algo. The moment detection system detects the forged packets, the defense mechanism is invoked to allow the legitimate traffic go through and drop the forged traffic and as soon as the system flags the traffic as normal the system unblocks the flagged traffic. The legitimate traffic floating through the network and the system will not be interrupted because of being already flagged as legitimate traffic by our proposed system.

Besides the detection system provide the consciousness about attacks through communications via encrypted messages. This kind of information exchange between the detectors enhance the security system by identifying the malicious behavior and if required deploy countermeasures.

VII. Design

We designed our solution to monitor the network continuously for malicious behavior by analyzing the header information of retrieved packets of the networks using trained artificial neural networks. Since retrieving a large amount of data in a network needs higher processing rate and is very expensive. Therefore, to overcome this for every protocol we used an individual packet threshold. If the amount of data packets in specific network is higher than the specified threshold of the protocol then the redeemed packets have to go through investigation. Based on our experiments, we selected the best threshold per protocol by counting the maximum number of data packets per unit time in selected distinctive environment where the true values of threshold are configurable. The amount of data packets are segregated and devised for examination, our proposed mechanism feeds those patterns into artificial neural network to decide the genuineness of the retrieved packets. One DDoS detection system is installed in every network to communicate through encrypted message with other DDoS detectors as shown in Fig. 8.

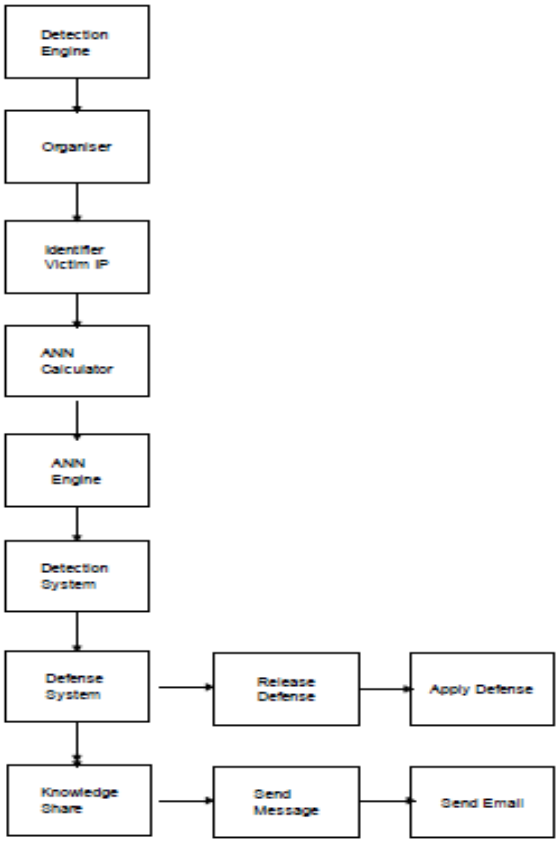


Fig. 8. Detection, defense and cooperative mechanism.

Following are the details of Fig. 7.

1) Install DDoS detectors on different networks.

2) Each DDoS detector will maintain the registered IP address of each hop DDoS detector in order to communicate through encrypted message whenever an attack is detected.

3) There should be continuous monitoring by DDoS detector for abnormal behavior or data.

4) Every passing packet is flagged as abnormal in case the value of passing packets is higher than the threshold.

5) If the value of passing traffic is higher than the threshold then:

a) The organizer removes the undesired characters and arranges the packets accordingly.

b) The victim IP addresses are identified by IP identifier.

c) The retried patterns are calculated by artificial neural network calculator and device them for artificial neural network engine.

d) The patterns are taken as input by artificial neural network engine and produce a single output i.e. 0 for normal and 1 for attack.

e) Step D is repeated three times to produce three outputs before the defense system is invoked.

6) Then the detection system sends the output to the defense system and:

A.

Output	Action	Status
000	0	Traffic clear and allow traffic

B.

111	1	Traffic malicious allow only genuine traffic to pass through
110	1	Traffic malicious allow only genuine traffic to pass through
101	1	Traffic malicious allow only genuine traffic to pass through
011	1	Traffic malicious allow only genuine traffic to pass through

C.

100	0	Repeat point 5
010	0	Repeat point 5
001	0	Repeat point 5

If outcome from C is:

	Output	Action	status
A	111	1	Attack
	110	1	Attack
	101	1	Attack
	011	1	Attack
B	100	1	Low rate attack
	010	1	Low rate attack
	001	1	Low rate attack
C	000	0	No attack

D. However, if the outcome matches none of the above combination then a value 2 is generated by the system that means the traffic is unknown and is not used in the process of training artificial neural networks. In this scenario the system scans its local database to check if some data is received or detected by other hop DDoS detectors. If the neighbor DDoS detection systems respond with 0 or 1 then the algo is obsolete and outmoded as the algo detection was too. Thus proving that the local detector's algo needs and offline retraining with up to date patterns else no action is executed.

7) The knowledge share block communicates with all enrolled neighbor DDoS detectors by sending them encrypted message in cooperating protocol used, destination IP and type of attack. This information is also forwarded to security

offices by emails to let them know about these attacks for logistics purpose.

When we train the algo with old datasets the outcome of the detection system is two and artificial neural network has the special characteristics to detect the unknown pattern if the type of attack or attack itself is similar to the pattern that the algo was trained with. However the experimental results proved that if we train the system with old datasets then the algo fails to detect the unknown patterns. The experiments also proved the fact that the system can detect the known and the unknown attacks if we train the system with up to date patterns while the algo that is trained with old datasets failed in such scenarios. In this situation the artificial neural network of DDoS detection system (detector) that failed to detect attack while other neighboring DDoS detectors detect the same attack that was trained with old datasets previously must be trained with latest up to date datasets but offline because training process is supervised process and different patterns must be instigated or re-instigated whenever required. Thus, when the algo training is not up to date the extra assistance can be acquired from the share knowledge between the detectors to make further decisions. In the meantime every detector sends a complete email including full report of DDoS attacks acquired during that period to the security officers. One deployed detector may collect all the attacks and forward it as a single email to the security officer. However, no information will be sent to the security officer in case the deployed central point is down by any reason and consequently no more countermeasures are deployed if needed. All the DDoS detectors are devised to work and process as a standalone element or distributed detectors which communicates with other registered detectors through encrypted message within the networks or that are deployed in different networks.

Our solution is not confined to a least number of detectors to communicate through encrypted messages. Thus in case one DDoS detector stops functioning the other detectors deployed in the system can still send and receive messages therefore making the solution durable, reliable and resistant to DDoS detector collapse or crash.

To implement our designed solution, we have devised our detection module as plug-in and amalgamated it with Snort-AI (19). Snort AI is devised on Snort signature IDS project (20) and authors of this project are active in providing Snort AI plug-in and other amalgamation processes. The outcome of the IDS is combined with destination IP address to request iptables (21) to elevate malicious or fake packets while allowing legitimate data to pass through. In addition to this, we have also used RSA encryption technique for message encryption over TCP connection while the deployed detectors act as sender and receiver both.

VIII. Evaluation

We used precision, susceptibility – expertise to recognize positive results and specificity – expertise to recognize malicious results, to evaluate our solution. Table 2 represents the comparison of our results with other four approaches and a signature based solution for which quantitative assessments are recorded. We used legitimate and attack data traffic (high and low rate) to test our solution in an isolated and controlled network environment. During our experiments we launched 60 rounds of genuine traffic and 60 rounds of DDoS attacks (ICMP, UDP, TCP) involving 80 to 90 zombies to target the destination. We used UMware boxes to install the zombies and attack from the virtual platform where the boxes were connected to the target devices using virtual routers. We deployed the DDoS detectors between the victims and the virtual router where they examined the data traffic for irregularity and deformity.

Based on the results obtained from our experiments our solution provided a better result in terms of detection, precision, susceptibility and specificity as compared to other solutions including Snort as shown in Table 3 and Fig. 10 to 12, when all the tools were placed in the same manner and same DDoS attacks were launched in the same environment at the same time.

The author (Author Name) used probabilistic neural network over two periods and the accuracy was calculated up to 92% and 97% for attack and normal traffic, respectively. Author name (6) compared back propagation and learning vector quantization. Since our solution is based on back propagation we compared our solution to back propagation that stipulates better precision and performance. In [22] Leu and Pai used as statistical method while [23] Xu, Wei and Zang used KPCA and PSO-SUM to detect DDoS Attacks. KPCA (Kernel Principle Component Analysis) is used to eliminate unnecessary features and PSO (Particle Swarm Optimization) to optimize SVM (Support Vector Machine). During the experiments our solution provided 98% detection accuracy while the percentage of known and unknown attacks was 50% and 48%, respectively. We further evaluated our approach and during the evaluation against low and high rate DDoS attacks the detection results for low and high rates DDoS attacks were 98% and 97.4%, respectively as compared to 93% and 92% of Snort results. We also trained our solution with existing and latest dataset and deployed various known and unknown DDoS attacks. Table 4 and Fig. 9 represent the experimental results.

TABLE III. Comparison of Different Approaches with Our Approach

Approach/Result %	Our Approach	Snort	PNN	BP	Chi-Square	K-PCA-PSO-SVM
Precision	98	93	92:97	90	94	NA
Susceptibility	96	90	NA	NA	92	96
Specificity	100	97	NA	NA	NA	NA

TABLE IV. RESULTS USING OLD AND UP-TO-DATE DATASETS

Our Solution	Accuracy	Susceptibility	Specificity	Precision
Old Datasets	92	88	96	92
Up-to-date Datasets	98	96	100	98

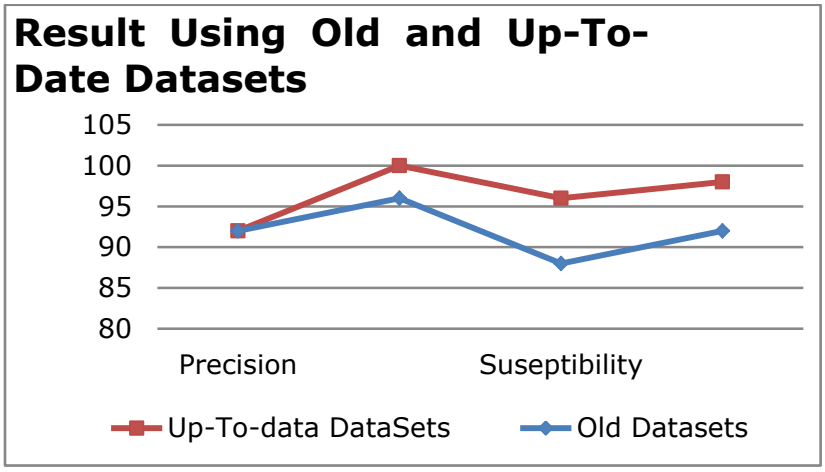


Fig. 9. Result using old and up-to-date datasets.

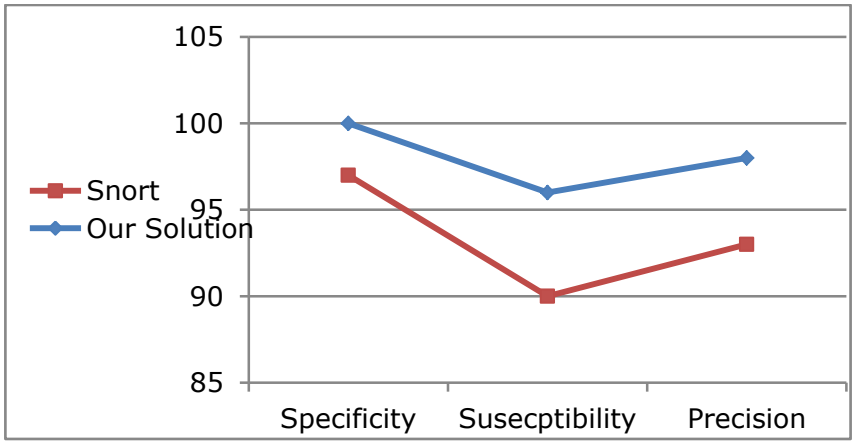


Fig. 10. Comparison result of our solution with Snort.

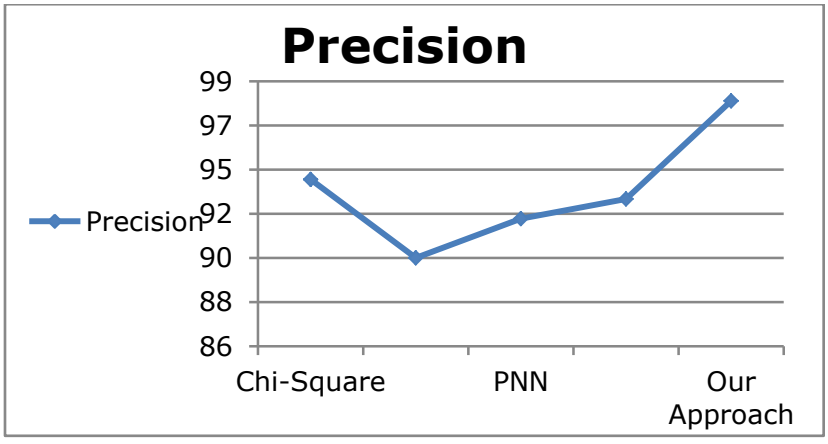


Fig. 11. Comparing our solution with others on Precision results.

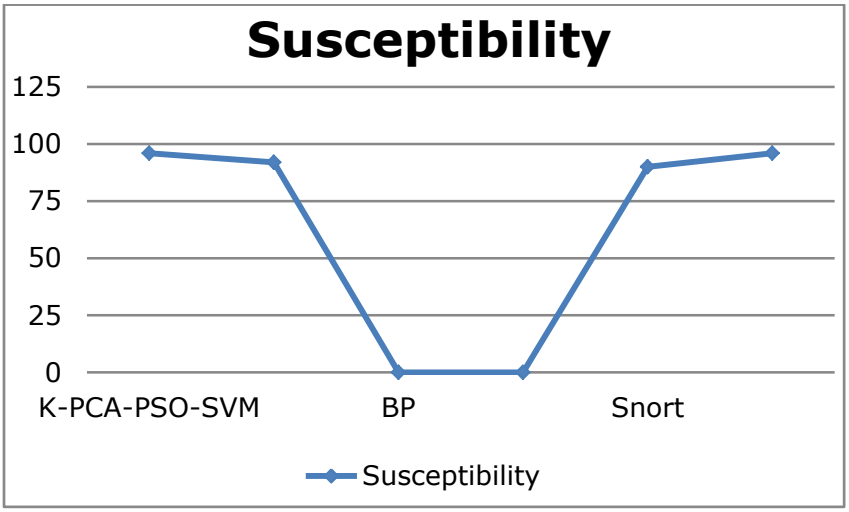


Fig. 12. Comparing our solution with others on susceptibility results.

The results in Table 4 shows that after training our solutions with old datasets, the system responded poorly with 92% of detection accuracy where the detection accuracy is 60% and 32% for known and unknown DDoS attacks respectively. After training our solutions with latest datasets the solution's detection accuracy was 98% with 50% and 48% for known and unknown attacks, respectively. This proved the fact that if we train artificial neural networks with latest and updated datasets the solution can provide better results with greater detection accuracy.

IX. Conclusion

We used trained ANN algo to identify TCP and UDP attacks using the basic key patterns that distinguish between authentic traffic from DDoS attacks. A mirror image of real network environment is used to start the learning process. We launched different DDoS attacks during the flow of the legitimate traffic through the network. JNNS were used to train the algorithm with prepared and pre-processed data sets and Snort AI was integrated with detection technique and got tested against different attacks. We evaluated our designed solution with other related research on signature based. We designed our solution to prevent malicious and fake data packets from reaching the target while letting go the legitimate traffic to pass through. We also evaluated our solution by training it with old existing and recently updated datasets and our designed solution provided better results and detected DDoS attacks that were almost indistinguishable with latest patterns it was trained with. Some DDoS attacks were not detected because the ANN was trained with old data patterns and thus proving that old datasets or improper training can display poor results but different DDoS cases can display better result in detecting DDoS attacks.

Acknowledgement

This research was funded and conducted at Prince Sattam bin Abdulaziz University, Alkharj, Saudi Arabia during the academic year 2017 under research number 2017/01/7091.

References

1. Tariq Ahamad, Abdullah Aljumah,"Detection and Defense Mechanism against DDoS in MANET", Indian Journal of Science and Technology, Vol 8, No. 33, Dec 2015.
2. 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 .
3. 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.
4. Tariq Ahamed Ahanger," An Effective Approach of Detecting DDoSUsing Artificial Neural Networks", IEEE international Conference on Wireless Communications, Signal Processing and Networking March 2017.
5. 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.
6. Tariq Ahamad, Abdullah Aljumah," Hybrid Approach Using Intrusion Detection System", International Journal of Engineering Research & Technology, Vol. 3 Issue 2, February - 2014.
7. 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
8. I. F. Akyildiz and I. H. Kasimoglu, "Wireless sensor and actor networks: research challenges," to be published Ad Hoc Networks, 2004.
9. 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.
10. 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.
11. A. D. Wood and J. A. Stankovic, "Denial of Service in Sensor Networks," IEEE Computer, pp:54-62, 2002.
12. 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.

13. P. J. Criscuolo, Distributed Denial of Service, Tribe Flood Network 2000, and Stacheldraht CIAC-2319, Department of Energy Computer Incident Advisory Capability (CIAC), UCRL-ID-136939, Rev. 1., Lawrence Livermore National Laboratory, February 14, 2000.
14. J. Mirkovic and P. Reiher, A taxonomy of DDoS attack and DDoS defense mechanisms, ACM SIGCOMM Computer Communications Review, vol. 34, no. 2, pp. 39-53, April 2004.
15. S. Ranjan, R. Swaminathan, M. Uysal, and E. Knightly, DdoS-Resilient Scheduling to Counter Application Layer Attacks under Imperfect Detection, IEEE INFOCOM'06, 2006.
16. http://ddosattackprotection.org/blog/large-scale-ddos-attacks/
17. https://www.incapsula.com/ddos/attack-glossary/dns-amplification.html
18. https://www.verisign.com/en_US/security-services/ddos-protection/what-is-a-ddos-attack/index.xhtml
19. https://business.bell.ca/web/Shop/resources/pdf/Voice/White-paper-DDoS-Forrester_Final%20EN.pdf
20. http://blog.bell.ca/costs-and-consequences-of-a-distributed-denial-of-service-ddos-attack/
21. https://www.arbornetworks.com/blog/insight/ddos-as-a-smokescreen-for-fraud-and-theft/
22. http://usa.kaspersky.com/about-us/press-center/press-releases/2015/collateral-damage-26-ddos-attacks-lead-data-loss
23. Mitchell T. M. (1997). Machine Learning, 1st ed. New York, McGraw-Hill Sci-ence/Engineering/Math, ch. 3,4,6,7 pp. 52-78, 81-117, 128-145, 157-198.
24. Pino, M. (September, 2005) "A Theoretical & Practical Introduction to Self Organization using JNNS". University of Applied Sciences Brandenburg.
25. Jayalakshmi, T.; Santhakumaran, A. (2011) "Statistical Normalization and Back Propagation for Classification," International Journal of Computer Theory and Engineering VOL. 3, NO. 1, pp. 89-93.
26. Bedón, C.; Saied, A. (January, 2009) Snort-AI (Version 2.4.3) "Open Source project". Available from: http://snort-ai.sourceforge.net/index.php
27. Roesch, M. (1998) Snort (Version 2.9) "Open Source Project". Available from: http://www.snort.org
28. Russell, R (1998) iptables (Version 1.4.21) "Open Source project". Available from: http://ipset.netfilter.org/iptables.man.html
29. Leu F.; Pai C. (2010) "Detecting DoS and DDoS Attacks Using Chi-Square", Fifth Inter-national Conference on Information Assurance and Security (IAS-09), 18-20 August 2009, Xian, pp.225-258.
30. Aljumah, Abdullah, and Tariq Ahamed Ahanger. "Futuristic Method to Detect and Prevent Blackhole Attack in Wireless Sensor Networks." *International Journal of Computer Science and Network Security (IJCSNS)* 17.2 (2017): 194.
31. Xu, X. ;Wei, D. ; Zhang, Y. (2011) "Improved Detection Approach for Distributed Denial of Service Attack Based on SVM". 2011 Third Pacific-Asia Conference on Circuits, Communications and Systems (PACCS) 17-18 July 2011, Wuhan, pp.1-3
32. Li, J.; Liu, Y.; Gu, L. (2009) "DDoS attack detection based on neural network" 2nd Inter-national Symposium on Aware Computing (ISAC), 1-4 Nov. 2010, Tainan, pp. 196 – 199
33. Akilandeswari, V. ; Shalinie, S.M. (2012) "Probabilistic Neural Network based attack traffic classification". Fourth International Conference on Advanced Computing (ICoAC), 13-15 Dec. 2012, Chennai, pp. 1-8
34. Siaterlis, C. ; Maglaris, V. (2005) "Detecting incoming and outgoing DDoS attacks at the edge using a single set of network characteristics". Proceedings of the 10th IEEE Symposium. on Computers and Communications, (ISCC) , 27-30 June 2005, pp. 469 – 475.
35. Gupta, B.B.; Joshi, C.; Misra, M. (2011) "ANN Based Scheme to Predict Number of Zombies in a DDoS Attack". International Journal of Network Security, VOL.13, No 3, pp.216–225
36. Badishi G.; Keidar I.; Romanov O.; Yachin A. (2006) Denial of Service? Leave it to Bea-ver, Project supported by Israeli Ministry of Science pp. 3-14.
37. Shi E.; Stoica I.; Andersen D. ; Perrig D. (2006) "OverDoSe: A Generic DDoS Protection Service Using an Overlay Network", Technical report CMU-CS-06-114, pp. 2-12 [Online] Available from: www.cs.umd.edu/~elaine/docs/overdose.ps
38. Chen Y.; Hwang K.; Ku W. (2007) "Collaborative Detection of DDoS Attacks over Multiple Network Domains", IEEE Transactions on Parallel and Distributed Systems VOL. 18 NO. 12, pp. 1649 – 1662.
39. Al-Duwairi, B. ; Manimaran, G. (2004) "A novel packet marking scheme for IP trace-back", Proceedings of the tenth International Conference on Parallel and Distributed Systems, 7-9 July 2004. (ICPADS), pp. 195-202
40. Gong, C. ; Sarac, K. (2008) "A More Practical Approach for Single-Packet IP Traceback using Packet Logging and Marking", IEEE Trans on Parallel and Distributed System, VOL. 19 NO. 10, pp.1310-1324.
41. Yu S. ; Zhou, W. ; Doss, R. ; Jia, W (2011) "Traceback of DDoS Attacks Using Entropy Variations", Transactions on Parallel and Distributed Systems VOL. 22, NO 3, pp. 412-425.
42. 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.