computing@computingonline.net
www.computingonline.net

Print ISSN 1727-6209
On-line ISSN 2312-5381
International Journal of Computing

PERFORMANCE ANALYSIS OF AGENT BASED DISTRIBUTED DEFENSE MECHANISMS AGAINST DDOS ATTACKS

Karanbir Singh [1], Kanwalvir Singh Dhindsa [2], Bharat Bhushan [3]

[1] IKG Punjab Technical University, Jalandhar, Punjab, India, karan_nehra@yahoo.co.in
[2] Baba Banda Singh Bahadur Engg. College, Fatehgarh Sahib, Punjab, India, kdhindsa@gmail.com
[3] Guru Nanak Khalsa College, Yamunanagar, Haryana, India, bharat_dhiman@hotmail.com

Paper history:
Received 19 December 2017
Received in revised form 10 March 2018
Accepted 20 March 2018
Available online 31 March 2018

Keywords:
DDoS attacks;
DDoS defense;
agent;
network security;
performance evaluation.

Abstract: The current internet infrastructure is susceptible to distributed denial of service (DDoS) attacks and has no built in mechanism to defend against them. The research on these kinds of attacks and their defense is significant for the security and reliability of the internet. We have already proposed a collaborative agent based distributed DDoS defense scheme which detect and prevents against DDoS attacks in ISP (Internet Service Provider) boundaries. The actual task of defense is carried out by agents and coordinators in each ISP. The defense system works by inspecting incoming traffic on edge router and identify the happening of DDoS attacks. The agent's implements an entropy-threshold based detection algorithm. The coordinators share attack related information with neighboring ISPs in order to achieve distributed defense. The performance of defense system is evaluated on the basis of some identified metrics. The effectiveness of the defense system is evaluated in the presence and absence of defense system. The result indicates that the proposed defense system does accurate attack detection with very few false positives and false negatives.

1. INTRODUCTION

Denial of Service is an attack having the target of stopping genuine users from the use of a particular network service/resource like a computer system, web server/service or website [1]. A DDoS attack is a coordinated attack, whose aim is to make a particular system, network service or network resource unavailable to its intended users. The DDoS attack is launched with the help of many intermediate compromised systems on the Internet. The aggregate traffic produced by the compromised system can easily cripple the target. The target will no longer be able to provide normal services to its intended users. DDoS attacks are very difficult to defend because they make an only one-way connection with the target. It is because they don't require the acknowledgment of packets sent to the target. This gives DDoS attacks an advantage of being more or less untraceable.

The frequently available attack tools like TFN (Tribe Flood Network), Trinoo, Shaft, TFN2K, and Stacheldraht help the attacker to perform a coordinated DDoS attack against any victim or Internet service [2]. In Feb. 2000, Yahoo becomes the victim of one of the first large-scale DDoS attack, which in results keeps it off from the Internet for nearly 2 hours. It results in costing it lost high advertising revenue [3]. Recently, attackers used a chain of DDoS attacks against many companies providing anti-spam services [4]. They are forced to shut down their services due to these attacks.

The report of PC crime and security survey lead by FBI/CSI (Federal Bureau of Investigation's /Computer Security Institute) in the U.S for the year 2004 [5] show that DDoS attacks are one the 2nd large one outside attacks discovered in computer domain straight away after virus and intrusion infections. In 2004 the survey based on computer crime and security conducted in Australia [6] shows the same kind of outcomes. The technologies like ISDN (Integrated Services Digital Network), dial-up and cable modems intended for home users have amplified the threat of distributed denial of service attacks. DDoS attacks cause organizations to suffer from 2nd most costly security incident overall. The assessments forecast the cost of a 12-hour outage for any large company could be approximately US$15 million. As per the study of Arbor Networks [7], in the year 2007, the biggest DDoS bandwidth attack was logged as 40 GB per second on the domain of Internet service providers and the size was almost doubled in the year 2008 from the earlier one. In spite of the fact that the businesses have occupied a variety of defensive measures such as learning machines, intrusions detection systems, statistics-based analysis methods but still due to the drawbacks of current IDSs such as lack of scalability, centralized detection, lack of real-time performance and mainly the lack of robustness, identifying and responding effectively to DDoS attacks is becoming increasingly challenging. In ancient, filtering specific source addresses was sufficient to control basic DoS attacks but in today's scenario DDoS attacks are more complex and sophisticated.

A lot of work has been done to fight against these attacks but they have some kind of weakness in carrying out the efficient defense. The work proposed in [8] motivates us to identify and review some important distributed defense techniques. It further helps us to propose a defense system which can defend DDoS attacks in a distributed environment. We have already proposed a distributed defense mechanism which detects and mitigates DDoS attacks in ISP domains with the help of collaborative agents and coordinators [24]. The proposed defense system is based on the transit-stub model of internet topology. The various defense related tasks like attack traffic characterization, attack detection, filtering/rate limiting of attack traffic will be distributed to agents working with edge routers in source stub networks. In each stub network, there exists a coordinator which synchronizes the working of the various agents and shares attack related information to the coordinators of neighboring stub domains. The defense system can be easily scaled to cover more ISP domains in incremental fashion. A brief description of simulation environment and scenario used in the experimentation is discussed here. The performance and effectiveness of the proposed defense system is also evaluated and discussed here.

2. RELATED WORK

There are some existing schemes which use distributed policies to handle DDoS attacks. This section identifies and studies some existing schemes which defend DDoS attacks in a distributed manner.

Kang and Kim [9] proposed a small-scale DDoS defense mechanism, which protects small networks such as ISPs, against DDoS attacks. This method works by utilizing the Routing Information Protocol (RIP) and Interior Gateway Protocol (IGP) inside the ISP to defend against DDoS attacks without affecting the working of existing routers. There are two main reasons for using this method. First, there can attacker found inside of these type of networks (such as ISPs). So it can efficiently handle the attacks traffic originating from attackers. Second, it effectively handles the consumption of bandwidth and network resources in ISPs by deflecting the traffic using routing updates of routing information protocol. This traffic deflection can further be utilized for traffic distribution. Nguyen et al. proposed a distributed DDoS defense scheme PaC [10], which is based on "pushback and communicate" idea. PaC uses proprietary messages to inform routers closer to the attack source to filter attacks, thus distributing the attack amongst many routers and not just the edge router to the server. This process begins when the victim detects a DDoS attack, but there is no information on how this process is completed. This defense requires the proprietary code to be distributed to the intermediate routers in order to be effective, but the work states that it does not require all routers to deter an attack. However, it is just a model needs to be tested in a real environment. Gupta et al. discussed a method Dynamic and Auto Responsive Solution [11], which independently detects and perfectly characterizes an extensive series of DDoS attacks in ISP domain. The attacks are identified by the continuous checking of propagation of sudden traffic deviations occurring inside the ISP network. This method uses a flow-volume based technique to build the profile of the traffic traversing the ISP network. It then regularly monitors and identifies the incoming traffic, whether it is going out of profile or not. The proposed defense system is scalable to various networks working under different network environments and attack traffic loads. The six-sigma technique is used to detect various threshold values to precisely identify and characterize the attack flow. Flow volume based approach has been widely assessed in a controlled test-bed environment.

Distributed Change-Point Detection [12] scheme identifies flooding attacks by checking propagation patterns of unexpected traffic deviations at various distributed points on the Internet. When a necessarily big CAT (change aggregation trees) is raised to surpass an already defined threshold value, a DDoS attack will be confirmed. The system is installed over many autonomous systems domains. Each ISP domain contains a central CAT server. The scheme detects abrupt traffic variations, aggregates suspicious alerts, flow propagation patterns and join CAT sub-trees from combined servers to form a global CAT tree. The defense system is made over attack-transit routers, which collaboratively work together. A CAT server in every ISP domain is used to combine the flooding alerts informed by routers. CAT domain servers cooperate with each other to make the final decision. Each domain in Coordinated Detection and Response Scheme [13] can be categorized as either a stub network or a transit network. A stub network is connected to local ISP and contains individual host. A transit network joins different stub networks to form a backbone network. Here stub agents are deployed on stub networks and perform the task of attack traffic detection and filtering. Transit agents are deployed on transit networks and perform only traffic filtering. This model tries to eliminate the attack traffic at its early stages but having some drawbacks. The rate limiting at transit network results in lowering the network performance. This method does not provide any defense against spoofed attacks. A very serious issue is the collateral damage of the normal traffic.

DefCom [14] is a distributed cooperative defense system for distributed denial of service attacks. DefCom constructs a peer-to-peer distributed network of supportive defense components, which are distributed everywhere on the Internet. The defense components interchange information & control messages with each other to discover attacks. They also cooperatively reply with each other and ensure better services to genuine traffic. This scheme effectively distinguishes between normal and attack packets, and dedicates the available free bandwidth to normal traffic and collaborates with other participating defense nodes to certify decent service to the normal users. The frequent communication between defense nodes invites the attackers to attack the DefCom system itself. Chen and Song proposed a Perimeter-based Defense Mechanism [15], which can be used by ISPs to offer the anti-DDoS services to their clients. This mechanism fully depends on various edge routers to supportively find various flooding sources & start rate-limiting filters to drop the traffic identified as attack traffic. This defense mechanism does not need any help from various routers inside or outside of the ISP. Due to this feature, it can be deployed locally and also put fewer burdens on various core routers of the ISP. This method requires widespread deployment and will not work well in non-contiguous deployment.

Tupakula and Varadharajan proposed a method Controller Agent Model [16], which counteracts DDoS attacks initially in one ISP domain but later it was applied to many domains [20]. Here agent's works with the edge routers and controllers are specialized trustworthy machines maintained by the ISP. As soon as a victim identifies an attack, it immediately sends a request to the controller machine to control the attack. The controller machine then informs all agents to mark every packet heading towards the victim. The victim can easily identify the entry point of attack traffic by looking into the marking field of the packet. The victim then provides the attack signature to controller machine and controller instruct the particular agent to filter that attack traffic. Therefore, the attack traffic is filtered at ingress edge router by the agent and normal traffic is allowed to pass through the domain. In [20] certain controllers of participating domains collaborate with each other to reduce the effect of attack and track the attack path used by the attacker. The main drawback of this method is that it uses third party tools for the detection and characterization of attack traffic. Cossack [17] deploys watchdogs at the edges of the network to detect abrupt traffic changes. It constructs a special cluster of defense components installed at victim and source networks. Every defense components can independently identify the attack traffic and communicate it to the cluster. A source side watchdog uses existing methods to identify and rate limits the attack traffic. The main drawback of Cossack scheme is that it does not handle spoofed DDoS attacks. The other limitation is that source and victim end uses different methods of attack detection, which makes the defense system more complex.

Mahajan et al. [18] offers a completely independent and self-defense solution known as Local Aggregate-Based Congestion Control. In this method, a single router is responsible for detection and rate-limiting of DDoS attacks. The routers continuously monitor the incoming traffic and identify high bandwidth traffic heading for a particular destination. It then drops the attack traffic by putting a rate limit on the traffic aggregates. The drawback of this scheme is that it also causes substantial harm to the genuine traffic sharing the same attack path. ASSYST (Active Security System) [19] provides distributed response against DDoS attacks with non-continuous placement. Every ASSYST nodes work likes a classifier node but they are installed merely on edge networks. Active Security Protocol permits a group of energetic routers to cooperate with each other so as to recognize the origin of the DDoS attack. Deployment and tuning of the Active Security System are preferably suitable for a Programmable Network environment. They are not able to control attacks from legacy networks which do not install their own defense systems.

3. PROPOSED SCHEME

Fig. 1 depicts the brief summary of the defense process carried out in the mitigation of DDoS attacks. The whole defense process is controlled by a coordinator and several agents in each ISP domain. The defense process can be initiated by the coordinator in order to protect their customers or the defense service can be requested by any of its customers. The coordinator can be the part of core router or a dedicated machine connected to the core router. The agents can be put on the edge routers and work on the behalf of their coordinator. The main aim of the defense mechanism is to identify and filter attack traffic in their source networks so as to avoid it to reach to the target network. The proposed defense system can achieve this by putting agents on the edge routers and executing detection and filtering algorithms. The agent can start defense by monitoring the incoming traffic on the edge router and identify the happening of suspicious activity by using entropy and threshold based detection algorithm (proposed earlier). Initially, we characterize the incoming flows and compute the NRE (normalized router entropy) value in the specific time window. The value of NRE is then compared against a pre-identified threshold value T1 to know whether a suspicious activity is happening or not. If a suspicious activity is found then the next step in the defense process is to know which flow is responsible for it. It can be done by computing and comparing the packet rate of current flows against a threshold value T2. After the identification of suspicious flow, the next step is to confirm whether it is related to a DDoS attack or just the part of the flash event. The value of entropy rate for the suspicious flow is computed on the current router and gateway router (for neighboring edge router). The confirmation of DDoS attack can be done by comparing the difference of entropies (E1, E2) against a threshold value T3.

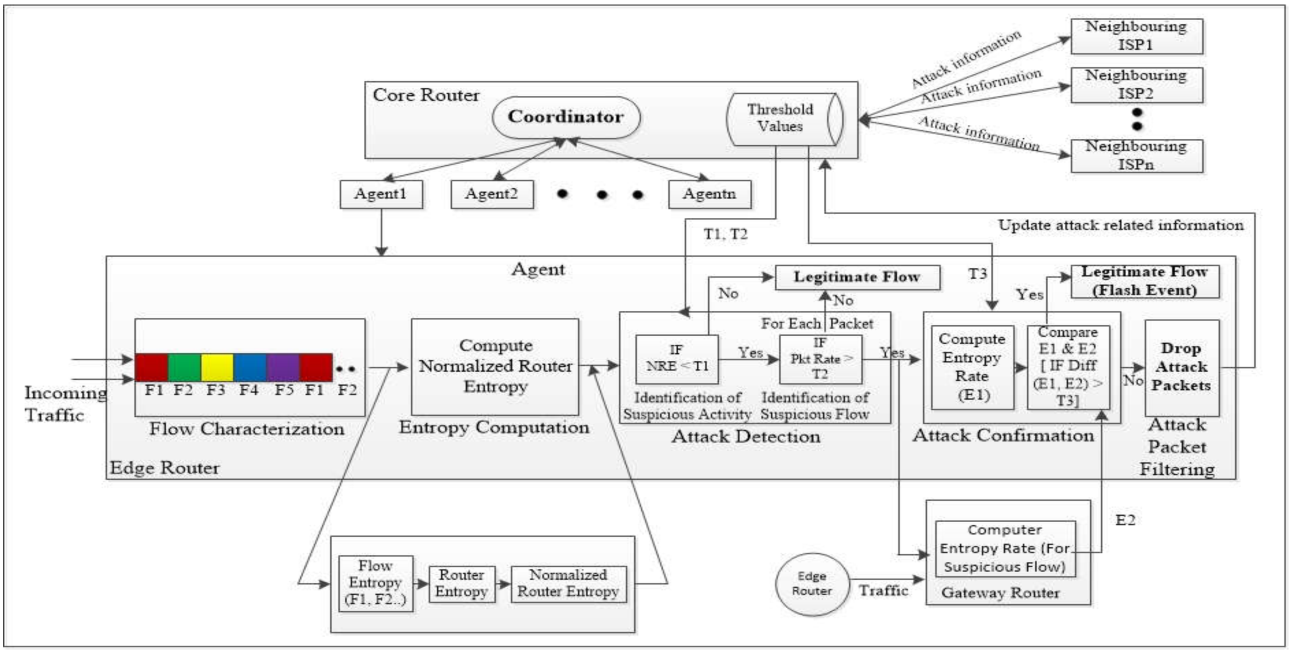

Fig. 1 – The Defense Process.

If a DDoS attack is confirmed, then the packets related to the suspicious flow are dropped and the coordinator will be updated with the attack related information. The coordinator then alerts its other agents about the attack and passes attack related information to the neighboring coordinators. The efficiency of defense system can be increased if it can be deployed on many numbers of ISPs.

4. EXPERIMENTATION

The proposed defense system is evaluated in simulation environment containing OMNeT++ [21], INET [22] and ReaSE [23]. OMNeT++ is a discrete event simulator and is widely used for the simulation of various types of research projects. INET is used with OMNeT++ to simulate internet like topologies. ReaSE is an extension of INET framework; it allows us to generate realistic simulation topologies contain attack as well as legitimate traffic. ReaSE can produce topology on both AS (autonomous systems) and Router level. The various objects required to perform DDoS attack and defense analysis are modeled in the simulations. The various objects include legitimate host, attackers, transit & stub domains, agents, coordinators etc.

4.1 SIMULATION SCENARIO

To perform simulation, we need to build our own network. ReaSE is used to generate AS level topologies to connect different ISP domains. It can generate topology of both AS level and router level so that it can reflect the hierarchical structure of internet. In AS level topology, the each AS can be categorized as either transit AS or stub AS. The transit AS is used to provide connections with other Transit AS and stub AS. Two stub AS can only communicate if they cross a Transit AS. In router level topology, each AS can further to be specified. Each AS can contain one or more core, gateway and edge routers. Core routers are used to connect with transit AS and edge routers can directly connects with the customer networks. The customer networks can have a variable number of hosts which includes legitimate as well as attack users. Table 1 shows the basic parameters used in the simulation process.

Table. 1 Basic simulation parameters

Parameter Name	Value
Number of AS (autonomous systems)	20
Number of transit AS	4
Number of stub AS	16
Number of core routers	20
Number of gateways	31
Number of edge routers	175
Number of attack host	238
Number of legitimate host	1032
Simulation time	25 Sec

4.2 TRAFFIC PARAMETERS

The simulated network should contain different traffic profiles to certify realistic traffic patterns of various protocols. The traffic profiles contain a mixture of various kinds of traffic like web, mail, interactive, ping, FTP, streaming etc. In router level topology the host systems are classified into client and servers. ReaSE represents client by the name InetUserHost and servers by Mail, Interactive and Web server. The bandwidth between different nodes is also specified through ReaSE. ReaSE uses TribeFloodNetwork tool to perform DDoS attack by randomly selecting clients as DDoSZombies. Table 2 gives the different traffic sources with their flow percentages used in the simulation.

Table 2. Traffic Sources with different flow percentages

Traffic Source	Protocol	Flow (%)
HTTP Traffic	TCP	56
FTP Traffic	TCP	20
Telnet Traffic	TCP	10
Streaming Traffic	UDP	4
Ping Traffic	ICMP	4
Mail Traffic	TCP	6

TCP – Transmission Control Protocol; FTP – File Transfer Protocol; HTTP – Hyper Text Transfer protocol; UDP – User Datagram Protocol; ICMP – Internet Control Message Protocol.

5. PERFORMANCE ANALYSIS

The performance of attack and legitimate traffic is evaluated in the presence and absence of defense mechanism. We conducted simulation experiments using different simulation scenarios reflecting realistic attack and legitimate traffic patterns. The detailed working of agent based distributed DDoS defense system and its incremental deployment in ISP networks is already presented in [25, 26]. The performance of the proposed defense system is evaluated on the basis of some identified metrics is discussed here.

5.1 ATTACK DETECTION METRICS

The threshold values play a key role in the detection algorithm and helps in the identification of attack traffic and DDoS attacks. In simulation scenario the attack will begin at t=10 seconds and continues for next 12 seconds. The effect of the threshold value and attack detection mechanism on the performance of attack and legitimate packets is discussed here.

5.1.1 Effect of detection system on attack packets

Fig. 2 shows the effect of attack detection mechanism and threshold values on the performance of attack packets passed by the edge router holding detection algorithm. The edge router will pass all the attack packets in absence of attack detection mechanism (during attack duration i.e. 10th to 22nd seconds) but in the presence of detection mechanism the attack packets will be dropped. The appropriate threshold value plays an important role in the detection of attack packets.

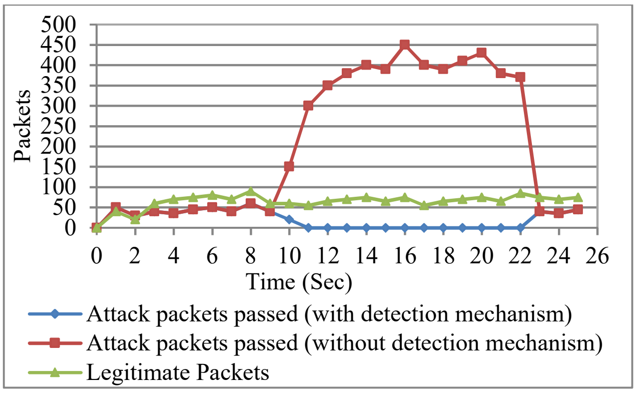

Fig. 2 – Status of attack packets at edge router the presence & absence of detection algorithm.

5.1.2 Detection rate

The detection rate (Rd) is the ratio of the number of attack packets detected by the detection mechanism to the total number of attack packets generated from different sources. It is measured as:

$$Rd = \frac{D}{N} \qquad (1)$$

where D= number of attack packets detected,
N= total number of attack packets generated.

The attack detection rate is almost 100% under a perfect threshold value i.e. T1 ≥ 0.80, identified by us during the design of detection algorithm. Fig. 4 shows the effect of threshold values on the detection of attack packets. Fig. 3 shows that the detection rate increases with the increase in threshold value. The threshold value chosen should be sufficiently high so that it will detect most of attack packets and will not put any effect on legitimate packets.

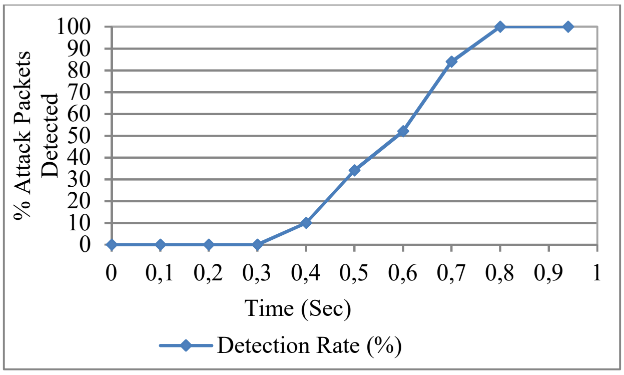

Fig. 3 – Effect of threshold value on detection rate.

5.1.3 False positive rate

False positive rate (Rfp) is the ratio of the number of legitimate packets which are wrongly detected as attack packets to the total number of legitimate packets. It is measured as:

$$Rfp = \frac{P}{M} \qquad (2)$$

where P= Number of packets detected as attack packets,
M= Total number of legitimate packets

The false positive rate under a threshold value i.e. T ≤ 0.94 is zero. But if we increase the value of threshold from 0.94 to 0.99 then false positive rate will start increasing. Fig. 4 shows the effect of threshold values on the performance of legitimate packets.

The accuracy of attack detection system is highly depends on the threshold values. The unsuitable threshold values can cause high false negative and false positive rates. If the value is too low, then it creates high false negatives and too high produces high false positives. So as per our observation it should be somewhere in the range of 0.80 to 0.94.

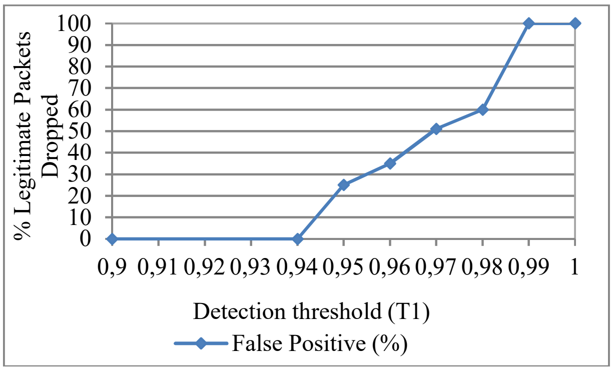

Fig. 4 – Threshold value effect on false positive rate.

5.2 ATTACK RESPONSE METRICS

The effect of DDoS attack and defense mechanism on the performance of legitimate traffic is explained below.

5.2.1 Response time

The effect of DDoS attack and defense system on the response time taken by legitimate packets during transmission is discussed here. Response time is the measure of the amount of time required for packets to travel across a network path from a sender to a receiver. It is the combination of time taken by a packet to travel from client to server, server delay and server to back client.

The response time remains normal in the absence of an attack. But, when an attack is launched (during 10th to 22nd second), the response time will start increasing due to the increase in attack packets strength. Fig. 5 shows that the maximum response time can touch even 1 second during the attack.

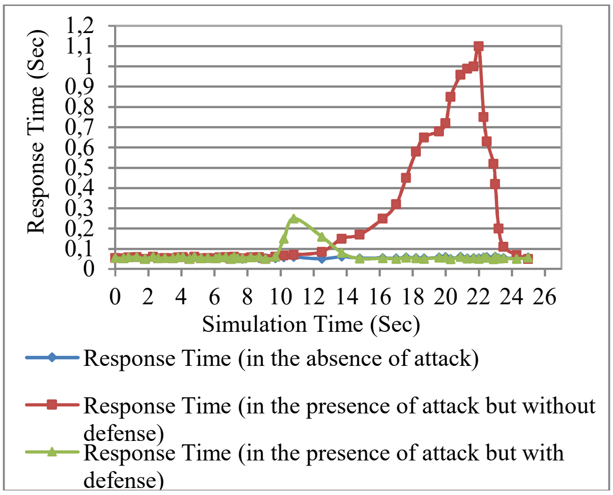

Fig. 5 – Response time variations.

Here we also identify the effect of defense method on the performance of response time. The response time will start increasing as soon as the attack is launched during the 10th second but soon it will be controlled by the invocation of defense system at the 12th second.

5.2.2 Throughput

Throughput is the rate at which a packet will be successfully delivered to a destination over a communication channel. Throughput can be used to check the performance and network efficiency in a way that a high throughput offers high network performance and vice versa. The throughput is usually measured in terms of the total number of packets delivered to the destination. When an attack is launched, legitimate and attack traffic, both use the bottleneck link. So throughput is defined as a number of legitimate packets received at the destination per second. Throughput can also be measured in terms of goodput and badput respectively. Goodput is defined as the number of bytes per second of legitimate traffic that is received at the server, and badput is defined as the number of bytes per second of attack traffic that is received at the server. The throughput is measured in terms of evaluating the number of legitimate packets delivered to the destination in the following three cases.

1. In the absence of attack & defense system,
2. In the presence of attack but in the absence of defense system, and
3. In the presence of both attack & defense system.

The attack starts at 10th seconds after the start of legitimate traffic and ends at 22nd seconds. Finally, we calculated the number of packets delivered to the destination in the cases mentioned above. Fig. 6 shows the performance of legitimate packets in above mentioned three situations.

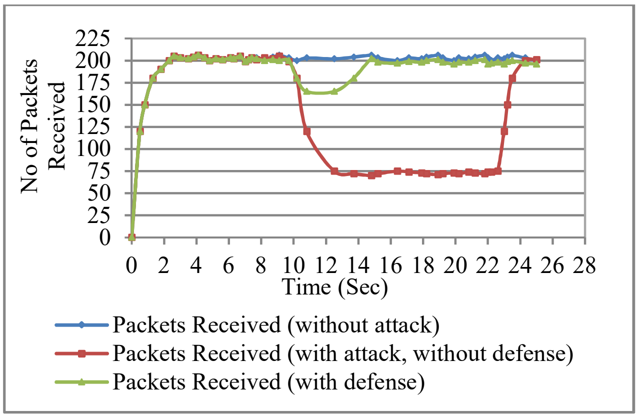

Fig. 6 –Throughput variations.

The X-axis represents time intervals in seconds, and the Y-axis represents the number of legitimate packets delivered to the destination in different situations.

5.2.3 Deployment

The effectiveness of the defense system can be increased if the defense system can be deployed on more number of edge routers. The edge routers of stub networks where defense system needs to be deployed are directly under the control of ISPs. So if they agree to participate in the defense process, the overall effectiveness of defense can be increased.

Fig. 7 displays the number of legitimate packets dropped due to false alarm rate will decrease gradually with the increase in the edge routers which joins the defense system. By implementing the defense system on a sufficient number of edge routers, the attack traffic can be identified and dropped more efficiently, and the number of the attack packets reaching the victim server will get decreased.

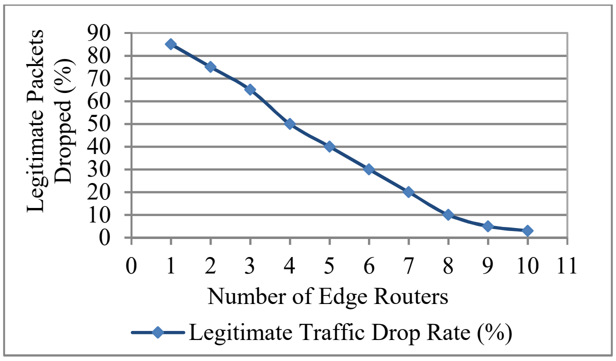

Fig. 7 – Edge router variations.

5.3 DEPLOYMENT METRICS

Here we measure and discuss the effect of incremental deployment of defense system on the following three performance metrics.

5.3.1 Throughput

Throughput is defined as the total number of packets transferred from source to destination in per unit time. In the case of DDoS attacks, both attack and legitimate traffic will flow from source to destination:

$$\text{Let } T = \frac{(Ta + Tn)}{\Delta} \tag{3}$$

where T – Total Traffic (Packets),
Δ – Time window,
Ta – Attack Traffic (Packets),
Tn – Legitimate Traffic (Packets)

The throughput can be divided into goodput and badput, where the goodput is defined as the number of legitimate packets delivered to the destination whereas badput is the number of attack packets delivered to the destination. The value of goodput and badput can be calculated as:

$$Goodput = \frac{Tn}{\Delta}, \quad (4)$$

$$Badput = \frac{Ta}{\Delta}. \quad (5)$$

Fig. 6 shows the goodput in terms of the total number of legitimate packets delivered to the destination in the specific time window. The attack starts at 10th second and continues up to 22nd second. Fig. 8 shows that the number of legitimate packets dropped will decrease with the increase in defense enabled ISPs.

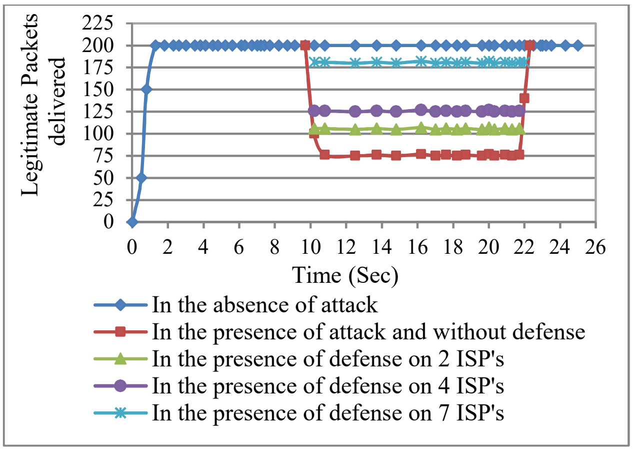

Fig. 8 – Goodput.

Fig. 9 shows the badput in terms of the total number of attack packets manage to reach the destination. The number of attack packets which reaches to the destination will get decreased with the increase in the participation from ISPs.

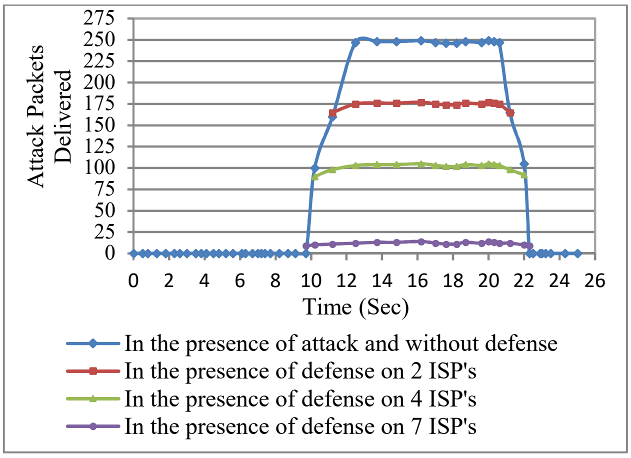

Fig. 9 – Badput.

5.3.2 Legitimate Packets Survival Ratio (LPSR)

The legitimate packet survival ratio (N) measures the delivered legitimate packets during an attack. Suppose Tn is total number of legitimate packets, and Ta is total number of attack packets, then

$$N = \frac{Tn}{(Ta + Tn)}. \quad (6)$$

It is a good parameter to evaluate the influence of the attack. The effect of attack can be identified by measuring the percentage of legitimate packets reaches to the destination during the attack. The value of LPSR should be high so as to ensure uninterrupted services. The value of LPSR starts decreasing with the increase in the rate of attack traffic. This happens due to the limited availability of link bandwidth which in results starts dropping legitimate packets. Fig. 10 shows the survival ratio of legitimate packets manages to reach destination.

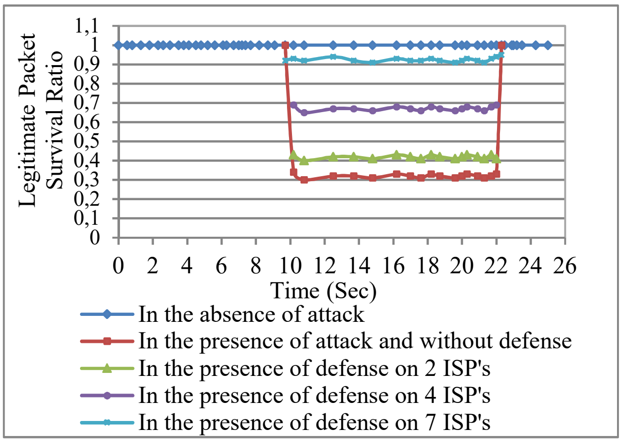

Fig. 10 – Legitimate packets survival ratio.

5.3.3 Percentage of Overhead Packets

The different entities involved in the defense system will communicate with each other through the secure messages containing attack and control information. We have tried our best to keep it as much minimum as possible because it creates an extra burden on the network performance. Fig. 11 shows the graph of overhead packets calculated in terms of percentage.

As the number of ISPs increases, the overhead packets will also increase. The overhead will increase with the increase in the number of participating ISPs. The overhead packets cannot be avoided because they will be the part defense mechanism. If we ensure full deployment then the maximum overhead even during the attack will not cross 1.6%.

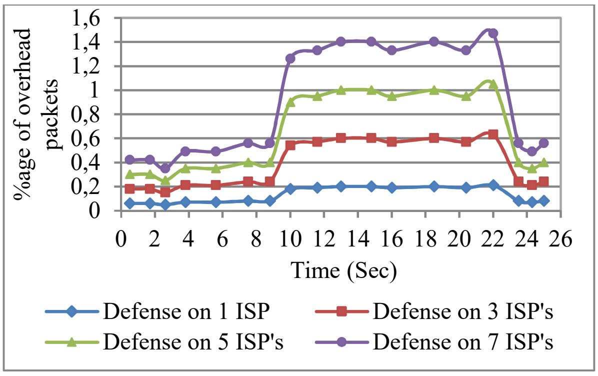

Fig. 11 – Percentage of overhead packets.

6. CONCLUSION & FUTURE SCOPE

DDoS attacks are the major security issues in Internet community because it will become a major cause of economic loss in many countries. There existing defense mechanism proposed the literature needs some improvements as attackers are changing their attack strategies with the passage of time. The proposed defense system is an effort in the direction to handle DDoS attacks with more accuracy and efficiency. The core parameter of the defense system is the accurate attacks detection, which need appropriate threshold values to identify the occurrence of DDoS attack. The threshold values used by us in the algorithm are calculated mathematically by taking sample scenarios reflecting real attack and legitimate traffic. These threshold values help us to increase the detection rate and lower the false positive values. The LPSR and throughput will be increased in the presence on defense system. The efficiency of defense system is increases as we increase the number of participating routers. The defense system also supports incremental deployment and some performance parameters like throughput and LSPR will be increased with the increase in participation from ISPs.

The future work is to reduce the percentage of overhead packets required in the communication process between agents, coordinators and customers.

REFERENCES

[1] D. Karig, R. Lee, *Remote Denial of Service Attacks and Countermeasures*, Department of Electrical Engineering, Princeton University, Technical Report CEL2001-002, 2001.

[2] C. Douligeris, D. Serpanos, *Network Security: Current Status & Future Directions*, Wiley-IEEE Press, 2007, 122 p.

[3] L. Garber, "Denial-of-Service attacks rip the Internet," *IEEE Computer*, vol. 33, no. 4, pp. 12-17, 2000.

[4] M. Brunker, *Spam block lists bombed to oblivion*, 2003, [Online]. Available: http://www.msnbc.msn.com/id/3088113/

[5] L. Gordon, M. Loeb, W. Lucyshyn, R. Richardson, *2005 CSI/FBI Computer Crime and Security Survey*, Technical Report, Computer Security Institute, 2005.

[6] AusCERT, *2005 Australian Computer Crime and Security Survey*, Tech. Report, Australian Computer Emergency Response Team, 2005, [Online]. Available: http://www.auscert.org.au/crimesurvey.

[7] R. Vamosi, *Study DDoS attacks threaten ISP infrastructure*, 2008, [Online]. Available: http://www.cnet.com/news/study-ddos-attacks-threaten-isp-infrastructure.

[8] K. Singh, K. Dhindsa, B. Bhushan, "Distributed defense: An edge over centralized defense against DDos attacks," *International Journal of Computer Network and Information Security*, vol. 9, no. 3, pp. 36-44, March 2017.

[9] H. Kang, S. Kim, "sShield: small DDoS defense system using RIP-based traffic deflection in autonomous system," *The Journal of Supercomputing*, vol. 67, pp. 820-836, 2014.

[10] T. Nguyen, C. Doan, V. Nguyen, T. Nguyen, "Distributed defense of distributed DoS using pushback and communicate mechanism," in *Proceedings of International Conference on Advanced Technologies for Communications* (ATC 2011), Da Nang, Vietnam, Aug. 2011, pp. 178-182.

[11] B. Gupta, R. Joshi, M. Mishra, "Dynamic and auto responsive solution for distributed denial of service attacks detection in ISP network," *International Journal of Computer Theory and Engineering*, vol. 1, no. 1, 2009.

[12] Y. Chen, K. Hwang, W. Ku, "Collaborative detection of DDoS attacks over multiple network domains," *IEEE Transactions on Parallel and Distributed Systems*, vol. 18, no. 12, 2007.

[13] H. Lam, C. Li, S. Chanson, D. Yeung, "A coordinated detection and response scheme for distributed denial of service attacks," in *Proceedings of IEEE Conference on Communications*, Istanbul, Turkey, June 2006, pp. 2165-2170.

[14] J. Mirkovic, M. Robinson, P. Reiher, G. Oikonomou, "A framework for collaborative DDoS defense," in *Proceedings of 22nd Annual Computer Security Applications Conference*, Miami, Florida, USA, Dec. 2006, pp. 33-42.

[15] S. Chen, Q. Song, "Perimeter-based defense against high-bandwidth DDoS attacks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 16, no. 6, 2005.

[16] U. Tupakula, V. Varadharajan, "A practical method to counteract denial of service attacks," in *Proceedings of the twenty-fifth Australasian computer science conference*, Darlinghurst, Australia, Feb. 2003, pp. 275-284.

[17] C. Papadopoulos, R. Lindell, J. Mehringer, A. Hussain, R. Govindan, "COSSACK: Coordinated Suppression of Simultaneous Attacks," in *Proceedings of DISCEX*, Washington, DC, USA, Apr. 2003, pp. 2-13.

[18] R. Mahajan, S. Bellovin, S. Floyd, V. Paxson, S. Shenker, "Controlling high bandwidth aggregates in the network," *ACM SIGCOMM Computer Communications Review*, vol. 32, no. 3, pp. 62-73, 2002.

[19] R. Canonico, D. Cotroneo, L. Peluso, S. Romano, G. Ventre, "Programming routers to improve network security," in *Proceedings of the OPENSIG 2001 Workshop Next Generation Network Programming*, London, UK, Sep. 2001.

[20] U. Tupakula, V. Varadharajan, "A controller agent model to counteract DoS attacks in multiple domains," in *Proceedings of Integrated Network Management, IFIP/IEEE 8th International Symposium*, Colorado Springs, USA, Mar. 2003, pp. 113-116.

[21] A. Varga, R. Horing, "An overview of the OMNeT++ simulation environment," in *Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops*, Marseille, France, March 2008.

[22] INET Framework for OMNeT++, manual, [Online]. Available: https://omnetpp.org/doc/inet/api-current/inet-manual-draft.pdf.

[23] T. Gamer, M. Scharf, "Realistic simulation environment for IP-based networks," in *Proceedings of 1st International Conference on Simulation Tools and Techniques for Communication and Systems & Workshops*, Marseille, France, March 2008.

[24] K. Singh, K. Dhindsa, B. Bhushan, "Collaborative agent-based model for distributed defense against DDoS attacks in ISP networks," *International Journal of Security and its Applications*, vol. 11, no. 8, pp. 1-12, 2017.

[25] K. Singh, K. Dhindsa, and B. Bhushan, "Coordinator-agent based distributed defense against DDoS attacks in transit-stub networks," *International Journal of Future Generation Communication and Networking*, vol. 10, no. 5, pp. 51-64, 2017.

[26] K. Singh, K. Dhindsa, B. Bhushan, "Deployment of agent-based distributed defense mechanism against DDoS attacks in multiple ISP networks," *International Journal on Information Technologies & Security*, vol. 9, no. 4, pp. 123-34, 2017.

Karanbir Singh, *is doing his Ph.D. in the field of Network Security from IKG Punjab Technical University, Kapurthala (Punjab). He obtained his MCA degree from Kurukshetra University, Kurukshetra (Haryana), India. He has a teaching and research experience of more than 14 years. He has authored more than 12 papers in various international journals & the proceedings of reputed national and international conferences. His research interests are in the fields of Computer Networks, Network Security, IoT, and Adhoc Networks.*

Dr. Kanwalvir Singh Dhindsa, *is working as Professor in the Department of CSE at Baba Banda Singh Bahadur Engg. College, Fatehgarh Sahib (Punjab). He obtained his Ph.D. in Computer Engg. (In the field of Mobile Computing & Information Systems) from Punjabi University Patiala. He has guided many M.Tech. students & is currently guiding 7 Ph.D. scholars. He has authored more than 70 publications in various esteemed international referred journals & proceedings of reputed national and international conferences. His research interests are in the fields of Cloud Computing, Big Data, IoT, Mobile Computing, Database & Security, and Web Engineering.*

Dr. Bharat Bhushan *is employed as Head and Associate Professor in the Department of Computer Science & Applications, Guru Nanak Khalsa College, Yamunanagar (Haryana). He has done Ph.D. in Computer Science & Applications from Kurukshetra University, Kurukshetra, India. He has more than 40 research papers to his credit in various referred international journals and reputed international conferences. His research interests are in the fields of Software Quality and Mobile Networks.*