International Journal of Security and Its Applications
Vol. 11, No. 8 (2017), pp.1-12
http://dx.doi.org/10.14257/ijsia.2017.11.8.01

Collaborative Agent-based Model for Distributed Defense against DDoS Attacks in ISP Networks

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

[1]*Research Scholar, IKG Punjab Technical University, Kapurthala (Punjab), India*
[2]*Professor, Deptt. of CSE, Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib(Punjab), India.*
[3]*Associate Professor, Deptt. of Computer Science, Guru Nanak Khalsa College, Yamunanagar (Haryana), India.*
[1]*karan_nehra@yahoo.co.in,* [2]*kdhindsa@gmail.com,*
[3]*bharat_dhiman@hotmail.com*
**Corresponding author*

Abstract

The attacks like denial of service (DoS) and more specifically the distributed denial of service (DDoS) are one of the biggest threat to host and services of the Internet. There are many schemes available in the literature, which try to detect and defend these kinds of attacks, but many among them face numerous problems in providing an effective defense. Some of them are not practically possible to implement and others are not effective in handling these attacks. Hence, there is a need of defense mechanism which can effectively protect any infrastructure against DDoS attack. Instead of building an isolated defense method, we require a distributed defense framework, in which defense components can be deployed at various places on the internet. The proposed distributed defense model can defend DDoS attacks by placing defense agents and coordinator at different places over the Internet. The defense agents will be installed at edge routers and coordinator at core router of each stub domain. The defense agents and coordinator will securely communicate with each other to share the attack related information and the same will be shared with neighboring internet service providers. In order to provide efficient defense, the overall defense process is divided into various levels.

Keywords*: DoS, DDoS, Distributed Defense, ISP Networks*

1. Introduction

A DoS is an attack having the target of stopping normal clients from using a particular Internet/network resource such as a computer system, web service or website [1]. A DDoS is a coordinated attack, whose aim is to make a particular system, network service or network resource inaccessible to its customers or 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.

In February 2000, the first large DDoS attacks were performed against Yahoo.com, which in results keeps it off from the internet nearly for 2 hours. It results in costing it lost high advertising revenue [2]. A cycle of DDoS attacks results in the shutdown of some leading websites for several hours [3]. The report of PC crime and security survey lead by FBI/CSI in the U.S for the year 2004 [4] show that DDoS attacks are one the 2nd large

ISSN: 1738-9976 IJSIA

one outside attacks discovered in computer domain straight away after virus and intrusion infections. A computer crime and security survey conducted in Australia for the year 2004 [5] shows the same kind of outcomes. The technologies like ISDN, dial-up and cable modems intended for home users have amplified the threat of DDoS attacks.

The study conducted by Arbor Networks [6], in 2007 show that the major DDoS bandwidth attack against ISPs was recorded as 40 gigabits per second. But the intensity of these attacks was almost doubled in 2008 from the previous year. The major portion of DDoS attacks are done using TCP, and a huge portion comes under the category of flooding attacks [7]. Therefore, our focus is on preventing a comprehensive range of TCP based flooding attacks.

In recent past, numerous techniques have been suggested on how to identify and defend these types of attacks. Some of them are a little bit effective but most of them face many kinds of problems. Some of them are practically not possible to deploy and others are not so much effective to control these attacks. Most of the proposed defense schemes treat only some portion of the DDoS attack traffic but not as a whole. The problem can be seen from the perspective of ISP domain because it is responsible for carrying a lot of useless traffic. So a defense mechanism is needed which can detect and drop attack traffic inside the ISP boundary.

Present DDoS defense schemes can be categorized as either autonomous or distributed defense. A distributed defense system provides the defense with the help of many defense components distributed at various places over the Internet. A distributed defense is more efficient because its defense components can detect and drop attacks traffic in the intermediate networks and prevents it from reaching the victim. Unfortunately, the distributed defense methods need wide deployment of its defensive components, which need to be spread across various domains managed by different ISPs, all possibly having different managerial and security policies. Due to these limitations, it is not easy to design a distributed defense system. Furthermore, some ISPs may not be ready to become the part of distributed defense because every ISP will not be directly benefited from this type of deployment. All these problems disappoint researchers from seeking a distributed defense method against DDoS attacks. So there is a need of a stable solution, which can detect and defend DDoS attacks early before it causes damage to the victim. This paper presents a model in which DDoS attacks are defended inside the ISP domain. The defense components are placed in the form of agents on routers in the participating ISP network. The agents deployed on the routers perform the task of characterizing and filtering the attack traffic by cooperating with each other. The proposed model can be tested on realistic topologies generated by ReaSE [8], which can create the Internet like topologies of different scales. The simulations of proposed model can be tested by using a discrete event simulator OMNeT++ [9]. The Internet-specific networks can be simulated in OMNeT++ by using INET framework [10]. INET simulation model is an extension of OMNeT++ and it contains many application models and TCP, UDP, IPv4 and IPv6 protocol implementations. It offers Internet-specific objects like a router and standard host that combine different layers to attain the functionality of intermediate and end nodes respectively.

2. Related Work

Here we will discuss some existing defense schemes proposed in the literature, which try to defend DDoS attacks in distributed environment.

In [11] the author proposed a distributed DDoS defense scheme, 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. A global DDoS defense system, which is made as an overlay network on top of the Internet was discussed by Zhang and Parashar [12]. There are two stages in this method. In the first stage, every defense node locally identifies traffic abnormalities by using some existing IDS tools. After separating attack traffic, the defense node sets a rate limit on attack traffic and prevents it from moving further. In the second stage, the attack information is shared among defense nodes by using a gossip-based communication technique. This gossip based technique is used to gather the overall information about DDoS attacks by using information sharing. The proposed scheme constantly observes the network traffic. When an attack starts happening, each defense nodes starts dropping attack traffic identified as per local information. But, as local detection has a high false alarm rate, normal traffic will also be dropped. Chen et al. [13] proposed a scheme which identifies DDoS attacks by checking the propagation patterns of unpredicted traffic variations at distributed points in the network. When a necessarily big CAT tree is created to surpass a specific threshold value, an attack is confirmed. This system is installed on many autonomous systems domains. In each ISP domain, there exists a central CAT server. The scheme detects abrupt traffic variations, aggregates suspicious alerts and flow propagation patterns, and merge all CAT sub-trees from combined servers to form a global CAT tree. This system is made over attack transit routers, which collaboratively work with each other. A CAT server in every ISP domain is used to combine the attack alerts informed by various routers. CAT domain servers cooperate with each other to make the final decision. A method in which each network can be categorized as either a stub or transit domain is identified by Lam et al. [14]. In this method, a stub domain is connected with local ISP and contains individual host. A transit domain joins different stub domains to form a backbone network. Here stub agents are deployed on stub domains and perform the task of attack traffic detection and filtering. Transit agents are deployed on transit domains 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 domain 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.

Mirkovic et al. [15] identified a distributed cooperative defense system for DDoS attacks. DefCom constructs a set of distributed cooperative defense nodes that are distributed everywhere on the Internet. The defense nodes interchange information & control messages with each other to detect DDoS attacks, cooperatively control them and allowing normal traffic to pass through. DefCom nodes can be divided into three types, depending upon the task they offer: alert generator nodes detects an attack and alerts to the remaining part of the peer network, the rate limiter node can be used to rate limits a huge volume of internet traffic heading towards the victim, but not able to separate genuine packets from attack packets and the classifier nodes performs the task of selective rate-limiting. This scheme effectively distinguishes between normal and attack packets, and dedicates the available bandwidth to normal traffic and collaborates with other defense nodes to certify decent service for the normal users. The frequent communication between defense nodes invites the attackers to attack the DefCom system itself. Canonico et al. [16] proposed a technique which provides distributed response against DDoS attacks with non-contiguous deployment. Every ASSYST nodes are alike of classifier nodes but they are installed only on edge networks. Active Security Protocol permits a set of active routers to interact with each other in order to recognize the sources of a DDoS attack. Deployment and tuning of the active security system are preferably suitable for a programmable network environment. They are not able to handle attacks from legacy networks that do not deploy their defense mechanisms. Xuan et al. [17] identified a mechanism in which routers act as gateways. Their main task is to identify and detect

DDoS attacks locally and discards packets having abnormal flows. Gateways are deployed in the perimeter of victim and source domains. They communicate with each other in order to provide a cooperative defense of a limited scope. A controller agent model identified by Tupakula and Varadharajan is used to neutralize DoS attacks inside one ISP domain which was later on extended to many domains [18]. In this scheme, agents are implemented on edge routers and controllers are implemented on any internal router in the ISP. When an attack is detected by the victim, it informs the controller to start the defense process. The controller instructs all the agents to start marking all the packets heading towards the victim. The victim can identify the source of attack traffic (edge router) by looking into the marking field. The victim then provides the attack signature to the controller and requests the particular agents to drop attack traffic. So the attack traffic can be filtered at the edge router in the source network. In [19], controllers from the multiple domains collaborate with each other provide DDoS defense. The main drawback of this mechanism is that it uses third party tool for the detection and characterization of attack traffic.

3. Model of Internet Topology

Our distributed defense strategy is based on the network model of the Internet topology. Today Internet can be seen as a pool of many routing domains interconnected with each other. These routing domains are also known as AS (autonomous systems). Each autonomous system on the Internet can be the part of either a transit AS or stub AS [20]. A stub AS is normally run by a local ISP and generally transmits packets to and from its client network/hosts. It consists of actual host systems, which are further connected with an edge, gateway and core routers. The purposes of transit AS is to interconnect stub AS efficiently. The large backbone of ISPs is classified as a transit AS. A transit domain mostly contains a set of high-speed core routers also known as backbone nodes. In transit AS, some backbone nodes are further connected to a number of stubs AS and remaining is connected with other transit AS. The proposed DDoS defense scheme is based on this transit-stub network model. Fig.1 shows the network model of the internet reflecting the internal structure of a single stub AS. The hosts in the stub AS are connected with edge routers, which are further connected with gateway nodes. A gateway node is used to connect one or more edge routers with the core routers. Core routers can further join one or more transit AS with each other. The size of routing domains can range from one or two nodes to thousands of nodes. Fig. 1 also shows that the end users (which can be attackers or normal users) are distributed in various stubs AS. The packets sent by attackers or normal users have to cross some edge or core routers, which are present in various stubs or transits AS, before finally reaching to the victim. So we need a defense solution which detects and stops the attack packet before they reach to the victim. The best possible place is to identify and drop attack traffic is source and intermediate networks. So there is a need of defense mechanism which is distributed in nature.

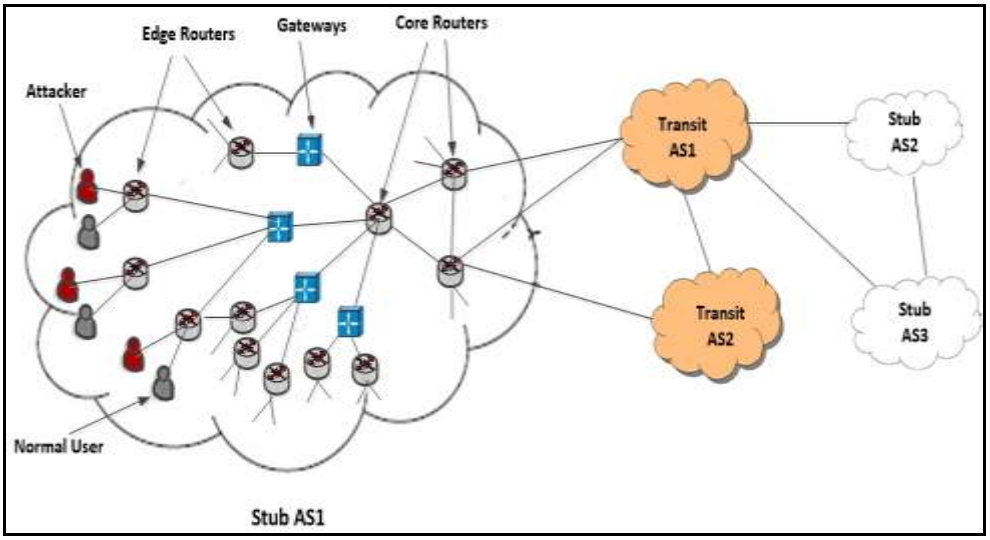

Figure 1. Transit-Stub Model of Internet Topology

4. Defense Model

In [21], we have already identified the various locations (i.e. source, intermediate and victim networks) where the defense system can be deployed. A distributed defense is that in which the defense components will be deployed at all the three locations i.e. source, intermediate and victim. The performance analysis in [21] proves that distributed defense is the only solution to effectively control the threat of DDoS attacks. So the proposed defense model is also based upon the distributed defense approach. As we have already seen that the whole Internet is divided into transit–stub domains. The customer's networks are connected to these stub domains, which are normally operated by local ISP. Fig. 2 shows only the picture of victim side stub domain. It shows the flow of two types of traffic i.e. attack traffic and normal traffic, which is heading towards the victim. So the aim of the defense model is to identify and eliminate the attack traffic on these stub domains. Most of the attack traffic originates from the customer networks of the stub domain; enter in the stub domain through the edge router and reaches to the victim through another edge router. Therefore, every attack packet moves through at least one edge routers before reaching to the victim. So the purpose is to identify and block the attack traffic at the edge routers in the ISP domain.

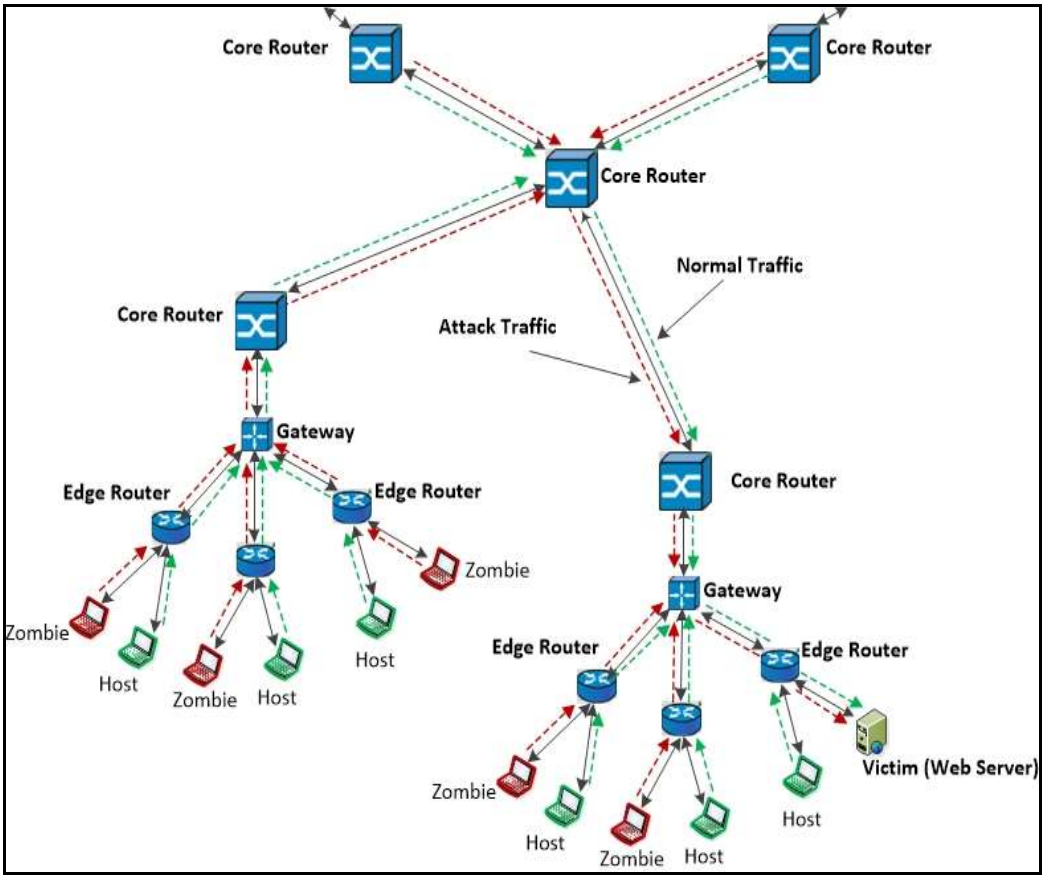

Figure 2. Snapshot of the Victim Side Stub Domain

The proposed model of distributed defense system utilizes the strengths of various deployment locations. This model is based on a controller-agent approach to be implemented on autonomous systems. In every stub domain, there exists a coordinator, which is used to coordinate and manage various defense agents. The controller will be implemented on the core router of the stub network. The actual defense will be carried out by a number of agents to be implemented on edge routers. The agents running detection algorithm will constantly monitor the traffic heading towards a specific destination at the edge router. They have the ability to analyze and take appropriate actions based on a given mission assigned to them. Here, agents are special modules which work on the behalf of targeted victims/networks within the given and others' domain networks. The defense scheme is initially be implemented on small topology, which can later to be extended for large topology.

5. The Defense Process

The major problem in existing DDoS defense techniques is to identify and detect the attack traffic accurately and efficiently. The main purpose of this scheme is to identify and extract attack traffic addressed to a specific destination and providing more bandwidth to the normal traffic from legitimate sources. The concept of entropy and threshold is used for the attack detection [22]. Entropy can be used in different ways for detection of anomalies in traffic features. This feature of information theory can be utilized in the monitoring of network traffic. The entropy can be used to measure the randomness of a flow passing through a given router. This property can be applied to various attributes of packet headers like source IP, destination IP, source port, destination port, the total number of packets etc. In case of DDoS attack, there can be one flow which

dominates other flows, which in results decrease the overall router entropy. Router entropy remains stable when there is no attack but it drops radically when there is a Flash event (FE) or DDoS attack. The overall defense process is divided into different steps.

The first step of defense process is to decide the various threshold values to be used in the detection algorithm. The values can be identified by performing extensive experiments on sample attack and legitimate traffic. The detection algorithms will be implemented as a part of defense agent on the edge router of stub network. It monitors the traffic passing through the edge routers and measures the randomness of flows by using the concept of entropy. When a flow dominates the other flows then it results in the decrease of normalized router entropy. The detection algorithm running on edge router will regularly checks for the normalized router entropy against a predefined threshold value and identify if there is any suspicious flow or not. In case of a suspicious flow, it is further confirmed whether it belongs to the flash event or a DDoS attack. If the flow is the part of DDoS attack then it will be dropped and the attack information is shared with the coordinator. The coordinator shares this information through the secure protocol to other nearby stub networks so that attack traffic can be dropped at their source. Fig. 3 illustrates the flow of different phases of proposed distributed defense model.

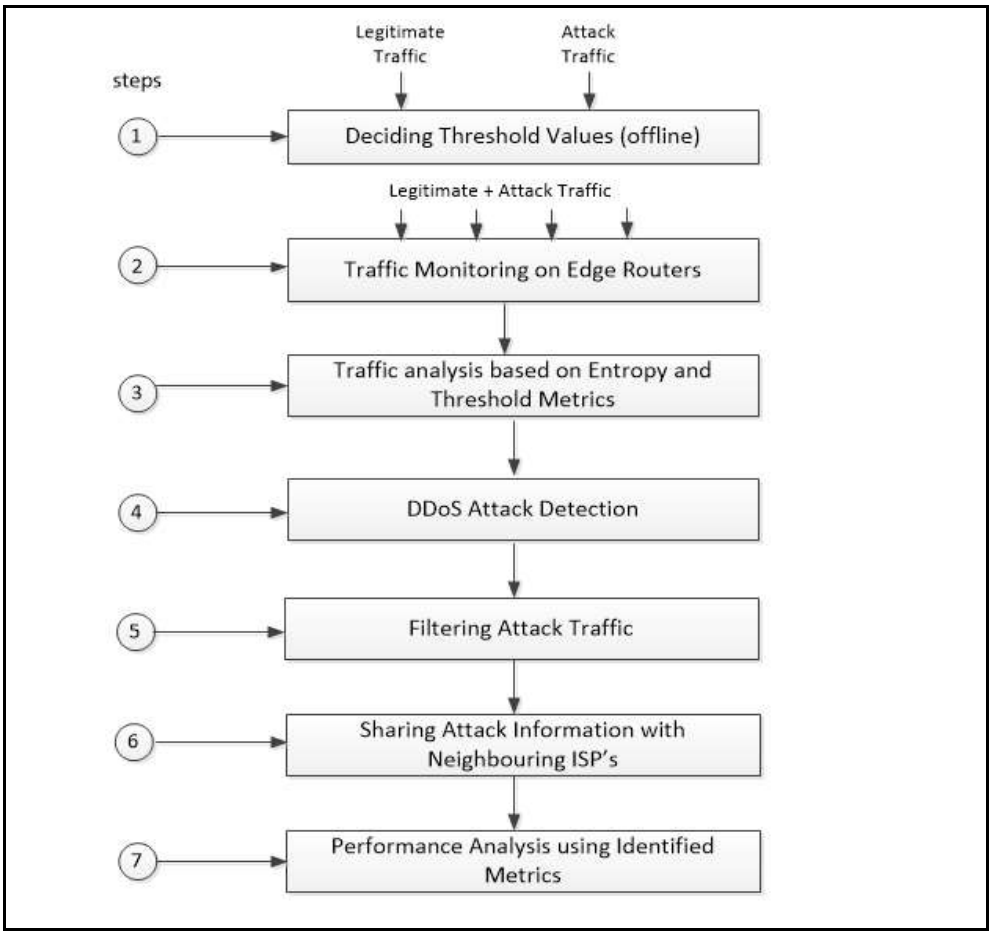

Figure 3. Flowchart Showing the Defense Process

During the defense process, agents communicate with each other through the coordinator. Their common goal is to identify and stop attack traffic at the early stages. They also share information like type of attack traffic, the source of attack traffic, target destination etc. it helps them to provide early defense attack against a DDoS attack. Messaging is the means of communication between coordinator and agents. The communication between agents and the coordinator is encrypted so as to avoid it from the

attackers. These agents will work corporately with the coordinator having a common goal of protecting the victim from various DDoS attacks. The coordinators across domain/ISPs also share information about valid agents in their domains. Fig. 4 shows the communication between central coordinator, agents, and coordinators between neighboring domains.

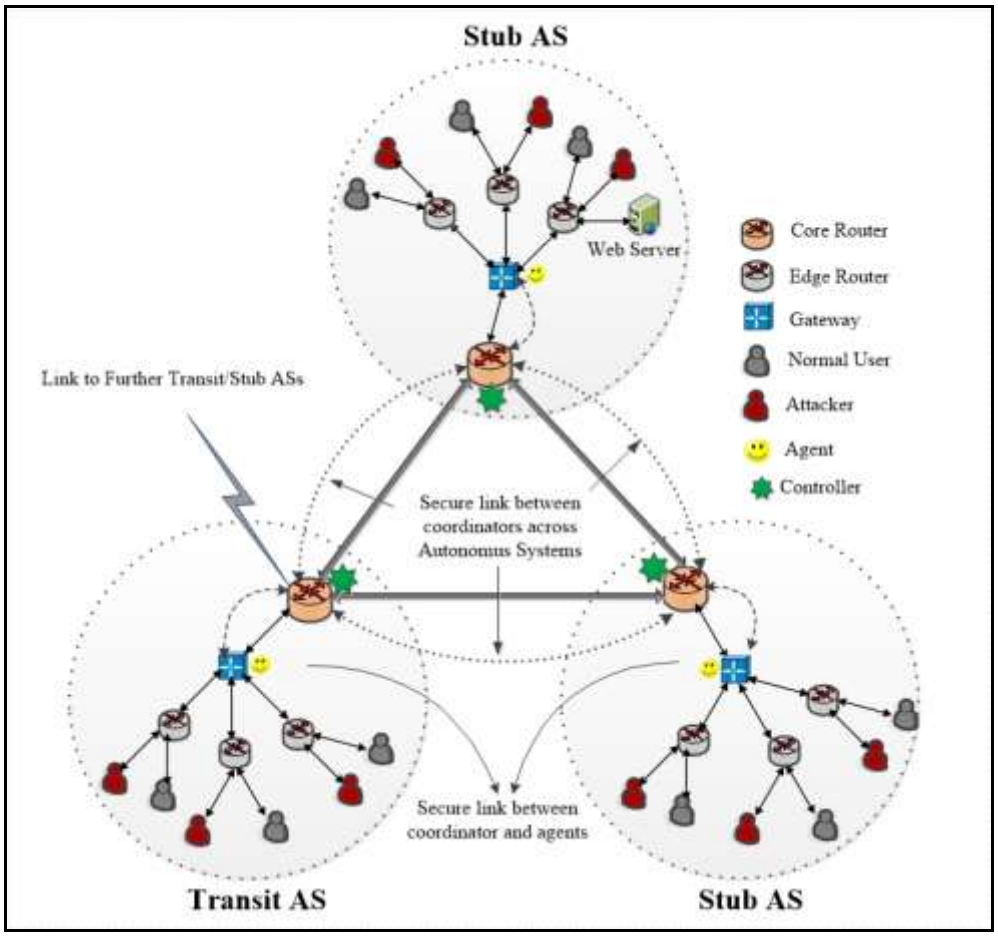

Figure 4. Communication between Agent, Central Coordinator and Coordinators Across ISPs

6. Performance Analysis Metrics

The performance of proposed system will be evaluated by implementing the functionalities of the defense system using simulations. We will perform intensive simulation experiments by using different sample attacking scenarios on predefined experimentation setup. The outcome of these scenarios allows us to evaluate the effectiveness of the proposed solution. Here we will identify the various performance evaluation parameters which can later be used to test and compare the performance with similar kind of defense systems.

Detection rate: The detection rate is the measure of the percentage of attacks detected among all actual attacks performed. The value of detection rate should be higher. The detection rate is defined as follows:

Detection rate = Number of detected attacks packets/Total number of attacks packets

Detection delay: The detection delay is the time taken by the defense system to detect the happening of an attack. This value of detection delay should be lower.

Detection delay = Time, when DDoS attack is detected - Time when DDoS attack is started

False negative rate: The false negative rate is the number of times the attacks packets will be considered as normal packets. The value of false negative rate should be low.

False negative rate = Number of false negative packets / Total number of attack packets

False positive rate: The false positive rate is the number of times the normal packets will be considered as attack packets. The value of false negative rate should be low.

False negative rate = Number of false negative packets / Total number of attack packets

Goodput: A/ (A+B) where A is the total number of attack packets dropped at the edge router after the invocation of the defense model. B is the attack packets that manage to reach the victim.

Percentage of overhead packets: The percentage (%) ratio of control packets communicated in the simulation to the total attack traffic in the simulation.

7. Conclusion & Future Work

There have been many efforts of defending against DDoS attacks through different ways and still, many researchers spend ample of their time on proposing various defense systems. However, numerous of these methods lack some of the critical features (functionalities) of DDoS defense such as accurate attack detection, attack protection, and collateral damage prevention. This paper proposed a distributed DDoS defense model using multiple defense agents, which work cooperatively in ISP domain on behalf of the victim. These agents perform the various defense tasks assigned to them within their working boundaries and collaborate with each other to achieve the target. The proposed model will provide defense against a variety of DDoS attacks by processing incoming traffic on the edge routers. The whole defense process is divided into various levels. The various levels include a screening of incoming traffic, characterization of traffic into different types, filtering and rate limiting of suspicious traffic by agents. The agents share attack related information with coordinator and coordinators exchange information to the coordinators of neighboring ISPs. The information is exchanged through a secure communication process. This model can effectively detect and characterize various types of DDoS attacks with very high detection rate and minimum collateral damage. The future work is to test the effectiveness of this model through intensive experiments using simulations.

References

[1] D. Karig and R. Lee, "Remote denial of service attacks and countermeasures", Princeton University, Department of Electrical Engineering Technical Report CEL2001-002, **(2001**).
[2] L. Garber, "Denial-of-Service Attacks Rip the Internet", IEEE Computer, vol. 33, no. 4, **(2000)**, pp. 12-17.
[3] G. Sandoval and T. Wolverton, "Leading Websites under Attack", **(2000**). http://www.cnet.com/news/leading-web-sites-under-attack/
[4] L. Gordon, M. Loeb, W. Lucyshyn and R. Richardson, "2005 CSI/FBI computer crime and security survey", Tech. Report, Computer Security Institute, **(2005**). https://www.globaltrust.it/documents/press/phishing/FBI2005.pdf
[5] AusCERT, "Australian computer crime and security survey", Tech. Report, Australian Computer Emergency Response Team, **(2005**). http://www.auscert.org.au/crimesurvey
[6] R. Vamosi, "Study: DDoS attacks threaten ISP infrastructure", **(2008).** http://www.cnet.com/news/study-ddos-attacks-threaten-isp-infrastructure/.

[7] D. Moore, C. Shannon, D. Brown, G. Voelker and S. Savage, "Inferring Internet Denial-of-Service Activity", ACM Transactions on Computer Systems, vol. 2, no. 2, **(2006)**, pp. 115-139.
[8] T. Gamer and M. Scharf, "Realistic simulation environment for IP-based networks". Proceedings of 1st International Conference on Simulation Tools and Techniques for Communication and Systems & Workshops, SIMUTools, Marseille, France, **(2008)**, March 3 -7.
[9] A. Varga, "The OMNeT++ Discrete Event Simulation System". Proceedings of 15th European Simulation Multiconference, Prague, Czech Republic, **(2001).**
[10] V. Andras, "INET Framework documentation and tutorial", **(2008).** http://www.omnetpp.org/staticpages/index.php?page=20041019113420757.
[11] T. Nguyen, C. Doan, V. Nguyen, T. Nguyen, M. Doan, "Distributed defense of distributed DoS using pushback and communicate mechanism", Proceedings of 2011 International Conference on Advanced Technologies for Communications, Da Nang, Vietnam, **(2011),** September 26.
[12] G. Zhang and M. Parashar, "Cooperative defense against DDoS attacks', Journal of Research and Practice in Information Technology, vol. 38, no. 1, **(2006)**, pp. 69-84.
[13] Y. Chen and K. Hwang and W, Ku, "Collaborative detection of DDoS attacks over multiple network domains", IEEE Transactions on Parallel and Distributed Systems, vol. 18, no. 12, **(2007)**, pp. 1649-1662.
[14] H. Lam, C. Li, S. Chanson and D. Yeung, "A coordinated detection and response scheme for distributed denial-of-service attacks", Proceedings of IEEE Conference on Communications Istanbul, Turkey, **(2006)**, June 11 – 15.
[15] J. Mirkovic, M. Robinson, P. Reiher and G. Oikonomou, "A framework for collaborative DDoS defense", In Proc. Int. Conf. 22nd Annual Computer Security Applications Conference, Miami, Florida, USA, **(2006)**, December 11 – 15.
[16] R. Canonico, D. Cotroneo, L. Peluso, S. Romano and G. Ventre, "Programming Routers to Improve Network Security", Proceedings of OPENSIG Workshop Next Generation Network Programming, London, UK, **(2001)**.
[17] D. Xuan, R. Bettati and W. Zhao, "A gateway-based defense system for distributed dos attacks in high-speed networks", Proceedings of the 2001 IEEE Workshop on Information Assurance and Security United States Military Academy, West Point, NY, **(2001)**.
[18] U. Tupakula and V. Varadharajan, "A practical method to counteract denial of service attacks", Proceedings of 26th Australasian Computer Science Conference, Darlinghurst, Australia, **(2003)**.
[19] U. Tupakula and V. Varadharajan, "Counteracting DDoS attacks in multiple ISP domains using routing arbiter architecture", Proceedings of 11th IEEE International Conference on Networks, Sydney, NSW, Australia, **(2003)**.
[20] E. Zegura, K. Calvert and S. Bhattacharjee, "How to model an Internet-work", Proceedings of IEEE INFOCOM'96, San Francisco, CA, USA, **(1996)**.
[21] K. Singh, N. Kaur and D. Nehra, "A comparative analysis of various deployment based DDoS defense schemes", Proceedings 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, Noida, India, **(2013)**, Jan 11–12.
[22] T. M. Cover and J. A. Thomas, "Elements of Information Theory", Second Edition, **(2007)**.

Authors

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 13 years. He is the member of various professional bodies like IAEME, UACEE, and IACSIT. He has authored more than 7 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.

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 been awarded the 'Best Ph.D. Thesis Award' in International Conference held in association with Computer Society of India (CSI) at Roorkee (Uttarakhand) in Nov. 2014. 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.

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. His qualification also includes MCA and Master of Science (Physics). He has teaching and research experience of more than 26 years. He is professional member of various reputed national and international associations. 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.

