A Study on Detection of Distributed Denial of Service Attacks Using Machine Learning Techniques

SRINIVAS KALIME[1], NARESH BODDULA[2]
Assistant Professor[1, 2],
Computer Science and Engineering[1, 2]
Jayamukhi Institute of Technological Sciences[1, 2]
Narsampet, Warangal, Telangana, India[1, 2]
jits.cse2006@gmail.com[1]

*Abstract:*Distributed Denial of Service (DDoS) attacks is a serious threat to the network security. Servers of many companies have been the victims of such novel type of attacks. In a short span of time, these attacks from the multiple bots controlled by the botmaster (cracker) can easily drain the computing and communication resources of the victim. As the attacker uses the spoofed IP address and therefore cracker leaves the botnet quickly after it executes the command, therefore detecting the attacker is extremely difficult. Thus we need an intelligent intrusion detection system (IDS) for DDoS attacks to defend the network services. To develop the system we utilized the various machine learning techniques for detection and analysis of the behaviour of DDoS packets using anomaly-based approach. In this paper, the work is carried out on the novel type of the DDoS attacks that may occur in the network and application layers such as (SIDDoS, HTTP Flood, Smurf and UDP Flood). This work incorporates various well-known classification techniques: Naïve Bayes, Multilayer Perceptron (MLP), and Support Vector Machine (SVM) and Decision trees.

Keywords – DDoS, Bots, IDS, anomaly-based approach, MLP, Naïve Bayes, SVM, Decision trees.

1. Introduction

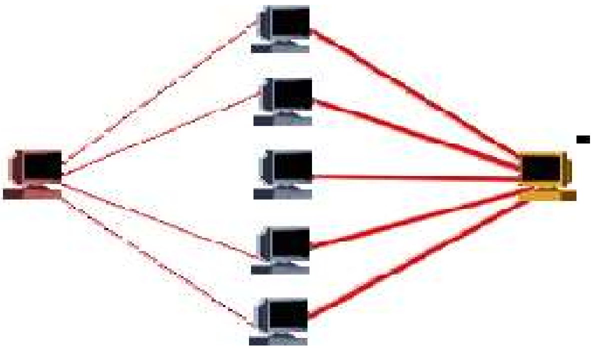
The internet provides the network services to the many organizations and the government firms. Recently the web and network services have suffered from the intruder attacks. The unavailability of these services even for a short time causes the loss of benefits to both users and the companies. Distributed Denial of Service (DDoS) attacks does not steal the data or money from the victims, rather its main purpose is to jam the service for a long time. Since the user might not be able to reuse the services jammed by the crackers, a company attacked by the attacker will lose many benefits.

A DDoS attack can be initiated from many computers (botnets or zombies) hijacked by the attacker (botmaster), and then every computer will send a large number of packets to the target server simultaneously. The bandwidth of the server gets exhausted drastically while responding to the incoming packets and finally, the services stop. A botmaster leaves the botnet quickly after it had executed the command and consequently detecting the cracker is extremely difficult. Therefore detection of these DDoS attacks is the right strategy rather than detecting the crackers.

The intrusion detection system (IDS) is one of the most common solutions to detect the DDoS attacks and preserves the confidentiality, integrity and the availability of the network resources. An IDS system uses the machine learning techniques to detect and analyze the various novel types of the DDoS attacks in an intelligent way. The classification and detection of network traffic is based on some features like average packet size, inter-arrival time, packet size, packet rate, bit rate, etc. which are used to measure and determine whether the network traffic is legitimate or spoofed.

II. Backgorund: Why Ddos Attack?

DDoS attacks have caused severe damage to servers and will cause even greater intimidation to the development of new Internet services. Recently global ransomware virus named as Wannacry have halted network services in about 99 countries. According to recent reports by Kaspersky Lab fourth quarter of 2015. witnessed that resources in 69 countries were targeted by Botnet assisted attacks. Also fourth quarter saw the longest Botnet based DDoS attacks which lasted for 371 hours (i.e. 15.5 days approxmately). Attackers used IoT devices to carry out DDoS attacks – for example, researchers found out that 900 CCTV cameras around the world were compromised and formed a botnet later on used for DDoS attacks. A new type of attack was detected by Kaspersky lab experts on web resources powered by the Word Press content management system (CMS), in which JavaScript code was injected into the body of web resources which then addressed the target resource on behalf of the user's browser. One such DDoS attack lasted 10 hours and thus it is clear that the power of DDoS attacks has not diminished with time [40].



III. DDOS Attack

Distributed denials of service (DDoS) attacks are one of the major threats to the current Internet. In DDoS attack an attacker attempt to prevent legitimate users of a service from using that service. DDOS is a distributed denial of service attack carried out from many sources simultaneously, so there's not just one or two IP addresses to block. The third party services like DNS or NTP became vulnerable to such attacks, so you are actually seeing packets from legitimate sites like businesses or universities which cannot be closed down, though there are ongoing projects to locate and advise these sites of the problem and get them to patch their service. We outline the details of such type of attacks for clarity as shown in fig 1. If ‘A’ an attacker has IP address 1.2.3.4 and ‘B’ victim has IP address 5.6.7.8, ‘A’ can send a packet with ‘B’ IP address 5.6.7.8 as the source to xyz.com and say "tell me all about X". So xyz.com sends a bunch of data to attacker ‘A’ that he didn’t ask for. If ‘A’ do that to abc.com, def.com etc.all asking them to send data to 5.6.7.8, that's a DDOS attack. As a result connection buffer of the victim will be filled up with pending connections which will never be completed, and thus prevent it from answering new requests that may be valid.

A. UDP Flood Attack

The most common type of the DDoS attack is the UDP flood attack. Since UDP (User Datagram Protocol) being the session less networking protocol, therefore it is vulnerable to the malicious attacks. In UDP Flood attack attacker sends large number of UDP packets to random ports of their target server, which results in saturation of the network and the depletion of available bandwidth for legitimate service requests to the victim system [10]. On receiving a UDP packet, a victims system will try to determine the waiting application on the destination port. An ICMP packet is generated if there is no application waiting on the port. If UDP packets being delivered to ports of the victim are large the host resources will be sapped which will lead to inaccessibility [1].The attacker can also spoof the IP address of the packets in the UDP flood attack .As a result, the return ICMP packets will not reach their host, thereby anonymzing the attack.

B. ICMP(Ping) Flood

It is similar to the UDP flood attack. This attack simply exploits the Internet Control Message Protocol (ICMP) used at the network layer, which enables users to send an echo packet to a remote host to check whether it’s alive. In a ICMP flood attack the victim’s network is flooded with request packets. These aim is to get a reply from the victim. By generally sending packets as fast as possible without waiting for replies results in the depletion of the bandwidth of the victim's network. This type of attack can consume both outgoing and incoming bandwidth, since the victim's servers will often attempt to respond with ICMP Echo Reply packets, resulting a significant overall system slowdown. Carrying out such an attack is dependent on attackers knowing the IP address of their target.

C. Smurf Attack

The Smurf attack uses the echo response mechanism of ICMP and is similar to the ICMP flood attack .In a Smurf attack, the victim is flooded with Internet Control Message Protocol (ICMP) echo-reply packets. This attack uses [37]IP broadcasting in which when a packet is sent to an IP broadcast address from a machine on the local network, that packet is delivered to all machines on that network. Under these circumstances, the attacker broadcasts packets with the spoofed source IP address targeted to the victim. Since the packets are sent at broadcast address, it is received by all the nodes within the network [9]. Each node responds back to the victim machine since the source IP address is spoofed as that of the victim's address. This creates a large amount of echo response packets thereby making the network unstable and causing a network congestion to the victim. However Smurf attacks are not effective under IPv6 as when a node receives a packet in IPv6 with a link layer broadcast address it doesn't generate a response.

D. Ping of Death (PoD)

In Ping of Death Attack (PoD), the victims system is flooded with a number of malformed or malformed ping packets to destabilize it or halt the victim's system and the attacker uses the oversized packets by just a simple ping command. Since the maximum packet length allowed at the application layer is 65,535 bytes. However, the Data Link Layer limits the maximum frame size to - for example 1500 bytes over an Ethernet network. Therefore the IP packets are fragmented into the multiple IP packets at the datalink and the recipient host reassembles the IP fragments into the complete packet. In a Ping of Death the attacker manipulates the fragment content and the victim ends up with an IP packet which is larger than 65,535 bytes when reassembled. This causes memory buffers overflow allocated for the packet, leading to denial of service for legitimate packets [10]. Although vulnerabilities leading to PoD are being patched in several systems, unpatched systems are still vulnerable to these attacks. In Ping of death attacks the victim's identity can be easily spoofed and also it does not require the detailed knowledge of the victim's machine, therefore PoD is quite effective.

E. HTTP Flood Attack

HTTP flood attack is the application layer attack in which the attacker exploits the HTTP GET or POST requests to attack a web server or application. This type of attack can cause bandwidth exhausting (HTTP flooding) and resource exhausting. The attacker may use the GET method to exploit the bandwidth exhausting by converging the source traffic to a group of points and results in the high HTTP request rate from the attacker.The server resources such as Sockets, CPU, memory, disk/database bandwidth, and I/O bandwidth can also be caused by the HTTP flood attack. These attacks are also significantly harder to detect and block. An HTTP client like a web browser—talks‖ to an application or server by sending an HTTP request either of GET or POST type [1]. A GET method is used to request a document from the server while a POST method is used to send some information from the client to the server or to access dynamically generated resources. However if the HTTP GET request is incomplete, the Client never sends the complete HTTP header but sends just a part of it. Client continues to send subsequent headers at regular intervals to keep socket alive. The flooding of these incomplete requests results in the exhausting of the bandwidth of the server's resources. Therefore all the legitimate users are denied access to these available resources. HTTP GET-based attacks are simpler to create, and can be more effective in case of a large number of botnets [37]. The POST method exploits the HTTP flood attack the same way the GET method by using the incomplete requests. It forces the server or application to allocate the maximum resources possible in response to each single request. As such it is the most resource consuming.

F. SIDDoS Attacks

SQL Injection Distributed Denial of Service (SIDDoS) is a modern DDoS application layer attack where attackers insert a malicious SQL statement as a string that will pass to the website's database as an equation (e,g through the input values in the website form), and then illegally allowing access to the resources or to the stored data on servers [1]. A SIDDOS attack consumes the server's resources if the malicious code is then forwarded to the server's execution indefinitely. The SIDDOS attack makes the service unavailable for clients by changing their personal information and thus can steal the user data. This type of DDoS will have a harmful effect on a web service and cause it to slow down temporarily and interrupting the services.

IV. Machine Learning Techniques Used In DDOS Attack Detection

Signature based IDS is a human dependent process as it requires several man hours to test, create and deploy those signature and again create new signature for unknown attacks. Thus it becomes necessary to offer a less human dependent system. Anomaly based IDS based on Machine Learning languages provides a solution to this problem, they help in implementing a system that can learn from data and provide prediction for the unseen data based on the learned data [40]. For example, we could train machine learning system on incoming packets so that it can distinguish between intrusive and normal packet. Fig below shows some of the commonly used machine learning techniques for detection of DDoS attack.

A. Naïve Bayes

Naive Bayes is based on the Bayesian method for performing the classification process. It is a simple and easiest technique for constructing classifiers: models that assign class labels to problem instances, represented as vectors of feature values, where the class labels are drawn from some finite set. Paper written by Kanagalakshmi.R et al. [13] proposed that use of Hidden Naïve Bayes (HNB) provides more accurate results than the traditional Naïve Bayes model. Hidden Naive Bayes (HNB) model can be applied to intrusion detection problems (DOS attacks) that suffer from dimensionality highly correlated features and high network Data stream volumes [13]. It is a data mining model that loosens the naive Bayes methods Conditional impartiality assumption. Mouhammad Alkasassbeh et al [1] in his paper collected new dataset that consist of DDOS attacks in different network layers. DDoS attacks are detected using three techniques Multilayer perceptron (MLP), Naïve Bayes and Random Forest. MLP showed the highest accuracy rate (98.63%) as compared to other techniques. Jasreena Kaur Bains et al in [15] proposed a hierarchical layered approach for detection rate of attacks. Model used Naive Bayes classifier with K2 learning process on reduced NSL KDD dataset for each attack class. In the proposed model every layer is trained to detect a single type of attack. The outcome of one layer is passed on to another layer to increase the detection rate. In [17] R Vijayasarathy et al uses a Naive Bayesian (NB) classifier to design a system to detect DoS attacks. The work includes network modelling for two protocols – TCP and UDP. V. Hema et al [18] paper encompasses incorporate flow correlation analysis along with Naïve Bayesian classification process in order to determine the intruded packets in the network. Since the classification scheme is based on posterior conditional probabilities, it identifies attacks that occur in an uncertain situation .The results show that the proposed scheme can effectively classify packets than existing classification models.

B. Support Vector Machine

Support Vector Machine (SVM) was initially proposed by Vapnik and since then has attracted a lot of attention in the machine learning research community. SVM performs the classification and regression by using the supervised learning method [7].Given a set of training examples, each marked as belonging to one of two categories, an SVM algorithm builds a model that predicts whether a new example falls into one of the two categories. Vipin Das et al. [9] in 2010 conducted an experiment to detect DOS attacks using RST (rough set theory) and SVM (support vector machines). Initially packets were captured from the network and RST was used to pre-process the data. The feature set selected by RST is sent to SVM model to learn and test respectively. Then the results are compared with PCA (Principal component analysis) and shows that RST and SMV could reduce false positive rate hence increasing the accuracy. T. Subbulakshmi et al [10] wrote a paper in which the main objective was to monitor the online network and automatically initiate a defence mechanism if any suspicious activity is encountered. Both non-spoofed and spoofed IP can be detected using this approach. The author uses Enhanced Support Vector Machines (ESVM) to detect Non spoofed IP" s and Hop Count Filtering (HCF) mechanism to detect spoofed IP" s These IP" s are used to initiate the defense process. Lanchester Law is used to calculate strength of the attack which is used to initiates the defense mechanism. Rung-Ching Chen et al [11] wrote a paper in which RST and SMV were used to detect dos attacks with different feature set (obtained from RST) supplied to SVM. The focus of paper written by T.Subbulakshmi et al [10] was to create the Distributed Denial of Service (DDoS) detection dataset and detect them using the Enhanced Support Vector Machines. The Enhanced Multi Class Support Vector Machines (EMCSVM) is used for detection of the attacks into various classes for a generated dataset and SVM is used for the evaluation of EMCSVM.

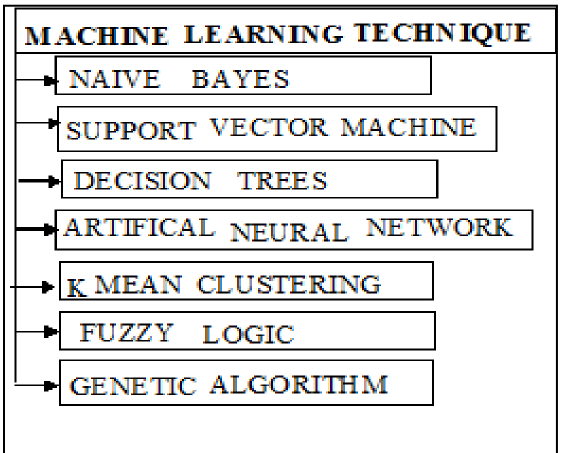


Fig MACHINE LEARNING TECHNIQUES

C. Decision Trees

Decision tree is one of the simple technique used in the machine learning and data mining. It is used as a predictive model in which observations about an item are mapped to conclusions about the item's target value. In the process of decision analysis, a decision tree can be used to represent decisions and decision making visually and explicitly. In this algorithm, the data set is learnt and modelled. Therefore, whenever a new data item is given for classification, it will be classified accordingly learned from the previous dataset [34] [40]. Decision Tree algorithm can also be used for DOS attack detection. Hoda Waguih [2], in his paper proposed a data mining approach to detect DOS attacks, using classification techniques. The above approach lays its basis on classifying "normal" traffic against "abnormal" traffic in the sense of DoS attacks. The paper evaluates the performance of J48 decision tree algorithm for the detection of DoS attacks and then compares it with two rule based algorithms which are OneR and Decision table. Yi-Chi Wu et al. [36] designed a DDoS-detection system based on a decision-tree technique in which after an attack is detected, the system trace back to the attacker's locations using a traffic-flow pattern-matching technique. A C4.5 classifier is used for detection of dos attacks. Dewan Md. Farid et al. [3] in their paper proposed a learning algorithm for anomaly based network intrusion detection system that distinguishes attacks from normal behaviors and identifies different types of intrusions using decision tree algorithm. Data set used is KDD99 benchmark network intrusion detection dataset. The classes in KDD99 dataset categorized into one normal class and four intrusion classes: probe, DOS, U2R, and R2L.

D. Artificial Neural Network

In 1943 McCulloc and Pitts introduced a set of simplified neurons in artificial neural network. These neurons were represented as models of biological networks into conceptual components for circuits that could perform computational tasks. The basic model of the artificial neuron is founded upon the functionality of the biological neuron [19]. Chandrika Palagiri showed that a modelling network can achieve a realistic result to demonstrate a Neural Network, especially for an individual attack. Researchers often focus on a Neural Network that can make decisions quickly and for real-time detection [14]. Wei Pan and Weihua Li used a hybrid Neural Network technique, in which a hybrid Neural Network consisting of a self-organizing map (SOM) and radial basis functions to detect and classify DDoS attacks. The proposed technique achieved a satisfactory accuracy rate result for detecting and classifying DDoS attacks [16]. In a paper written by Madhav Kale et al [21] Resilient Back Propagation (RBP) is chosen as base classifier for research. This paper focused on improving the performance of the RBP classifier by a combination of ensemble of classifier outputs and Neyman Pearson cost minimization strategy, for final classification decision. Detection accuracy and Cost per sample were the two metrics evaluated to analyze the performance of the RBPBoost classification algorithm. Results show that RBPBoost algorithm achieves high detection accuracy with fewer false alarms. Aim of this paper written by Mohammed Salem et al [22] was to determine if it is it is possible for a firewall to analyze its own traffic patterns to identify attempted denial of service. In this paper, a baseline of the network was determined by carrying out the statistical analyses of firewall logs for a large network. Estimated traffic levels were projected using linear regression and Holt-Winter methods for comparison with the baseline. The results of the research were positive with variance from the projected rejected packet levels successfully indicating an attack in the test network. In [23] author Mohammad Masoud Javidi et al proposed IDS, that uses supervised neural network to detect DDOS intrusions in NSLKDD database.In the proposed IDS, author also used signature-based technique. IDSs is designed using the neural network that can identify different types of DoS attacks and designed a separate IDS for each one to detect that specific attack.

E. K-Mean Clustering

K-means clustering is a clustering technique commonly used to automatically partition a data set into k groups. The K-means clustering algorithm works by selecting k initial cluster centers in a data set and then iteratively refining them as follows:

1. Each instance is assigned to its closest cluster centre.
2. The mean of its constituent instances is updated to each of the cluster centre.

The algorithm converges when there is no further change in assignment of instances to clusters. [5] Mangesh, D. Salunke et al[7] proposed an architecture that captures packets ,these packet are the manipulated according to the requirement such as feature selection, transformation etc. then k-means and naïve Bayes classification techniques are used to classify whether the packet is normal or is DOS attack. The simulated botnet traces were mixed with the normal Internet traffic in an experiment carried out by Xiaonan Zang et al. [6] by unifying the RTT extracted from real candidate traffic after filtering. Then the botnet C&C traffic are distinguished using hierarchical and K mean clustering algorithms. This preliminary experiment has shown the capability of the Hierarchical and K mean clustering in detecting botnet flows and provides a RTT adjustment method in mixing the botnet trace with the background normal internet traffic.

F. Fuzzy Logic

Fuzzy logic is derived from fuzzy set theory under which reasoning is approximate rather than precisely derived from classical predicate logic. By the help of fuzzy variables or linguistic terms, intrusion detection features can be viewed easily and decision of normal and abnormal activity in the network are based on its fuzziness nature that can identify the degree of maliciousness of a node [31][35] .In [32] author N.Ch.S.N. Iyengar et al. proposed a fuzzy logic based defense mechanism that can be set with predefined rules by which, it can detect the malicious packets and takes proper counter measures to mitigate the DDoS attack. In the paper written by Stavros N. Shiaeles et.al [33] a method for DDoS detection by constructing a fuzzy estimator on the mean packet inter arrival times is proposed. The problem was divides into two challenges, the first being the actual detection of the DDoS event taking place and the second being the identification of the offending IP addresses. Also author managed to obtain results under a 3 sec detection window. In [24] the author R. Shanmugavadivu designed a fuzzy logic-based system for effectively identifying the intrusion activities within a network. Author used automated strategy for generation of fuzzy rules, which are obtained from the definite rules using frequent items. The experiments and evaluations of the proposed intrusion detection system were performed with the KDD Cup 99 intrusion detection dataset. In [25], author Vladimir et al proposed a detection and prediction mechanism against DDoS attacks in IEEE 802.15.4 using Fuzzy logic system. The main contribution of Fuzzy based detection and prediction system (FBDPS) was to detect the DDoS attackers by comparing the energy consumption of sensor nodes. The nodes with abnormal energy consumptions are identified as malicious attacker. Furthermore, FBDPS is designed to distinguish the types of DDoS attack according to the energy consumption rate of the malicious nodes.

G. Genetic Algorithms

Genetic Algorithms are another machine learning approach based on the principles of evolutionary computation [26]. In other words A Genetic Algorithm (GA) is a programming technique that mimics biological evolution as a problem solving strategy [27].Genetic algorithm based intrusion detection system is used to detect intrusion based on past behavior. A profile is created for the normal behavior based on that genetic algorithm learns and takes the decision for the unseen patterns. Genetic algorithms also used to develop rules for network intrusion detection [34]. In [28] the author Anurag Andhare et al generates rules using Genetic algorithm (GA) based approach to detect DoS attacks on the system. Rule set is generated by training GA on KDD Cup 99 data set to detect attacks on the system. To generate a rule set, the algorithm considers different features in network connections of KDD Cup 99. In[29] author Mohammad Sazzadul Hoque et al proposed an Intrusion Detection System (IDS) which efficiently detects various types of network intrusion, by applying genetic algorithm (GA). A number of Parameters and the evolution processes for GA are discussed and implemented. This approach uses evolution theory to information evolution in order to filter the traffic data and thus reduce the complexity. In [30] author Pankaj Salunkheet et al detects DOS attacks by using Genetic Algorithm (GA) based approach. GA is used to generate rules to detect DOS attacks. The GA is trained on KDD (Knowledge discovery and data mining) cup 99 dataset to generate a rule set that can detect DOS attacks. These rules are applied on IDS system which has a function of data encryption for protecting packets from intruders.

V. CONCLUSION

After thorough review, it is concluded that network attacks are very dangerous and IDS/IPS does not cater to the latest attacks which are affecting the networks. Machine learning techniques are playing vital role in accessing the severity of the attack and thus helping the organizations to take appropriate decisions to restrict such attacks. In future a comprehensive study will be carried out on the data sets which contains the latest types of attacks like HTTP flood, SIDDoS, Smurf and UDP flood etc. collected from the university network using machine learning techniques. This will help to find the severity of the attacks over the university network or any organization, so that appropriate firewall rules will be applied to the network.

VI. REFERENCES

[1] M. Alkasassbeh, G. Al-Naymat et.al," Detecting Distributed Denial of Service Attacks Using Data Mining Technique," (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, pp. 436-445, 2016. Science and Information Technologies, Vol. 6 (2), pp. 1096-1099, 2015.

[2] Hoda Waguih, “A Data Mining Approach for the Detection of Denial of Service Attack”, International Journal of Artificial Intelligence, vol. 2 pp. 99- 106(2013).

[3] Dewan Md. Farid, Nouria Harbi, Emna Bahri, Mohammad Zahid ur Rahman, Chowdhury Mofizur Rahman,‟ Attacks Classification in Adaptive Intrusion Detection using Decision Tree “International Journal of Computer, Electrical, Automation, Control and Information Engineering, Vol:4, No:3, 2010.

[4] Kiri Wagsta,Claire Cardie ,Seth Rogers ,Stefan Schroedl,‟ Constrained K-means Clustering with Background Knowledge‟ Proceedings of the Eighteenth International Conference on Machine Learning, 2001, p. 577-584.

[5] Mangesh D. Salunke ,Prof. Ruhi Kabra,‟ Denial-of-Service Attack Detection “International Journal of Innovative Research in Advanced Engineering (IJIRAE),Volume 1 Issue 11 (November 2014)

[6] Xiaonan Zang, Athichart Tangpong, George Kesidis and David J. Miller Botnet Detection through Fine Flow Classification‟ , CSE Dept. Technical Report No.CSE11-001, Jan. 31, 2011.

[7] V.Vapnik.The Nature of Statistical Learning Theory. NY:Springer-Verlag.1995

[8] Mangesh Salunke, Ruhi Kabra, Ashish Kumar.‟ Layered architecture for DoS attack detection system by combine approach of Naive Bayes and Improved K- means Clustering Algorithm‟ , International Research Journal of Engineering and Technology (IRJET), Volume: 02 Issue: 03, June-2015.

[9] Nour Moustafa, Jill Slay, “Creating Novel features to Anomaly Network Detection using DARPA-2009d Data set”, School of Engineering and Information Technology, Australia, July 2015.

[10] T. Subbulakshmi et.al, ‟ A Unified Approach for Detection and Prevention of DDoS Attacks Using Enhanced Support Vector Machine and Filtering Mechanisms‟ , ICTACT Journal on Communication Technology, June 2013.

[11] Rung-Ching Chen ,Kai-Fan Cheng,Ying-Hao Chen and Chia-Fen Hsieh,‟ Using Rough Set and Support Vector Machine for Network Intrusion DetectionSystem‟ , 2009 First Asian Conference on Intelligent Information and Database Systems

[12] T.Subbulakshmi ,K.BalaKrishnan ; S.M.Shalinie ; D.Anand Kumar ; V.Ganapathi Subramanian ; K. Kannathal.‟ Detection of DDoS attacks using Enhanced Support Vector Machines with real time generated dataset‟ , ICTACT Journal on Communication Technology, Volume: 04, Issue:02, June 2013.

[13] Kanagalakshmi.R, V. Naveenantony Raj,‟ Network Intrusion Detection Using Hidden Naïve Bayes Multiclass Classifier Model,‟ International Journal of Science, Technology & Management ,Volume No.03, Issue No. 12, December 2014.

[14] A. Bivens, C. Palagiri, R. Smith, B. Szymanski, M. Embrechts, et al, “Network-based intrusion detection using neural networks,” Intelligent Engineering Systems through Artificial Neural Networks, vol. 12, no. 1 , pp. 579–584, 2002.

[15] Jasreena Kaur Bains ,Kiran Kumar Kaki ,Kapil Sharma,‟ Intrusion Detection System with Multi-Layer using Bayesian Networks‟ , International Journal of Computer Applications (0975 – 8887) Volume 67– No.5, April 2013.

[16] H. Shahriar, S. North, and W. Chen, “Early detection of SQL injection attacks,” International Journal of Network.

[17] R.Vijayasarathy,Balaraman-Ravindran,S.V Raghavan,‟ A System Approach to Network Modeling for DDoS Detection using a Naive Bayesian Classifier,‟ Department of Computer Science and Engineering IIT Madras, India.

[18] V. Hema and C. Emilin Shyni, ‟ DoS Attack Detection Based on Naive Bayes Classifier, ‟ Middle-East Journal of Scientific Research 23 (Sensing, Signal Processing and Security): 398-405, 2015.

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

[20] 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.

[21] Madhav Kale and D.M. Choudhari, ‟ DDOS Attack

Detection Based on an Ensemble of Neural Classifier, " IJCSNS International Journal of Computer Science and Network Security, VOL.14 No.7, July 2014.

[22] Mohammed Salem, Helen Armstrong," Identifying DOS Attacks Using Data Pattern Analysis," Australian Information Security Management Conference Security Research Institute Conferences,2008.

[23] Mohammad Masoud Javidi, Mohammad Hassan Nattaj, " Journal of mathematics and computer Science 6 (2013), 85-96.

[24] R. Shanmugavadivu, " Network Intrusion Detection System Using Fuzzy Logic, Indian Journal of Computer Science and Engineering (IJCSE), Vol. 2 No. 1.

[25] C Balsrengadurali and Dr.S Saraswathi," Fuzzy Based Detection and Prediction of DDoS Attacks in IEEE 802.15.4 Low Rate Wireless Personal Area Network," IJCSI International Journal of Computer Science Issues, Vol. 10, Issue6, No 1, November 2013.

[26] Vladimir, M., Alexei, V., and Ivan, S. The MP13 approach to the KDD'99 classifier learning contest. SIGKDD Explorations, 2000 ACM SIGKDD. 1(2). January 2000.

[27] Chittur A."Model Generation for an Intrusion Detection System Using Genetic Algorithms, publications/gaidsthesis01.pdf, accessed in 2006.

[28] Mr. Anurag Andhare, Prof. Arvind Bhagat Patil," International Journal of Engineering Research and Applications (IJERA) , Vol. 2, Issue 2,Mar-Apr 2012, pp.094-098.

[29] Mohammad S. Hoque, et.al," An Implementation Of Intrusion Detection System Using Genetic Algorithm," International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012.

[30] Prof. Pankaj Salunkhe ,Mayur Shishupal," Denial-Of -Service Attack Detection Using KDD," International Journal of Application or Innovation in Engineering

& Management (IJAIEM), Volume 4, Issue 3, March 2015.

[31] B. Shanmugam and N. B. Idris, “Anomaly Intrusion Detection based on Fuzzy Logic and Data Mining”, In Proceedings of the Postgraduate Annual Research Seminar, Malaysia 2006.

[32] N.Ch.S.N. Iyengar,et.al," A Fuzzy Logic based Defense Mechanism against Distributed Denial of Service Attack in Cloud Computing Environment" , International Journal of Communication Networks and Information Security (IJCNIS) Vol. 6, No. 3, December 2014.

[33] Stavros N. Shiaeles , Vasilios Katos , Alexandros S. Karakos , Basil K. Papadopoulos," Real time DDoS detection using fuzzy estimators," Elsevier 2012 .

[34] Jayveer Singh, Manisha J. Nene, " A Survey on Machine Learning Techniques for Intrusion Detection Systems, " International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 11, November 2011.

[35] M. Wahengbam and N. Marchang, “Intrusion detection in Manet using fuzzy logic”, 3rd IEEE National Conference on Emerging Trends and Applications in Computer Science (NCETACS, pp.189 – 192, Shillong, 30-31 March 2012.

[36] Yi-Chi Wu, Huei-Ru Tseng, Wu Yang* and Rong-Hong Jan,” DDoS detection and trackback with decision tree and grey relational analysis”, Int. J. Ad Hoc and Ubiquitous Computing, Vol. 7, No. 2, 2011.

[37] M.Aijaz, S. Parveen,” Analysis of Dos and DDoS Attacks”, International Journal of Emerging Research in Management &Technology, Volume-5, Issue- 5.2012.

[38] B.S. Kiruthika Dev et.al,” An Impact Analysis: Real Time DDoS Attack Detection and Mitigation using Machine Learning, International Conference on Recent Trends in Information Technology,2014.

[39] Sherif Saad et.al,” Detecting P2P Botnets through Network Behavior Analysis and Machine Learning”, Ninth Annual International Conference on Privacy, Security and Trust,2011.

[40] Niharika Sharma, Amit Mahajan, Vibhakar Mansotra, Identification and analysis of DoS attack Using Data Analysis tools,” International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Issue 6, June 2016.