Distributed Capabilities-based DDoS Defense

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

Maitreya Natu
Tata Research Development and
Design Centre,
Pune, India[$]
Email:maitreya.natu@tcs.com

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

***Abstract*— Existing strategies against DDoS are implemented as single-point solutions at different network locations. Our understanding is that, no single network location can cater to the needs of a full-proof defense solution, given the nature of DDoS and activities for its mitigation. This paper gives collective information about some important defense mechanisms discussing their advantages and limitations. Based on our understanding, we propose distribution of DDoS defense which uses improved techniques for capabilities-based traffic differentiation and scheduling-based rate-limiting. Additionally, we propose a novel approach for prediction of attack to determine the prospective attackers as well as the time-to-saturation of victim. We present two algorithms for this distribution of defense. The proposed distributed approach built with these incremental improvements in the defense activities is expected to provide better solution against the DDoS problem.**

Keywords— Attack detection; Distributed defense; Distributed Denial-of-Service; Network security; Rate-limiting; Traffic differentiation

I. INTRODUCTION

We can divide the activities involved in DDoS defense mechanisms as: (1) Traffic differentiation, (2) Attack detection and (3) Rate-limiting. Over the years, different methods have been devised based on these activities to work at various network locations for combating DDoS attacks. Some defense systems implement client based approaches as in [1], [2] to prevent malicious or spoofed traffic from entering the internet. Client based approaches reduce the traffic policing burden on intermediate routers. But, these approaches fail to protect against intermediate intruders. Some other defense systems implement approaches at the victim-end as in [3], [4], [5], [8], [9]. Motivations for implementation near victim-end include accuracy of information and economy of implementation. However, defenses at victim-end may be crashed by simply flooding its link beyond its capacity. This mandates involvement of upstream routers in filtering this attack traffic as done in [6], and [7]. But, filtering traffic at upstream routers may affect their performance. The limitations of these approaches suggest that a DDoS attack and its effects are difficult to deal with any solution implemented at a single network location. We claim that a solution with functionalities split and implemented at different locations would perform better than a mechanism concentrated at a single network location. In this paper, we propose a distributed defense solution.

Recent advancements in the capabilities-based DDoS defense implemented at victim-end show great potential to protect against sophisticated attacks [8], [9] and [3]. Traffic differentiation based on capabilities followed by an efficient rate-limiting technique also takes care of false positives (chances of misclassification of legitimate traffic as attack traffic). These systems use advanced form of packet marking called capabilities (also termed as ticket) to distinguish between the legitimate traffic and attack traffic. They are stamped in the IP identification field of a packet. [9] describes some properties of capabilities as followed. For capabilities to be reliable, robust and efficient, they are granted by the destination to the sender. Their verification is transparent to hosts. They are valid for a limited time and they do not impose large overhead. Capabilities establish authorized paths between the communicating hosts and prohibit unauthorized flows. These strengths make the capabilities-based mechanism suitable for practical use. Looking at the potential and the scope for improvement with current capabilities-based approaches, we plan to extend the basic concept for traffic differentiation in our defense solution.

Furthermore, many of the existing systems are reactive in nature. There is a need for a preventive solution, so that the victim would get timely warning of a prospective attack. This warning can be used to take required actions. Various time-series forecasting solutions have been used in the past. Among these solutions, regression analysis, exponential smoothing and ARIMA (Auto Regressive Integrated Moving Average) models capture different behaviors in data. We plan to use these models for attack prediction in our preventive defense.

The rest of the paper is organized as follows: Section II presents the related work. Section III presents the proposed mechanism for defense distribution with improved techniques for traffic differentiation, attack detection and rate-limiting. Initial ideas on improvements in these techniques and challenges in: (i) current methods of capabilities calculation for traffic differentiation, (ii) applying various regression models on network traffic data to predictively detect the attacks (iii) applying scheduling concepts to develop a rate-limiting technique are discussed in Sections IV, V and VI respectively. Section VII concludes the paper.

[$]Partial Sponsor

978-1-4799-6272-3/15/$31.00(c)2015 IEEE

II. RELATED WORK

A. Client-based Solutions

Authors of D-WARD [1] system mention that, "It is a self-regulating reverse feedback system. It monitors two-way traffic between pre-allocated address set and the rest of the internet. It compares online traffic statistics periodically with predefined normal-traffic models. It uses this ratio to rate-limit non-complying traffic and dynamically adjusts the rate-limits. It polices data-flows originating only from its own network and guarantees good service to legitimate traffic even during attack". MULTOPS [2] maintains a multilevel tree for collecting statistics derived from the disproportional packet rates between hosts and subnets. The tree expands or contracts within memory bounds and monitors the traffic characteristics. The system examines the ratio between outbound and inbound packets. Under normal circumstances, packet rates are proportional. If the rate deviates from the specified threshold for a particular host, it implies as either the host is an attacker or it is under attack. Packets exchanged with such a host are dropped. However, it has two major limitations: (a) significant memory requirement (b) treatment of non-TCP packets either as attack-flows or special traffic.

B. Intermediate router-based Solutions

Mahajan et al. [10] proposed a dual approach to effectively deal with the flash crowds. They use a local mechanism to detect and control an aggregate at a single router; whereas a cooperative pushback mechanism is used for aggregate-based congestion control (a router can ask adjacent routers to control an aggregate upstream). The identification is based on the destination IP address-prefixes. The traffic flows are examined based on their destination IP addresses and dropping rates for excessive traffic. The rate-limiting technique is based on the random-early-dropping (RED) rate. By examining the drop history, it determines how much rate-limit should be applied to which aggregate traffic. Path Identification (Pi) is a scheme that involves special type of packet marking and packet filtering. All packets following the same path are given same Pi-marks by the intermediate routers. However, this does not take into account the presence of legacy routers and assumes entire network to contain Pi-enabled routers. The Pi-filter detects attack with a single packet that behaves abnormally. It then drops all subsequent packets with the same Pi-mark. This imposes collateral damage to the legitimate packets that may follow the abnormally behaved packet. StackPi [7] adds ability for incremental deployment in the original Pi scheme with the use of two marking schemes – Stack-based and Write-ahead marking. With Stack-based marking, it treats the IP-identification field of the received packets as a stack, and performs push and pop operations on it. The IP-ID filed is divided into $\lfloor(16/n)\rfloor$ marking spaces for the intermediate routers to add their marks. StackPi-enabled routers add the Pi-marks for previous as well as next hops, if not already present in the marking of the received packets. This strategy takes care of legacy routers that might fall between the StackPi-enabled routers. The Pi-IP filter examines the packets for tuple <Pi,IP> that originate from the same source and are intended for the same destination and stores it for short intervals during normal operation. During attack, this tuple deviates and the mismatch with the stored tuple detects the attack. The detected packets are simply rejected.

C. Victim-based Solutions

Garg and Reddy [4] take a resource-regulation based approach to keep the server resource usage at an accepted level at network layer of QoS regulator. They implement rate-control for bandwidth, and window-control for fixed resources that depend on capacities. Violation of resource-specific limits causes QoS regulator to take action to free up resources, or take administrative actions or changes policies for resource consumption using state information. Use of separate window for each resource avoids their over-usage, thus prohibiting successful DoS attacks.

IP Easy-Pass [5] attempts to prevent denial of quality-of-service i.e. DQoS attacks in data plane. In this technique a source identifier is appended to each packet and it is used to reliably recognize clients. The pass is a random number that is encrypted to protect from the adversaries. The presence of the valid pass ensures legitimacy of the packets. The authors assume some existing resource reservation protocol (e.g., RSVP) for access control. SIFF [8] uses lightweight time-based capabilities-granting; whereas, TVA [9] applies costlier traffic-based capabilities. The capabilities are stamped in the IP header by end-hosts and all the routers in the path. They are short-lived and change over time. Both SIFF and TVA generate binary capabilities and communicate with upstream routers constantly for their calculation. None of them bind capabilities to packets. Also, the capabilities are not encrypted. This leaves a loophole for legitimate packets being stolen and spoofed. To overcome these limitations, Natu and Mirkovic [3] use clients' reputation as the basis to generate fine-grained capabilities in their DDoS defense mechanism. The mechanism eliminates router dependence in the process of ticket-granting. The whole process is about making the victim self-sufficient to determine the client behavior during ticket-granting. This is achieved by taking into account the client reputation and generating fine-grained capabilities composed of credits and penalties and binding them to the packets. Instead of categorizing a client in binary classes of good and bad, the capabilities rate client's behavior ranging between these classes. The fine-grained capabilities are then used to employ rate-limiting in terms of resource share allocated to each class of clients. It also aims at reducing the overall operational cost.

III. PROPOSED DEFENSE MECHANISM

Taking into account the need for distributed and preventive defense mechanism, and the initial ideas suggested in Sections IV and VI, we propose to distribute the defense activities in the victim network and include a set of carefully chosen upstream routers. These defense nodes would be equipped with the capability to perform traffic differentiation and rate-limiting. The capabilities-based mechanisms proposed in Section IV would be used to differentiate traffic and the rate-limiting scheme proposed in Section VI for rate-limiting traffic. Each defense node needs also to be equipped with the attack predictor mechanism proposed in Section V. The

defense node on predicting an impending attack would send a warning message to all other defense nodes.

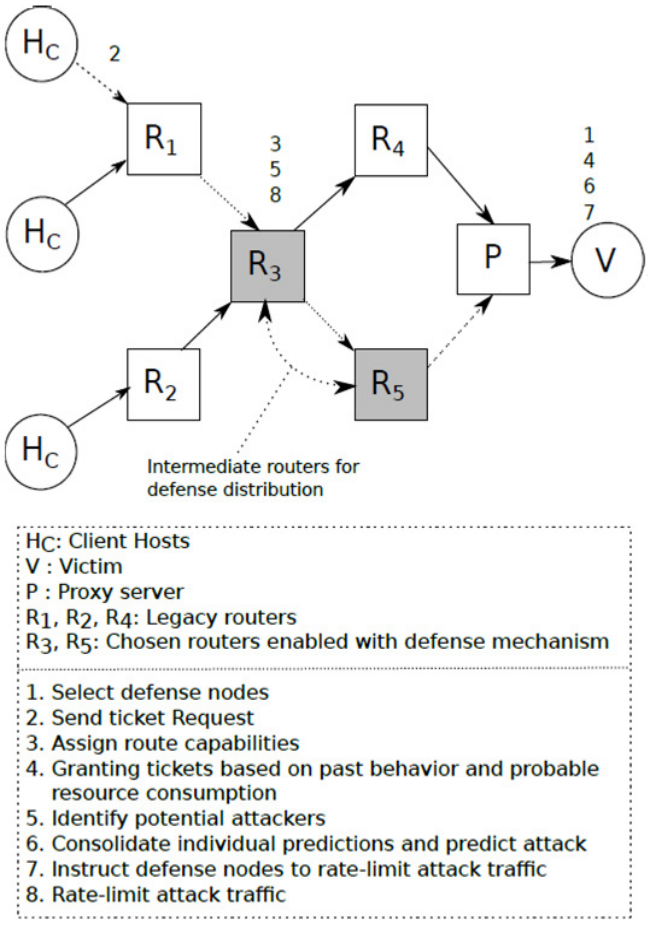

Fig. 1 Proposed defense mechanism

The distributed defense mechanism which can predictively detect the attack is illustrated in Figure 1 with activities at the corresponding network locations. The capabilities assignment would take place as described in Section IV; whereas the rate-limiting would take place as described in Section VI. For selecting a subset of upstream routers as the defense nodes, we propose two algorithms: *Weak-Path-First* Search and *Max-Coverage-Node-First* Search.

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 refers to the paths covered by M, then coverage of M, C_M is calculated as follows:

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

Placement of defense nodes is associated with deployment cost; hence it is important to maximize the coverage by strategic placement of the defense nodes. The problem of defense node placement is defined as follows:

> "Given a network of N nodes, 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 nodes where defense can be placed. This set is a union of all nodes on all the k-hop paths to v. The set of potential defense nodes ND is computed as follows:

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

Weak-Path-First Search

The key rationale behind Weak-Path-First (WPF) 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. The pseudo-code is described in the Algorithm 1.

Algorithm 1: WPF algorithm for defense node selection

Input: Victim node v, Path matrix P, required number of defense node d
Output: Set of d defense nodes

Compute a set P_k of all k-hop paths to node v;
Compute the set of N_D of all nodes on paths in P_k: $\cup_{p \in Pk}$ Nodes(p);
foreach path p $\in$ P_k **do**
    Compute the number of paths that intersect with p as follows:
    Identify the set of paths Q, where $\forall q \in Q$ Nodes(Q) $\cap$ Nodes(p) > 0;
    Intersection(p) = |Q|;
end
uncovered_paths = P_k;
foreach path $p \in P_k$ in increasing order of *Intersection(p)* **do**
    foreach node $n \in Nodes(p)$ **do**
        Compute coverage of the node n, C_n as follows:
        C_n = *paths_covered(n)* $\cap$ *uncovered_paths;*
    end
end
Select the node n that provides maximum coverage $Coverage_n$;
Remove *paths_covered(n)* from the set *uncovered_paths*;
Remove the selected node n from the set N_D;
Repeat steps 9 to 17 until d nodes are not selected or *uncovered_paths* is *NULL*;

Max-Coverage-Node-First Search

Max-Coverage-Node-First (MCNF) approach 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 by selecting the node *n* as the defense node. The potential increase 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. The pseudo-code is described in the Algorithm 2.

With suggested improvements in both – traffic differentiation and rate-limiting in Sections IV and VI respectively, and a new approach towards attack detection described in Section V, this solution is expected to: (i) reduce bandwidth contention problem, (ii) reduce flooding problems (iii) bring pro-activeness in attack detection, and (iv) ensure consistent good service to legitimate clients.

Algorithm 2: MCNF algorithm for defense node Selection

Input: Victim node *v*, Path matrix *P*, required number of defense node *d*

Output: Set of *d* defense nodes

1 Compute a set P_k of all *k*-hop paths to node *v*;
2 Compute the set N_D of all nodes on paths in P_k: $N_D = \cup_{p \in P_k} Nodes(p)$;
3 *uncovered_paths* = P_k;
4 **foreach** node $n \in N_D$ **do**
5 Compute coverage of the node n, Cn as follows:
6 *Cn = paths_covered(n) \ uncovered_paths*;
7 **end**
8 Select the node *n* that provides maximum coverage C_n;
9 Remove *paths_covered(n)* from the set *Uncovered_paths*;
10 Remove the selected node *n* from the set N_D;
11 Repeat steps 4 to 10 until *d* nodes are not selected or *uncovered paths* is *NULL*;

IV. TRAFFIC DIFFERENTIATION

In this section, we discuss the problem of differentiating legitimate traffic from attack traffic. We present different existing approaches, initial ideas for improvements and open issues.

Packet marking is the most commonly used technique for traffic differentiation. The markings are usually added in the IP-identification field of packets. Easy-pass [5] however, attaches 64-bit encrypted order-sensitive information (that authenticates the valid packets) to every real-time data packet as a trailer. ISP edge router knows the valid sequence of passes and hence drops the detected forged packets with stale or duplicate passes.

The capabilities-based traffic differentiation is devised in SIFF [8]. In this technique, the capabilities are changed independently at each router with a certain frequency. A window of valid markings is maintained at routers and these routers signal a change of marking to a packet recipient by replacing old markings in the embedded capability with new ones. With TVA [9], a client that initiates request for capabilities receives pre-capabilities from routers and then the capabilities from the destination. Communication between the source and destination gets initiated without authenticating subsequent packets. Hence, though both the techniques apply time-limits to assigned capabilities, the risk of theft and misuse of the capabilities persists. Fine-grained capabilities based mechanism [3] calculates the capabilities in terms of credits and penalties only at the victim-end. Credit implies contribution of the client to congestion during flooding attack; whereas penalty is assigned to clients that experience persistent packet drops. The calculation takes into account previous values of credits and penalties, and total traffic sent per unit time by the client. Encryption is applied to the calculated capabilities. However, two important limitations with this mechanism are: (i) Only victim-end implementation does not provide defense against the intermediate intruders, and (ii) It relies only on reverse feedback from server for behavioral analysis and hence for calculation of the capabilities. This may degrade the pro-activeness of the solution.

We propose to enable traffic differentiation based on fine-grained capabilities at (a) victim-end (b) strategically chosen upstream routers. In effect, the packets would be assigned dual capabilities: route-capabilities and client-capabilities in the same sequence. This will make it more distributed, and address the issue of defense against intruders. The second problem can be addressed by adding more dimensions to calculation of credits-and-penalties which constitute the fine-grained client-capabilities. The calculation process may take into account - (i) Probable requirement of resources, (ii) Frequency of receiving packets from a particular client (iii) Application time, (iv) Previous behavior, (v) Combination of these parameters. We address the problem of selection of defense nodes in Section III. Protecting the route-capabilities from intruders is also a critical issue. The process of traffic differentiation should be able to - (i) identify malicious traffic from the incoming aggregate quickly, (ii) minimize chances of misclassification, (iii) make the calculation of client-capabilities robust and impervious to attack, and (iv) accurately identify critical resource requirement.

V. ATTACK DETECTION

In this section, we discuss the problem of detecting attack in reactive manner. We present different existing approaches, initial ideas for improvements and open issues.

Many of the existing mechanisms deal with the attack traffic in reactive manner. As mentioned in Section II, MULTOPS [2] detects attack after observing deviation in the disproportional packet rates beyond certain threshold. Whereas, D-WARD [1] detects attack after observing the deviation of real-time traffic from pre-defined traffic model rules. This increases the chances of *false positives* and *false negatives*. A *false positive* implies misclassification of a legitimate client as an attacker, while a *false negative* implies misclassification of an attacker as a legitimate client. Mechanisms based on some form of packet marking [8],[9],[5],[7] are also reactive in nature. They detect attack only on receiving at least one attack packet. Such approach in attack detection either causes collateral damage to the subsequent legitimate packets or a large dependence on only past behavior of individual clients. Due to their reactive nature these defense mechanisms also suffer from following limitations: (i) some amount of attack traffic succeeds in entering the victim network, (ii) victim does not get sufficient time to take necessary actions in order to avoid flooding of its link.

We propose to proactively deal with the attack traffic by mining attack patterns in the network's historic data to predict any prospective attack. We can then further analyze and forecast attack from individual client to identify the prospective attackers. This would involve finding answers to the following questions: (i) Which clients are malicious? (ii) What is the rate at which they generate traffic? (iii) Which routes are used to send the attack traffic? (iv) Is there any specific period for commencement of attack(s)? (v) What has been the nature and severity of previously occurred attacks? (vi) What kind of resources do they request for? (vii) Is there any repeated ill-behavior? If yes, at what frequency?

With the distributed defense approach, the defense nodes would involve subset of upstream routers along with the victim node. Each defense node can maintain the history of both aggregate traffic as well as traffic from individual clients. Thus, a set of time-series can be maintained and incrementally updated with incoming traffic. These time-series would then be analyzed to forecast future traffic. Various time-series forecasting solutions have been proposed in the past. We propose to use two approaches: (i) Regression models for capturing linear, piecewise linear behaviors in network traffic, and (ii) ARIMA models. The functionalities in predictive attack detection may be distributed; such that (i) aggregate traffic analysis is performed at victim end for predicting time-to-saturation, and (ii) individual client traffic analysis is performed at defense nodes to identify the prospective attackers.

For predictive analysis, obtaining sufficient historic and real-time data is necessary. As the attacks mutate and become sophisticated, their prediction and identification becomes difficult. Major challenge in performing predictive attack detection with the proposed approach is building regression and ARIMA models. It is important to accurately capture the relationship between the *total traffic observed at the victim node and the traffic observed at the network link between the proxy server and the victim*.

VI. RATE-LIMITING

Rate limiting is a technique to prevent illegitimate traffic from accessing the victims resources. In this section, we discuss the limitations of current rate-limiting strategies, and propose a new technique to overcome these limitations. We also discuss the challenges in its development.

Existing capabilities-based mechanisms minimize the access of resources to illegitimate traffic by using fair queuing based rate-limiting [9]. They use multiple queues for traffic flows with different capabilities and request types. This ensures allocation of fair percentage of the total available bandwidth and other resources to all requests. It works well in case of authorized traffic competing for bandwidth, but is vulnerable to flooding attacks. SIFF [8] and TVA [9] grant absolute access to the destination to all ticket-carrying traffic. This strategy allows a reasonable share of bandwidth to each request with capabilities. But, it can cause harm to legitimate clients in case of mutable attackers.

Fine-grained capabilities based mechanism [3] classifies the clients based on the assigned credits and penalties. For these classes, it uses multiple queues. Each class is assigned a resource share. A client can access the resource share assigned to its class and all lower classes. When all resources are consumed, further requests are discarded. For consistently aggressive clients, it maintains a blacklist. Penalties are used when legitimate traffic causes more congestion than the illegitimate traffic. This mitigates the risks from low-rate flooding attacks. By quickly identifying and severely penalizing the attackers, the access to critical resources is controlled. The mechanism correlates behavior of an attacker with human behavior. It claims that, "if a service request by a person does not receive a response, then the person is unlikely to maintain or increase the rate of request generation".

However, we see the following limitations with this mechanism: (i) It relies only on the behavioral analysis (expressed in terms of credits and penalties) to assign priorities to critical resource access. (ii) It does not apply rate limiting for non-critical resource access. (iii) No systematic approach is suggested for the decision about number of queues, size and resource share of queues. (iv) The queues grant critical resource access to incoming requests in FIFO fashion. However, this may not always be suitable.

We propose a cooperative functioning between suggested capabilities based traffic differentiation and the prospective attacker identification by predictive attack detection. We propose to closely monitor the traffic received from the prospective attackers as identified by the defense nodes. A blacklist for aggressive clients takes care of repeated severe attacks [3]. We retain this concept in our proposed idea and discard the requests from such clients. In addition, we also

propose to maintain a white-list and a gray-list as illustrated in Figure 2.

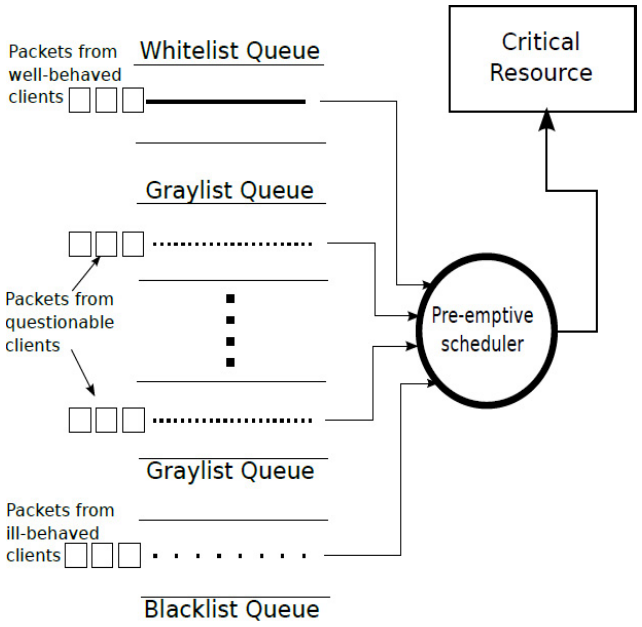

Fig. 2 Proposed queuing for rate-limiting

A white-list would be created for identified and trusted well-behaving clients. These clients would always be guaranteed the resource access. For clients that show suspicious behavior in past, we create a gray-list that contains number of queues. These queues isolate critical resource requests from the non-critical resource requests. Required resources are identified from capabilities calculated with the improved traffic differentiation method suggested in Section IV. Our idea is to apply pre-emption instead of FIFO scheduling to the queues in this list.

Maintenance of the blacklist, white-list and gray-lists may impose some non-trivial memory overhead. Keeping this overhead to a minimum level is a major concern. Additionally, resource availability is bound to change dynamically which needs continuous attention. The predictions for resource consumption should be accurate. Avoiding over-utilization or under-utilization of resources is also an important issue.

VII. CONCLUSION AND FUTURE WORK

In this paper, we discussed various DDoS defense mechanisms implemented at different network locations. A robust DDoS defense involves different activities. Any solution at a single network location cannot perform all of them efficiently. Based on this understanding, we presented a distributed defense solution. We proposed two algorithms for the defense nodes placement. Further, we proposed some initial ideas to improve traffic differentiation activity. We have also suggested adding a predictive analytical approach in identifying occurrence of an attack and identifying prospective attackers. Our proposed rate-limiting scheme is based on pre-emptive scheduling. It is aimed at avoiding bandwidth crunch caused by genuine traffic and flooding attack. With rate-limiting deployed for attack traffic, this defense would ensure consistent service to the legitimate clients.

With these insights, we try to foresee the requirements and challenges in implementing these ideas. We plan to explore and investigate more on the suggested solutions. Our immediate next step would target the development of prediction algorithm for preventive defense described in Section V and traffic differentiation suggested in Section IV. We also aim at performing more detailed evaluation of the defense node placement algorithms.

REFERENCES

[1] J. Mirkovic, G. Prier, P. Reiher,"Attacking DDoS at the Source", In Proc. 10th International Conf. Network Protocols, November 2002, pp. 312-321.

[2] T. Gil, M. Poletto, "MULTOPS: a data-structure for bandwidth attack detection", In Proc. 10th Usenix Security Symp., August 2001, pp. 23-38.

[3] M. Natu, J. Mirkovic, "Fine-Grained Capabilities for Flood- ing DDoS Defense Using Client Reputations", In Proc. 2007 workshop on Large scale attack defense, New York, NY, USA, August 2007, pp. 105-112.

[4] A. Garg and A. L. N. Reddy, "Mitigation of DoS attacks through QoS Regulation", In Proceedings of IWQOS workshop, May 2002, pp. 45-53.

[5] H.Wang, A.Bose, M.Gendy, and K.Shin, "IP Easy-pass: Edge Resource Access Control", In Proc. IEEE INFOCOM, Vol. 4, March 2004, pp. 1247-1260.

[6] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical Network Support for IP Traceback", In Proc. 2000 ACM SIG- COMM Conf., Stockholm, Sweden, August 2000, pp. 295306.

[7] A. Yaar, A. Perrig, and D. X. Song, "StackPi: New Packet Marking and Filtering Mechanisms for DDoS and IP Spoofing Defense", IEEE Journal on Selected Areas in Communications, Vol. 24 Issue 10, NJ, USA, October 2006, pp. 1853-1863.

[8] A. Yaar, A. Perrig, and D. X. Song, "SIFF: A Stateless Internet Flow Filter to Mitigate DDoS Flooding Attacks", In Proc. IEEE Symposium on Security and Privacy, Oakland, CA, USA, 2004, pp. 130-143.

[9] X. Yang, D. Wetherall, and T. Anderson, "A DoS-limiting network architecture", In Proc. of ACM SIGCOMM Review, Vol. 35, Issue 4, 2005, pp. 241252.

[10] R. Mahajan, et al., "Controlling high bandwidth Aggregates in the network", ACM SIGCOMM Comp. Comm. Review, Vol. 32 Issue 3, NY, USA, July 2002, pp. 62-73.