International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.3, 2015

RESEARCH ARTICLE

ISSN: 2321-7758

DDoS DETECTION IN A WIRELESS SENSOR NETWORK USING GENETIC ALGORITHM

PRABHJOT KAUR[1], GURPREET SINGH[2]

[1,2]Dept. of Computer Engineering, Punjabi University, Patiala, India

Article Received: 02/05/2015 | Article Revised on:08/05/2015 | Article Accepted on:12/05/2015

PRABHJOT KAUR

ABSTRACT

Distributed denial of service (DDoS) attack is solitary latest attack that is exhibiting a momentous menace to internet because of its ability to make network resources and server unavailable to the legitimate user by creating a huge amount of unwanted traffic and user becoming incapable of performing normal transactions. The probability of being attacked increases, as the commercial websites such as yahoo, twitter, etc. and the users are becoming more dependent on internet that invites attacker. Amongst all the web application attacks, DDoS are challengingto detect and prevent. While dealing with wireless sensor network, security and privacy are the two important parameters that need to be considered because WSN carry sensitive information critical to the application and operate in an unattended environment.In accumulation, data can be tainted, computer information systems can fail, and interconnect networks may experience distributed denial of service attacks leading to complete failure of system .Therefore this paper focuses on detection of DDoS attacksin WSN by using genetic algorithm which applies crossover, mutation on selected parameters of network traffic to ensure the network strength and consistency.

Keywords-DoS,DDoS,WSNs, GN

1. INTRODUCTION

However like another cyber threats, DDoS attacks are measured as a severe threat to the uptime of website, servers and network. DDoS attacks are defined as attacks propelled from multiple ends of a wireless sensor network in the direction of genuine sensor node, with intent to vitiate the services by draining their limited energy resources [1]. DDoS attacks can lead to the extensive negotiation of all the sensor nodes. Hence, if these attacks are left unnoticed, entire network comes to termination. DDoS attacks are the upgraded version of DoS (denial-of-service) attack enlarged by number of attackers. Fig 1. Indicates the functioning of DDoS attacks. There is one or more than one master computers which are under the control of real attacker.Master machine communicates with the slave or zoombie machine which obeys the control instructions from master machine for launching the attacks by flooding the victim with huge amount of bogus traffic. As, this attacks comes from various compromised machines it results into difficult detection of DDoS.Therefore these are the biggest concern for security professionals.

DDoS attacks can be grouped into three categories[6]:-

- Protocol attacks
- Volume based attacks
- Application layer attacks

In protocol attacks, the attackers main motive is to drench the server resources of the victim so that the services become unavailable to the victim. This attack also influence the midway communication equipment(load balancers, firewalls, etc.). This category comprises ping of death, SYN floods, smurf DDoS and more. In volume based attacks, the attacker attacks by drenching the bandwidth of the victim. It includes attacks like UDP flood, ICMP flood, and other spoofed-packet flood. When attacker's goal is to target application, it comes under application layer attacks. Attacker does not send high amount of fictious traffic ratherthey try to exhaust the resource limits of the web services. It includes attacks like HTTP flood attack, slowloris, etc.

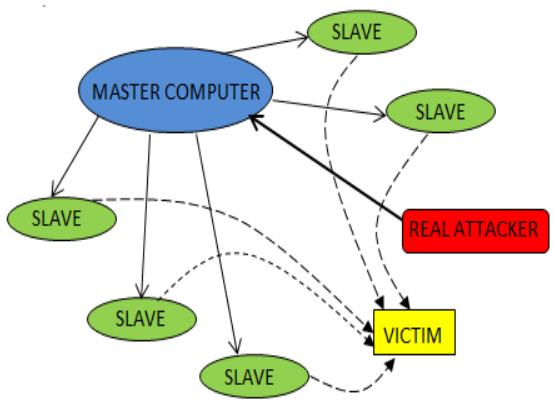

Fig 1. Functioning of DDoS attacks

II. WIRELESS SENSOR NETWORKS(WSNs)

A WSNs composed of large number of sensor nodes which are interconnected and interact with environment to sense the change in the physical conditions and collect the data using wireless medium[2].WSNs transfer the data from the sensor node(source) which sense some event in the environment to the sensor node requiring information about that event(base station). WSNs are penetrating more and more in our life and have many application in military as well as civilian fields. WSNs are vulnerable to many security threats. Therefore, in certain applications , it is essential to protect confidential data and hence ensuring the security of WSNs. Each sensor node is capable to sensing, processing and communicating yet there are many constraints on resources such as memory capacity, battery power, low bandwidth, processing speed make it vulnerable to many kinds of attacks[3] . The nature of wireless medium also helps the attacker to interrupt the gennuine traffic. The security in WSNs is extremely important because physical protection is not present[7]. The most common attacks in wireless sensor network are DDoS(distributeddenial-of-service) and DoS(denial-of-service) attacks. They reduces the network capacity and affects the transmission of information. Therefore, uncovering of these attacks are more important than to recover these attacks.

DDoS attacks are launched by instigating a set of sybil nodes, which adopts multiple routing paths to generate malicious traffic towards a set of victim nodes. When attacker takeoffs DDoS attack, it inserts the nodes into the network which results into the exhaustion of resources of the victim node and attacker have the opportunity to steal the identities of these nodes and then attacker reallot them to the injected fake nodes, initially operating as fictitious sybil nodes. In some cases, the damage caused by DDoS attacks are irreversible and can be catastrophic to all network operations. Therefore, this paper presents the methodolgy which is used for successful detection of these attacks in WSNs.

III. PARAMETERS THAT GET AFFECTED DURING DDoS ATTACKS

Traffic rate analysis was defined as measuring packet traffic in a network [4]. It examines the occurrence rate of a specific type of packets within the stream of monitored network traffic, and is composed of the followingparameters of network traffic that get mostly affected due to the DDoS Attacks lauched by attackers:-

1. Status of Connection

Flag represents the status of connection end whose values includes SF(normal connection end) and REJ(connection requests refusal).

2.Packet loss

Packet loss occurs on broadcast of packets from sender to receiver when number of packets received are less than number of packets sent by the sender. There can be reasons which results into packet loss and DDoS attacks are one among them.

3.Flag rate

TCP header has six flags:-SYN,FIN,RST,PSH,URG,ACK. These flags are tested to determine whether they are set or not. The flags which are set, counted up. So, flag rate is calculated as:-

$$flag\ rate = \frac{\sum(set\ flags\ in\ a\ header)}{\sum(total\ no\ of\ packets)}$$

4. Number of requests per connection

5. Number of tcp sessions established simultaneosly

By investigating these parameters carefully, we can able to sense DDoS attack.

IV. INTRODUCTION TO GENETIC ALGORITHM

Genetic algorithms are search algorithms that are able to create a high quality solution. It uses the principle of evolution and selection for a given problem to produce several solutions. The algorithm starts from an initial population of randomly generated individuals[5]. Individuals are any possible solution and is represented by a string of symbols. Each individual is called as chromosome and is composed of predefined number of genes[8]. At each generations it includes operations like selection, crossover and mutation.

- **Selection:** Selection is usually the first operation applied on a popultion. It give preference to better individuals, that individuals pass their genes to next generation. Goodness of each individual is regulated by fitness that can be an objective function or a subjective judgement.
- **Crossover:** A crossover operator is used to recombine two chromosome/parents which is an array of variable values to be optimized. It is done to get better new two strings/offspring as shown in fig 2.
- **Mutation:** Mutation operator is applied with very low probability, in which the new descendants get few of its bits flipped. The main purpose of mutation is topreserve assortment in the population.

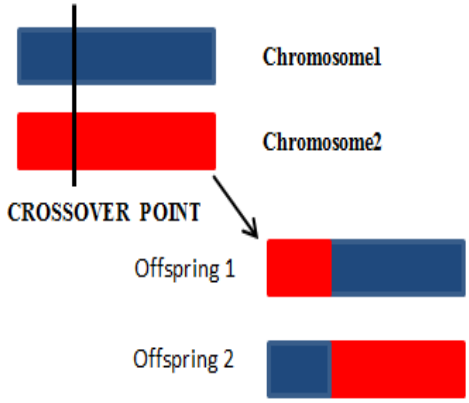

Fig 2. Crossover in two chromosome

V. PROPOSED METHODOLOGY

Figure 3 illustrates the working flowchart of proposed methodolgy that is making use of genetic algorithm to detect the DDoS attack:-

Step 1. Create a wireless sensor network with n nodes and m*n area.

Step 2. User input for no. of generations

Step 3. Set counter=1

Step 4. Select the better individuals(p) among the population

Step 5. Repeat step 5 to 9

Step 6. Select two chromosome

C1=set of three parameters

C2=set of two parameters

Step 7. Assign fitness function

$$\text{Fitness}=\sum_{k=1}^{n} p(k) + \sum_{k=1}^{n} \frac{1}{q(k)}$$

Where p(k) rise with attack and q(k) are those whose value decreases with attack

Step 8. Compare the fitness value with threshold

Step 9. If the condition is true, terminates and display no attack

Step 10. Else apply onepoint, twopoint crossover to selected chromosome with specific probability, entered by user and calculate the fitness function after the crossover

*Step 11.*Apply arithmatic mutation with very low probability

Step 12. Increment counter by 1

Step 10. Increase the generation

Step 13. Compare the counter with the no of generations

Step 14. If it evaluates to true, DDoS attack is present

Step 15. Else , some other problem is present

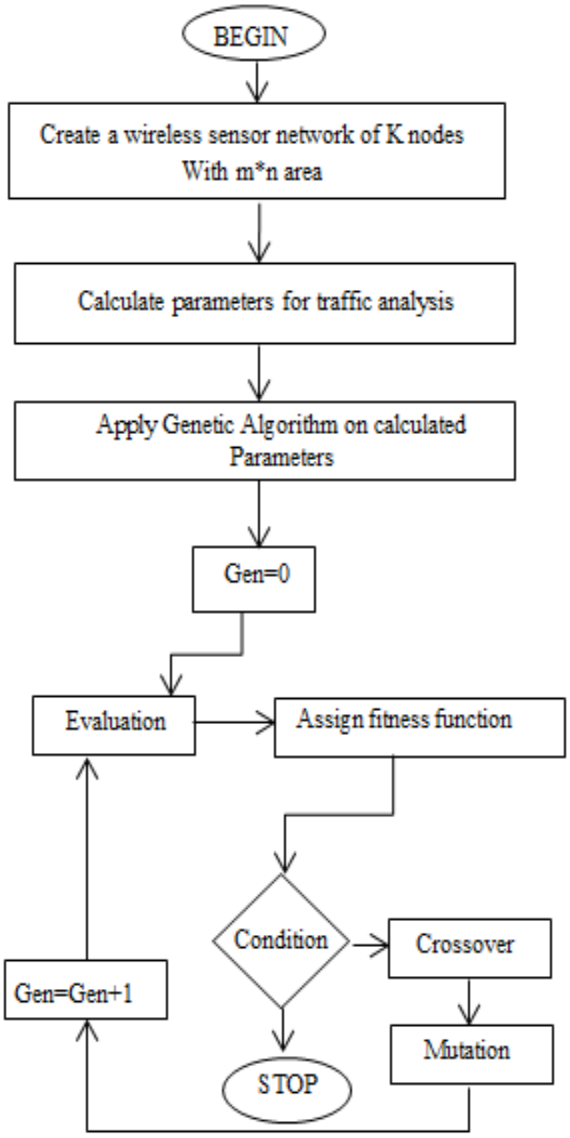

Fig 3. Flowchart of proposed methodology

After the conception of wireless sensor network as shown in fig 4 , parameters are premeditated and genetic algorithm is made functional. In evaluation stage enhanced folks are selected, and allocated the fitness function. A case termination condition is set, if it is reached algorithm execution will be ended, otherwise execution of progression mechanisms will be jerked.

V.RESULT ANALYSIS

The experimental setup consists of 50 nodes at random positions in 100*100 space. Individual nodes preferences up a random position amongst coordinate (0,0) and(100,100) and it is randomly dispensed an ip address Various parameters are calculated which get mostly affected by DDoS attack. Genetic algorithm is implemented and the results are shown in table 1. Figure 6. depicts the relationbetween the packet loss rate and the attack, where 100 value parallels the DDoS ATTACK, 50 to OTHER and 0 to NO ATTACK. With increase in packet loss rate the DDoS attack is detected.

Fig 7. Shows comparison between no of tcp sessions established simulatenously, no of request per connection with some specific crossover probability. On the commence of attack the no of request per connection increases and tcp sessions decreases.

Table 2. embodies the performance of genetic algorithm on wireless sensor network. The proposed algorithm is executed for number of rounds with some specific crossover and mutation probability and indentification of nodes are done. True indentification Corresponds to the number of detected attacks and in fact it is an attack whereas false indentification corresponds to the number of detected attacks but attacks but it is in fact normal. The efficiency of genetic algorithm for detection of DDoS attack is calculated as:-

$$\eta = \frac{true\ node}{true\ node + false\ node} * 100$$

It is observed that genetic algorithm on wireless sensor network shows maximum detection of 95% at crossover probablity of 0.6 and mutation probability of 0.2, executed

for 20 number of rounds, in which 19 nodes are truly identified.

Minimum efficiency is observed at 0.8 crossover probability and 0.1 mutation probability with detection rate of 83.33% for 6 number of rounds, in which 5 nodes are truly identified with average packet loss of 33.0012. Fig 8. Compares the true indentify node with false identify node, which explains that genetic algorithm is successful in indentifying true nodes with overall efficiency of 90.08%.

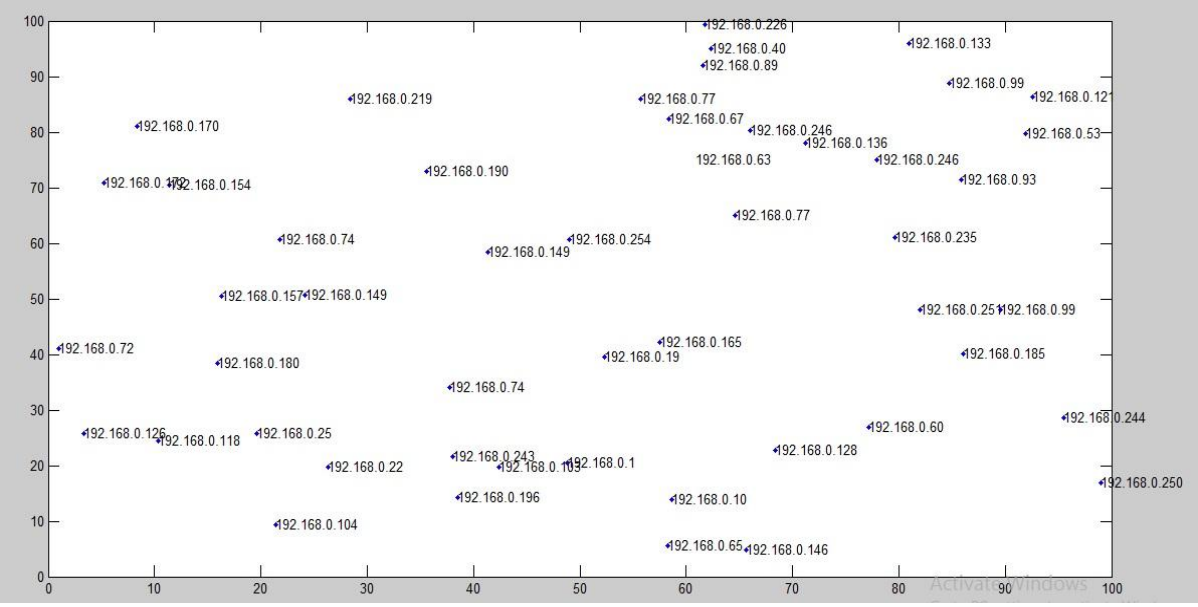

Fig 4. Wireless Sensor Network Deployment

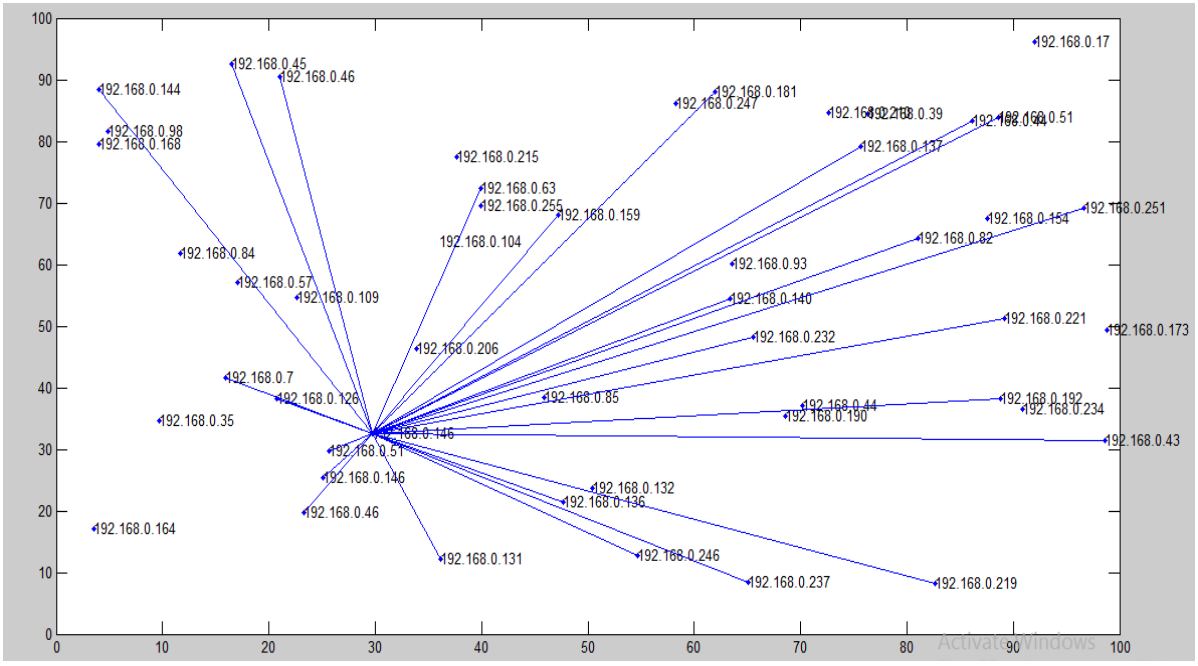

Fig 5. Attack on victim from various machines

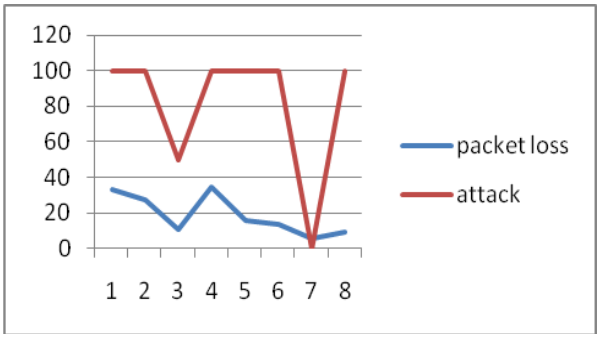

Fig 6. Comparison of packet loss rate with

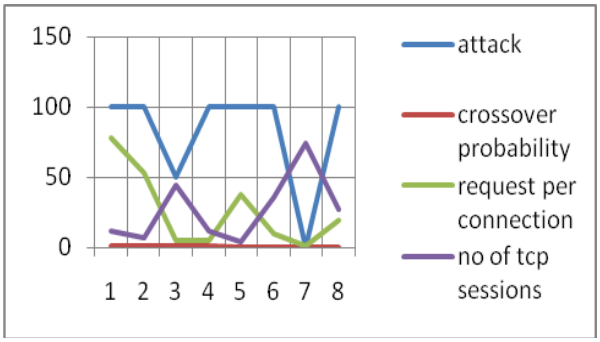

Fig 7. Comparison of request per connection, no of tcp sessions with attack

TABLE I. Results of genetic algorithm on specific crossover and mutation probability

Crossover probability	Mutation probability	Generations	status of connection	Flag rate	No of tcp sessions	Request per connection	Packet loss	Result
0.8	0.1	1000	0	0.0031	12	78	33.4572	Attack
0.7	0.1	972	0	0.0109	7	53	27.0229	Attack
0.6	0.1	72	1	0.0909	44	5	11.0094	Other
0.5	0.1	782	0	0.0253	12	5	34.5833	Attack
0.4	0.1	562	0	0.0069	4	38	15.6802	Attack
0.3	0.1	456	0	0.0105	36	10	13.3381	Attack
0.2	0.1	35	0	0.0072	74	1	5.6529	No attack
0.1	0.1	274	0	0.0082	27	19	9.3464	Attack

TABLE II. Efficiency of DDoS detection with crossover probability

Crossover probability	Mutation probability	No of rounds	Identify true node	Identify false node	Average packet loss	Efficiency
0.8	0.1	6	5	1	33.0012	83.33
0.7	0.1	15	13	2	28.0988	86.67
0.6	0.2	20	19	1	32.4514	95
0.5	0.3	35	33	2	35.2546	91.43
0.4	0.2	50	47	3	34.4751	94

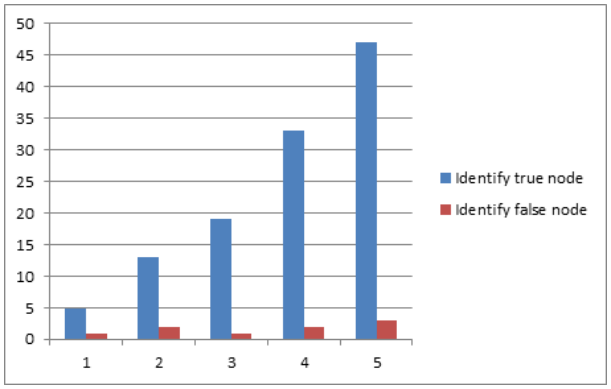

Fig 8. Comparison of true node with false

Figure 9. shows that when average packet loss is high , detection rate of genetic algorithm also increases. Maximum detection rate of 95% is achieved when average packet loss is 32.4514 .

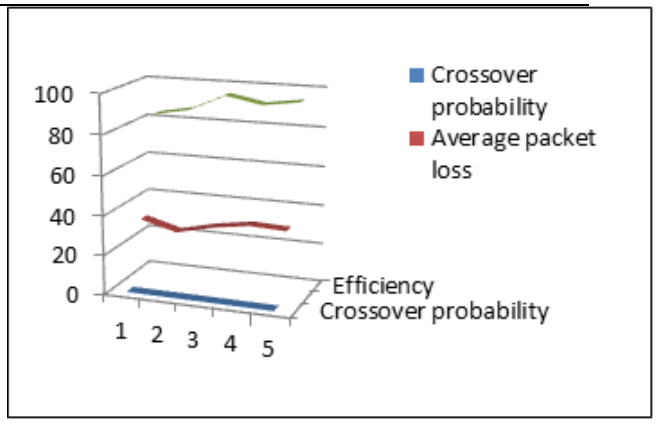

Fig 9. Comparison of average packet loss with efficiency

VI. CONCLUSION AND FUTURE SCOPE

The availability of sensor nodes is under constant threat from Distributed denial of service attacks. This paper offerings a methodology which is making use of genetic algorithm for efficacious detection of DDoS attacks in wireless sensor network with the assistance of three operations selection, crossover and mutation. This paper, aiming at the characteristics of difficult detection

and prevention as to DDoS attacks,proposes a detection modelthat internments the boundaries of network traffic that are predominantly get stimulated by DDoS attack, genetic algorithm is implemented, which is able to perceive attacks with an proficiency of 90.08%.

Data mining is gigsntic field that can be used for intrusion detetion and prevention system. Refined aggressor can easily conquest the security mechanisms. Therefore, many other data mining techniques can be applied for detection of DDoS.

VII. REFERENCES

[1]. KanwalGarg and RshmaChawla, "Detection of DDoS attacks using data mining", International Journal of Computing and Business Research (IJCBR) , ISSN 2229-6166, vol. 2, issue 1, 2011.

[2]. G. Padmavathi and D. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," International Journal of Computer Science and Information Security, vol. 4, 2009.

[3]. J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sensor network security: A survey," Security in Distributed, Grid, and Pervasive Computing, 2006.

[4]. Lee, C., Noh, S., Choi, K., and Jung, G.: Characterizing DDoS Attacks with Traffic Rate Analysis, In Proceedings of the IADIS e-Society, vol. 1, (2003) 81-88

[5]. Hoque M., Mukit M. and Bikas M., "An Implementation of Intrusion Detection System using Genetic Algorithm," International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012

[6]. Yoohwan Kim, Wing Cheong Lau, MooiChooChuah And Jonathan H. Chao,"Packetscore: Statistical-Based Overload Control Against Distributed Denial-Of-Service Attacks" IEEE INFOCOM 2004 ,The 23rd Annual Joint Conference of the IEEE Computer and Communications Societies, Hong Kong, China, March 7-11, 2004. IEEE, 2004.

[7]. Perrig A, Stankovic J and Wagner D, "Security in Wireless Sensor Networks", Communications of the AcM,2004, 47(6), 53-57.

[8]. Mabu S., Chen C., Shimada K., "An Intrusion-Detection Model Based on Fuzzy Class-Association-Rule Mining Using Genetic Network Programming," IEEE Transactions Systems, Man, Cybernetics C, Application and Reviews, volume 41, number 1, pp. 130–139, January 2011.

[9]. SujathaSivabalan and Dr P J Radcliffe, "A Novel Framework to detect and block DDoS attack at the Application layer", IEEE, pp. 578-582, 2013.

[10]. Poongothai and sathyakala, "Simulation and Analysis of DDoS Attacks", IEEE, ISBN 978-1-4673-5144-7, pp. 78-85, 2012.

[11]. P.Sundari, Dr.K.Thangadurai" An Empirical Study on Data Mining Applications" Global Journal of Computer Science and Technology, Vol. 10 Issue 5 Ver. 1.0 pp23-27 July 2010

[12]. YashPravinkumarRaithatha and ChiragSuryakantThaker, "Various Methods used for the Protection, Detection and Prevention of Application Layer DDOS Attacks", International Journal of Computer Science and Management Research , Vol 2, Issue 5, ISSN 2278-733X, pp. 2564-2570, 2013.

[13]. S. Renuka Devi and P. Yogesh, "An Effective Approach to Counter Application Layer DDoSAttacks",IEEE, ICCCNT'12, july 2012.

[14]. SamanTaghaviZargar, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks", IEEE communications surveys & tutorials, vol. 15, No. 4, pp. 2046-2069, 2013.

[15]. SuratoseTritilanunt, SuphanneeSivakorn, ChoochernJuengjincharoen, AusaneeSiripornpisan "Entropy-based Input-Output Traffic Mode Detection Scheme for DoS/DDoS Attacks", IEEE, pp. 804-809, 2010.

[16]. Nisha H. Bhandari, "Survey on DDoS Attacks and its Detection &Defence Approaches", International Journal of Science and Modern Engineering (IJISME), ISSN: 2319-6386, Vol. 1, Issue 3, February 2013.

[17]. Harshal R. Borse, Abhijeet G. garud, jagrutiS.chopada "Advanced Intrusion Detection System Using Data Mining", International Conference of Advance Research and Innovation (ICARI), ISBN 978-93-5156-328-0, pp. 260-263, 2014.