Distributed and Predictive-Preventive Defense Against DDoS Attacks

Manjiri Jog
NBN Sinhgad School of Engineering
Pune, India
contactmanjiri@gmail.com

Maitreya Natu
Tata Research Development and Design Centre
Pune, India
maitreya.natu@tcs.com

Sushama Shelke
NBN Sinhgad School of Engineering
Pune, India
sushama.shelke@sinhgad.edu

ABSTRACT

Distributed Denial of Service (DDoS) attacks are a perpetual threat to today's business. Existing strategies against DDoS are implemented as single-point solutions, or reactive solutions, or focus on differentiating traffic and localizing attackers. Our understanding is that no single network location can cater to the needs of a full-proof defense solution. In this paper we propose a solution based on two principles – 'distributed defense for distributed attack' and 'need for a preventive solution over a reactive solution'. We present a system architecture for distributed and predictive-preventive defense mechanism. We also propose two algorithms for systematic placement of the defense nodes in the victim's upstream router network. We compare the performance and efficiency of the proposed algorithms through simulation results. We also present an algorithmic approach for prediction of attack to determine the potential attackers as well as the time-to-saturation of victim. We present experimental evaluation to show the effectiveness of the proposed approach.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: General—*Security and Protection*

General Terms

Management, Measurement, Security

Keywords

Distributed denial of service defense, Traffic policing and forecasting, Predictive defense

1. INTRODUCTION

DDoS attacks are a perpetual threat to today's business and cause severe business loss, customer unrest, and financial penalties. Despite numerous research and commercial endeavours to design DDoS defense, DDoS attacks are becoming an increasing threat. The increasing scale, complexity, and mutation in attack patterns is further adding to the complexity of the problem. Research has yielded several approaches to combat DDoS attacks at various network locations. Client based approaches reduce the traffic policing burden on intermediate routers. But, they fail to protect against intermediate intruders [2], [3]. Whereas, motivations for implementation near victim-end include accuracy of information and economy of implementation [1], [7], [4]. Most of these are reactive solutions and are implemented as single-point solutions. Past research in DDoS defense has led to the following insights:

Insight 1 A defense needs to be deployed near victim. Victim is in the best position to determine if client's traffic is malicious. Furthermore, victim has the best economic incentive to deploy defense.

Insight 2 A distributed attack demands a distributed defense. A carefully chosen set of defense nodes in the victim network, including a subset of upstream routers, can make the defense effective, and robust to single-point of failure.

Insight 3 There have been several reactive solutions. There is a need for a predictive-preventive solution. The victim should get timely warning of a potential attack. Victim can use this warning to take preventive actions. We use these insights to develop a distributed and preventive DDoS defense. In this paper, we contribute by presenting: (a) Algorithms for systematically placing defense nodes such that defense nodes are not overwhelmed by the attack. (b) Algorithms that mine attack patterns to predict any potential attack; and forecast attack from individual IP addresses to localize the potential attackers. (c) A detailed experimental evaluation of the proposed algorithms.

ICDCN '15, January 04 - 07 2015, Goa, India

http://dx.doi.org/10.1145/2684464.2684503.

2. DESIGN RATIONALE

The proposed solution is based on two principle needs: (a) a distributed defense for distributed attacks, (b) early warnings to the victim by predicting potential attack.

2.1 Defense node selector

We propose to deploy defense at multiple nodes, as single-point defense solutions carry the risk of getting overwhelmed by the attack. The nodes are chosen in the k-hop radius of the victim network. The nodes are selected such that defense nodes are placed on all paths to the victim node. We assume that the knowledge of the network topology and the routing information is available. We assume a *consistent IP routing model*[5]. It is important to optimize the placement of de-

fense nodes, as it affects cost and feasibility. The selector uses network topology and routing information to select the right locations to place defense nodes. Theses defense nodes perform traffic differentiation, rate-limiting, and detect any potential attackers.

2.2 Attack predictor

We propose to equip the defense nodes with the proactive ability to predict any potential attacks and attackers. The defense nodes maintain the historical data of incoming traffic. We propose an algorithm that mines the historical traffic data to predict the expected behavior. It computes the expected time for saturation of the bottleneck resource. In the event of any potential threat, the predictor further mines the traffic of individual IP addresses to localize the potential attackers.

The predictor thus gives an early warning to all defense nodes. It estimates the intensity of attack, the expected time for saturation, and the potential attackers. The defense nodes use this information to take preventive measures through traffic differentiation and rate-limiting.

2.3 Proposed defense mechanism

We propose the following defense mechanism using the levers of defense node selector and attack predictor.
(i) The defense nodes are selected offline in the k-hop radius of the victim node. (ii) Each defense node is equipped with the capability to perform traffic differentiation and rate-limiting. (iii) Each defense node is also equipped with the attack predictor mechanism. The defense node on predicting an impending attack sends a warning message to all other defense nodes. The warning message contains the time to attack, intensity of attack, and the potential attacker nodes. (iv) We assume a separate control-channel of communication between defense nodes.

3. DEFENSE NODE PLACEMENT

In this section, we present algorithms to systematically select the defense nodes.

Consider a network of a set of nodes N and a victim node $v \in N$. We propose to place defense nodes in the k-hop radius of the node v. The defense nodes are to be placed such that maximum number of k-hop paths to the victim node are covered. A defense node d covers a path p if it is present in the path p, i.e. $d \in Nodes(p)$, where $Nodes(p)$ refers to nodes on the path p.

We define coverage of defense nodes $M \subseteq N$ as the percentage of k-hop paths to v that are covered by at least one node in M. Thus, if the set P_k refers to all k-hop paths to v, and the set P_k^M refers to the paths covered by M, then coverage of M, C^M is calculated as follows:

$$C^M = P_k^M / P_k \times 100 \quad (1)$$

Strategic defense node placement can minimize the number of defense nodes, maximize the coverage, and thus reduce deployment cost. This problem is formally defined as follows:

> Given a network of nodes N, a victim node $v \in N$, and set P_k of k-hop paths to node v, select the set of d nodes where defense nodes should be placed such that maximum paths in the set P_k are covered.

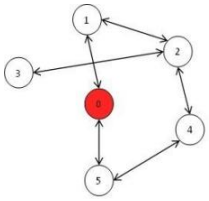
We first construct a set of potential defense nodes N_D. This set is a union of all nodes on all the k-hop paths to v, and is computed as follows.

$$N_D = \cup_{p \in P_k} Nodes(p) \quad (2)$$

Below we present various algorithms to compute the set of d defense nodes from the set N_D.

3.1 Optimal Approach

The optimal placement of defense nodes can be computed using a combinatorial approach.



Number of nodes, N	6
Number of paths to victim P_k = N-1	5
Defense node percentage	40%
Number of defense locations to be selected N_D	2
Paths to victim: 1-0	
2-1-0	
3-2-1-0	
4-5-0	
5-0	

Figure 1: Sample topology

This approach involves a systematic search of all possible combinations of d nodes in the set of potential defense nodes N_D. For each combination $M \subseteq N_D$ of d nodes, it computes the coverage C_M. The algorithm selects the combination that gives largest coverage. The optimal combination is chosen as defense node set for a sample topology in Figure 1. Assuming that 2 defense nodes are to be placed, in step 1 all the combinations of size 2 are calculated. In step 2, coverage of each set is calculated. As the set (1,5) gives maximum coverage, this set is selected as the defense node set. The coverage C_M is calculated using Equation 1.

This algorithm will provide the optimal solution. But, it is a compute-intensive algorithm and is not suitable for larger networks. We next propose heuristics to derive the set of defense nodes. We use the Optimal approach as a benchmark to compare the effectiveness of the proposed heuristics.

3.2 Maximum-Coverage-Node-First (MCNF) Approach

MCNF is a greedy approach that iteratively selects the node that maximizes the coverage. For each potential defense node $n \in N_D$, the algorithm computes the potential increase in coverage (c^+) by selecting the node n as the defense node. c^+ is computed as percentage of previously uncovered paths in P_k that will get covered by selecting the node n. The node that provides maximum coverage is selected. The algorithm iterates these steps until d nodes are selected.

Figure 2 shows the MCNF iterations on the sample topology in Figure 1. MCNF and Optimal approaches give the same result in this case, whereas, MCNF is computationally lighter and faster than the Optimal approach. We have skipped its illustration because of space constraints. We later show through experimental evaluation that MCNF provides near-optimal results, and scales better for larger networks.

3.3 Weak-Path-First (WPF) Approach

While the MCNF approach focuses on the nodes with maximum coverage, often the selections are governed by the paths that are weakly inter-connected with other paths. The

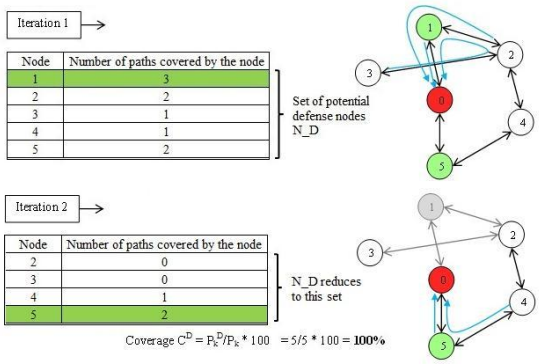


Figure 2: Defense nodes Selection by MCNF

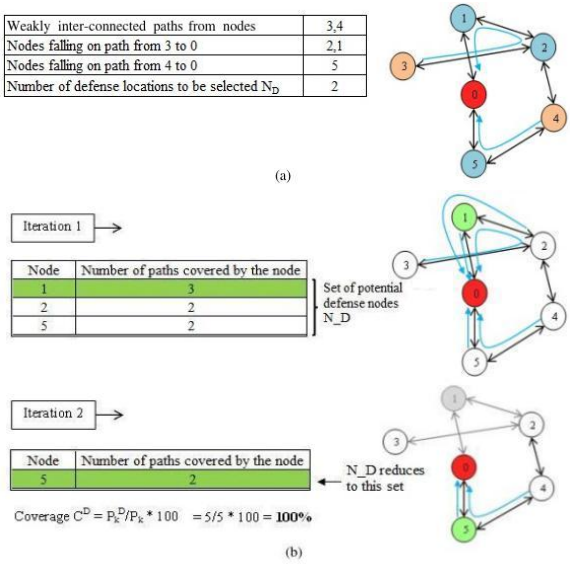


Figure 3: WPF search (a) Precomputation of the least intersecting paths, (b) Selection of defense nodes

crux of this approach is to iteratively select the path that least intersects with other paths. Of all the possible nodes that can cover this path, select the node that maximizes the increase in coverage. Iterate this process until the permissible number of defense nodes d are selected.

As shown in Figure 3(a), the precomputation involves finding the least interconnecting paths to victim. Next, N_D is found which includes the nodes which cover these paths. Figures 2 and 3 show that results for MCNF and WPF are same in this example.

4. PROACTIVE ATTACK DETECTION

We propose to mine trends and patterns in the historical data and predict potential traffic behavior in future. Below we present the application of the state-of-the-art forecasting techniques for attack prediction.

4.1 Predicting potential attack

Each defense node maintains the history of both cumulative traffic as well as traffic from individual IP addresses.

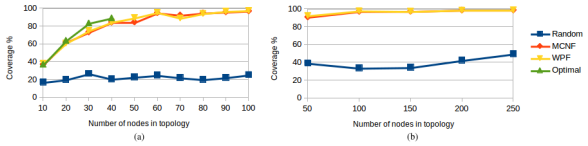


Figure 4: Coverage results for Defense node percentage = 10%, degree=3

Thus, a set of time-series is maintained and incrementally updated with incoming traffic. These time-series are then analyzed to forecast future traffic. Various time-series forecasting solutions have been proposed in the past. We propose to use regression models and autoregressive integrated moving average (ARIMA) models for forecasting the time-series data. In cases, where a single model cannot best capture the traffic variation, we can use multiple models for different levels of traffic or different intervals of time. We use the derived trend and periodic patterns from regression function to forecast future behavior.It should be noted that, for accurate model-fit, we perform data-preparation steps such as outlier detection and aggregation.

4.2 Computing time for saturation

The victim node uses the traffic-time models to estimate the time for saturation of it's resources. Consider that the bottleneck resource is the network bandwidth of the link l between the proxy server and the victim. Victim predicts the time for saturation of this bandwidth as follows:
Construct a model m to capture the relationship between total traffic observed at victim node v and the traffic observed at network link l. Forecast the traffic expected at the link l. Use model m to forecast the expected values of the traffic on victim v. If the forecast values for traffic at link l cross a high-risk threshold, then report the time as the expected time for saturation. The threshold can be customized as per the system needs. Victim identifies the severity of the attack as low, medium, high based on the time-to-saturation and the expected intensity of the attack.

4.3 Localizing potential attackers

Forecasting solutions can also be used to localize potential attackers. We propose to monitor traffic of individual IP addresses and apply the above forecasting approach to predict the future incoming traffic from each IP address. Clients expected to show a significant increase in the traffic can be reported as potential threats.

Instead of identifying each client with an IP address, we can use the concept of capabilities [4] and path identifiers [6] to uniquely identify each traffic generator. Furthermore, instead of maintaining time-series of each client, we can narrow down clients based on the their past history, overall traffic received so far, and their capability scores. Traffic of these clients can be closely monitored and forecasted.

Thus, attack prediction module can be implemented at any of these locations - (i) only victim end (ii) only upstream defense nodes (iii) both victim and upstream defense nodes by splitting the functionalities. This can be achieved by performing cumulative traffic analysis at victim end and individual client traffic analysis at defense nodes.

5. EXPERIMENTAL EVALUATION

In this section, we present the experimental evaluation of the proposed algorithms.

5.1 Evaluation of Defense Node Placement

We simulated various network topologies with different network sizes (N) and average node degrees (AD). We randomly selected a victim node from the network and built a model to represent the paths to victim from all non-victim nodes. For each experiment we selected a pre-defined number of defense nodes We then executed the defense node selection algorithms on the network. Each point plotted on the graphs is an average of 10 experiment runs on different network topologies. We evaluated the performance of the algorithms for coverage and execution time. We compared these algorithms with the Optimal and Random approaches.

The comparison of WPF and MCNF is shown in Figures 4 and 5. Optimal approach, being compute intensive, could not run for network sizes greater than 100 nodes. Hence the experiments were conducted on network size with N = 10 to 100 nodes and AD varying from 3 to 5. Both MCNF

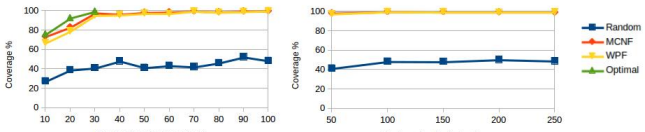


Figure 5: Coverage results for Defense node percentage = 20%, degree = 5

Search and WPF Search provide near optimal coverage. Full coverage is achieved with the defense node percentage as low as 20% for larger networks of sizes 50 to 250 nodes. The proposed algorithms significantly outperform Random search algorithm from the coverage aspect.

We can show that the execution time of these two approaches is significantly less than that of Optimal search approach and is comparable to that of the Random search approach, but have skipped it because of space constraints.

5.2 Evaluation of predictive attack detection

In this section, we present experimental evaluation via simulation of the algorithm proposed in Section 4.

We created a 20 node topology and selected a victim node v. From each node, we generated traffic for victim node with random traffic rates. We randomly selected n_A number of attackers. For each attacker, we gradually increased its attack traffic by a factor δ.

Each point plotted on the graphs is an average of 10 experiment runs where each experiment was run on a different network topology of size 20 nodes. We evaluated the attack detection rate for various attack detection rates and number of attackers.

We executed the prediction algorithm for network size of 20 nodes with the number of attacker nodes varying from 1 to 5 and the attack traffic increase rate varying from 1.2 to 2.2. Performance of the algorithm is shown in Figure 6. With a single attacker the attack traffic is quite insignificant and hence it is difficult to predict any future threat. However, with increase in number of attackers the attack becomes more aggressive and hence the detection rate improves. The small attack traffic increase rates do not lead

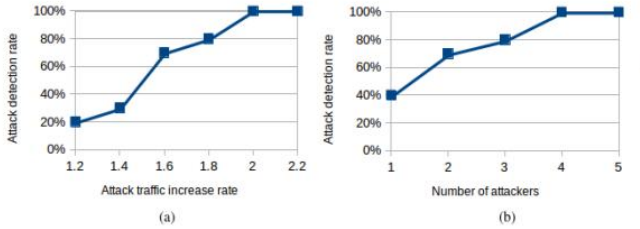


Figure 6: Sensitivity Analysis of prediction

to significant attack volumes at the victim and hence are difficult to detect. However, with increase in attack traffic, the algorithm is able to predict an impending attack with better accuracy.

6. CONCLUSION AND FUTURE WORK

In this paper, we proposed distributed and preventive approach to protect the victim from any potential DDoS attacks. For distribution of defense, we presented two algorithms for strategic placement of defense nodes in the victim's upstream router network. We compared the coverage of the proposed approaches with that of the Optimal search and showed that the results are near optimal and computationally efficient. We proposed a prediction algorithm that warns the victim to take preventive actions.

As part of our future work, we aim to relax our assumptions of consistent IP routing model and support more complex routing scenarios. We also intend to make the defense mechanism robust to failure of defense nodes. We also aim to consider adaptive selection of defense nodes based on the network traffic conditions, and conduct comprehensive experimental evaluation for various advanced attacks.

7. REFERENCES

[1] A. Garg and A. Reddy. Mitigation of DoS attacks through QoS regulation. *Microprocessors and Microsystems*, 28(10):521–530, 2004.

[2] T. M. Gil and M. Poletto. MULTOPS: a data-structure for bandwidth attack detection. In *USENIX Security Symposium*, pages 23–38, 2001.

[3] J. Mirkovic, G. Prier, and P. Reiher. Attacking DDoS at the source. In *Proceedings of the 10th IEEE International Conference on Network Protocols*, pages 312–321. IEEE, 2002.

[4] M. Natu and J. Mirkovic. Fine-grained capabilities for flooding DDoS defense using client reputations. In *Proceedings of the 2007 workshop on Large scale attack defense*, pages 105–112. ACM, 2007.

[5] M. Natu and A. S. Sethi. Application of adaptive probing for fault diagnosis in computer networks. In *Network Operations and Management Symposium, 2008. NOMS 2008. IEEE*, pages 1055–1060. IEEE, 2008.

[6] A. Yaar, A. Perrig, and D. Song. StackPi: New packet marking and filtering mechanisms for DDoS and IP spoofing defense. *IEEE Journal on Selected Areas in Communications*, 24(10):1853–1863, 2006.

[7] X. Yang, D. Wetherall, and T. Anderson. A DoS-limiting network architecture. *ACM SIGCOMM Computer Communication Review*, 35(4):241–252, 2005.