DEPLOYMENT OF AGENT-BASED DISTRIBUTED DEFENSE MECHANISM AGAINST DDOS ATTACKS IN MULTIPLE ISP NETWORKS

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

[1] Research Scholar, IKG Punjab Technical University, Kapurthala, Punjab
[2] Dept. of CSE, Baba Banda Singh Bahadur Engg. College, Fatehgarh Sahib
[3] Dept. of Computer Science, Guru Nanak Khalsa College, Yamunanagar
e-mails: karan_nehra@yahoo.co.in, kdhindsa@gmail.com, bharat_dhiman@hotmail.com
India

Abstract: In today's scenario, distributed denials of service (DDoS) attacks are creating a big problem for the Internet services. Here we present the deployment and working of the proposed defense system on multiple Internet service providers (ISP). The main aim of the proposed defense system is to monitor the incoming traffic on the edge router, identify the happening of DDoS attack, and rate limiting or blocking the attack traffic. The success of the defense system will largely depend upon the accuracy during attack detection and the collaboration among the various participating ISP domains. The defense system can be incrementally deployed on the participating ISPs. So here we will discuss the deployment of DDoS defense mechanism in multiple ISPs and will prove that the performance of defense system can be increased by increasing the participation from ISP domains.

Keywords: DDoS, Defense, Attacks, Entropy, Threshold, Agent.

1. INTRODUCTION

Distributed denial-of-service (DDoS) attacks, attempt to disrupt services provided to legitimate users by overwhelming the target with a large number of attack packets [1, 2]. These attacks are often conducted through botnets. The DDoS attacks have grown larger year by year. In 2013, the largest attack volume peaked at 300 Gbps. As per arbor networks [3], the largest attack reported this year was 800 Gbps, 60% increase over last year. As per the report, the service provider customers remain the number one target of DDoS attacks, with an increasing proportion of attacks targeting them. In recent times, DDoS attacks have become shorter in duration, often lasting only a few hours or even just minutes. According to Akamai [4], the average attack lasts 17 hours. In addition to the reduced duration, the attacks are getting more sophisticated and varying the methods used, making them harder to mitigate. There exist many solutions to the DDoS problem but they suffer from some kind of disadvantages. So we need a solution which ensures the early detection and mitigation of DDoS attacks.

Here we proposed an agent based defense mechanism, which can be invoked when ISP received a defense request from its customer network or it can be deployed as a self-

defence mechanism to ensure uninterrupted services to their customers. The deployment of defense mechanism can be done in phases. We will start the deployment from destination network and can extend it to neighbouring ISPs. The level of expansion will entirely depend on ISPs which are willing to participate in the defense. The defense can be initiated by the coordinator, asking its agents to monitor the traffic passing through their edge routers. The agent starts observing the incoming traffic passing through the edge router by invoking a detection algorithm. The detection algorithm helps in the identification of DDoS attack. As soon as a DDoS attack is identified & confirmed, the packets which belong to the attack traffic will be dropped. The agent takes the help of gateway router in the confirmation of a DDoS attack. Furthermore, the agent shares attack related information to their coordinator using secure messaging. The coordinator then alerts the other agents to start filtering the traffic heading towards the identified destination. The coordinator further shares attack related information to the coordinators of neighbouring ISPs. The neighbouring ISPs then initiate the defense by instructing their agents to filter the attack traffic for the particular destination. The proposed defense system can handle some common types of DDoS attacks as described in [13].

The remainder of this paper is organized as follows. The existing distributed defense methods in literature are identified in section II. Section III highlights the defense architecture and the defense process in detail. Section IV describes the process to be followed in the incremental deployment. In Section V, simulation scenario is presented and a performance evaluation using identified metrics is discussed in Section VI. Sections VII concludes with findings of research work.

2. RELATED WORK

In literature, researchers have suggested numerous kinds of DDoS defense mechanisms under various environments. The related work for this paper reflects the different areas related to distributed DDoS defense and agent-based network modelling and simulation.

A range of architectures and frameworks have been identified and developed in the recent past to counteract DDoS attacks. There exist many defense mechanisms like PaC [5], Distributed Change-Point Detection [6], DefCOM [7], COSSACK [8], sShield [9], perimeter-based defense [10], which works in a cooperative manner to handle DDoS attacks. There exist many approaches like discrete-event and agents-based simulations [11-12], that can be useful to explore network modelling and simulation. The choice of specific approach depends on some factors like level of defense, protocols, traffic and scalability of models. Our aim is to test the defense mechanism by deploying it at various places on the Internet.

Recently, the concept of agents has been incorporated by the researcher in their implementations. There exist many defense systems, as reflected in the references [14-15], which uses the concept of agent in carrying out the defense. The agents not only deliver the reasonable benefits by improving defense quality but also incorporate the latest technology and specific proficiency. The proposed defense system also carries distributed defense with the help of agents and coordinators.

In [16], we have already identified the various locations in the Internet/network where a defense system can be deployed and came with the fact that distributed defense is the best solution to control DDoS attacks efficiently. Later in [17], we have also proved that distributed defense is far better than centralized defense. We have already identified the entropy and threshold based detection and filtering mechanisms which can monitors the

incoming flow on edge router and identify the occurrence of a DDoS attack. In case, when a DDoS attack happens, it will drop all the attack packets and informs about attack related information to its coordinators. We have already tested its performance in single ISP network. So our contribution in this paper includes:

- The generation of Internet like realistic topology based on autonomous systems including single or multiple domains
- Traffic generation between hosts resembles realistic traffic patterns in order to get meaningful and accurate evaluation result
- Implementation of defense algorithms on edge & core routers in the form of agents and coordinators

The focus of this paper is to evaluate the effectiveness of DDoS defense mechanism in multiple ISP networks. The performance can be tested by adding more and more ISP networks in defense process incrementally.

3. DEFENSE ARCHITECTURE

The proposed defense architecture is based on coordinators and agents, which work on the behalf of Internet service providers. The following entities are involved in carrying a distributed DDoS defense.

3.1. Coordinator Mechanism

There exists a central coordinator in each stub network. The coordinator can be implemented as a dedicated machine connected with the core router or it can be the part of core router itself. The main function of the coordinator is to manage various agents deployed on edge routers and collaborating with the coordinators of neighbouring participating ISPS's. The coordinator asks their agents to monitor and identify the happening of DDoS attacks. The coordinator can receive attack related information from any agents and instruct other agents to filter the attack traffic. The other responsibility of coordinator is to share attack related information with the neighbouring coordinators so that they can initiate defense in their respective domain and further alerts to their neighbouring autonomous systems.

3.2. Agent Mechanism

The main functions assigned to the agents are traffic monitoring, attack detection, and filtering/rate limiting of attack traffic. We have already proposed an entropy and threshold based attack detection algorithm that can be implemented on the edge routers. The agents holding detection algorithm will monitor the incoming traffic and identify the happening of DDoS attack. A part of detection mechanism is also to be implemented on the gateway router which helps in the confirmation of DDoS attacks. If an attack is detected then the packets related to attack traffic will be filtered and attack related parameters will be passed to the coordinator.

3.3. Secure Communication

Messaging is the means of communication between agents and coordinators. The agent communicates with coordinator through secure messaging, so as to avoid it from hackers and attackers. Here we discuss the authentication process for communication between customer networks, coordinators, and agents. It is assumed that customer networks are already registered with the ISP domains. Coordinators and agents are trusted entities within the ISP domain. The DDoS defense call can be requested by the customer network

or it can be initiated by coordinator as a part of self-defence. During communication, the customer, coordinator, and agents exchange their public keys. The coordinator can authenticate a customer network by retrieving its public key from its database by using the 32-bit source IP address and later verifying the signed hashed digest. The coordinator retrieves the session key by decrypting the encrypted portion using its private key. Now it responds to the customer with a new signed hashed digest. The customer network can verify the signed digest using the public key of coordinator. The coordinator uses the similar process to authenticate different agents within its domain and other coordinators in neighbouring domains.

3.4. Defense Process

DDoS attack detection can be performed by applying any of the three approaches i.e. anomaly based approach, signature based approach or entropy based approach. Signature based approach identifies DDoS attacks by matching their signature against a database but it can detect only known attack and fails against new attacks. Anomaly based approach monitors and compares the network behaviour against a base value to detect DDoS attacks but the main drawback is that it can results in false positives if the base value is configured incorrectly. Entropy is a feature of information theory [21] that can be used to identify the randomness in flows. The value of entropy (calculated during continuous time intervals) and threshold value (predefined) can be used to detect the presence of attacks. The main advantage of entropy based scheme is that it is fast and more accurate as compare to others. The proposed agent based defense system also uses an advanced entropy based attack detection algorithm which uses predefined threshold values for detecting DDoS attacks.

Fig. 1 shows the internal architecture of DDoS defense mechanism which can work in both isolated & distributed mode.

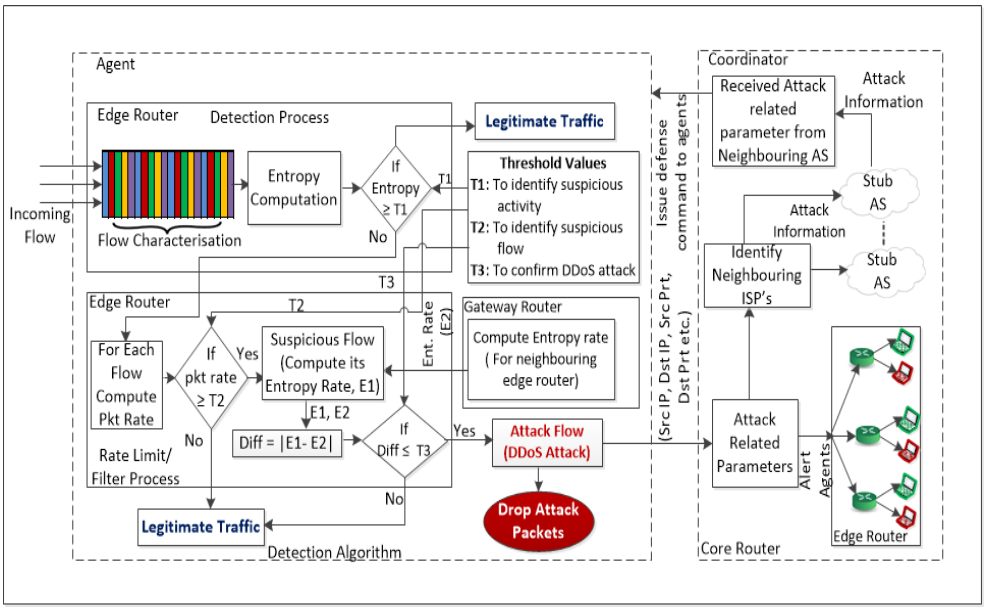

Fig. 1. Distributed DDoS defense architecture

The coordinator can instruct the agents to initiate a DDoS defense against a particular destination (if a defense request is received from a particular customer network) or can start the defense in self-mode, so as to provide reliable service to its customers. As soon as an agent receives a defense request from its coordinator, it enables the detection algorithm. The detection algorithm works by characterizing the incoming flow and computes entropy for each flow and normalized router entropy. The normalized router entropy is compared against a predefined threshold value to check whether the router is experiencing a suspicious activity or not. If a suspicious activity is happening then next step is know the flow which is responsible for the suspicious activity. Once the suspicious flow is identified then the last step is to check whether it is a DDoS attack or a flash event (having similar characteristics like DDoS attacks). The happening of a DDoS attack can be confirmed by comparing the difference of entropy rates at edge and gateway router against a threshold value. If the flow is confirmed as an attack flow then its packets will be dropped.

4. INCREMENTAL DEPLOYMENT

The defense system can be deployed on the edge routers of the stub networks. Initially, we start by deploying the defense mechanism in target ISP/stub network. It can be further enhanced by covering more and more stub networks in an incremental fashion. Fig. 1 shows the placement of coordinator and agents in the target stub network. The coordinator is placed on the core router and agents will be placed on the edge routers. The agents monitor the incoming traffic passing the edge router with the help of threshold-entropy based detection. The detection algorithm helps the agents in the detection of a DDoS attack and attack packets. The agent's further rate-limit/drop the attack packets and the attack related information is shared with the coordinator. The coordinator then instructs other agents to rate limit/filter the attack traffic heading towards the particular destination. Fig. 2 shows the placement of coordinator and agents on core and edge routers. The dotted line shows the secure communication happens among them.

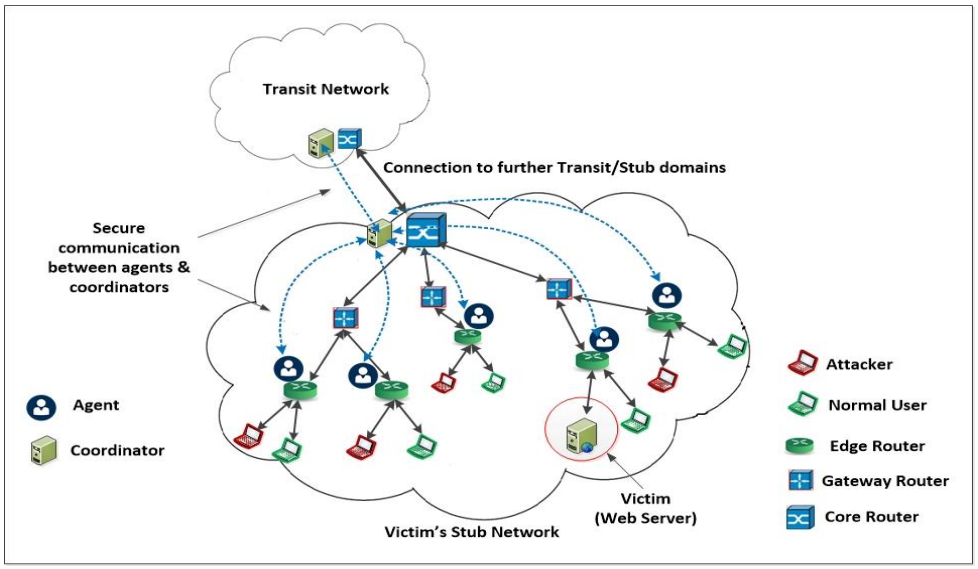

Fig. 2. Defense scenario of victim side stub network

The effectiveness of the defense system can be increased if the maximum number of neighbouring ISPs will become ready to participate in the defense process. The true purpose of distributed defense can only be achieved if we are able to deploy the defense system on a maximum number of source stub networks. The attack traffic originated from source stub networks will travel through transit networks and later reaches the destination. So our aim is to detect and filter the attack traffic at their source. The defense system can be deployed on any number of stub networks, more is the coverage better will be the defense. Fig. 3 illustrates the incremental deployment and communication between coordinators of neighbouring ISPs.

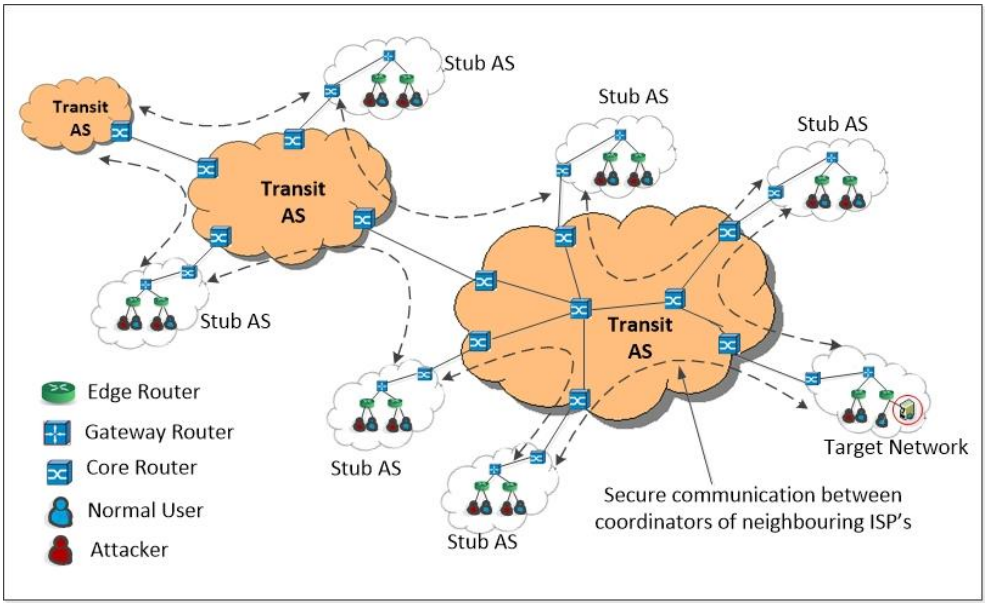

Fig. 3. Incremental deployment of defense system

The coordinators share attack related information with their neighbouring coordinators. As soon as a coordinator receives attack related information from its neighbouring coordinator, it instructs its agents to start the defense process against the on-going attack on identified destination.

5. EXPERIMENTATION

We analysed our defense model using simulations carried out using OMNeT++ [18], INET [19] and ReaSE [20]. OMNeT++ is a discrete event simulator and mostly used in large scale simulations. INET framework extends the OMNeT++ by providing Internet specific protocols like TCP/IP etc. ReaSE is a tool that can be integrated with OMNeT++ and is used to create a realistic autonomous system based Internet topologies. ReaSE extends INET in order to provide the functionality of basic TCP/IP protocols for OMNeT++. Fig. 4 shows the transit stub autonomous system based Internet topology containing 02 transit autonomous systems and 07 stub autonomous systems. The term ISP domain, stub network and autonomous system will reflect the same meaning in this paper. Fig. 4 presents the detailed view of proposed topology connecting 07 autonomous systems.

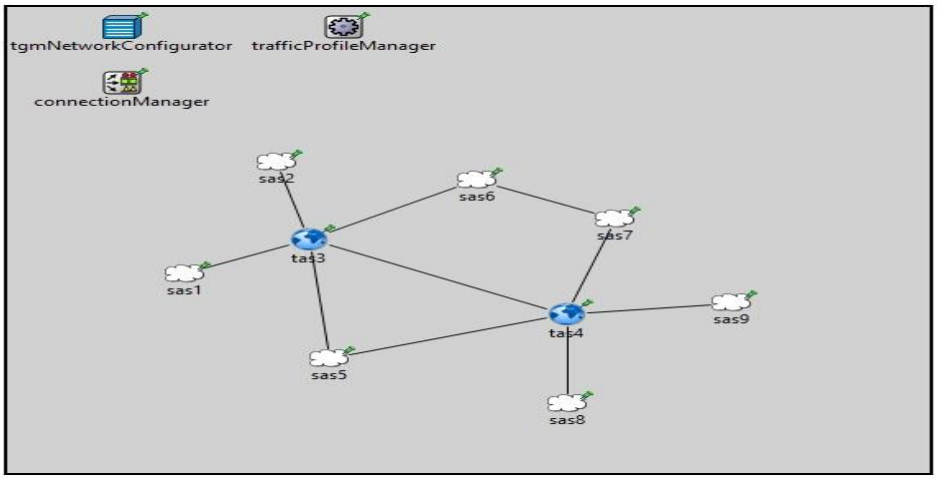

Fig. 4. Transit-stub based Internet topology

In each autonomous system, the router-level topology can be further identified. Due to the hierarchical structure of the Internet, the topologies generated by the ReaSE can be divided into two parts. The first part is AS level in which the connections between different domains are specified. The second part is related to the connection between core, gateway (aggregate), and edge routers in each autonomous system, as shown in Fig. 5.

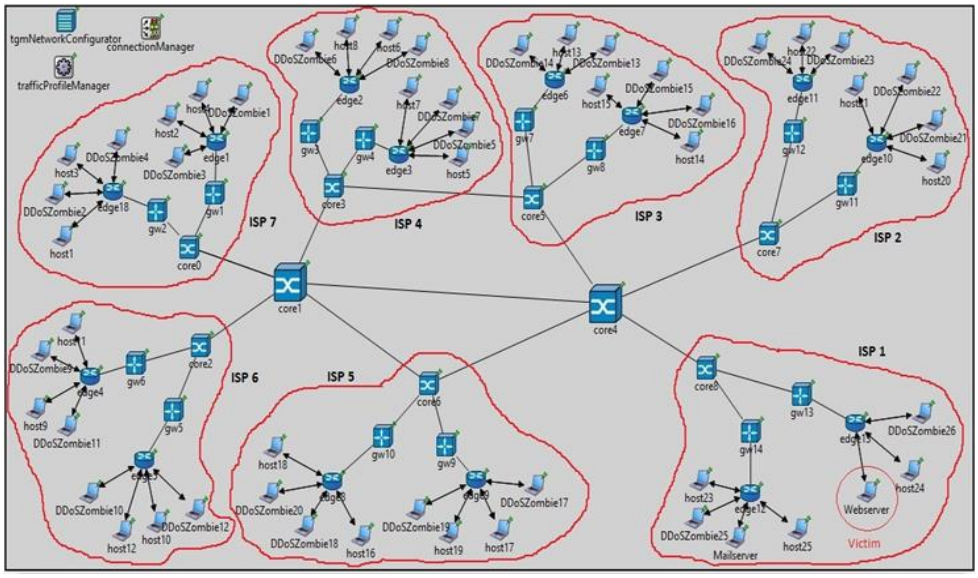

Fig.5. Detailed view of autonomous system based Internet topology

The cores routers are high proficient routers and all are connected with each other through very high-speed communication links. They are mostly used to connect different autonomous systems with each other. The core routers further connects to gateway routers through high-speed links. The gateway router further connects with multiple edge routers.

Finally, the edges connect to several hosts with lower speed links. Table 1 presents the chosen parameters for link metrics.

Table 1. Link parameters for simulation

Router Level	Link Speed	Delay
Core to Core	2.5 Gbps	1 ms
Core to Gateway	1 Gbps	1 ms
Gateway to Edge	155 Mbps	1 ms
Edge to Server	10 Mbps	5 ms
Edge to Host	0.768 Mbps	5 ms
Host to Edge	0.128 Mbps	5 ms

6. PERFORMANCE ANALYSIS

Here, we investigate the benefit of increased deployment of the DDoS defense system. The defense system running detection and filtering algorithm is implemented on the edge routers of stub networks. The defense agents identify and share the attack information to its coordinator and the coordinators further share this information to the coordinators of nearby ISPs. By adding more and more number of ISPs in the defense system, attack traffic can be dropped efficiently and the number of attack packets reaching the victim server will be decreased. The performance of the defense system is specially checked during the attack i.e. between 10^{th} to 22^{nd} sec in the simulation run. The results of the simulation will be collected in the form of scalar and vector output values. The scalar has a single output value (e.g. the number of packets received) but vector stores series of time-value pairs during the simulation period. These statistics can later be analysed to evaluate the effect of DDoS attack and defense mechanism on the performance of legitimate traffic. Here we specially measure and discuss the effect of incremental deployment of defense system on the following three performance metrics.

6.1. Throughput

Throughput is defined as the 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.

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

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

So here, 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;

$$\text{Goodput} = \frac{Tn}{\Delta}, \quad \text{Badput} = \frac{Ta}{\Delta}$$

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 10^{th} second and continues up to 22^{nd} second. Fig. 6 shows that the number of legitimate packets dropped will decrease with the increase in defense enabled ISPs.

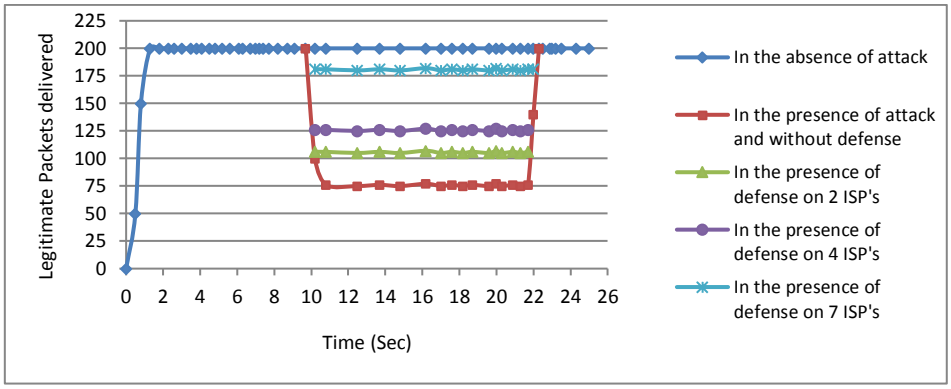

Fig. 6. Goodput

Fig.7 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.

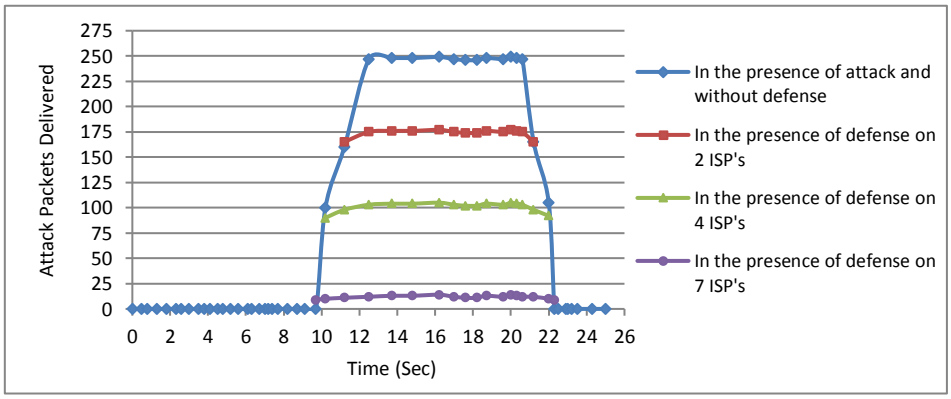

Fig. 7. Badput

6.2. Legitimate Packet Survival Ratio (LPSR)

The legitimate packet survival ratio 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

$$N = \frac{\mathrm{Tn}}{(\mathrm{Ta} + \mathrm{Tn})}$$

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 NSPR should be high so as to ensure uninterrupted services. The value of NPSR 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. 8 shows the survival ratio of legitimate packets manages to reach destination.

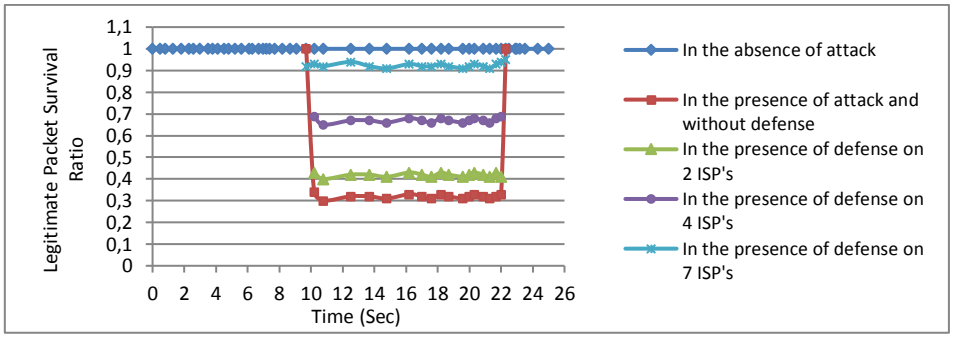

Fig. 8. Legitimate packets survival ratio

6.3. 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. The following kinds of communications can happen during the defense process:

Coordinator to edge routers: Coordinator asks the agents on edge router to start defense system in request mode or self-mode.

Edge router to coordinator: Feedback messages at regular intervals for the attack traffic identified and dropped by the agent.

Edge router to Gateway router: Messages to request the gateway router to measure entropy rate against the suspected flow for nearby edge routers.

Gateway router to Edge router: It will reply with the entropy rate for the neighbouring edge router

Coordinator to Coordinator: Coordinator of one ISP sends attack related messages to the coordinators of neighbouring ISPs.

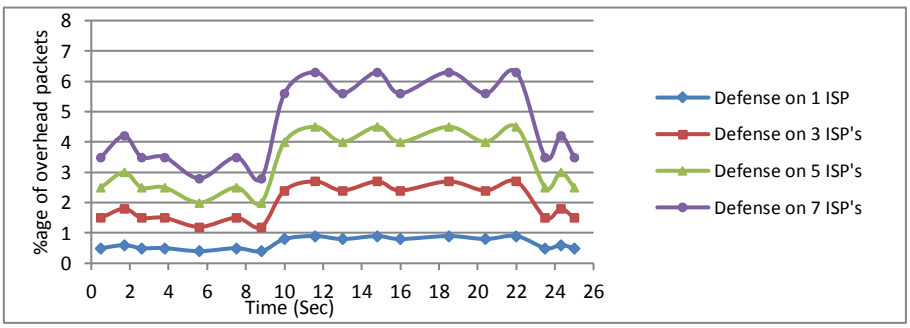

Fig. 9. Percentage of overhead packets

Fig. 9 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 7%.

7. CONCLUSION

Here we described the deployment process of a DDoS defense mechanism on multiple ISP domains. The main focus of this paper is to unveil the benefits of increased deployment of DDoS defense system on multiple ISP domains in an incremental fashion. The performance is tested with the deployment of defense system on varying number of ISPs. The throughput is evaluated in terms of goodput and badput. The goodput i.e. the number of legitimate packets delivered to the destination increases with the increase in the number of participating ISPs. Similarly the badput i.e. the number of attack packet manages to reach the destination will decrease with increase in participations from ISPs. The normal packet survival ratio will also increase with the increase in the number of participating ISPs. The only drawback of the scheme is the percentage of overhead packets which increases very little with the increase in participating ISPs.

REFERENCES

[1] Criscuolo, P. Distributed Denial of Service, Tribe Flood Network 2000, and Stacheldraht. CIAC-2319, Department of Energy Computer Incident Advisory Capability (CIAC), (Tech. Rep. UCRLID - 136939, Rev. 1). Lawrence Livermore National Laboratory.

[2] Todd, B. Distributed Denial of Service Attacks. Available: http://www.linuxsecurity.com/resource files/intrusion detection/ddos–whitepaper.html, 2000.

[3] "akamai's security report", Available: https://www.akamai.com/us/en/multimedia/documents/state-of-the-Internet/q4-2016-state-of-the-Internet-security-report.pdf, 2016.

[4] "Arbor Networks Special Report", Worldwide Infrastructure Security Report, Vol. XII, Available: https://pages.arbornetworks.com/rs/082-KNA-87/images/12th_Worldwide_Infrastructure_Security_Report.pdf, 2017.

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

[6] Chen, Y., Hwang, K., and Ku, W. Collaborative detection of DDoS attacks over multiple network domains. IEEE Transactions on Parallel and Distributed Systems, **12**(vol. 18), Dec. 2007, pp. 649 – 1662.

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

[8] Papadopoulos, C., Lindell, R., Mehringer, J., Hussain, A., and Govindan, R. COSSACK: Coordinated Suppression of Simultaneous Attacks. *Proc. of DISCEX*, Washington, DC, USA, April 2003, pp. 2-13.

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

[10] Chen, S., and Song, Q. Perimeter-based defense against high-bandwidth DDoS attacks. *IEEE Transactions on Parallel and Distributed Systems*, **6**(vol. 16), June 2005, pp. 526-537.

[11] Guizani, M., Rayes, A., Khan, B., and Al-Fuqaha, A. *Network Modeling and Simulation: A Practical Perspective*. Wiley-Interscience, Chichester, West Sussex, UK, 2010.

[12] Wehrle, K., Gunes, M., and Gros, J. *Modeling and Tools for Network Simulation*. Springer-Verlag, Berlin, 2010.

[13] Peng, T., Lechie, C., Rama, K., and Rao, M. Survey of network based defense mechanisms countering the DoS and DDoS problems. ACM Computing Surveys, 1(vol. 39), article 3, Apr. 2007.

[14] Kassa, M., and Libsie, M. A Synchronized Distributed Denial of Service Prevention System. *Computer Science & Information Technology*, 2012, pp. 09-23.

[15] Tupakula, U., Varadharajan, V., Gajam, A., Vuppala, S., and Rao, P. DDoS: Design, implementation, and analysis of automated model. *International Journal of Wireless and Mobile Computing*, **1**(vol. 2), 2007, pp. 72-85.

[16] Singh, K., Kaur, N., and Nehra, D. A comparative analysis of various deployment based DDoS defense schemes. *Proc. of 9th International Conference on Quality, Reliability, Security and Robustness in Heterogeneous Networks*, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 115, 2013, pp. 606-616.

[17] Singh, K., Dhindsa, K., and Bhushan, B. Distributed Defense: An Edge over Centralized Defense against DDos Attacks. *International Journal of Computer Network and Information Security*, **3**(vol.9), Mar. 2017, pp. 36 - 44.

[18] Varga, A., and Horing, R. An overview of the OMNeT++ simulation environment. *Proc. of the 1st international conference on Simulation tools and techniques for communications, networks and systems & workshops*, Marseille, France: ACM Press, 2008.

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

[20] Gamer, T., and Scharf, M. Realistic simulation environment for IP-based networks. *Proc. of 1st International Conference on Simulation Tools and Techniques for Communication and Systems & Workshops*, Marseille, France: ACM Press, 2008, pp. 83:1-83:7.

[21] Cover, T. and Thomas, J. *Elements of Information Theory*. Second edition, John Wiley & Sons, 2007.

Information about the authors:

Karanbir Singh, is doing his Ph.D. in the field of Network Security from IKG Punjab Technical University, Kapurthala (Punjab). He has a teaching and research experience of more than 13 years. He has authored more than 8 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, and Adhoc Networks.

Dr. Kanwalvir Singh Dhindsa, Ph.D., is working as Professor in the Department of CSE at Baba Banda Singh Bahadur Engg. College, Fatehgarh Sahib (Punjab). 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, Web Engineering, Mobile Computing.

Dr. Bharat Bhushan, Ph.D., is employed as Head and Associate Professor in the Department of Computer Science & Applications, Guru Nanak Khalsa College, Yamunanagar (Haryana). He has more than 30 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.

Manuscript received on 19 July 2017