A Distributed Mechanism to Protect Against DDoS Attacks

Negar Mosharraf, Anura P. Jayasumana, Indrakshi Ray

A Distributed Mechanism to Protect against DDoS Attacks *

Negar Mosharraf[1], Anura P. Jayasumana[2], and Indrakshi Ray[3]

[1] Forcepoint Security Labs, Forcepoint LLC, San Diego, CA, USA
nmosharraf@forcepoint.com
[2] Dept. of Elec. and Comp. Engg., Colorado State University, Fort Collins, CO, USA
anura.jayasumana@colostate.edu
[3] Dept. of Computer Sc., Colorado State University, Fort Collins, CO, USA
indrakshi.ray@colostate.edu

Abstract. Distributed Denial of Service (DDoS) attacks remain one of the most serious threats on the Internet. Combating such attacks to protect the victim and network infrastructure requires a distributed real-time defense mechanism. We propose Responsive Point Identification using Hop distance and Attack estimation rate (RPI-HA) that when deployed is able to filter out attack traffic and allow legitimate traffic in the event of an attack. It dynamically activates detection and blocks attack traffic while allowing legitimate traffic, as close to the source nodes as possible so that network resources are not wasted in propagating the attack. RPI-HA identifies the most effective points in the network where the filter can be placed to minimize attack traffic in the network and maximize legitimate traffic for the victim during the attack period. Extensive OPNET©based simulations with a real network topology and CAIDA attack data set shows that the method is able to place all filtering routers within three routers of the attacker nodes and stop 95% of attack traffic while allowing 77% of legitimate traffic to reach victim node.

1 INTRODUCTION

Denial of Service (DoS) attacks, that make network service unavailable to legitimate users, have been known since early 1980s. Distributed Denial of Service (DDoS) attacks originate and propagate in a distributed manner making them harder to mitigate. DDoS attacks against commercial websites like Yahoo, Ebay and E*Trade have provided evidence of how DDoS attacks block legitimate users and cause financial loss [9]. Moreover, emergency and essential services rely on the network infrastructure, and thus DDoS attacks may have severe consequences, such as loss of life. Consequently, techniques for preventing, detecting,

* This work was partially supported by NSF I/UCRC Award Number 1650573 and funding from CableLabs. The views and conclusions contained in this document are those of the authors and should not be automatically interpreted as representing the official policies, either expressed or implied of NSF and CableLabs.

and surviving such attacks [2] are needed. Despite significant research into countermeasures, DDoS attacks still remain a major threat [3]. DDoS attack can appear like a flash crowd, i.e., a large number of legitimate users connecting to a server/site simultaneously [10]. A comprehensive defense mechanism should include preventing, detecting, and responding techniques to counter DDoS attacks since there is no one-size-fit-all solution to the DDoS problems [15]. Prevention mechanisms aim to stop the occurrences of attacks [9, 14], while detection mechanisms aim to identify attack traffic [5, 7]. The response mechanisms attempt to identify the sources of attack and react to those [6]. Our work belongs to this last category and tries to identify the attack source and prevent the propagation of attack traffic.

Responsive techniques identify the source and mitigate DDoS attacks by filtering or limiting attack packets [1, 3, 4]. Such schemes comprise two parts: attack detection and packet filtering. The characteristics of attack packets, such as source IP address or marked IP header values [11, 14], are often used to detect and identify attack traffic and packet filtering. Note that packet filtering can be applied either close to the attack node [5, 7] or close to the victim node [14] where all the attack aggregate. However, applying filtering close to at the victim has two drawbacks. First, the victim may crash while dealing with an overwhelming volume of attack traffic. Second, the high volume of attack traffic may still overwhelm upstream Internet resources. At these traffic intensities, the infrastructure upstream from the intended victim becomes severely affected necessitating attack traffic be filtered as close as possible to the attack sources. However, it is difficult to anticipate and identify such nodes as the attack may originate at widely distributed nodes and spread through various routes [15]. Our approach aims to solve this problem.

This paper proposes a novel distributed DDoS defense mechanism for achieving Responsive Point Identification algorithm using Hop distance and Attack estimation rate (RPI-HA), which does not consume any router resources in the process of identifying routers for upstream filtering. The approach tries to minimize the modifications required to the routers and the current protocols to combat DDoS attacks and such modifications have a low complexity and are scalable. The mechanism aims to maximize the arrival rate for legitimate traffic and minimize the attack flow during the attack. The approach consists of four parts. The first part develops rules to create a history-based profile of high confidence legitimate IP addresses that serve to differentiate the good traffic from the malicious [8]. The second part represents the IP address history in the form of a Bloom filter for efficient transfer. The third and fourth parts, the main contribution of this paper, identify how and where this history is used to prevent the attacks. Placing filters in upstream routers incur storage and performance costs since the filter must be applied to multiple routers. Placing the filter closer to the victim causes the link capacity to become saturated and wastes network resources. Our scheme introduces an algorithm that identifies the routers where the filters can be placed. To the best of our knowledge, this is the first work that considers the optimal placement of the filters to mitigate DDoS attacks.Section 2 describes our

responsive defense mechanism. Section 3 presents our simulation results. Section 4 concludes the paper.

2 DISTRIBUTED RESPONSIVE DEFENSE APPROACH

This section presents our scheme to identify upstream routers, and block the DDoS attacks at these routers to minimize the impact both to the victim and to the upstream network during the attack time. The DDoS mitigation mechanism consists of the following components:(1) identification model to discriminate attack traffic from legitimate traffic based on a history-based profile, (2) capture the history-based profile in the form of a Bloom filter for efficient transfer, (3) identify the responsive points (router/switch) which carry the attack traffic, and (4) activate packet filtering at selected points. We use the mechanisms detailed in [8] for the first two steps. The main contributions of this paper are the last two components, and the resulting overall architecture.

2.1 IDENTIFICATION MODEL

History based profiles the specific attack features as well as normal traffic characteristics for history based profiles to discriminate between the attack traffic from legitimate traffic are investigated in [8]. A key observation is that the DDOS attacks tend to use randomly spoofed IP addresses [8] and other packet features, such as port number and size of packet are randomly distributed as well. Our experiments [8] with the CAIDA 2007 dataset [12] indicated that such as filtering model can protect the victim node from 95% of attack traffic while allowing 70% of legitimate traffic.

2.2 BLOOM FILTER MECHANISM

The filtering mechanism must be applied at upstream routers which must process all packets targeted towards the victim node. Since the network bandwidth may already be saturated during an attack, transferring the entire history and looking it up in the upstream routers is rather expensive. A Bloom filter is thus proposed for representing the contents of the IP based history [8]. Such a filter helps reduce the communication and computation costs and also the storage requirements at upstream routers that check for malicious traffic. There are three fundamental performance metrics for Bloom filters where the size of the Bloom filter is an adjustable parameter based on the accepted false positive rate as well as number of hash functions.

2.3 RESPONSIVE POINTS' IDENTIFICATION

The third step constitutes the main contribution of this paper and it is how and where to use this filter to minimize the impact of the attack. Proposed

solution addresses this problem by using a recently developed technology, typically implemented as Small Formfactor Probes (SFP) using Field Programmable Gate Arrays (FPGAs). Our proposed approach monitors traffic by using SFPs to efficiently identify router/switch which carry high volume of attack traffic and then applies packet filtering at selected routers as the responsive point of defense mechanism. An example of such hardware is JDSU SFProbes and Packet Portal [16]. SFProbes can plug into any SFP compatible elements such as switches/routers in such a way that it taps into the normal fiber without interfering with the traffic flow. It can be programmed over the network using the same fiber to do tasks such as counting the number of packets with certain values in header fields and forward information about link traffic to a remote base station. Our approach uses these probes at a subset of ports in the network to identify the upstream links, and thus nodes, which carry attack traffic. A main advantage of using SFProbes is that they plug into the routers/switches and do not require modifying the router's operation and software to apply our scheme.This feature is used to send the history based profiles to identify the paths with high intensity of attack traffic. Moreover, the portal base station (PBS) has knowledge about SFProbes attached to the routers throughout the network and can collect data from SFProbes and perform the computation needed for our scheme, obviating the need for routers performing such computations.
Upon detection of an attack, the proposed approach starts to protect a victim node as illustrated in Figure 1. At this point, the victim network sends the Bloom filters that it had created to PBS. The PBS sends the Bloom filter to those SFProbes that are plugged into different routers as shown in Figure 1. SFProbes start monitoring the intensity of traffic directed toward the victim node.

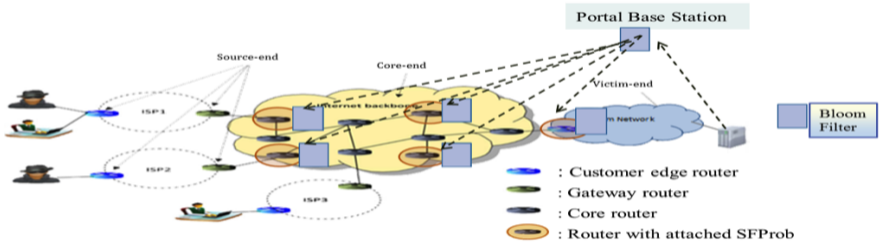


Fig. 1: Responsive defense mechanism

Let $t_1, t_2, ...t_m$ be discrete time slots and $X(t_m, i)$ be the number of packets received by a router during time slot m at SFProbe i destined to the victim node. Eq. (1) is defines the historical estimate of the average number of packets received by a router, where α is a weighted value between 0 and 1.

$$\bar{X}(t_m, i) = (1 - \alpha)\,\bar{X}(t_{m-1}, i) + \alpha X(t_m, i) \tag{1}$$

Let $A_j(t_m, i)$ represent a Boolean variable which equals 1 if the packet P_j is received at router i at time slot t_m and matches the corresponding Bloom filter $B(v)$ for point v, and is 0 otherwise, i.e.,

$$A_j(t_m, i) = \begin{cases} 1 & \text{if} \quad P_j(t_m, i) \in B(v) \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

Let $\bar{W}(t_m, i)$ be the historical estimate of the average number of packets received by the router at SFProbe i during time slot m that match the Bloom filter. Thus, $\bar{W}(t_m, i)$ Eq. (3) shows the average number of packets that is considered as the legitimate traffic by the Bloom filter directed towards the victim where, n is the total number of packets flowing toward the victim node in time slot t_m:

$$\bar{W}(t_m, i) = (1 - \alpha)\bar{W}(t_{m-1}, i) + (\alpha)\sum_{j=1}^{n} \frac{A_j(t_m, i)}{n} \tag{3}$$

During the attack time, if the number of IP addresses that do not match Bloom filter is higher than a specific threshold β, then the router is likely to be carrying significant attack traffic. Such routers are candidates for filter placement. We define Eq. (4) Attack Estimation Rate (ASR) $R(t_m, i)$ to determine the average number of packets that do not match Bloom filter.

$$R(t_m, i) = \frac{\bar{X}(t_m, i) - \bar{W}(t_m, i)}{\bar{X}(t_m, i)} \tag{4}$$

Upon detection of an attack, the SFProbes start monitoring traffic going towards the victim nodes and send $R(t_m, i)$ estimate to PBS. Next we decide the points at which the filters are to be placed. Save network resources, the best routers to apply the filtering mechanism must be as far away as possible from the victim node. The volume of potential attack traffic passing through a router has to be considered as well. Thus, we use two factors to determine the best routers to place the SFProbes - the Attack Estimation Rate of Eq. (4) and the hop distance $H_i(v)$ that shows how far the SFProbe i is from the victim node v. For each SFProbe i computer the weighted attack estimation rate $H_i(v)$ is given by:

$$S(t_m, i) = \frac{\bar{X}(t_m, i) - \bar{W}(t_m, i)}{\bar{X}(t_m, i)} * H_i(v) \tag{5}$$

The routers with higher value of $S(t_m, i)$ are selected routers to apply filtering mechanism. We call this approach as the Responsive Point's Identification algorithm using Hop distance and Attack estimation rate (RPI-HA). In addition to the hop distance and the volume of attack traffic, other issues must also be considered while placing the filters. One such additional factor is the number of routers on which filters are placed based on the distribution of the attack traffic. We present a new formula that adjusts the number of routers according to the attack traffic distribution that we refer to as the Responsive Point's Identification algorithm using Hop distance, Transmission rate and Attack estimation rate

(RPI-HTA). In this scheme, the transmission rate of traffic directed towards the victim node as well as hop distance is considered to determine the best filtering points. SFProbes collect the information of attack estimation rate $R(t_m, i)$ and traffic transmission rate $T(t_m, i)$ during m time slots and send this information to the PBS. To select the filtering points the attack estimation rate $D(t_m, i)$ is computed as follows:

$$D(t_m, i) = \frac{\bar{X}(t_m,i) - \bar{W}(t_m,i)}{\bar{X}(t_m, i)} * \frac{\bar{T}(t_m,i)}{C(v)} * H_i(v) \tag{6}$$

$$\bar{D}(t_m, i) = (1 - \alpha)\bar{D}(t_m, i) + (\alpha)\sum_{i=1}^{n} \frac{D(t_m, i)}{n} \tag{7}$$

In Eq. (6) we consider the distribution of traffic towards the victim node as an important factor that helps to determine how the attack has followed, where traffic transmission rate $T(t_m, i)$ and capacity of the victim node $C(v)$ are considered. $D(t_m, i)$ determines if the attack is distributed or centralized. If the attack is highly distributed, we need to consider more filtering points to stop the attack whereas if the attack is more centralized we apply filters on few of the routers. The historical average attack estimation rate is given by $\bar{D}(t_m, i)$ in Eq. (7) where n indicates total number of participating SFProbes that collects the data. We select only those routers $\bar{D}(t_m, i)$ higher than average attack estimation rate as filtering points. Thus, the number of filters in the RPI-HTA depends on traffic transmission rate, hop distance, as well as attack estimation rate and it will be vary according to $\bar{D}(t_m, i)$ and $D(t_m, i)$.

2.4 PACKET FILTERING

The last step of the proposed approach is activating packet filtering at selected points. According to the previous section, PBS selects those routers which carry the attack traffic for applying Bloom filtering. So PBS sends created Bloom filters to these selected routers and the routers start to filter incoming traffic directed towards the victim node. This process continues during the attack.

3 EVALUATION

Performance of our approach is evaluated next using a real network topology from Oregon route-views between March 31 and May 26 2001 [18] and set it up on OPNET©. We test the effectiveness of the responsive defense mechanism using the DARPA 1998 intrusion detection dataset [17] which contains 7 weeks of training datasets that we use to establish an IP address history and 2 weeks of testing dataset to evaluate our techniques. The first step is creating the IP address history from the DARPA training dataset and then create corresponding Bloom filter, the details of which was presented in [8]. The next step, evaluates the responsive defense approach based on the created IP address history in OPNET©. We also have validated our model by real network traffic collected at University of Auckland [13] and CAIDA attack dataset [12] in Section 3.5.

3.1 METRICS

Responsive defense mechanism is evaluated, (i) *Attack Traffic Detection Rate* (ii) *Normal Traffic Detection Rate* , and (iii) *Link Utilization Rate*. Attack Detection Rate is the percentage of attack dataset that is correctly detected as the attack and cannot pass through the Bloom filter to reach the victim node. Normal Traffic Detection Rate is defined as the percentage of normal traffic that can correctly pass through the Bloom filter during the attack period. False Negative Rate is defined as the percentage of attack traffic that is incorrectly marked as normal traffic and therefore can pass through the Bloom filter. Link Utilization Rate is defined as the percentage of the network's bandwidth that is currently being consumed by the network traffic.

3.2 PERCENTAGE of COLLABORATIVE SFPROBES

The effectiveness of the responsive defense mechanism relies on the collaboration of SFProbes through the network. Increasing the number of SFProbes attached to the routers enables more close monitoring and more effective filtering. We look at four different scenarios to validate this. We assume a different percentage of routers (80% to 25%) have SFProbes attached to them to monitor network traffic to address the case where only a fraction of routers implement the mitigation technique. The number of filtering routers is either fixed according to the RPI-HA or variable based on RPI-HTA algorithm. In the RPI-HA algorithm, the number of filtering routers considered 8, 5 and 3 as 20%, 12.5% and 7.5% of the total routers through the network. We also looked at a fifth scenario where the filters are placed in random locations throughout the network without applying any algorithm to stop the attack traffic. Figure 2 shows the average attack detection rate over 5 runs. We use a time slot of 60 seconds. The results demonstrate the effectiveness of using the RPI-HTA algorithm, which considers all the three features (hop distance, transformation rate and attack estimation rate) together. The RPI-HTA algorithm produces an attack traffic detection rate of 91% when 80% of routers use SFProbes. Note that, by applying the random selection to determine placement of filters the attack traffic detection rate reduces by more than 14% and up to 23%. These results show how the location of filters plays an important role in protecting the victim node. Recall that the number of filtering points for RPI-HTA algorithm is variable and depends on attack distribution, transmission rate, and hop distance. 7 filters for networks having 80% and 60% probes and 6 filters for those having 40% and 25% probes are selected according to the RPI-HTA algorithm. As shown in Figure 3 the attack traffic detection rate for RPI-HTA algorithm for 80% and 60% probes is equal or higher than when RPI-HA algorithm is applied by 8 filtering routers through the network. This means that the RPI-HTA algorithm can provide comparable or better filtering mechanism by using lower number of filtering routers by placing the filters in the appropriate locations. The other important parameter to evaluate is how many normal packets can reach the victim node. As shown in Figure 3, normal or legitimate traffic detection rate is around 72% for RPI-HTA algorithm with

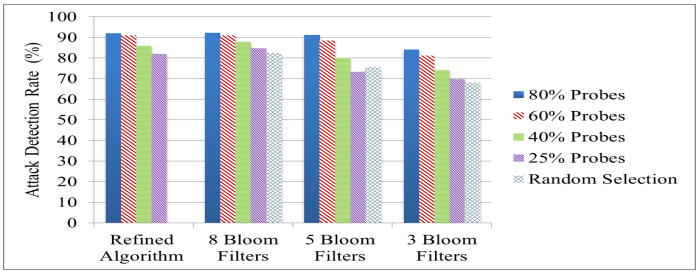


Fig. 2: Attack traffic detection rate

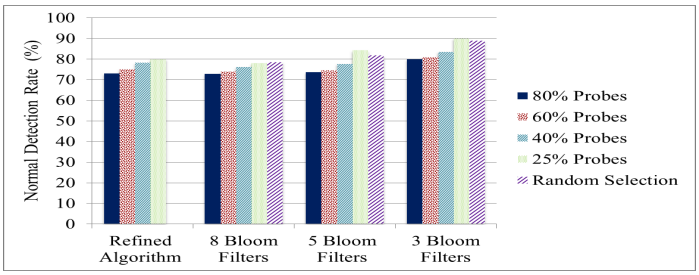


Fig. 3: Normal detection rate

80% probes and it increases to around 80% if fewer filters are used to stop attack traffic. Thus, there is a trade off between accuracy of the attack traffic detection rate and the normal detection rate.

3.3 EFFICIENCY of DISTRIBUTED APPROACH

Figure 4 depicts the fraction of attack traffic dropped at different hop distances from the victim, and thus the source. It shows that 60% of the attacks in total are detected and blocked in the first two routers from attacker, with 23% in the first and 37% in the second. Thus, it shows that RPI-HTA algorithm can effectively select routers further from the victim node and close to attacker. Furthermore, it shows that having more probes is more effective and we can select farther routers as well. For instance, with 80% probes all the filtering points are selected at least 3 hop distances away from victim node, while with 25% probes the filtering points must be within 1 and 2 hop distances from victim node. In this experiment, the $25th$, $50th$ (median), $75th$ percentiles, minimum and maximum value of attack traffic detection rate for all 3 scenarios are computed as well. As shown in Figure 5(a), the first layer of router from attacker (fifth hop distance from victim) has relatively good attack traffic detection rate close to 20% for 50% of simulations in the RPI-HTA algorithm, whereas, this detection rate reduces to less than 10% for random selection scenario. This proves that RPI-HTA algorithm can accurately select desirable filtering points during the attack period. Thus, it can

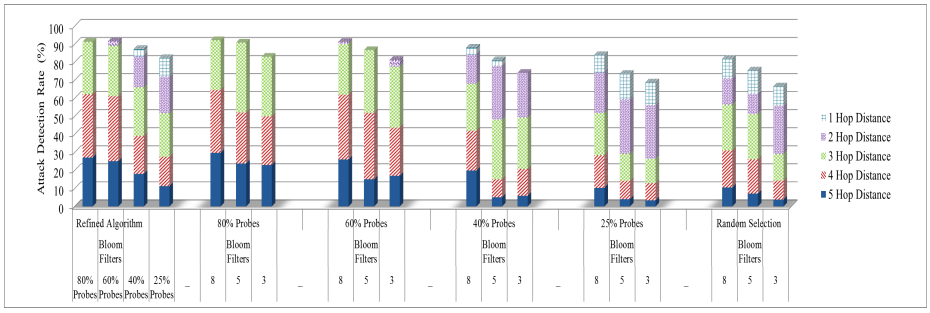
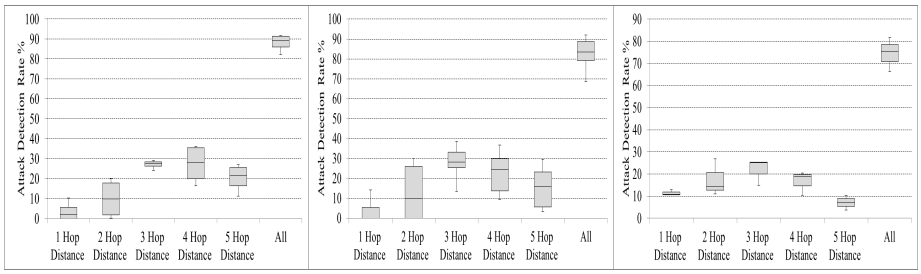


Fig. 4: Attack detection rate and location of selected routes

be observed that the core of detection and prevention mechanism is located at the router with hop distance 4, 3, and 5 from victim node in that order.



(a) RPI-HTA (b) RPI-HA (c) Random selection

Fig. 5: Result of attack detection rate

3.4 END USER'S UTILIZATION

The other part of our evaluation is specifying utilization of the victim node and other end-users before and after applying filtering mechanism. In Fig. 6(a), the last link utilization of victim node without applying filtering approach shows that it is fully utilized during the attack time. However, the link utilization reduces to around 60% after deploying Bloom filter through the network based on RPI-HTA algorithm.The result shows that 80% probes through the network give 50% link utilization rate for the victim node - this is the least link utilization rate that we get in our experiments. Figure 6(b) shows the last link's utilization for other end-users increases with applying the filtering routers. It means the other end-users can receive normal traffic during the attack time. This is good as it provides service availability in the presence of DDoS attacks and minimizes the attack impact during an attack time.

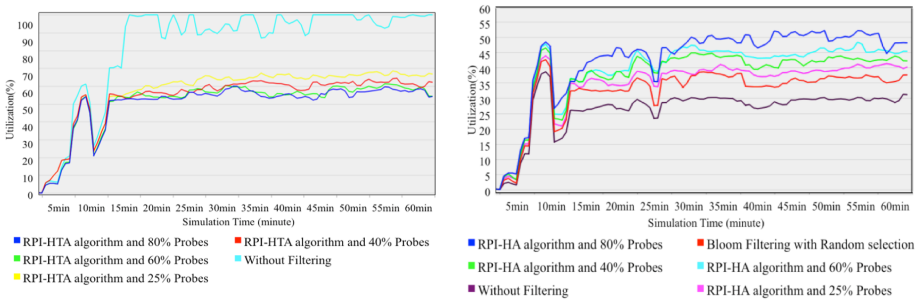


Fig. 6: Victim node's utilization. (b) Average of last link utilization of end-users

3.5 VALIDATION with REAL NETWORK DATASET

In this experiment, the effectiveness of responsive defense approach is tested using real network trace from University of Auckland in New Zealand. The packet trace contains 6.5 weeks IP header trace taken with 155 Mbps Internet links [13]. We use The CAIDA attack dataset 2007 [12] in the experiments as attack traffic. The dataset is run with same topology that was used in previous part by distributing the dataset traffic over the network. History-based profile of normal traffic going to the victim node is created using the trace collected from the University of Auckland. The corresponding Bloom filter will be created based on the scheme [8] in the second step and then rpresented approach is applied during the attack time. Figure 7 shows the attack traffic detection rate against the CAIDA attack traffic. Attack traffic detection rate is around 95% with 80% probes in the RPI-HTA algorithm where it was around 91% for DARPA dataset. Overall the attack traffic detection rate increases slightly compared with DARPA dataset, where the Bloom filter accuracy played a role in this situation. In Fig.8,

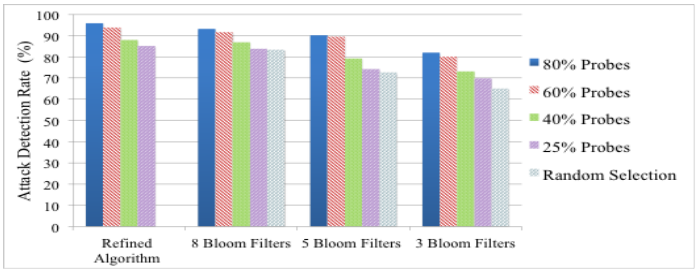


Fig. 7: Attack traffic detection rate

the $25th$, $50th$ (median), $75th$ percentiles, minimum and maximum value of attack traffic detection rate of RPI-HTA algorithm is shown for CAIDA dataset

traffic; this can be compared with Fig. 5(a) for DARPA dataset as well. As shown for 75% of simulations, the most portion of attack is detected and blocked at the first layer of routers from the attacker (hop distance 5 from victim node) followed by the one in the second layer of routers from attacker. The router with fifth hop

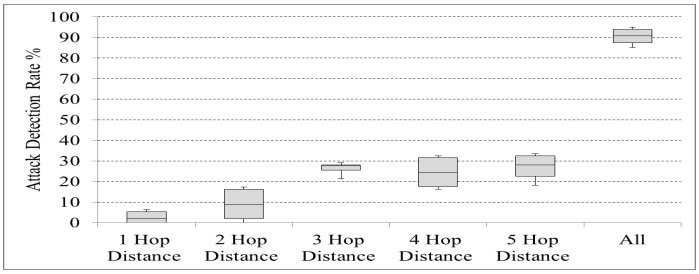


Fig. 8: Attack traffic detection rate of RPI-HTA for CAIDA attack traffic

distance from victim has a better attack traffic detection rate close to 25% for 50% of simulations in the RPI-HTA algorithm, whereas this detection rate was 20% for DARPA dataset. Moreover, it shows that router with hop distance 5, 4 and 3 in that order were the core of attack detection. This proves that RPI-HTA algorithm accurately selected desirable filtering points during the attack period for CAIDA attack traffic as well.

4 CONCLUSION

A responsive defense approach to defend against DDoS attacks was presented. A key contribution is the distributed mechanism that identifies in real-time the best response points where filters are to be activated so as to minimize attack traffic and maximize legitimate traffic during the attack. The technique has been validated with two real-world data sets. Results for CAIDA attack set, e.g., indicate that the responsive mechanism protects the victim nodes from 95% of attack traffic close to the source of attack, while allowing 77% of legitimate traffic. The method is light in terms of computational and communication overheads. Results also demonstrate the effectiveness of the mechanism in preserving valuable network resources and link utilizations for other end-users during the attack time, thus preserving the service availability and minimizing the attack impact. Our future work includes validating the scheme with very recent real-world network dataset. A part of our future work also includes extending our identification scheme for IPv6 addresses.

ACKNOWLEDGMENT

The authors gratefully thank Forcepoint LLC for their funding support.

References

1. Aghaei Foroushani, Z. H.: TDFA: traceback-based defense against DDoS flooding attacks, In Proc of 28th International Conference on Advanced Information Networking and Applications(AINA) IEEE 2014, Victoria, BC, pp. 710-715 (2014)
2. Cabrera, J. B. D., Lewis, L., Qin, X. Z., et al.: Proactive intrusion detection and distributed denial of service attacks-A case study in security management, Journal of Network and Systems Management, 10(2), pp. 225-254 (2002)
3. Chen, C., Park, J.-M.: Attack Diagnosis: Throttling distributed denial-of-service attacks close to the attack sources, Proc. of IEEE Int'l Conf. on Computer Communications and Networks, pp. 275-280 (2005)
4. J Francois, J., Aib, et al.: a collaborative protection network for the detection of flooding DDoS attacks, IEEE/ACM Trans. Net., 20(6), pp. 1828-1841 (2012)
5. Gil, T. M., Poletto, T.: MULTOPS: A data-structure for bandwidth attack detection, In Proc. of 10th conference on USENIX Security Symposium, Washington, D.C, USA (2001)
6. John, A., Sivakumar, T.: DDoS: Survey of traceback methods, International Journal of Recent Trends in Engineering ACEEE (Association of Computer Electronics and Electrical Engineers), 1(2), (2009)
7. Mahajan, R., Bellovin, S. M., et al.: Controlling high bandwidth aggregates in the network, ACM SIGCOMM Computer Comm. Review, 32(3), pp. 62-73 (2002)
8. Mosharraf, N., Jayasumana, A., Ray, I.: A Responsive defense mechanism against DDoS attacks, In Proc.7th of International Symposium on Foundations and Practice of Security (FPS 2014), Montreal, Canada (2014)
9. Peng, T., Leckie, CH., Ramamohanarao, K.: Proactively detecting distributed denial of service attacks using source IP address monitoring, Proc. of 3th International IFIP-TC6 Networking Conference. Athens, Greece, pp. 771-782 (2004)
10. Peng, T., Leckie, C., Ramamohanarao, K.: Survey of network-based defense mechanisms countering the DoS and DDoS problems, ACM Computing Surveys, 39(1), pp. 1-42 (2007)
11. RioRey, Inc. 2009-2012, RioRey taxonomy of DDoS attacks, RioReyTaxonomyRev2.32012,2012.,[Online].Available:[online]http://www.riorey.com/xresources /2012/RioRe.
12. The CAIDA DDoS Attack 2007 Dataset. Available: http:// www. Caida .org/data/passive/ddos-20070804dataset.xml.
13. W.A.N.D.R.Group,http://wand.cs.waikato.ac.nz/wand/wits/auck
14. Yaar, Y., Perrig, A., Song, D.: Pi: A Path identification mechanism to defend against DDoS attacks, Proc. of the 2003 IEEE Sym. on Security and Privacy, Pittsburgh, PA (2003)
15. Zargar, S., Joshi, J., Tipper, D.: A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks, IEEE Communications Surveys and Tutorials 2013, 15(4), pp. 2046-2069 (2013)
16. http://www.jdsu.com/en-us/Test-and-Measurement/Products/a-z-product list/ Pages/ packetportal.aspx
17. http://www.ll.mit.edu/mission/communications/cyber/CSTcorpora/ideval/data 1998data.html
18. https://snap.stanford.edu/data/oregon1.htmlhttp://www.darkreading.com/attacks-and-breaches/ddos-attack-hits-400-gbit-s-breaks-record/d/d-id/1113787