1-1-2010

Near-Optimal Defense Strategies against DDoS Attacks Based upon Packet Filtering and Blocking Enabled by Packet Marking

Frank Yeong-Sung Lin
National Taiwan University, yslin@im.ntu.edu.tw

Pei-Yu Chen
National Taiwan University, d96006@im.ntu.edu.tw

Chun-Wei FanChiang
National Taiwan University, r96041@im.ntu.edu.tw

NEAR-OPTIMAL DEFENSE STRATEGIES AGAINST DDOS ATTACKS BASED UPON PACKET FILTERING AND BLOCKING ENABLED BY PACKET MARKING

Frank Yeong-Sung Lin, Department of Information Management, National Taiwan University, Taipei, Taiwan, R.O.C., yslin@im.ntu.edu.tw

Pei-Yu Chen, Department of Information Management, National Taiwan University, Taipei, Taiwan, R.O.C., d96006@im.ntu.edu.tw

Chun-Wei FanChiang, Department of Information Management, National Taiwan University, Taipei, Taiwan, R.O.C., r96041@im.ntu.edu.tw

Abstract

In the paper, the DDoS scenario is modelled as a mathematical programming problem. The defender strategically utilizes the limited resources to maximize the legitimate traffic, and he can adopt packet marking to observe the network status. The information extracts from the marking field can help the defender develop a defense strategy which combines packet filtering and packet blocking. A Lagrangean relaxation-based algorithm is proposed to optimally solve the problem.

Keywords: Distributed-Denial-of-Service (DDoS), Filtering, Blocking, Packet Marking, Mathematical Programming, Optimization and Lagrangean Relaxation.

1 INTRODUCTION

The Internet has become an essential tool in today's world. Huge financial losses can be incurred from even 1 hour internet downtime due to main operational server crashes due to a DDoS attack. From "Computer Crime and Security Survey" conducted by CSI 2008 (Richardson 2008), among all security incidents, the percentage of Denial of Service ranked high, despite a gradually decreasing trend of the past four years. In 2008, the largest reported distributed denial-of-service (DDoS) attack reached 40 gigabits per second against one single target, which is 100-fold increase from 2001. As can be seen from these reports, the DDoS attack is still a problem and the damage caused by it is far more than it can be imagined.

As is commonly known, there are several types of DDoS attack, such as TCP connection and SYN flooding attack. (Mirkovic and Reiher 2004) has listed a Taxonomy of DDoS Attack and DDoS Defense Mechanisms. Yet, the one being addressed here is involves the attacker sending millions of unwanted packets in an effort to try to overwhelm a victim server (Yau et al. 2001). There are many approaches to defend against a DDoS attack and one effective approach is a filtering mechanism, which regulates the incoming traffic, both attack traffic and legitimate traffic, to a manageable level. Even though the filtering mechanism has been proven to be a valid solution, it leads to another problem: the legitimate packets might also be throttled as malicious ones, resulting in so called "collateral damage."

In order to alleviate the collateral damage and develop the optimal defense strategy, any extra data could be transformed into valuable information and help the defender to refine his/her defense strategy. To know more specific information, the source of packets should be known. 32-bit IP address is not accountable, because the IP address can be easily spoofed by the attacker (Stallings 2006). Therefore, "IP traceback" is taken into consideration and combined with a filtering mechanism and an application-level blocking policy, which performs on the server's side. Nonetheless, the preciseness of blocking depends on the marking probability. With prior information provided by IP traceback, the filtering remaining ratio and blocking policy can be further refined.

There has been a lot of research focussing on packet marking (Park et al. 2007 and Goodrich 2008). According to these studies and the statistical results from (RFC791 2008), IP fragments constitute a very small proportion of the actual Internet traffic (less than 0.25 percent). And the 8-bit Type-of-Service field is seldom used (Stoica 1999); moreover, Reverse Flag in IP protocol has not been predefined (Stevens 1994). From the above-mentioned, 25 modifiable bits is available as traceback information field. Here, the 25-bit marking field was cut into two parts, 13 bits for the first part and 12 bits for the second part. The first part is used to recode the unique ID of the incoming interface of the edge router where a specific packet enters.

In this paper, the defender utilizes these three defense schemes to learn the attack features and develop a corresponding defense strategy. We then apply the Lagrangean Relaxation Method with the combination of subgradient method (Fishe 1981) to optimally solve this problem. The remainder of this paper is organized as follows. In Section 2, a mathematical formulation of the scenario is proposed. In Section 3, a Lagrangean Relaxation-based solution approach is presented. The computational results of the experiments are shown in Section 4. Finally, Section 5 is the conclusion.

2 PROBLEM FORMULATION

The problem being addressed here is how the ASP's limited resources, such as marking scheme, filtering mechanism and blocking policy. In order to throttle the attack traffic more precisely, the traceback method of a packet marking scheme is introduced into this model and formulates the marking rate as a cost, and which is an extra charge service provided by the ISP. With the limited defense budget, the defender's objective is to maximize the legitimate traffic, i.e., to minimize the collateral damage caused by the DDoS attack. In order to describe our problem in a more comprehensive way, the related issues in defending against the DDoS attack s are considered.

To begin with, the *marking mechanism* is considered. The ASP has a table which lists the amount of legitimate traffic of each time zone over a period of time. Thus the ASP realizes the network utility is higher during the peak period and lower when off-peak period. The higher the marking rate the more precisely the ASP can know in which interface the malicious traffic enters and roughly the amount of each malicious traffic stream. Yet, the charge of the marking scheme is higher when the ASP subscribes a higher marking rate. The ASP can dynamically adjust the *filtering* rate of each interface on an edge router. These adjustments should be optimised, because it might lead to critical collateral damage, otherwise the effort to defend the DDoS attack might be in vain. Next, the "*Blocking Policy*" performed by the ASP is taken into consideration. Since the filtering cost might be too high to subscribe for a low rate attack. Although the blocking might have a lower monetary cost, the extra traffic might degrade the service quality, such as the end-to-end delay or response time, of the legitimate user. For these reasons, the blocking policy needs to be considered carefully.

In this paper, we take marking costs, filtering costs and blocking costs into account. And the summation of all costs cannot exceed the defender's total budget. The scenario is elaborated as follows. First, when network status is normal, only legitimate traffic exists and the marking scheme is always on at a very low probability. At this time, the defender can approximately estimate the amount of the legitimate traffic in each time zone and table the observation. Due to the marking scheme, the defender can calculate any unusual increase of attack traffic. Furthermore, the defender might raise the marking probability in order to learn precisely how serious the attack is and how to develop a near optimal defense strategy in a timely manner. After optimal calculation, the defender decides the filtering mechanism and blocking policy which forms a corresponding defense strategy.

Moreover, the target network discussed here is at the Autonomous System (AS) level network (Magoni 2001). Since this is an operational problem, it is assumed that all edge routers are capable of filtering and marking. Edge routers cannot be compromised and the marking field of all packets will be set to default value when entering the AS by edge routers. Each edge router and each interface on an edge router will have a locally unique ID pre-numbered by ISP; both ISP and ASP know the ID. Finally, it is assumed there is a real-time communication mechanism between the ISP and the ASP and both the attacker and the defender have the complete information.

The problem is described in detail and a mathematical model with specific assumptions and problem objective to the target network is proposed. The given parameters and decision variables are defined in Table 1 and Table 2, respectively. In this probabilistic packet marking based filtering ratio and blocking probability adjustment strategy (PPM-FRABS) model, the defender utilizes these three defense schemes to learn the attack features and develop a corresponding defense strategy.

Given Parameters	
Notation	**Description**
N	The index set of all nodes in an AS
E	The index set of all entry nodes, where $E \subset N$
S	The index set of all victim servers, where $S \subset N$
I_e	The index set of all interfaces on a node e, where $e \in E$
ϕ_v	The threshold of the a victim server v, where $v \in S$
$\hat{g}_v$	The threshold of the aggregate traffic below which the aggregate traffic is regulated to defend the DDoS attack for a victim server v, where $v \in S$
Z	The index set of all botnets
A	The attacker's total budget
D	The defender's total budget
W_k	The index set of all OD pairs, where the origin is node o and the destination is node d, where $o \in I_e, d \in S, k \in Z$

FC_e	The unit cost of traffic filtering of an edge router e, where $e \in E$
MC_e	The unit cost of traffic marking of an edge router e, where $e \in E$
BC_v	The unit cost of unmarked traffic processing of victim server v, where $v \in S$
BC_{wv}	The unit cost of marked traffic processing of victim server v, where $v \in S, k \in Z, w \in W_k$
γ_{kw}	The good traffic on an OD pair w, where $k \in Z, w \in W_k$
Ω_f	The set of all discrete values, say, 0.1, 0.2, ……, between 0 to 1.
Ω_m	The set of all discrete values, say, 0.1, 0.2, ……, between 0 to 1.
Ω_b	The set of all discrete values, say, 0.1, 0.2, ……, between 0 to 1.
Ω_x	The product set of f_w and m_w.
Ω_y	The product set of f_w, m_w and b_{wv}.
Ω_l	The product set of f_w and b'_v.
Ω_n	The product set of f_w, m_w and b_{wv}.
C_w	The attack budget allocated on an OD pair w, where $k \in Z, w \in W_k$
ζ_{kw} (C_{kw})	The maximum attack traffic, which is the linear function of an OD pair w that is a function of the attack budget, where $k \in Z, w \in W_k$
β_{kw}	The (real) attack traffic on an OD pair w, where $k \in Z, w \in W_k$
Decision Variables	
f_w	The filtering remaining ratio on an OD-pair w, where $k \in Z, w \in W_k$
m_w	The marking probability of on an OD-pair w, where $k \in Z, w \in W_k$
b_{wv}	The specific blocking remaining probability of a node v, where $v \in S$, $k \in Z, w \in W_k$
b'_v	The overall blocking remaining probability of a victim server v, where $v \in S$

Table 1 Given and decision Variables

In order to reduce the complexity of the product form, four discrete auxiliary variables, which are used to transform the continuity of the product form into several discrete data, are introduced. Since the variables, f_w, m_w, b_{wv}, b'_v , are all percentages, we will use different precisions as different adjustable units, and the adjustable unit can be smaller if needed. After variable transformation, there are no more than 10^6 combinations. Clearly, some accuracy of the original problem might be lost because of the discrete problem transformation, a so-called approximation approach. Yet, there is debate whether the trivial loss of accuracy is worth it compared to the gain in performance. Moreover, the class interval being addressed above is adjustable which means the accuracy is controllable. Considering the pricing strategy of the network operator, 0.1 has been taken as default interval. All the discrete variables are listed as below.

$$
\begin{aligned}
x_w &= f_w m_w && k \in Z, w \in W_k \\
y_{wv} &= f_w m_w b_{wv} && v \in S, k \in Z, w \in W_k \\
l_{wv} &= f_w b'_v && v \in S, k \in Z, w \in W_k \\
n_{wv} &= f_w m_w b'_v && v \in S, k \in Z, w \in W_k
\end{aligned}
$$

Objective function :

$$
\begin{aligned}
Z_{IP2} = & \max_{f_w, m_w, b_{wv}, b'_v} \sum_{k \in Z} \sum_{w \in W_k} \sum_{v \in S} \gamma_{kw} f_w [m_w b_{wv} + (1 - m_w) b'_v] \\
& \Rightarrow \min_{f_w, m_w, b_{wv}, b'_v} - \sum_{k \in Z} \sum_{w \in W_k} \sum_{v \in S} \gamma_{kw} [f_w m_w b_{wv} + f_w b'_v - f_w m_w b'_v] \\
& \Rightarrow \min_{f_w, m_w, b_{wv}, b'_v} - \sum_{k \in Z} \sum_{w \in W_k} \sum_{v \in S} \gamma_{kw} (y_{wv} + l_{wv} - n_{wv})
\end{aligned}
\qquad \textbf{(IP 1)}
$$

Subject to :

$$x_w = f_w m_w \qquad \forall k \in Z, w \in W_k \qquad \text{(IP 1.1)}$$

$$\varepsilon \le x_w \le 1 \qquad \forall k \in Z, w \in W_k \qquad \text{(IP 1.2)}$$

$$y_{wv} = f_w m_w b_{wv} \qquad \forall k \in Z, w \in W_k, v \in S \qquad \text{(IP 1.3)}$$

$$\varepsilon \le y_{wv} \le 1 \qquad \forall k \in Z, w \in W_k, v \in S \qquad \text{(IP 1.4)}$$

$$l_{wv} = f_w b'_v \qquad \forall k \in Z, w \in W_k, v \in S \qquad \text{(IP 1.5)}$$

$$\varepsilon \le l_{wv} \le 1 \qquad \forall k \in Z, w \in W_k, v \in S \qquad \text{(IP 1.6)}$$

$$n_{wv} = f_w m_w b'_v \qquad \forall k \in Z, w \in W_k, v \in S \qquad \text{(IP 1.7)}$$

$$\varepsilon \le n_{wv} \le 1 \qquad \forall k \in Z, w \in W_k, v \in S \qquad \text{(IP 1.8)}$$

$$D \ge \sum_{e \in E} \sum_{k \in Z} \sum_{w \in W_k} (\beta_{kw} + \gamma_{kw})[(1 - f_w) FC_e + m_w MC_e] + \sum_{v \in S} \sum_{k \in Z} \sum_{w \in W_k} (\beta_{kw} + \gamma_{kw})[(x_w - y_{wv}) BC_{wv} + (f_w - x_w - l_{wv} + n_{wv}) BC_v] \qquad \text{(IP 1.9)}$$

$$[y_{wv} + l_{wv} - n_{wv}] \ge \phi_e \qquad \forall e \in E \qquad \text{(IP 1.10)}$$

$$\frac{x_w \beta_{kw}}{\beta_{kw} + \gamma_{kw}} \ge (1 - b_{wv}) \qquad \forall k \in Z, w \in W_k, v \in S \qquad \text{(IP 1.11)}$$

$$\frac{\sum_{k \in Z} \sum_{w \in W_k} \beta_{kw} (f_w - x_w)}{\sum_{k \in Z} \sum_{w \in W_k} (\beta_{kw} + \gamma_{kw})} \ge (1 - b'_v) \qquad \forall v \in S \qquad \text{(IP 1.12)}$$

$$\hat{g}_v \ge \sum_{k \in Z} \sum_{w \in W_k} f_w (\beta_{kw} + \gamma_{kw}) \qquad \forall v \in S \qquad \text{(IP 1.13)}$$

$$f_w \in \Omega_f \qquad \forall k \in Z, w \in W_k \qquad \text{(IP 1.14)}$$

$$m_w \in \Omega_m \qquad \forall k \in Z, w \in W_k \qquad \text{(IP 1.15)}$$

$$b_{wv} \in \Omega_b \qquad \forall k \in Z, w \in W_k, v \in S \qquad \text{(IP 1.16)}$$

$$b'_v \in \Omega_b \qquad \forall v \in S \qquad \text{(IP 1.17)}$$

$$x_w \in \Omega_x \qquad \forall k \in Z, w \in W_k \qquad \text{(IP 1.18)}$$

$$y_{wv} \in \Omega_y \qquad \forall k \in Z, w \in W_k, v \in S \qquad \text{(IP 1.19)}$$

$$l_{wv} \in \Omega_l \qquad \forall k \in Z, w \in W_k, v \in S \qquad \text{(IP 1.20)}$$

$$n_{wv} \in \Omega_n \qquad \forall k \in Z, w \in W_k, v \in S \qquad \text{(IP 1.21)}$$

The defender's objective is to maximize the remaining good traffic by utilizing probabilistic packet marking in advance, which aims at providing a prior knowledge to improve the performance of the filtering rate adjustment and blocking probability adjustment, where the decision parameters of the outer problem are given. Constraints (IP 1.1) to (IP 1.8) introduce the four auxiliary variables to simplify the problem and all the auxiliary variables must lie in between ε and 1. Constraint (IP 1.9) enforces the summation of the total marking cost, total filtering cost and total blocking cost, which must not exceed the defender's marker budget D. Constraint (IP 1.10) enforces the percentage of filtered legitimate traffic over the filtered aggregate traffic, which must exceed the threshold, ϕ_v, for each victim server v. Constraint (IP 1.11) restricts the blocking probability of each OD pair w destined for victim server v, which must be smaller than the ratio of the summation of filtered legitimate traffic over the summation of filtered aggregate traffic (both ends at victim server v) in order to maintain the service quality. Note that the blocking probability is used when marked traffic is received by a victim server v. Constraint (IP 1.12) restricts overall blocking probability of each victim server v, which must be smaller than the ratio of the overall summation of filtered legitimate traffic over the overall summation of filtered aggregate traffic in order to maintain the service quality. Note that the blocking probability is used when unmarked traffic is received by a victim server v. Constraint (IP 1.13) restricts the aggregate traffic, after filtering and blocking, from exceeding the threshold which the victim server v can process, thus reaching the goal of DDoS attack mitigation. Constraints (IP 1.14) to (IP 1.17) limits the continuous region of f_w, m_w, b_{wv}, b'_v to a discrete region. Constraints (IP1.18) to (IP 1.21) limits the feasible region of all the auxiliary variables.

3 SOLUTION APPROACH

Heuristics are proposed to solve the problems. We adopted a LR-based heuristic for solving the PPM-FRABS model.

3.1 Lagrangean Relaxation

The Lagrangean Relaxation Method was first used to solve large-scale mathematical programming problems during the 1970s [17]. The most important concept of this method is "decomposition", which can substantially reduce the complexity and the difficulty of the primal problem. Because its efficiency and effectiveness in solving complicated programming problems, Lagrangean Relaxation has become one of the most popular tools to solve optimization problems.

To implement LR onto this problem, these constraints, (IP 1.1), (IP 1.3), (IP 1.5) and (IP 1.7), are firstly transformed from the product form into the logarithm form without losing the optimality.

$$x_w \le f_w m_w \qquad \forall k \in Z, w \in W_k \qquad \text{(IP 1.1)}$$
$$\Rightarrow \log(x_w) \le \log(f_w) + \log(m_w)$$
$$y_{wv} \le f_w m_w b_{wv} \qquad \forall k \in Z, w \in W_k, v \in S \qquad \text{(IP 1.3)}$$
$$\Rightarrow \log(y_{wv}) \le \log(f_w) + \log(m_w) + \log(b_{wv})$$
$$l_{wv} \le f_w b'_v \qquad \forall k \in Z, w \in W_k, v \in S \qquad \text{(IP 1.5)}$$
$$\Rightarrow \log(l_{wv}) \le \log(f_w) + \log(b'_v)$$
$$n_{wv} \le f_w m_w b'_v \qquad \forall k \in Z, w \in W_k, v \in S \qquad \text{(IP 1.7)}$$
$$\Rightarrow \log(n_{wv}) \le \log(f_w) + \log(m_w) + \log(b'_v)$$

Secondly, some constraints are relaxed and the problem is transferred into a LR problem. Later on, the LR problem is further decomposed into eight sub-problems according to the eight variables, i.e. f_w, m_w, b_{wv}, b'_v, x_w, y_{wv}, l_{wv}, and n_{wv}, each of which is solved by exhaustive search.

3.2 Solution Approach for the PPM-FRABS Model

Firstly, the result from sub-problems 1.2 to 1.4 is duplicated as our initial defense strategy. Second, the defense strategy list is quick sorted, in a descending form, according to its ratio of attack traffic to normal traffic and then all filtering remaining ratios are set as 1. As for the next step, each victim server is checked to see whether the loading is enough to process the aggregate traffic. If not, a lower filtering remaining ratio is set. Fourth, each OD pair is checked for the minimum threshold of the remaining good traffic. If it is violated, a higher marking probability or specific blocking probability is set. The final defense strategy is the overall blocking remaining probability, since the filtering remaining ratio has been decided. Finally, for each victim server, all possible overall blocking remaining probabilities are exhaustively tried out. Once all the optimal overall blocking remaining probabilities are found, the defense strategy is determined.

4 COMPUTATIONAL RESULTS

In this part, one resource-allocation heuristic and one simple algorithm are proposed for comparison to show that our heuristic for getting primal feasible solution is more effective.

4.1 Experiment Results for the PPM-FRABS Problem

The Iteration Counter Limit and Improve Counter Limit are set to 2000 and 50 respectively. The step size of scalar, λ, is initialized as 2 and is halved if the objective function value, Z_D, is not improved after several times of Improve Counter Limit. As mentioned before, in order to solve the inner

problem, an approximation technique is implemented to make the continuous variables discrete. In order to observe the accuracy and efficiency under different precisions of approximation, three kinds of precision, 5, 10 and 20, are designed. To eliminate the interference caused by different traffic distribution, the traffic distribution is fixed. The Initial Good Traffic is fixed as 25000.

Since the issue of multiple victim servers under a DDoS attack is taken into consideration, three different number of victim servers are designed. By means of examining different number of victim servers, one can hopefully develop a guideline to maintain more legitimate traffic under the limited budget. Figures 2 to 7 are the experiment results for the PPM-FRABS Problem. The details are discussed in the next section.

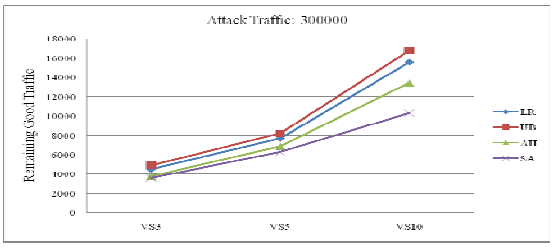

Figure 2: The Remaining Good Traffic under Attack Budget 300000

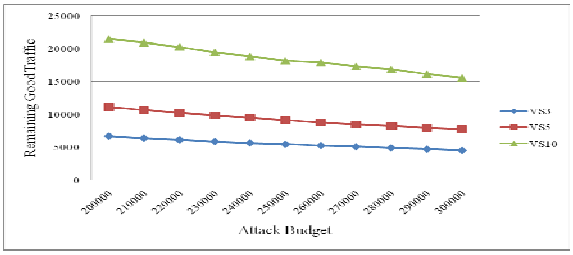

Figure 3: The Remaining Good Traffic with Different Attack Budget

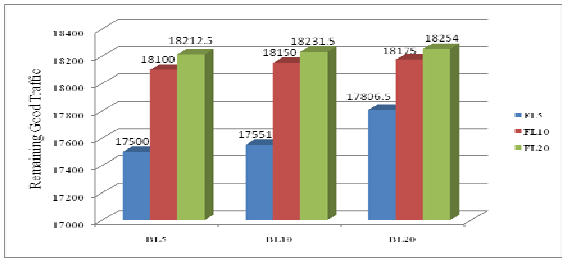

Figure 4: The Remaining Good Traffic with Different FL and ML

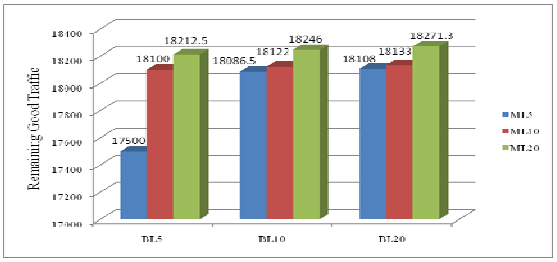

Figure 5: The Remaining Good Traffic with Different ML and BL

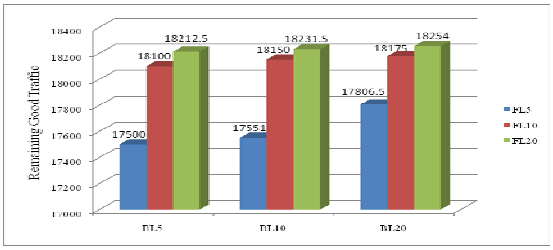

Figure 6: The Remaining Good Traffic with Different FL and BL

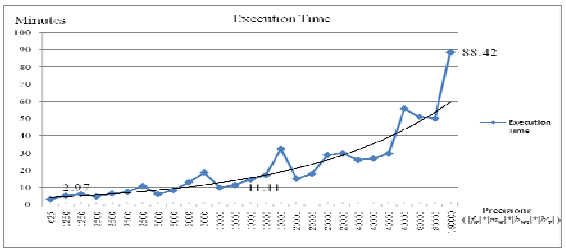

Figure 7: The Execution Time and Exponential Trend Line under Different Precision of Approximations (mins)

4.2 Discussion of Results

Figure 2 shows the solution quality of our proposed Lagrangean Relaxation-based algorithm compared with the resource allocation heuristic and simple algorithm, and it shows the gap between LRs and UBs. It is clear that our proposed heuristic performs better than both resource allocation heuristic and simple algorithm. Moreover, in Figure 3, we can observe the remaining good traffic under different total attacker's budget. This figure illustrates the relationship between the remaining good traffic, attack budget and the number of victim servers. As can be seen, it shows growth and decline. Surely when the attack budget increases the remaining good traffic shall decrease. Yet the total loading of victim servers plays a critical role in this attacker-defender interaction scenario.

Figure 4 to Figure 6 compares the performances under different precisions of approximation. Figure 4 shows the relationship between the Filtering Level and Marking Level; Figure 5 presents the relationship between the Marking Level and Blocking Level. The relationship between the Filtering Level and Blocking Level is illustrated in Figure 6. It can be learned from Figure 4 that ML 10 has better performance than ML5 and convergence happens when the precision is raised from ML10 to ML 20. For the remaining Figure 5 and Figure 6 one can tell that the interaction between ML and BL is closer than that between FL and BL. All of the Figures indicate that the more precise the approximation, the better the performance.

Figure 7 illustrates the execution time of one defense strategy deployment under a specific attack strategy and shows the exponential trend line. Since the defender has three defense mechanisms, all of the precisions vary from 5 to 20. As can be seen, the execution times are distributed from 2.97 to 88.42 minutes and the execution time rises with the increase of the precision of approximation.

5 CONCLUSION

This paper illustrates the scenario of a successful defense against a DDoS attack, in which the attacker tends to strategically allocate its attack budget to interfere the legitimate user with his/her daily request. That is, the attacker tries to paralyze the function by sending a huge amount of traffic, while the defender tries to defend against the attacker by the effective use of a filtering mechanism and blocking policy with the information provided by a packet marking mechanism. Ultimately, after several rounds of seesaw battle, an equilibrium is reached by both the attacker's and defender's strategies.

The proposed mathematical model to describe the PPM-FRABS problem, which illuminates the interaction between the attacker and the defender, is the main contribution in our work. Our proposed algorithms can defend against various attack strategies in a reasonable time manner. Even more, the solution found by our proposed algorithm can be claimed as a near optimal solution. For those who may suffer from the threat of a DDoS attack, it is hoped that the several defense guidelines derived from our proposed algorithm can help them throttle the DDoS attack and minimize the collateral damage. This model provides guidelines for service providers, on developing a near optimal defense strategy based on the proposed joint defense mechanism.

References

Richardson, R. (2008). 2008 CSI/FBI Computer Crime and Security Survey, Computer Security Institute.

Mirkovic, J. and Reiher, P. (2004). A Taxonomy of DDoS Attack and DDoS Defense Mechanisms, ACM SIGCOMM Computer Communications Review, 34(2), 39-54.

Yau, K.Y., Liang, F., and Lui, C.S. (2001). On Defending Against Distributed Denial-of-Service Attacks with Server-centric Router Throttles, CERIAS Tech Report.

Stallings, W. (2006). Cryptography and network security, Prentice Hall, 4th Edition.

Park, J.M., Marchany, R. and Chen, R.L. (2007). A Divide-and-conquer Strategy for Thwarting Distributed Denial-of-Service Attacks, IEEE Transactions on Parallel and Distributed Systems, 18(5), 577-588.

Goodrich, M.T. (2008). Probabilistic Packet Marking for Large-scale IP Traceback, IEEE/ACM Transactions on Networking, 16(1).

RFC791. (1981). Information Sciences Institute University of Southern California, Internet protocol.

Stoica, I. and Zhang, H. (1999). Providing guaranteed services without per flow management," Proceedings of the ACM SIGCOMM'99.

Stevens, W. R. (1994). TCP/IP Illustrated, 1, The Protocols, Addison-Wesley Professional.

Fisher, M.L. (1981). The lagrangean relaxation method for solving integer programming problems, Management Science, 27(1), 1-18.

Magoni, D. and Pansiot, J.J.(2001). Analysis of the autonomous system network topology, ACM SIGCOMM Computer Communication Review, 31(3), 26-37.