ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2013.0105

A UNIFIED APPROACH FOR DETECTION AND PREVENTION OF DDOS ATTACKS USING ENHANCED SUPPORT VECTOR MACHINES AND FILTERING MECHANISMS

T. Subbulakshmi[1], P. Parameswaran[2], C. Parthiban[3], M. Mariselvi[4], J. Adlene Anusha[5] and G. Mahalakshmi[6]

[1]*Department of Information Technology, Sethu Institute of Technology, India*
E-mail: subbulakshmitce@yahoo.com
[2,3]*Tata Consultancy Services, India*
E-mail: [2]periyasamy.parameswaran@gmail.com and [3]parthibantce@gmail.com
[4, 5, 6] *Department of Computer Science and Engineering, Thiagarajar College of Engineering, India*
E-mail:[4]mmselvi93@gmail.com, [5]adlenejoshva@gmail.com and [6]mahaganapathy.lakshee@gmail.com

Abstract
Distributed Denial of Service (DDoS) attacks were considered to be a tremendous threat to the current information security infrastructure. During DDoS attack, multiple malicious hosts that are recruited by the attackers launch a coordinated attack against one host or a network victim, which cause denial of service to legitimate users. The existing techniques suffer from more number of false alarms and more human intervention for attack detection. The objective of this paper is to monitor the network online which automatically initiates detection mechanism if there is any suspicious activity and also defense the hosts from being arrived at the network. Both spoofed and non spoofed IP's are detected in this approach. Non spoofed IP's are detected using Enhanced Support Vector Machines (ESVM) and spoofed IP's are detected using Hop Count Filtering (HCF) mechanism. The detected IP's are maintained separately to initiate the defense process. The attack strength is calculated using Lanchester Law which initiates the defense mechanism. Based on the calculated attack strength any of the defense schemes such as Rate based limiting or History based IP filtering is automatically initiated to drop the packets from the suspected IP. The integrated online monitoring approach for detection and defense of DDoS attacks is deployed in an experimental testbed. The online approach is found to be obvious in the field of integrated DDoS detection and defense.

Keywords:
DDoS Attacks, Lanchester Linear Law, Enhanced Support Vector Machines, Rate Based Limiting, History Based IP Filtering

1. INTRODUCTION

1.1 COMPUTER SECURITY

The term computer security is used frequently, but the content of a computer is vulnerable to few risks unless the computer is connected to other computers on a network. As the use of computer networks, especially the Internet, has become pervasive, the concept of computer security has expanded to denote issues pertaining to the networked use of computers and their resources.

The major issue faced by today's network is its security against the unauthorized access. Security is the main issue when network is open to public as anyone could have access to the resources available. Attacks are the major concern of the network security. Attacks are bombardment of useless packets into the network. These simply occupy the bandwidth and deplete the resources available for the legitimate users. As this denies the service provided, these sorts of attacks are known as Denial of Service (DoS) attacks. The attack when deployed form various systems globally distributed, then it is known as Distributed Denial of Service (DDoS). In order to recover it from the attackers and provide it to the legitimate users, the attack has to be stopped. This can only be done if the original attacker's IP is known. The packet structure is created such that it contains the source IP in it. Due to the strong technical knowledge of the illegitimate users, the attacks are brilliant enough such that the contents of the packet header's are changed according to the user desire. This could be reflected on the source IP field of the IP header making it not reliable to find the source IP. This is called IP spoofing. Also the dynamic nature of the network makes it difficult to find the real attacker. Hence alternate mechanism has to be adopted to find the attack source.

1.2 TYPES OF DDOS ATTACKS

In order to create the necessary amount of traffic, a network of zombie or bot computers is most often used. Zombies or botnets are computers that have been compromised by attackers, generally through the use of Trojans, allowing these compromised systems to be remotely controlled. Several techniques can be used to facilitate a Distributed Denial of Service attack. Two of the more common are HTTP GET requests and SYN Floods. One of the most notorious examples of an HTTP GET attack was from the MyDoom worm, which targeted the SCO.com website. The GET attack works as its name suggests it sends a request for a specific page (generally the homepage) to the target server. In the case of the MyDoom worm, 64 requests were sent every second from every infected system. With tens of thousands of computers estimated to be infected by MyDoom, the attack quickly proved overwhelming to SCO.com, knocking it offline or several days. A SYN Flood is basically an aborted handshake. Internet communications use a three-way handshake. The initiating client initiates with a SYN, the server responds with a SYN-ACK, and the client is then supposed to respond with an ACK. Using spoofed IP addresses, an attacker sends the SYN which results in the SYN-ACK being sent to a non-requesting (and often non-existing) address. The server then waits for the ACK response to no avail. When large numbers of these aborted SYN packets are sent to a target, the server resources are exhausted and the server succumbs to the SYN Flood DDoS. Several other types of DDoS attacks can be launched, including UDP Fragment Attacks, ICMP Floods, and the Ping of Death [3].

2. RELATED WORK

Whenever the attack is suspected, the network admin has to undergo a manual process of monitoring the interfaces, calculating the attack strength, detect the spoofed IP's using HCF, calculate the defense strength, compare and choose the suitable filtering mechanism by using Lanchester Law to detect and defense attacks

The detection of attacks is an important aspect of defense of DDoS attack and the detection results can affect the overall performance of attack defense. Recently, the DoS attacks are tending to use true source IP address to perform an attack, so it has become more difficult to distinguish between the normal traffic flow and the attack flow, which makes an early and accurate detection more difficult.

It is difficult to distinguish malicious packets from legitimate packets because attackers use general packets for DDoS attack and considering the detection accuracy and complexity in order to detect the attack. For these reasons, a statistical detection method is efficient for detecting DDoS attack. In representative statistical method, packet inter-arrival time, entropy and chi-square algorithm are used. [2]

Brokering agent architecture is considered, as c consisting of a packet collecting agent and an adaptive reasoning agent - an alarming agent – that analyze network traffic, detect DDoS network flooding attacks upon the traffic rate, and finally issue an alarmin case of DDoS attacks. Thus, various machine learning algorithms compile the models of network traffic into different functions l. [6]

Most of the current defense systems are passive, which means the defense actions are taken only after the DDoS attacks are launched. In order to suppress the attack as early as possible, active DDoS defense system is used. In functional range of active defense approaches, the defense system can protect victims before the attack starts.

The system includes a protecting communicating system, which is used to communicate with other coordinated defense system located at different grids. Because the DDoS attacks usually come from different networks, this part is essential to make a successful defense system. Other components of this defense model are intrusion surveillance system, attack control and traceback system. The intrusion surveillance system automatically monitors the potential intrusion actions. It is very important for an effective defense system. In our work, we apply the statistical method to analyze the network characteristics. When its sensors find the malicious scanning, propagation, communication actions or symptoms by flood of possible attackers, it alerts the attack control system and traceback system, and sends the alarm message to coordinated defense systems. The traceback system also plays a key role in the defense system. We find that an effective traceback system relies on an ingenious intrusion surveillance system. Simply passively dropping the malicious packets is not enough to be a strong protection system against DDoS attacks. So the attack control system not only blocks the source attack traffic, but also record the crime actions for later forensic purposes.[2]

Filtering requires being able to filter the flood packets. This can be achieved with signature-based packet filter. If one can create signatures for typical flood packets (TCP packets with zero data size for example or usually large ICMP packets), and filter out those packets, one can then filter the flood packets while allowing normal traffic to proceed. Another filtering option to reject the first IP packet from any IP address. This works with many current generations of attack tools because they tend to use a at distribution random number generator to generate spoofed source addresses and they only use each random address once. Another possibility is to divert traffic based on IP protocol to different servers or even route it differently. Thus for a web server it might be possible to route ICMP and UDP traffic bound for the web server somewhere else entirely or even block it at the router, so that only TCP based floods will succeed. This al least narrows the scope of attacks that can be made. Another filtering technique is called ingress filtering. This filtering prevents spoofed attacks from entering the network by putting rules on point-of-entry routers that restrict source addresses to a known valid range. Filtering can also be based on channel control. This method is known as channel control filtering and can be achieved by filtering out DDoS control messages. This prevents the attacker from causing the attack servers to begin the attack. This can also be accomplished using a signature-based packet filter. If we can develop signatures for most control channel packets, we can simply reject them at the control channel packet filter, and they will disappear from the network. [2]

3. THE PROBLEM STATEMENT

3.1 PROBLEM DEFINITION

Let ‘Ai’ be the number of attackers and ‘V’ be the victim. The attack strength is ‘S’ and defense strength is ‘D’. The Lanchester Law is used to calculate the attack strength ‘S’ form the attack detection results to initiate the corresponding defense mechanism based on the defense strength ‘D’.

3.2 PROBLEM DESCRIPTION

In DDoS attack most of the attacks are spoofed IP. There are two possibilities for spoofed DDoS attack. They are classified as a large amount of traffic comes from a small number of spoofed IP's and a small amount of traffic comes from a large number of spoofed IP's (i.e.) an automated script that will change the spoofed IP from every time period to time. For the early, rate based defense mechanism is suitable while proactive method is suitable for the later. But these techniques have to be implemented manually by the network admin. In order to automate this method Lanchester Linear Law is used to identify the attack strength and from that defense technique can be chosen.

3.3 NEED FOR MONITORING

An essential element of any effective DDoS protection approach is proactive monitoring for traffic anomalies that may be indicators of a growing attack. To keep up with the dynamic nature of attack profiles, respond quickly to suspicious activity, and minimize unnecessary mitigation, organizations must have a flood understanding of what normal network traffic looks like and be able to identify anomalies quickly and accurately. It is

mainly used for Distinguishing suspicious traffic from legitimate traffic, dealing with botnets, managing and defending against DDoS attacks (e.g., by infiltrating or taking down DDoS command-and-control servers).

The integrated approach monitors all the network interfaces both wired and wireless. It is compatible for all types of DDoS attacks such as TCP, UDP, ICMP and Ping Flood. The ten derived and real time parameters which are selected for ESVM training from the literature add more importance to the approach. A single variable is used for calculation of various categories of attacks and combined attacks. The approach provides better accuracy with false alarms. Since the system runs continuously both the detection and defense mechanism are initiated and runs automatically. Enhanced Support Vector Machine (ESVM) is used to improve the detection performance. A suspect confirmation interval is mentioned to determine the type of attack and to reduce false alarms. Lanchester Law is implemented to calculate the attack and defense strength and thereby to initiate the corresponding defense mechanism.

4. THE PROPOSED ARCHITECTURE

DDoS attack classification system consists of eleven major phases, Normal user access behaviors are used to construct normal profile. Application layer and Network layer DDoS attacks such as TCP flooding, UDP flooding, ICMP flooding, Land flooding, HTTP flooding and Session flooding are generated to the web server using the traffic generation program. Information about the attack is collected, preprocessed and fed to the Enhanced Support Vector Machine (ESVM). The phases of attack classification system is listed as,

- Monitoring the victim network
- Attack generation and Attack Strength Calculation
- Non - Spoofed IP's Detection using ESVM
- Spoofed IP's Detection using HCF
- Attack and Defense Strength Calculation using Lanchester Law
- Defense Mechanism Implementation

4.1 MONITORING THE VICTIM NETWORK

It is designed in a portable manner such that all the network interface cards which are in the server are monitored. Even though if the interface address is assigned using DHCP the program automatically gets the interface address and monitors the incoming packets for that server. The attack detection and logs are maintained separately for each network interface and are monitored simultaneously. The number of packets is calculated for each protocol and the attack suspect and confirmation

4.2 ATTACK GENERATION

Attacks are bombardment of packets into a particular system or a network. These attack packets may be of any protocol. The various attacks generated are IP, TCP, UDP, Ping floods. These are generated using C scripts.

4.2.1 Attack Strength Calculation Using Lanchester Law:

In DDoS attack and defense scenario, there are two parties. One is attack party and another is defense party. The network is monitored from victim side. The normal behavior of a network which includes packet arrival rate, individual protocol arrival rate and individual arrival rate from single IP is known already. The network is monitored and any deviation in the normal behavior of the network is suspected as attack and the input traffic is given to the ESVM to confirm the attack. If the attack is confirmed then HCF module is initialized. The reason behind the initialization of HCF is that most of the DDOS attacks are from spoofed IP's so the spoofed IP's need to first eliminated. It would take some little time to analyze the normal behavior and train the SVM.

$$\text{Attack Strength} = \frac{\text{Total no.of packets received from suspected IP}}{\text{Total no. of packets received by the server}} * 100 \quad (1)$$

Lanchester Linear Law is a mathematical technique for calculating the relative strength of prey/predator pair. With firearms engaging each other directly with aimed fire from distance, they can attack multiple targets and can receive fire from multiple directions. The rate of attrition now depends only on the number of weapons firing. Lanchester determined that the power of such force is proportional not to the number of units it has but to the square of number of units. The attack strength is already calculated using the Eq.(1).

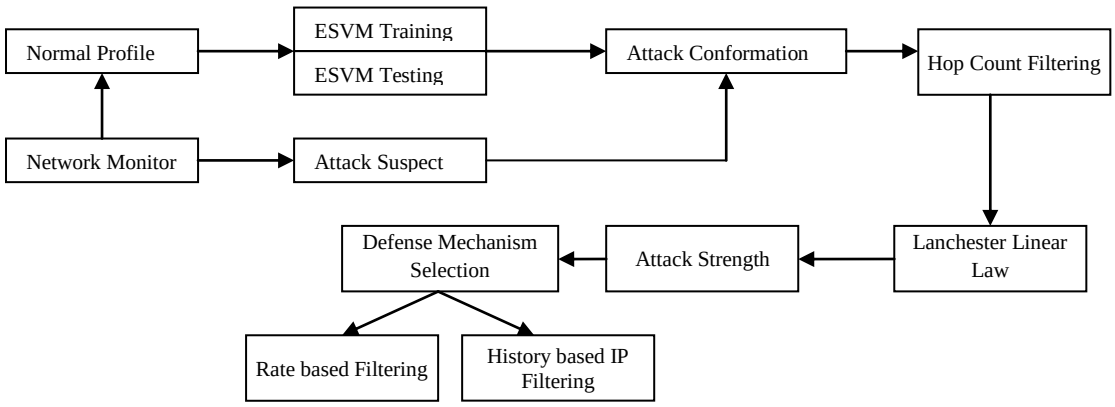

Fig.1. Unified System Architecture for Detection and Defense of DDoS Attacks

4.3 NON SPOOFED IP'S DETECTION USING ESVM

First before monitoring an interface, the normal traffic pattern is analyzed. It is important to set the threshold value properly. Threshold value is the limiting factor and the interfaces crossing these limiting values are considered as attack suspect. The normal profile is generated by the monitoring program considering the arrival traffic as normal traffic. The sample SVM learning file is to be created by manually generating some simple attacks. SVM is ready for online testing.

The parameters used for detection of non-spoofed IP's are in Table.1.

Table.1. SVM Parameters

Sl. No.	Parameters
1	Total Number of packets / duration
2	Number of ICMP packets / duration
3	Number of TCP packets / duration
4	Number of UDP packets / duration
5	Maximum number of ICMP packets
6	Maximum number of UDP packets
7	Maximum number of TCP packets
8	Maximum number of packets
9	Total Number of IP
10	Packet Inter Arrival Time

Table.1 shows the SVM parameters chosen from various literature surveys. Multiclass SVM is used to detect seven types of attacks. The first three classes represent three individual attacks ICMP, TCP and UDP flooding attacks. The next three classes represent the detection of combined attack and the last class represents the combination of these three attacks. The attack classes detected by SVM are given in Table.2.

Table.2. Attack Classes

Class	Attacks
0	Unclassified Attack Suspect
1	ICMP attack suspect
2	TCP attack suspect
3	UDP attack suspect
4	ICMP and TCP
5	ICMP and UDP
6	TCP and UDP
7	ICMP and TCP and UDP

4.4 SPOOFED IP'S DETECTION USING HCF

Hop Count Filtering (HCF) is highly effective in identifying spoofed IP address. An accurate IP2HC table is constructed. The algorithm extracts the course IP address and final TTL value from each IP packet. The algorithm infers the initial TTL value and subtracts the final TTL value from it to obtain the hop-count. The source IP address serves as the index into the table to retrieve the correct hop-count for this IP address. If the computed hop-count matches the stored hop-count, the packet has been authenticated; otherwise the packet is classified as spoofed. HCF is highly effective in identifying spoofed IP address. If TTL matches with the table then it is a normal packet, else it's a spoofed packet. When new IP's arrive, three way hand shake is used to find whether it is legitimate packet or spoofed packet.

4.5 DEFENSE STRENGTH CALCULATION USING LANCHESTER LINEAR LAW

The defense strength of HCF is calculated. Based on the attack and defense strength the proper defense mechanism has to be chosen. According to Lanchester Law, the attack strength depends on two factors namely number of attackers and individual attack rate. The attack packets prevented by the defense algorithm is the defense strength. This is the effectiveness of the defense algorithm.

$$\text{Defense Strength} = \frac{\text{Total no of attack packets before defense}}{\text{Total no of attack packets after dense}} \quad (2)$$

4.6 DEFENSEMECHANISM IMPLEMENTATION

If the attack rate is very high from small number of host IP's, rate limiting can be applied. If the attack rate is even from large number of host, then history based IP filtering is chosen. In Rate based filtering technique, based on the level crossing rate is devised. It adapts the frequency rate and the filter order following the input signal local variations. Thus it correlates the processing activity with the signal variations. Victim which is above the given rate is suspected and the record is inserted into the IP table of the router and blocked which protects it from the attack. In History based IP filtering, the gateway keeps a history of all the legitimate IP addresses which have previously appeared in the network. When the edge router is overloaded, this history is used to decide whether to admit incoming packets. Victim keeps behavioral history for source IP's from low-trust sources. Addresses that appear frequently or send sufficient number of packets in previous communication interval are denoted as trustworthy.

5. IMPLEMENTATION DETAILS

5.1 CREATION OF ENVIRONMENT

The environment is created in a manner that all the packets that are directed to the victim should pass through the gateway. When the attack is confirmed, the packets from the attacking hosts are blocked in the gateway itself protecting the victim machine.

5.2 DETECTION AND DEFENSE SCENARIO

The attack traffic is generated by executing the C program for different attacks. The basic ping flood can be generated using the command

ping - f[destination IP] - c[count]

TCP, UDP and ICMP attacks are generated using packet generation program.

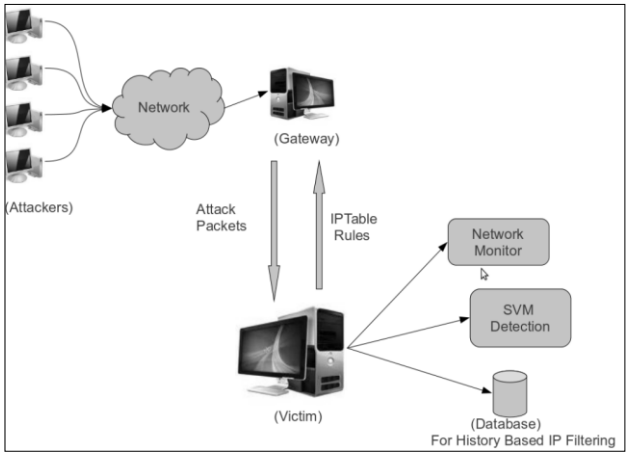

Fig.2. Environment Scenario

Table.3. SVM parameters and calculation

Parameters	Calculation
Total Number of packets / duration	Number of Packets reaching the Server in Particular duration
Number of ICMP packets / duration	Number of ICMP Packets reaching the Server in Particular duration
Number of TCP packets / duration	Number of TCP Packets reaching the Server in Particular duration
Number of UDP packets / duration	Number of UDP Packets transmitted from a single IP to the server after suspection reaching the Server in Particular duration
Maximum number of ICMP packets	Maximum Number of ICMP packets transmitted from a single IP to the server after suspection
Maximum number of UDP packets	Maximum Number of UDP packets transmitted from a single IP to the server after suspection
Maximum number of TCP packets	Maximum Number of TCP packets transmitted from a single IP to the server after suspection
Maximum number of packets	Maximum Number of packets transmitted from a single IP to the server after suspection
Total Number of IP	The Number of Hosts in Communication with the Server
Packet Inter Arrival Time	Time interval between arrival of two consecutive packets

The Table.3 shows the calculation of SVM parameters. Every interface is monitored and if any attack is to be found in the network, first it is predicted, SVM testing _le is generated simultaneously. If the predicted attack doesn't continue for a period of time it is termed as False Alarm. If the predicted attack is suspected then the SVM training _le is processed by Hop Count Filtering, which is chosen as the first defensive mechanism as most of the DDoS attacks are spoofed attacks. Simultaneously attack strength is also calculated, IP monitoring is also done to find the suspected hosts.

The spoofed IP's are eliminated by Hop Count Filtering and thus the number of original suspected hosts which are considered as attackers are found. According to Lanchester Linear Law, attacking strength depends on number of attackers and their individual attack strength. Thus the deviation from the normal behavior can be found easily as suspected hosts and their individual strength is available. So depending the deviation, either rate based filtering or history based IP filtering mechanism is chosen.

For rate based filtering, considering the rate of packet arrival the IP is removed from the IP table. For history based IP filtering, the IP record is updated in the database and the log is maintained for two days.

6. RESULTS AND DISCUSSIONS

6.1 MODEL OF NORMAL PROFILE

A model of normal profile is created from the network traffic given in Table.4. Class -1 represents no attack, Class 1 represents ICMP Attack, Class 2 represents TCP Attack and Class 4 represents UDP attack. For parameters refer Table.3. The period of updation of normal records is 50 seconds.

Table.4. Model normal profile

Class	1	2	3	4	5	6	7	8	9	10
-1	30	30	0	0	30	0	0	30	1	0
1	3756	3756	0	0	3756	0	0	3756	2	0
2	4332	0	4332	0	0	4332	0	4332	1	0
4	5727	0	0	5727	0	0	5727	5727	2	0

6.2 MONITORING THE VICTIM NETWORK

All the network interfaces are monitored. User can start/stop the network monitoring, results can be fetched from the database and sample attacks can be generated. The number of interfaces in the victim is observed and for each and every interface their IP are found.

Table.5. Interfaces Monitored

Sl. No	Interface Number	IP
1	0	10.7.5.46
2	1	192.168.45.113
3	11	127.0.0.1

Interface number represents eth0 having contact with 10.7.5.46, eth1 having contact with 192.168.45.113 and loopback having contact with 127.0.0.1 respectively.

Table.6. Monitoring the Interface

Time(sec)	ICMP	TCP	UDP	Total number of packets
5	5	2	0	7
10	7	30	4	41
15	11	40	6	57

While monitoring the network, the ICMP, TCP, UDP and total number of packets arrived are given in the above table with the duration in seconds.

Table.7. Normal Traffic

Source IP	Total	ICMP	TCP	UDP	Total number of packets in last 5 sec
10.7.5.1	900	100%	0	0	35
10.7.5.109	25	100%	0	0	5
10.7.5.9	70	0	90%	0	2
10.7.5.6	50	0	0	100%	3

The above table shows the normal traffic from various IP's. It contains of total number of packets, ICMP, TCP, UDP and total number of packets arrived in last 5 sec from the respective IP's.

6.3 ATTACK STRENGTH

The attack strength is calculated from the log of suspected IP's.

$$\text{Attack Strength} = \frac{\text{Total no.of packets received from suspected IP}}{\text{Total no. of packets received by the server}} * 100$$

Table.8. Attack Traffic

Source IP	Total	ICMP	TCP	UDP	Total number of packets in last 5 sec
10.7.5.1	90000	100%	0	0	6000
10.7.5.109	25	100%	0	0	5
10.7.5.9	7000	0	90%	0	200
10.7.5.6	5000	0	0	100%	150

The above table shows the attack traffic and the deviation from normal traffic.

Table.9. Attack Strength

Suspected IP	Suspected Count	No. of packets transmitted	Suspect %
10.7.5.1	11	90000	91%
10.7.5.44	14	85000	85%
10.7.5.46	14	65000	67%
10.7.5.47	14	82000	82%
10.7.5.48	14	77000	79%

The above table shows the attack strength from the respective IP's and the suspect percentage. Eventually a dump file is created for HCF. Thus the calculated strength is termed as the defense strength of HCF.

6.4 SVM TRAINING RESULTS

Table.10. SVM Training results

Type of SVM	Type of kernel	Gamma Value	No of class	No.of SV	Training Time
N_svc	Rbf	0.1	7	63	50

The above table shows the SVM training results stating the type of SVM, kernel, gamma value, number of class and number of support vectors and training time.

6.5 SVM TESTING RESULTS

Table.11. SVM Testing Results

No. of records	Accuracy	Attack Confirmed/ Not confirmed
10	45	Attack not confirmed
10	64	Attack confirmed
10	86	Attack confirmed

The above table shows the SVM testing results for deciding the attack confirmation.

6.6 SPOOFED IP'S DETECTION USING HCF

The following is the list of spoofed IP's detected using HCF.

Table.12. List of spoofed IP's

Source IP's	Hop Count
10.7.5.*	0
10.2.*.*	8

The list of spoofed IP's are shown in the above table. All IP's mentioned in the subnet mask are considered as spoofed IP's.

6.7 LANCHESTER LAW

Total number of attacking hosts = Suspected IP's – Spoofed IP's

Average arrival from IP

$$\text{Deviation from Normal Behavior} = \frac{\text{calculated for attack strength t able}}{\text{Normal Threshold Value}}$$

By comparing the attack and defense strength, the appropriate suitable mechanism is chosen.

Table.13. Algorithm Selection

Sl. No	No of IP's in contact	Max no. of packets from single IP	Defense Mechanism
1	4	100	-
2	2	3000	Rate based filtering
3	146	200	History based IP filtering
4	10	5000	Rate based filtering

The above table shows the decision making to select the appropriate filtering mechanism.

6.8 RATE BASED FILTERING

Table.14. Initial IP table of Gateway

Target	Prot	Opt	Source	Destination
ACCEPT	All	- -	10.7.1.1	Anywhere
DROP	All	- -	10.7.0.0/16	Anywhere

The above table shows the initial IP table of gateway.

Table.15. IP table after attack confirmed from 10.7.5.110

Target	Prot	Opt	Source	Destination
ACCEPT	All	- -	10.7.1.1	anywhere
DROP	All	- -	10.7.0.0/16	anywhere
DROP	All	- -	10.7.5.110	10.7.5.121

The above table shows the IP table after attack confirmation from 10.7.5.110.

6.9 HISTORY BASED IP FILTERING

Table.16. Sample records in database

IP	Max arrival rate	Max arrival date	Last contact rate	Last contact date
10.7.5.1	100	2011-2-15	15	2011-2-16
10.7.5.110	45	2011-2-16	5	2011-2-16
10.0.0.14	30	2011-2-16	30	2011-2-16
10.0.0.13	40	2011-2-16	40	2011-2-16
10.0.0.1	1	2011-2-15	0	2011-2-15
10.20.0.31	400	2011-2-16	200	2011-2-16

The above table shows the sample records in the database featuring history based IP filtering.

7. CONCLUSION

The integrated approach is implemented in the experimental testbed and performance metrics for suspecting DDoS attack are monitored, comparison of attack and defense strength is done by using Lanchester Law and the malicious packets are filtered. The network is also trained for detecting the onset of DDoS attacks. The tool which is generated is an initial step to suspect the DDoS which uses only two filtering mechanism (i.e.) rate based filtering and history based filtering. In near future, the tool will be enhanced in way that supports all the available filtering mechanism.

REFERENCES

[1] Zhongwen Li and Yang Xiang, "Mathematical Analysis of Active DDoS Defense System", *International Conference on Computational Intelligence and Security*, Vol. 2, pp. 1563 - 1566, 2006.

[2] Tao Peng, Christopher Leckie and Kotagiri Ramamohanarao, "Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring", *Proceedings of the Third International IFIP-TC6 Networking Conference*, pp. 771 - 782, 2004.

[3] Byunghak Song, Joon Heo and Choong Seon Hong, "Collaborative Defense Mechanism Using Statistical Detection Method Against DDoS Attacks", *IEICE Transaction on Fundamentals /Communication /Electronic /Information and System*, Vol. E85-A/B/C/D, No. 1, pp. 1 - 10, 2007.

[4] Yan Zhang, Jun Zheng and Miao Ma, "*Handbook of Research on Wireless Security*", Information Science Reference, 2008.

[5] Sanguk Noh, Cheolho Lee, Kyunghee Choi and Gihyun Jung, "Detecting Distributed Denial of Service (DDoS) Attacks Through Inductive Learning", *Lecture Notes in Computer Science Series 2690*, pp. 286 - 295, 2003.

[6] T. Subbulakshmi et al., "Detection of DDoS attacks using Enhanced Support Vector Machines with real time generated dataset", *Third International Conference on Advanced Computing*, pp. 17-22, 2011.

[7] Eldrige S. Adams and Michael Mesterton-Gibbons, "Lanchester's attrition models and fights among social animals", *Oxford Journals*, Vol. 14, No. 5, pp. 719 - 723, 2003.

[8] A Ramamoorthi, T Subbulakshmi and S. Mercy Shalinie, "Real time detection and classification of DDoS attacks using Enhanced SVM with string kernels", *International Conference on Recent Trends in Information Technology*, pp. 91 - 96, 2011.

[9] Afroze, A.Farah and T. Subbulakshmi, "Multiple learning based classifiers using layered approach and Feature Selection for attack detection", *International Conference on Emerging Trends in Computing, Communication and Nanotechnology*, pp. 308 - 314, 2003.