International Journal of Advanced Information Science and Technology (IJAIST) *ISSN: 2319:2682*
Vol.5, No.11, November 2016 DOI:10.15693/ijaist/2016.v5i11.73-79

A Hybrid Approach to mitigate DDoS attacks in Wireless Sensor Network

Kamaljeet kaur
Student/Department of CSE
DAVIET Jalandhar,Punjab, India

Parveen kakkar
Assistant Professor/Department of CSE
DAVIET Jalandhar,Punjab, India

***Abstract*— The key objective of distributed denial of service attack is to compile the multiple systems across the internet with infected agents. These agents are designed to attack a particular network with different type of packets. These agents are remotely controlled by an attacker or self installed Trojans that are programmed to launch packet flood. Zombies are the agents used to initiate the DDoS attack. The purpose of this study is to mitigate the DDoS attack using Hybrid Neuro Fuzzy technique in Wireless Sensor network environment. In this paper proposed work shows on three parameters Accuracy, F-measure, Error rate and these parameters shows the better results than the previous one. By applying Hybrid Neuro Fuzzy to the attacked nodes, the system achieves higher accuracy.**

Index terms – DDoS attacks, neuro-fuzzy, accuracy, F-measure, Error rate.

I. INTRODUCTION

A. Distributed Denial of Service Attacks

Distributed denial of service is where the attack source is more than one often thousands of, unique IP addresses. The objective of distributed denial of service attack is to compile multiple systems across the internet with infected agents. These agents are designed to attack a particular network with different types of packets. The infected systems are remotely controlled by an attacker. DDoS attacks are serious security issue that cost organization and individuals a great deal of time, money and reputation. DDoS attacks are launched by affecting the victim in following forms:

- Attacker can find some bug in the software implementation to suspend the services.
- Some attacks deplete all the bandwidth and resources of the target system.

Botnets are been used widely to perform DDoS attacks. This section explains botnet architectures and the tools that have been used to launch DDoS flooding attacks. Many computers are used for launching a DDoS Attack. It makes use of client server technology.

B. Components of DDos attack

In general, DDoS attack comprises of Master, Handler, Agents and victim (as show in Fig) The zombies (agents) are the one used by the master to form a botnet. Larger the number of zombies, more disruptive the attack will be. The Master communicates with agents via handlers. For Example,

handlers can be programs installed on a set of compromised devices (e.g., network servers) that attackers communicate with to send commands. Attacker sends command and controls their agent through handlers. Bots are devices that have been compromised by the handlers. The bots actually carry out the attack on the victim's system. Attacker uses many scanning techniques for finding a vulnerable machine.

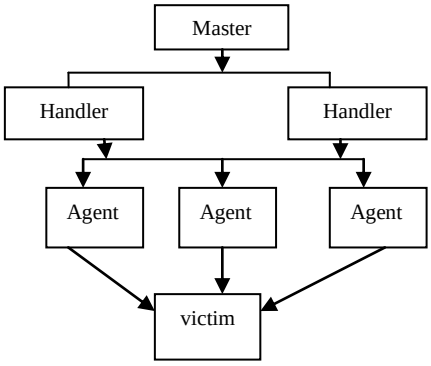

Figure 1. Components of DDoS attack

Random Scan is a simplest strategy which randomly scans whole IPv4 address space as the worm doesn't know where the host is present. It effective only for IPv4 as address space space of IPv6 is too vast.

Hitlist Scan has a list which contains IP address vulnerable hosts in the Internet. The scanning is done in this list. When it makes another machine a host, part of the initial hit list will be sent to that machine.

Route-based Scan reduces the search addresses BGP routing prefixes are used and this prefixes information can reduce the search space drastically.

In Divide-and-conquer Scan technique the scanning is done by different hosts on different part of address space hence saving the resources. Apart from these there are other strategies too like Permutation Scan, Local Preference Scan and Topological Scan. Once host is found after scanning, vulnerabilities of that

host need to be found to gain its control. More information about these vulnerabilities is available on internet.

Classification of DDoS attack

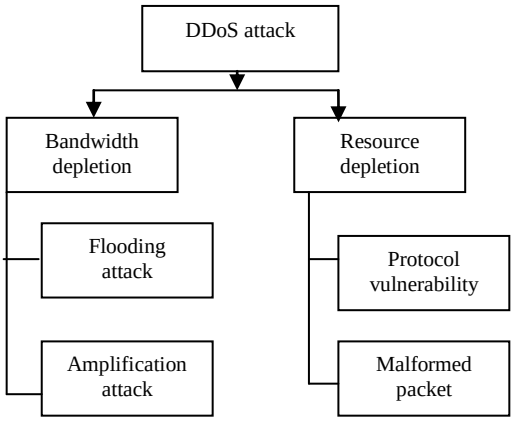

Figure 2. Classification of DDoS attack

The major types include Bandwidth based and resource based attacks. Both types consume the entire bandwidth and resources of the network that's been exploited. Through the analysis made, taxonomy has been depicted in the Fig. Depending upon the exploited vulnerability it can be further divided into different types:

Bandwidth Depletion Attacks: This type of attack consumes the bandwidth of the target system by flooding the unwanted traffic to prevent the legitimate traffic from reaching the victim network. Tools like Trinoo are usually used to perform these attacks. Bandwidth depletion attacks are categorized further as:

• **Flood Attacks**: This attack is launched by an attacker sending huge volume of traffic to the target system with the help of zombies that clogs up the victim's network bandwidth with IP traffic. The victim system undergoes a saturated network bandwidth and slows down rapidly preventing the legitimate traffic to access the network. This is instigated by UDP (User Datagram packets) and ICMP (Internet Control Message Protocol) packets.

• **Amplification attacks:** The attacker sends a large number of packets to a broadcast IP address. In turn causes the systems in the broadcast address range to send a reply to the victim system thereby resulting in a malicious traffic. This type of attack exploits the broadcast address feature found in most of the internetworking devices like routers. This kind of DDoS attack can be launched either the attacker directly or with the help of zombies. The well-known attacks of this kind are Smurf and Fraggle attacks.

Resource Depletion Attacks: The DDoS Resource depletion attack is targeted to exhaust the victim system's resources, so that the legitimate users are not serviced. The following are the types of Resource depletion attacks:

• **Protocol Exploit Attacks**: The goal of these attacks is to consume the surplus quantity of resources from the victim by exploiting the specific feature of the protocol installed in the victim. TCP SYN attacks are the best example of this type.

• **Malformed Packet Attacks**: The term malformed packet refers to the packet wrapped with malicious information or data. The attacker sends these packets to the victim to crash it.[4]

Within this context, the purpose of study is to mitigate the DDoS attack using hybrid neuro-fuzzy technique in wireless sensor network environment. We have chosen hybrid neuro fuzzy technique to mitigate DDoS attack. Hybrid neuro fuzzy technique is the combination of neural network and the fuzzy systems. The neural network has the ability to recognize patterns and to cope with the changing environment. On the other hand fuzzy systems incorporates human knowledge and performs inferencing and decision making. In Hybrid neuro fuzzy system a neural network is used to learn some parameters of the fuzzy system in an iterative way. In this the parameters of fuzzy sets, fuzzy rules & weights of rules are used. It is a five layered architecture.

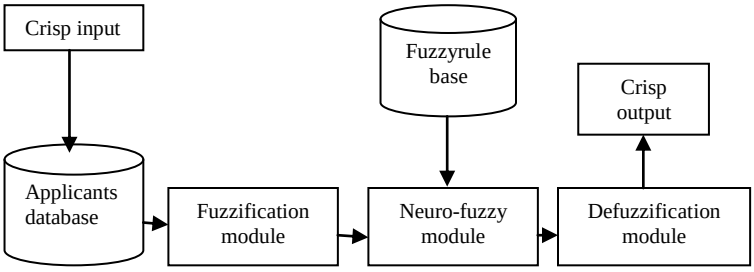

Figure3. Neuro fuzzy architecture

The five phases of Neuro Fuzzy Architecture are shown in fig 3, and these are explained below:

A. Input: Linguistic variables are given input to the input module of the system.
B. Fuzzification: The linguistic variables of the fuzzy rules are expressed in the form of the fuzzy sets where these variables are defined in terms of their associated membership functions. This method of calculating the degree of belongingness of crisp input in the fuzzy set is called fuzzification.
C. Aggregation: After the degree of each linguistic statement is evaluated, they are combined by logical operators such as AND and OR.
D. Activation: Degree of rule fulfillment is used to calculate the output activation of the rules.
E. Accumulation: Output activation of all the rules are joined together to give rise to fuzzy output of system.
F. Defuzzification: If a crisp value of the system is required, the final fuzzy output has to be defuzzified.

II. RELATED WORK

Various methodologies and techniques for reducing the effects of DDoS attack in different network environments

have been proposed and evaluated. Feng qiaojuan and Wei Xinhong[11] proposes an improved network security model and analyzed its advantages. They combined the features of current and proposed security model. Jin li yong liu[2] presented a neural network for ddos attack detection to analyse the server resources and network traffic and they use the learning vector quantisation neural network for post anomly detection. Ruiping lua amd kin choong yow [12] introduced intelligent fast flux swarm network and used the intelligent water drop algorithm for distributed and parallel optimization and fast flux used to connect the swarm nodes, clients, servers. They show that simulation consisting of 400,000 clients node and 10,000 swarm nodes can maintain 99.96 percent packet delivery ratio when the network is under attack. Akilandeswari and shalinie[3] have introduced a probabilistic neural network based attack traffic classification to detect different DDoS attacks. The authors focus on separating flash crowd event from denial of service attacks. They have used the Bayes decision rule for Bayes inference coupled with Radial basis function neural network for classifying DDoS attack traffic and normal traffic. Bansidhar Joshi [13] tested the efficiency of a cloud traceback model dealing with DDoS attacks using backpropagation neural network. Cloud traceback check by using the flexible deterministic packet marking which provides a defense system for finding out the real sources of attacking packets. Mohamed Karim and Belhassen[8] provided a description of massive DDoS attacks and a conceptual framework for detecting and reacting to this type of attack in coordinated fashion. This approach proposes to enhance the security level of SAHER's architecture. The process continues in three rounds: detection phase, exchange of intrusion data, response phase. Mehdi Bharti [1] used the new hybrid detection method using genetic and artificial neural network and deployed for feature selection and attack detection and the multi-layer perceptron of artificial neural network was used to improve the detection rate and accuracy of the system. Javed Asharf[14] analyse the various machine learning techniques which can be used to handle the issues of intrusion and DDoS attacks to software defined networks. Keisuke and Vitaly[6] analyzed a large number of network communication packets and implemented a DDoS attack detection system using the patterns of each IP address. The author selected the SVM with RBF (gaussian) kernel to train and test the DDoS attack detection system. Yuri G. Dantas[7] proposes the technique for mitigating network layer DDoS attacks. They proposes a defense for application layer DDoS attacks based on adaptive selective verification. The defense system is formalized in computational system Maude and evaluated by using statistical model checker PVeStA used to prevent ADDoS. Qiao yan and Richard[5] discuss the new trends and characteristics of DDoS attacks in cloud computing and provide a survey of defense mechanism against DDoS attack in software define network. Author reviewed about launching DDoS attacks on control layer, infrastructure layer and application layer of SDN and methods against DDoS in SDN. YunheCuia and LianshanYan[9] proposed mechanism consisting of four modules attack detection trigger, attack detection, attack traceback, attack mitigation. Mechanism is evaluated on SDN testbed. Experimental results show that the method can quickly initiate the attack detection. Opeyemi osanaiye[10] presented a taxonomy of different types of cloud DDoS attacks and DDoS defense taxonomy. Author reviewed academic literature on DDoS attacks against cloud services and the mitigation strategies published between January 2010 and December 2015.

Some previous research has focused on the source of the attack for the purpose of detection. Various authors presented the review on different techniques for DDoS defense and various machine learning techniques. Although artificial neural network have shown quite significant improvement, in order to detect the DDoS attacks in efficient manner. But still suffers from slow speed and introduces high latency. So to handle these issues hybrid neuron fuzzy system is propose to mitigate DDoS attack.

III. OVERVIEW OF THE PROPOSED MECHANISM

A. Overview of the proposed Mechanism

In this paper we propose a hybrid technique in which neural network and fuzzy logic are combined and worked on different nodes to detect attack in the network.

- The objective of this paper is to study the limitations of existing technique .
- To propose and design hybrid neuro fuzzy system to mitigate DDoS attacks.
- To compare the existing technique with some performance metrices.

DDoS attacks are serious security issue that cost organisations and individuals a great deal of time, money, and reputation they do not usually result in loss of data. The purpose of this study is to propose Hybrid Neuro Fuzzy system to mitigate DDoS attack.the hybrid technique is the combination of neural network and the fuzzy system. Neural network have efficient learning algorithms which are used by the fuzzy system for tuning and to enhance the performance of fuzzy system.The system is prepared in MATLAB 2010. When the nodes start communication within a network some nodes may try to crack the data which are communicating. Save the nodes actions and apply the Hybrid Neuro fuzzy system to detect the attack. Attack is detected by using the fuzzy membership function to decide whether it is attack traffic or genuine traffic using (0,1) 1 represent the attack and 0 represent the normal traffic. If the attack is detected then apply the defense mechanism and mitigate the system from DDoS attack and if not no action is required.

In this J48 classifier model is used which is the dataset of system and there are number of decision trees and based on these trees results are evaluated.

B. Experimental Setup of proposed Mechanism

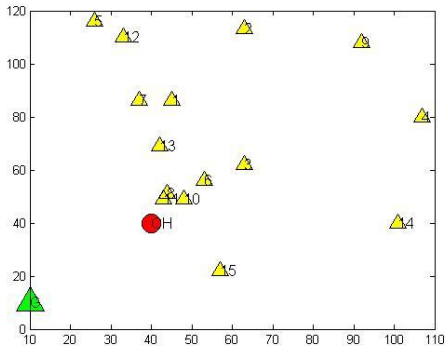

Figure4. Experimental setup of proposed work

In this experimental setup, the interaction between main server, cluster head and nodes have taken place. In this setup, the open flow of data between nodes and cluster head has been considered. In this the architecture is controlled by central server. Here 'G', which is in the green color is the main server or central controller and 'H', which is in red color is the cluster head which further provide data between the nodes. The Data which is required by nodes is fetched from the main server by the cluster head and then the data is passed onto the nodes which require that data. When nodes which are attacker node try to get those data then that nodes are considered as attacker nodes and they will try to request to cluster head to provide data, that nodes will be attacker nodes. The proposed approach has been implemented in MATLAB simulation tool. We have taken the simulation scenario of 15 nodes as shown in Fig.4. Where nodes 2,9,15 are detected as the malicious nodes.

IV. EFFICIENT DDOS DETECTION SYSTEM

A. Neuro fuzzy system

In our proposed system, nodes are dispersed randomly and communicate with each other through server and the cluster head. Main objective of this work is to mitigate DDoS attack using hybrid technique which is the combination of neural network and the fuzzy systems. Neural network has the ability to recognize the patterns and to adapt with changing environment and fuzzy system incorporates the human knowledge and performs inferencing and decision making.

This work is evaluated in the different phases of neuro fuzzy system. In which input is the linguistic variables which is converted to the fuzzy values and output is again a fuzzy values which have to convert to crisp values by using defuzzification method. Proposed technique uses the fuzzy membership functions to decide whether the particular node is attacker node or the genuine node as (1,0). 1 represents the attack and 0 represents the normal traffic. Different phases of the technique are discussed below:

Each layer in the Neuro fuzzy system is associated with a particular step in fuzzy inference process. In this first layer is the input layer. Each neuron in this layer transmits external crisp signals directly to the next layer. That is,

$y_i^{(1)} = x_i^{(1)}$

These are the linguistic variables of the fuzzy rules.

Next layer is the fuzzification layer. In this Crisp values converted to the fuzzy values and these values are the input to the fuzzy sets. Neuron receives a crisp input and determines the degree to which this input belongs to the neuron's fuzzy set. The activation function of a membership neuron is set to the function that specifies the neuron's fuzzy set. We use triangular sets, and the activation functions for the neurons in layer 2 are set to triangular membership functions. A triangular membership function can be specified by two parameters {a,b} as follows:

$$y_i^{(2)} = \begin{cases} 0, \ if\ x_i^{(2)} \le a - \frac{b}{2} \\ 1 - \frac{2\left|x_i^{(2)} - a\right|}{b}, if\ a - \frac{b}{2} < x_i^{(2)}\ a + \frac{b}{2} \\ 0, if\ x_i^{(2)} \ge a + \frac{b}{2} \end{cases}$$

Layer 3 is the fuzzy rule layer. Each neuron in this layer corresponds to a single fuzzy rule. A fuzzy rule neuron receives inputs from the fuzzification neurons that represent fuzzy sets in the rule.

In a neuro-fuzzy system, intersection can be implemented by the product operator. Thus, the output of neuron *i* in layer 3 ia obtained as:

$$y_i^{(3)} = x_{1i}^{(3)} \times x_{2i}^{(3)} \times \ldots\ldots\ldots\ldots\ldots\ldots \times x_{ki}^{(3)}$$

$$y_{R1}^{(3)} = \mu_{A1\times}\mu_{B1} = \mu_{R1}$$

Rules are applied to the fuzzy values.

Layer 5 is defuzzification layer. Each neuron in this layer represents a single output of the Neuro fuzzy system. It takes the output fuzzy sets clipped by the respective integrated firing strengths and combines them into a single fuzzy set.

Neuro fuzzy system can apply standard defuzzification methods, including the centroid technique.

We will use the sum-product composition method.

The sum product composition calculates the crisp output as the weighted average of the centroids of all output membership functions. For example the weighted average the centroids of the clipped fuzzy sets C1 and C2 is calculated as,

$$y = \mu_{C1} \times a_{C1} \times b_{c1} + \mu_{C2} \times a_{C2} \times b_{C2} / \mu_{C1} \times b_{C1} + \mu_{C2} \times b_{C2}$$

These are the phases of the Neuro fuzzy system and evaluated step by step taking the input and applied fuzzy rules on these inputs and output is obtained.

V. PERFORMANCE EVALUATION

A. Simulation Model and Parameters

In the proposed system database weka is used with the dataset j48 classifier model. Weka is Waikato environment for knowledge analysis and contains a collection of visualization

tools and algorithms for data analysis and predictive modelling. Weka was a front-end to modelling algorithms written in other programming language. Weka is freely available under the GNU General Public License. Weka supports several standard data mining task, data processing, clustering, classification, regression and feature selection. J48 is used as the dataset in the proposed work. It is a classifier of weka. Decision tree J48 is implementation of algorithm ID3 (iterative Dichotomiser 3) developed by weka project team. In the j48 classifier model different number of trees are used for the comparison with existing work as shown in table1. In which the number of trees are 14, 15, 16 and proposed work shows the better results. The accuracy and F-measure is increased from the existing work and error rate is decreased.

Our simulation settings and parameters are summarized in table 1.

No. of leaves	25
Size of tree	49
Instances	3333
Attributes	21
Simulation Time	32 sec
Pruning confidence	0.4
Model	Radio transmission

B. Performance Metrics

We evaluate mainly the performance according to the following metrics.

A. Accuracy: Accuracy is the proportion of true results among number of cases. Accuracy is used to describe the closeness of a measurement to the true value. When the term is applied to sets of measurements, it involves a component of random error and a component of systematic error. In this case trueness is the closeness of the mean of a set of measurement results to the actual value. It is also referred to as rand accuracy or rand index. It is a parameter of test. Accuracy is measured with respect to reality. Accuracy is calculated by following equation. In which true positive rate, true negative rate and false positive, false negative rate is considered for the calculation.

Accuracy=(true positive + truenegative)/(truepositive+ trueneagtive + falsepositive + falsenegative)×100

B. F-measure: F-measure is also referred to as F_1 score and it is a measure of a test's accuracy. It considers both the precision *p* and the recall *r* of the test to compute the score: *p* is the number of correct positive results divided by the number of all positive results, and *r* is the number of correct positive results divided by the number of positive results that should have been returned. The F_1 score can be interpreted as a weighted average of the precision and recall, where an F_1 score reaches its best value at 1 and worst at 0. The F-measure can be viewed as a compromise between recall and precision. It is high only when both recall and precision are high. It is equivalent to recall when $\alpha = 0$ and precision when $\alpha = 1$. The F-measure assumes values in the interval [0,1]. It is 0 when no relevant documents have been retrieved, and is 1 if all retrieved documents are relevant and all relevant documents have been retrieved. F-measure is calculated by following equation:

F-measure=2.precision.recall / precision + recall

C. Error rate: Error rate is the frequency of errors. Error rate has many types like bit error rate, bayes error rate, pre comparison error rate and many more. Error rate is calculated by taking the sum of false positive false negative values and divided by the sum of true negative true positive false negative and false positive values. The equation for calculating the error rate is as follows:

ErrorRate =(falsepositive + falsenegative)(truenegative + truepositive + falsepositive + falsenegative)

D. Results

Proposed work is implemented in MATLAB and using J48 classifier model. The results of different parameters compared with existing work are shown in table1. In this we consider the number of trees as 14, 15, 16 and according to this the values are shown. Three parameters are accuracy, F-measure, Error rate in which accuracy is improved from previous work and its 95.6796. F-measure is also improved and its 95.5 error rat eis decreased from previous work and its 4.3204 which is very low.

Table2 results of existing technique and proposed technique

	Existing work			Proposed work
Number of trees	14	15	16	
Accuracy	89.709	86.1086	89.3489	95.6796
F-measure	87.2	80.2	86.6	95.5
Error rate	10.291	13.8914	10.6511	4.3204

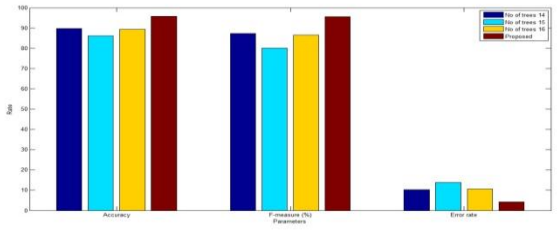

Figure 5. Results of Parameters compared with Proposed Technique

The above graph shows the results of the existing technique with proposed one using three parameters accuracy, F-measure, error rate. This shows that even when the number of trees are increased as 14 ,15 & 16 the results of the proposed technique are higher than the existing technique. The darker color shows the proposed approach and in accuracy its higher and F-measure is also increased from existing technique and error rate is very low with respect to the previous technique. Finally our approach shows the better results as compared with other existing techniques.

VI. CONCLUSION

In this paper a hybrid system is used to mitigate DDoS attacks in wireless sensor network. In which the neuro fuzzy is used for the attack detection and for mitigating it as the DDoS attacks are the serious security issue these days. More work is needed to be done in DDoS attacks attackers uses many techniques to listen and to steal the information of their use and more research is needed in this area. In this paper hybrid neuro fuzzy system is applied to the dataset in which decision trees are used and this technique shows the better results as compared with existing one. In this system is prepared in MATLAB and they have taken the scenario of 15 nodes and when they start communicating some nodes are malicious nodes and try to attack the system and by saving these nodes actions the proposed approach is applied and shows better results. The system shows the more accuracy and less error rate.

REFERENCES

[1]. Mehdi bharti,"Distributed Denial of Service detection using hybrid machine learning technique",IEEE international symposium on biometrics and security technologies 2014 pp268-273.

[2]. jin li yong liu," DDoS attack detection based on neural network",IEEE 2010 pp 196-199.

[3]. V. Akilandeswari," Probabilistic Neural Network based attack traffic classification", IEEE fourth international conference on advance computing 2012.

[4]. Rashmi v. Deshmukh and Kailas k. Davadkar ,"Understanding DDOS attack and its effect in cloud environment ", Procedia computer science 49(2015) pp. 202-210.

[5]. Qiao Yan, F. Richard Yu, "Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges",IEEE communication surveys & tutorials, vol. 18, no. 1, first quarter 2016.

[6]. Keisuke Kato & Vitaly Klyuev,"Large scale packet analysis for intelligent DDoS attack detection development", 9th international conference for internet technology and secured transactions 2014 pp360-364.

[7]. Yuri G. Dantas,"A selective defense for application layer DDoS attacks", 2014 IEEE joint intelligence and security informatics conference",pp 75-82.

[8]. Mohamed Karim Aroua & Belhassen Zouari,"A distributed and coordinated massive DDoS attack detection and response approach",2012 IEEE 36th international conference on computer software and applications workshops pp 230-235.

[9]. YunheCuia, LianshanYan,"SD-Anti DDoS: Fast and efficient DDoS defense in software defined networks",Journal of Network and Computer Applications 68(2016) pp65–79.

[10]. Opeyemi Osanaiye,"Distributed denial of service (DDoS) resilience in cloud: Review and conceptual and cloud framework",Journal of Network and ComputerApplications 67(2016)147–165.

[11]. Feng Qiaojuan,Wei Xinhong,"A new research on DOS/DDOS security detection model",2010 IEEE 2nd international conference on computer engineering and technology vol.3 pp 437-440.

[12]. Ruiping lua and kin choong yow,"Mitigating DDoS attacks with transparent and intelligent fast flux swarm network", 2011 IEEE pp 28-33.

[13]. Peng Xiao," Detecting DDoS attacks against data center with correlation analysis," Elsevier Computer Communications 67 (2015) 66–74.

[14]. Javed Asharf," Handling intrusion and DDoS attacks in Software Defined Networks using machine learning techniques",IEEE National Software Engineering Conference 2014 pp. 55-60.

[15]. Bansidhar Joshi, "Securing cloud computing environment against DDoS attacks",IEEE international conference on computer communication and informatics 2012.

[16]. Alen Saied,"Detection of known and unknown DDoS attacks using Artificial Neural Networks" Elsevier journal of Neurocomputing 172(2016) 385-393.

[17]. Dr S. Saraswathi & J Srikanth,"A fuzzy based detection technique for jamming attacks in 802.15.4 low rate wireless personal area network" IEEE 2012 pp253-259.

[18]. Suchita Goswami & Lalit Kumar P. Bhaiya" A hybrid Neuro-Fuzzy Approach for Brain Abnormality Detection Using GLCM based Feature Extraction" IEEE 2013.

[19]. Q.Zhang,S.Sun,Weighted data normalization based on Eigen values for artificial neural network classification, in :Proceedings of the 16th International Conference on Neural Information Processing, ICONIP, 2009, pp.349– 356.

[20]. T. subbulakshmi, K.BalaKrishnan, S. Mercy Shalinie, D. Anand Kumar, V.Ganapathi Subramanian, K.Kannathal,"Detection of DDoS attacks using support vector machines with real time generated dataset ", IEEE Advanced computing 2011 third international conference 2012.

[21]. 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).

[22]. L.Buczak and E.Guven "A survey of data mining and machine learning methods for cyber security intrusion detection", IEEE, VOL. 18, NO. 2, 2016.

[23]. Siti Hajar Aminah Ali, Seiichi Ozawa, Tao Ban, Junji Nakazato, Jumpei Shimamura,"A neural network model for detecting DDoS attacks using darknet traffic features", IEEE, 2016, pg:2979-2985.

[24]. Neha gupta, Ankur Jain, Pranav Saini and Vaibhav Gupta,"DDoS attack algorithm using ICMP flood", IEEE 3rd international conference on computing for sustainable global development, 2016, pgs: 4082-4084.

[25]. Yonghong Chen, Xin Chen, Hui Tian,"A blind detection method for tracing the real source of DDoS attack packets by Cluster matching", IEEE 8th international conference on communication software and networks, 2016, pgs:551-555.

[26]. Sumeet Kumar and Kathleen M. Carley,"DDos cyber attacks network: who's attacking whom" IEEE conference on intelligence and security informatics, 2016, pgs: 218-218.

[27]. Y. Shui, T. Y. hong, G. Song and W. O. Dapeng. "Can We Beat DDoS Attacks in Clouds", IEEE Transactions on parallel and distributed systems, vol. 25, no. 9, September 2014.

[28]. T. Chin, X. Mountrouidou, X. Li and K. Xiong, "An SDN-supported collaborative approach for DDoS flooding detection and containment," Military Communications Conference, MILCOM 2015 - 2015 IEEE, Tampa, FL, pp. 659-664, 2015.

[29]. B. Wang, Y. Zheng, W. Lou, Y. T. Hou, "DDoS attack protection in the era of cloud computing and Software-Defined Networking" in Computer Networks, Science direct, pp.308–319, 2015.

[30]. K.Santhi. "A Defense Mechanism to Protect Cloud Computing Against Distributed Denial of Service Attacks". IJARCSSE Volume 3, Issue 5, pp. 416-420, May 2013.

Author Profile

Mrs. Kamaljeet Kaur, student of M.tech computer science and engineering. Pursuing M.tech from DAV institute of engineering and technology, Jalandhar. She completed her B.tech from the college of engineering and management Kapurthala, Punjab in 2013. Her area of interest is network security and soft computing technologies and clustering.

Mr. Parveen kakkar, Assistant professor and head of MCA department and incharge of M.tech (CSE) part-time. Qualification is B.tech, M.tech and pursuing Ph.D. His area of interest is information security, handling operating system, Advance computer architecture. Publications: 25 national, international journals and conference. He is a life member of ISTE and life member of Punjab academy of science.